I KNOW MY TRUTH... NOW TELL ME YOURS: FROM ACTIVE MEASURES TO COGNITIVE WARFARE IN THE RUSSIAN INVASION OF UKRAINE

UDC 355.4'244.1'422.1(470)(477)
https://doi.org/10.53679/2616-9460.2.2022.02

Paul Burke[1] –
Director of Global Projects
for Glengulf International, United Kingdom
ORCID: 0000-0002-8764-7266

Adam Henschke[2] –
Assistant Professor,
Philosophy Section, University of Twente,
Enschede, Netherlands
ORCID: 0000-0002-2956-0883

In recent years, international attention has been turned to the ways that states use disinformation to further their own political ends. Propaganda, information conflict and active measures have long been a tool of statecraft, but the parallel development of information and communication technologies with increased levels of internal discord and social tension within states have made such disinformation campaigns both more effective and more worrying. This paper provides a brief history of Soviet "active measures", before examining the role of Russian disinformation and cognitive warfare in Russia's 2022 invasion of Ukraine. The examination of this topic is not solely confined to a description of the methods used; it also highlights some of the ethical issues involved in Russia's use of cognitive warfare and its heavy reliance on disinformation. Whereas information warfare focuses on controlling the flow of information, cognitive warfare instead has a more subtle yet potentially more damaging goal of shaping not simply what people think, but how they think and how they react to information. One of the significant features of the current conflict in Ukraine is the role that disinformation is playing in both driving and describing the conflict, and this paper explores the history and ethical implications of modern cognitive warfare, particularly in relation to the current conflict in Ukraine.

Keywords: active measures, cognitive warfare, disinformation, Ukraine invasion, PSYOPS, hybrid, NATO.

[1] *Dr. Paul Burke* is an Intelligence and counter-terrorism professional with 30 years of strategic experience in managing the Intelligence and security domain primarily within UK government. He edited *"Global Jihadist Terrorism – Terrorist Groups, Zones of Armed Conflict and National Counter-Terrorism Strategies"* [1].

[2] *Dr. Adam Henschke* is an applied ethicist and works at the interface of ethics, technology, and national security. He is currently part of the Dutch Research Council *"Ethics of Socially Disruptive Technologies"* project, which is funded through the Gravitation programme of the Dutch Ministry of Education, Culture, and Science and the Netherlands Organization for Scientific Research (NWO grant number 024.004.031).

Пол Бьорк, Адам Геншке

У МЕНЕ СВОЯ ПРАВДА… А В ТЕБЕ ЯКА? ШЛЯХ ВІД АКТИВНИХ ЗАХОДІВ ДО КОГНІТИВНОЇ ВІЙНИ ПІД ЧАС РОСІЙСЬКОГО ВТОРГНЕННЯ В УКРАЇНУ

Останніми роками міжнародна увага була прикута до того, як держави використовують дезінформацію для досягнення власних політичних цілей. Пропаганду, інформаційні конфлікти та активні заходи вже давно використовують як засоби керування державою. Але процеси розвитку інформаційних і комунікаційних технологій, зростання внутрішнього розбрату й соціальної напруги в державах, що відбуваються одночасно, сприяють підвищенню ефективності дезінформаційних кампаній, а також посилюють занепокоєння щодо їх наслідків. У цій статті подано короткий огляд радянських «активних заходів» та проаналізовано роль російської дезінформації та когнітивної війни у вторгненні Росії в Україну в 2022 році. Дослідження цієї теми не обмежується лише описом методів, які застосовуються. Також висвітлено деякі етичні проблеми, пов'язані з використанням Росією інструментарію когнітивної війни та сильною залежністю останньої від дезінформації. У фокусі інформаційної війни перебуває контроль над потоком інформації, натомість когнітивна війна має менш чітку, але потенційно більш згубну мету – формувати не лише те, про що люди думають, а й те, як вони думають і як реагують на інформацію. Однією зі значущих особливостей нинішньої агресії Росії проти України є роль дезінформації, яку остання відіграє як у розпалюванні конфлікту, так і в його висвітленні. Автори статті досліджують значення дезінформації на тлі історії та етичних наслідків сучасної когнітивної війни, зокрема у зв'язку з конфліктом в Україні, що нині триває.

Ключові слова: активні заходи, когнітивна війна, дезінформація, вторгнення в Україну, ІПСО, гібридність, НАТО.

> *"Russia's information operations are used by the Kremlin as both a prelude to war, an alternative to war, and a handmaiden in war".* [3]

Introduction

In recent years, international attention has been turned to the ways that states use disinformation to further their own political ends. Propaganda, information conflict, and active measures have long been a tool of statecraft [2], but the parallel development of information and communication technologies with increased levels of internal discord and social tension within states have made such disinformation campaigns both more effective and more worrying. One of the significantly notable features of the current conflict in Ukraine is the role that disinformation is playing in both driving and describing the conflict.

This paper[4] provides a brief history of Soviet "active measures", before examining the role of Russian disinformation and cognitive warfare in Russia's 2022 invasion of Ukraine. The examination of this topic is not solely confined to a description of the methods used; it also highlights some of the ethical issues involved in Russia's use of cognitive warfare and its heavy reliance on disinformation. Where information warfare focuses on controlling the flow of information, cognitive warfare instead has a more subtle yet potentially more damaging goal of shaping not simply what people think, but how they think and how they react to information.

[3] Attributed to the Henry Jackson Institute by John Sipher (2018) [3].

[4] This research was part-funded by the following projects: the Australian Research Council Discovery Project number DP180103439 *"Intelligence And National Security: Ethics, Efficacy And Accountability"*, the European Research Council's Advanced Grant program *"Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies"* (GTCMR. No. 670172), and the Dutch Research Council *"Ethics of Socially Disruptive Technologies"* project, which is funded through the Gravitation programme of the Dutch Ministry of Education, Culture, and Science and the Netherlands Organization for Scientific Research (NWO grant number 024.004.031).

Active Measures

The term "active measures" (*Russian: активные мероприятия*) refers to a very broad set of covert activities from the supporting of political opposition parties to assassinations of dissident individuals. The term itself is believed to have first been used in the late 1950s or early 1960s, but the conceptual idea of active measures was being used by the post-revolutionary government of the newly formed Soviet Union in the early 1920s. As early as 1972, active measures were comprehensively defined as a concept by the KGB's Felix Dzerzhinsky Higher School, in its publication *"Dictionary of Counterintelligence", as: "acts of counter-intelligence making it possible to penetrate the intentions of the enemy, allowing his unwanted steps to be anticipated, to lead the enemy into error, to take the initiative from him, to thwart his actions of sabotage. Active measures, in contrast to defensive measures, e.g. those concerning the maintenance of a regime of secrecy and the protection of state and military secrets, are offensive in nature, allowing the detection and prevention of hostile activities in their early stages, forcing the opponent to expose himself, imposing the will to act on him, forcing him to act in adverse conditions and in ways desired by the counterintelligence services. In practice, active measures as practised in counterintelligence activities by the organs of state security include projects aimed at building up the position of spies in the camp of the enemy and its surroundings, conducting operational games with the enemy, disinformation directed at him, compromise and demoralisation, the transfer onto the territory of the USSR of persons of special operational value, obtaining intelligence information, etc."* [4, pp. 161–162].

As a former General in the KGB, Oleg Kalugin headed the Foreign Counter-Intelligence Branch (K Branch) in the agency's First Chief Directorate. Well versed in the theory and practice of active measures, Kalugin described them in a 1998 interview: *"On the other hand – and this is the other side of the Soviet intelligence, very important: perhaps I would describe it as the heart and soul of the Soviet intelligence – was subversion. Not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs. To make America more vulnerable to the anger and distrust of other peoples"* [5].

In practical terms, active measures included a very broad bunch of operational tools, including, but definitely not limited to, funding sympathetic political groups and parties, producing counterfeit documents and currency, supporting civil opposition groups, producing and disseminating disinformation, supplying and training paramilitary groups to be used as proxy tools, penetrating designated organisations or communities and, where deemed appropriate, the assassination of key individuals. If, as Clausewitz said, war is *"a continuation of political intercourse, a carrying out of the same by other means"* [6, bks. 6, Defence], (often paraphrased as *"war is an extension of politics"),* then active measures can be considered as an extension of political warfare, using covert methods.

Rid provides three defining characteristics of active measures [2]. First, these are not "simple, uncoordinated lies" told by powerbrokers such as politicians or government officials. By contrast, they require a considerable amount of forward planning, ongoing management, deconfliction with other agencies and coordination of execution. It is clear that the deconfliction and coordination, in particular, are crucial elements to the success of such an operation. The risk of counter-briefing or puzzled denials by an agency or government department left outside the loop could bring a well-planned deception operation crashing down in quick time.

His second point is that dishonesty lies at the core of all active measures, but herein lies the subtlety. Blatant lies are more likely to be poorly received than carefully crafted messaging which skilfully incorporates a blend of truth, half-truth and fiction. Pointing to a conclusion without explicitly stating it, and providing a suitable smorgasbord of facts and fiction, can allow the target audience to feel as if they have come to their own, critically considered, conclusion. The deception may attempt to mask the essence of the active measure, such as President Putin's claims that Russia was forced to invade Ukraine *"to protect the people that are subjected to abuse, genocide from the Kiev regime…(and) demilitarize and de-nazify Ukraine"* [7], claims widely dismissed by the United Nations and the international community [8].

The deception may primarily involve the masking or fake attribution of the person or persons responsible for stealing and/or leaking information, such as the hacking and leaking of emails from US political entities including the Democratic National Committee (DNC) in 2015 and 2016, the hacking of a contractor to the Republican National Committee (RNC) in 2021 and the ransomware attacks against Colonial Pipeline in 2021 [9]. Rid's third characteristic is that active measures will always be designed with an explicit geopolitical aim in mind, and usually this aim will be the weakening of an opponent. One only needs to consider the aforementioned leaks of the DNC, to see the scale of potential damage that one can inflict on an opponent through the use of such a measure.

Operation TRUST

One of the earliest operations of this type provides a timeless and classic example of the genre. In the early 1920s, the OGPU or Joint State Political Directorate (Russian: *Объединённое государственное политическое управление* – the Soviet agency responsible for Intelligence and internal security), began Operation TRUST, a counter-Intelligence operation which used disinformation to lure Russian royalists and other assorted "counter-revolutionaries" back to the Soviet Union, where they could be arrested, imprisoned and interrogated. The operation was heavily based on the use of the "Monarchist Union of Central Russia" (also referred to in some writings as the Monarchist Association of Central Russia"), to achieve its ends. There is some historical disagreement as to whether this grouping was actually created as a front organisation by the OGPU, or whether it was an existing organisation that was eventually heavily penetrated by the OGPU [7; 10, pp. 33–35; 11, pp. 1–3]. Regardless of its genesis, the operation had two primary aims according to Grant [12]. First was the monitoring of activities by anti-Bolsheviks outside of Russia, and second was the creation of pathways for the delivery of *"shrewdly contrived disinformation"*. Among the notable successes of Operation TRUST was the luring of Boris Savinkov, an anti-Bolshevik émigré, and Sidney Reilly (famously known as "the Ace of Spies") into the Soviet Union in 1925. Both men were arrested, interrogated and either executed, in Reilly's case, or supposedly committed suicide, in Savinkov's case.

Operation DENVER

Another example of Soviet active measures, one which still draws in adherents to this day, was Operation DENVER, the 1980s disinformation campaign that amplified and repeated the story that the HIV virus, which causes AIDS, had been developed by the US military and had inadvertently escaped from the U.S. Army Medical Research Institute for Infectious Diseases (USAMRIID) at Fort Detrick [2, pp. 298–311]. As early as 1983, disinformation on the AIDS virus had already begun to appear in the press of developing countries, such as a letter to the editor of the Patriot newspaper in India, purporting to be from an anonymous but respected American "scientist and anthropologist". The letter, unusually printed on the newspaper's front page, made the claim that the AIDS virus had been manufactured by the US in the Fort Detrick facility. The writer made a clever linking bridge between the allegation that AIDS was a US-manufactured virus, and the risk to it spreading across India, as the article claimed that the US was conducting experiments of a similar nature across the border in Pakistan. An examination by Christopher Nahring of official documents in the Bulgarian State archives revealed a request from the KGB's First Directorate in Moscow to Bulgarian State Security, for their assistance in conducting a disinformation campaign to promote the false narrative of a US-created HIV virus. The KGB request stated: *"We are conducting a series of [active] measures in connection with the appearance in recent years in the USA of a new and dangerous disease, 'Acquired Immune Deficiency Syndrome – AIDS' …and its subsequent, large-scale spread to other countries, including those in Western Europe. The goal of these measures is to create a favorable opinion for us abroad that this disease is the result of secret experiments with a new type of biological weapon by the secret services of the USA and the Pentagon that spun out of control"* [13].

The disinformation operation was directed by the Soviet KGB, facilitated by the German Democratic Republic's (GDR) Stasi (German: *Ministerium für Staatsicherheit*) and Bulgarian State Security and assisted by the Czech StB (Czech: *Státní bezpečnost*).

In 1986, the Stasi produced a faked report entitled *"AIDS: Its Nature and Origin"*, based upon a fictitious scientific research study conducted by Professor Jakob Segal and his wife, Lilli Segal, both citizens of the Soviet Union. This was initially published and distributed as a booklet entitled *"AIDS: USA home-made evil, NOT out of AFRICA"*, for the 7th summit meeting in Harare in 1986, of the Non-Aligned Movement in 1986. The fake theory took off and by 1987 the KGB would inform their Bulgarian counterparts that Segal's publications and the spreading of his theory had achieved *"attained great renown… (and) gained considerable resonance in African countries"* [13]. The formal support of the KGB in propagating the AIDS disinformation through Operation DENVER officially ceased in late 1987, following strenuous objections by US Secretary of State George Schulz when he met with Soviet leader Mikhail Gorbachev [14].

One problem with a disinformation campaign, however, is that it can be incredibly difficult to persuade the genie that it should get back into the bottle whence it came, and so it was with Operation DENVER. While the KGB may have actively stopped their direct involvement in propagating the falsehood around AIDS, the story developed a life of its own. In 2014, Russia's SPUTNIK news agency published an article strongly suggesting that an outbreak of Ebola in Sierra Leone and Liberia could have been the fault of the US, as the article claimed that both countries were *"known to host American biological warfare laboratories"* [15]. As Pebody noted, quoting the January 2015 edition of the American Journal of Public Health, *"The idea that AIDS was created as part of a government-led conspiracy to decimate the African American population remains salient to a significant minority of black people"* [16]. Even as recently as February 2018, Russia's SPUTNIK news agency's African arm was still publishing stories on the hidden dangers posed by US bases including Harvey Point, Fort Detrick and Edwards Air Force Base [17].

Some 38 years after Operation DENVER was released into the wild, it continues to fuel theories that the US has been responsible for a variety of outbreaks of disease, usually based on the premise that these diseases were either manufactured or were genetically modified by the US. The inaccurate linking of Fort Detrick with US-manufactured or US-modified viruses found a willing audience when the SARS-COV-2 virus began to spread in December 2019, before global transmission erupted in January 2020. Even the social media behemoth Facebook stated in May 2021 that the platform would *"no longer remove the claim that COVID-19 is man-made from our apps"* [18; 19].

Net-Centric Warfare and Information Warfare

The fall of the Berlin Wall in 1989 and the dissolution of the Soviet Union in 1991 were followed by a number of shifts in NATO military thinking. The first was the concept of network-centric warfare (NCW), a vision articulated and expanded in the mid-1990s, by a number of writers including then-Vice Chairman of the US Joint Chiefs of Staff (JCS) Admiral William Owens [20], Vice Admiral Arthur Cebrowski, then-Director for Space, Information Warfare, Command and Control (N6), and Stein et. al., who defined network-centric warfare as *"an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization"* [21, pp. 2–3].

NCW was designed to combine the full complement of sensors, communications systems, Intelligence systems and weapons systems and provide all of this in as near-real-time as possible, to provide dominant battlefield awareness. It was a major step forward from the previous concept of platform-centric warfare. This was the true start of the technological promises of the late 1980s and 1990s advances starting to become a more concrete reality and it was also the precursor to the next development, that of information warfare (IW).

As communications systems matured and the speed and bandwidth of systems increased to be capable of handling much greater volumes of data, it was clear that the infosphere would become an increasingly important battleground in future operational scenarios. An early definition from 1996 viewed IW as *"actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks"* [22, p. 2-2].

Some 25 years later, a more refined definition would see IW as *"controlling one's own information space, protecting access to one's own information, while acquiring and using the opponent's information, destroying their information systems and disrupting the information flow"* [23]. An aspect of IW, from the military perspective at least, is that of deception but there is a distinction to be made here. The use of military deception should not be confused with the current tactics of using social media to deceive population groups; rather, it is a tightly focused element of that targets the armed forces of the opponent through the use of tactics such as spoofing, electronic warfare (EW), or the deployment of dummy assets. The key battleground of IW is the actual flow of information.

Cognitive Warfare

The next logical evolution in the information battleground is cognitive warfare, a far more ambitious, far-reaching and potentially more damaging development of the infosphere as a battleground. Instead of being the tool itself, cognitive warfare uses disinformation, fake news, propaganda and alternative facts as a fuel source to frustrate the abilities of individuals, groups and wider society to make informed, critically assessed decisions on what they believe to be true. Rather than the targeting of information, which is a considerably easier task, cognitive warfare targets people's opinions, how they are formed and how people react to them, a much more dangerous and far-reaching outcome, especially for liberal democracies. As Applebaum notes: *"There is no easy way to distinguish between conspiracy theories and true stories. False, partisan, and often misleading narratives now spread in digital wildfires, cascades of falsehood that move too fast for fact checkers to keep up. And even if they could, it no longer matters: a part of the public will never read or see fact-checking websites, and if they do they won't believe them"* [24, p. 205].

Cognitive warfare comes with the convergence of technologies (Nanotechnology, Biotechnology, Information Technology and Cognitive Sciences, or NBICs), which collectively have the potential to improve and enhance human capability and performance, but are also capable of being used for more insidious purposes. With the instant and global reach of social and other media platforms, cognitive warfare methods can subvert areas such as the national perception of domestic security and peace, social fabric and the social order, broad public outlook and even economic security and well-being. It allows the application of force to concentrate on the informational and cognitive space, rather than taking a kinetic approach to hard targets.

Definitions of Cognitive Warfare

Cognitive warfare fuses elements of network-centric warfare, information warfare, psychological operations (PSYOPS) and shaping and influencing operations and various definitions of the concept exist. It is useful at this point in the paper to provide a number of definitions of cognitive warfare. Focusing on China's use of it in regard to its stance on Taiwan, it is described as *"activities designed to control others' mental states and behaviors"* [25, p. 1]. Looking primarily at Hamas and Hezbollah, Mackiewicz describes it as *"a disinformation process to psychologically wear down the receivers of the information"* [26, p. 1]. A definition derived from studying Russia's attempts to disrupt and influence the US Presidential elections describes cognitive subversion as the *"manipulation of the public discourse by external elements seeking to undermine social unity or damage public trust in the political system"* [27].

After a lengthy analysis of the topic, Ottewell first defines the cognitive domain before then defining cognitive warfare as *"Manoeuvres in the cognitive domain to establish a predetermined perception among a target audience in order to gain advantage over another party"* [28]. Backes and Swab, discussing the threat posed by Russian interference in the integrity of elections in the Baltic states, define it as *"a strategy that focuses on altering how a target population thinks – and through that how it acts"* [29, p. 8]. A paper written for the NATO Innovation Hub, which takes a more holistic view of the entire subject matter, sees cognitive warfare as *"the weaponization of public opinion, by an external entity, for the purpose of (1) influencing public and governmental policy and (2) destabilizing public institutions"* [30, p. 3].

To some extent, cognitive warfare seeks to encourage the opponent to destroy itself from the inside out. Through the amplification of existing divisions, the creation of new divisions where none might previously have occurred, and the ratcheting up of inflammatory rhetoric to exacerbate the idea that multiple groups or sub-groups are under threat from others, effects can be achieved which may otherwise be unobtainable without resorting to the application, or threat, of force. As a RAND report on disinformation states, *"all other things being equal, messages received in greater volume and from more sources will be more persuasive"* [31, p. 3]. Soviet tactics, using tanks, infantry and artillery, always subscribed to the adage of *"quantity has a quality all of its own"*[5]. The same approach has been taken by Russia's Intelligence organs on the digital battlefield, where high-volume, lower-quality output can often achieve the same effect as higher-quality, low-volume output.

For a cognitive warfare strategy to be successful, it must be flexible, methodical, resilient and coordinated. It should ideally be able to rapidly encompass new developments and fold them into the existing strategy. When a target of opportunity presents itself, it usually comes with a narrow, temporal window in which to exploit the target before it is either overtaken by events, or the opponent is able to minimise or negate the opportunity to use it as an attack vector. We discuss an example of this in more detail in the "discredit" section. Instigating and managing the strategy needs to be done methodically, to ensure that follow-up measures such as new releases of information follow seamlessly on from their predecessors. For an operation based upon a developing timeline, the continuum of the narrative will be of utmost importance. In an internet environment populated by countless interested individuals, there is no room for error in presenting the chronicle of events.

The operational planning must include resilience measures, to be able to either deflect (*"you are only saying this to draw attention away from your actions involving X and Y"*), deny (*"this is nothing to do with us"*), rebut (*"you may think it was us but you are wrong, and here is our assessment of the facts"*) or refute (*"it categorically was not us, and here is the supporting evidence"*) an accusation from the opponent or even the public, that there is a

[5] The quote is variously attributed to Josef Stalin, Napoleon Bonaparte and others. This same approach is still being used by the Russian Army, in its colossal use of artillery firepower against Ukrainian targets, often in support of siege tactics.

cognitive operation ongoing. It is difficult to envisage how a sophisticated cognitive warfare operation could be mounted without approval from, and possibly the ongoing involvement by, the highest levels of political authority. This is especially so, given the potential for "blowback", or for the operation to be uncovered through poor tradecraft or by events outside the control of the operational machinery. Such a coordinated approach is essential to ensure that multiple government departments are not counter-briefing each other, or unwittingly contradicting or exposing the operation.

The Cognitive Warfare Toolbox

The methods of cognitive warfare can be broadly summarised as follows:

- distract
- demoralise
- discredit
- deceive
- divide
- deny
- dislocate expectations
- destroy from within.

Distract

A favoured ploy in warfare is to provide a distraction for the enemy, which removes or reduces their focus on something else, to concentrate on the distraction. Disinformation can provide this instantly, and at scale, when required. In November 2014, US General Philip Breedlove went public with a US Intelligence assessment that Russian military vehicles and other equipment was entering Ukrainian territory. One month later, Russia accused the West of providing lethal equipment support to Ukraine and the scene was set for another information-based attack by Russia. The first appearance of a hacking group calling itself CyberCaliphate came on Christmas eve, when a regional media outlet in Albuquerque had its website hacked, with an ISIS flag and the quote *"I love you isis"* inserted alongside [32]. On 06 January, it was the turn of a Maryland-based television channel to be hacked. The next day, the spate of terror attacks in Paris began, when the offices of the *Charlie Hebdo* magazine were attacked by Islamist militants claiming allegiance to Al Qa'eda in the Arabian Peninsula (AQAP) and the CyberCaliphate threat looked very real [33; 34].

Just days after the Paris attacks, some of the social media accounts belonging to the website of US Central Command (USCENTCOM), including its Twitter feed, were hacked, and a number of messages were broadcast by the group, using the compromised Twitter account [35]. This delivered a publicity coup for the hackers, generating more than 200 global media reports in just one month [2, p. 367]. Less than two weeks later, French television channel TV5/Monde had its network covertly penetrated, in preparation for a spectacular hack that took all 11 of its channels of the air for several hours and left its website defaced with images and Arabic text claiming to be from the CyberCaliphate group. The attack was perfectly timed, with the takedown occurring 3 minutes before the launch of a new TV channel by the network [36–39]. This broad-spectrum series of cyber attacks and disinformation-spreading took place over a period of several months and created a considerable degree of global paranoia about IS-led cyber warfare but the much more tangible result was that it caused a sufficiently major distraction to ensure that Russian military intervention in Ukraine was no longer at the top of the global media focus list.

Demoralise

Four days after the start of Russia's invasion, TASS reported that Russia had achieved air superiority over the skies of Ukraine [40]. It is possible that the Russian air force had in mind a different, more favourable, definition of air superiority than the NATO one [41], but from the start of the invasion, Russia has never achieved air superiority (*"the degree of control of the air by one force that permits the conduct of its operations at a given time and place without prohibitive interference from air and missile threats"*), let alone air supremacy (*"that degree of control of the air wherein the opposing force is incapable of effective interference within the operational area using air and missile threats"*) [41]. While there have been countless attempts to demoralise the Ukrainian public since the start of the invasion, the Russian disinformation campaigns aimed at demoralising the Ukrainian population have so far failed to achieve critical mass.

Discredit

Ukraine's move towards closer ties with the EU took a major step backwards on 21 November 2013, when President Yanukovych suddenly announced that he would not be signing the Brussels-Kiev pact, and would instead be concentrating on restoring economic ties with Russia [42]. Using a "carrot and stick" approach, Yanukovych was threatened with the loss of billions of dollars of Russia-Ukraine trade per year, while also being offered a loan totalling $15 billion from Russia, and a cut in natural gas prices by around one-third, to sweeten the decision to move away from the EU and to bring Ukraine back into the Russian orbit [42; 43]. The decision was a catalyst for massive street protests that would last several months, with hundreds of thousands of Ukrainians angry about the abrupt removal of any ambitions for Ukraine to join the EU, and instead return to Russia's orbit of influence. A week after the protests began, Yanukovych deployed the Berkut, a specialist Militia unit responsible to the Interior Ministry, to break up the protests.

The violence used by the Berkut against the protestors simply inflamed the situation and drew more people to join with the protestors. In December 2013, a month after the start of the protests, a US political delegation met with Yanukovch, to discuss the situation. On the morning of 11 December, US Ambassador Geoffrey Pyatt and US Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland mingled with protestors in Maidan Square, and handed out food to protesters as well as to Police and Berkut officers [44]. The highly visible actions of Nuland and Pyatt meant that they were immediately on the radar of Russian Intelligence.

On 04 February, an audio recording was leaked online, allegedly intercepted between Pyatt and Nuland discussing next steps. Both politicians were keen to see more concrete actions taken against Yanukovych's government for the brutal suppression of the civil rights protests in Ukraine, and both seemed dissatisfied with the collective response of the EU in relation to this. In the intercepted call, the person alleged to be Nuland informs the other party that she would like to get the United Nations involved, as this would *"help glue this thing together…and, you know, f**** [expletive masked] *the EU*". The response of the other party, alleged to be Pyatt, was: "*Exactly. And I think we've got to do something to make it stick together because you can be pretty sure that if it does start to gain altitude, the Russians will be working behind the scenes to try to torpedo it"* [45]. Then-Chancellor Merkel responded to the accusation, saying that she considered the statement about the EU *"… absolutely unacceptable … and … that [EU foreign policy chief Catherine] Ashton is doing an outstanding job… The European Union will continue with its intensive efforts to calm the situation in Ukraine".*

A second intercepted and leaked call was allegedly between Helga Schmid (deputy to EU foreign policy chief Catherine Ashton) and Jan Tombinski (EU ambassador to Ukraine). The voice alleged to be Schmid says *"It's very annoying that the Americans are going around criticizing the EU and saying we are too soft"* [45–47]. The leaks could not have been better timed, causing a minor fissure in EU-US relations but generating a much bigger story worldwide that painted US political dealings in a less favourable light. As an active measure, the whole set-up was professionally planned, timed and executed to ensure the public discrediting of the parties allegedly involved.

Deceive

Writing on deception, the historian Liddel-Hart said that its aim was *"to deprive the enemy of his freedom of action, and it should operate in the physical and psychological spheres… In the psychological sphere, the same effect is sought by playing upon the fears of, and by deceiving, the opposing command"* [48, pp. 327–328]. Just two days after the start of the Russian invasion of Ukraine, in a move clearly designed to deceive the Ukrainian population and the global media, the Russian State-owned media outlet TASS announced that Ukrainian President Zelenskyy had fled the capital to Lviv, along with his political entourage, and that any videos henceforth were pre-recorded fakes [49].

On the contrary, Zelenskyy had publicly and avowedly rejected any possibility of leaving Ukraine, and he then released video messages of himself outside the front of Ukraine's Chimeras house, opposite the Presidential office, with the Prime Minister and members of his cabinet, telling Ukrainians that *"our troops are here, citizens are here. All of us are here protecting the independence of our country. We are all here, and it will continue to be this way"* [50]. The tactic blatantly failed, as Zelenskyy began to deliver a nightly video address to the nation, often being filmed outside well-known landmarks, to emphasise to Ukrainians that he remained in Ukraine alongside them.

Divide

The US Presidential elections of 2016 provided Russia with the perfect environment in which to test a variety of disinformation approaches. Whereas active measures during Soviet times were usually more focused on groups, political parties or causes which were broadly supportive of, or at least closely allied to, the prevailing Weltanschauung (which in itself could change dramatically at short notice), the contemporary approach employed by Russia in its cognitive warfare methodology is more focused on creating chaos, confusion and dissent, on polarising sectors of the population, on increasing the perception within different groups, of being under threat or siege, of pitting one or more groups against others, and on increasing internal conflicts in target countries, regions or groups. Quoting an Intelligence Community Assessment of 2017, the Senate Select Committee noted that *"Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency"* [51].

Paid adverts posted on prominent social media platforms purported to from US citizens and targeted groups based upon race, religion, veteran status, immigration beliefs, sexual identification, annual income. Some of these included the famous "Army of Jesus" adverts, which told US citizens that Hilary Clinton was a Satan, and exhorted Americans to vote for Donald Trump instead [52]. In its findings of an investigation into the illegal manipulation of social media by Russian entities such as the Internet Research Agency, the US Senate Permanent Select Committee on Intelligence stated: *"This newly released data demonstrates how aggressively Russia sought to divide Americans by race, religion and ideology, and how the IRA actively worked to erode trust in our democratic institution. Most troublingly, it shows that these activities have not stopped"* [53].

The traditional tactic of "divide and conquer" seems to have been refined by the Russian leadership into "divide and manage". Creating and exploiting as many social fissures as possible allows for a greater number of smaller-sized groups to be more effectively targeted and dealt with, while simultaneously broadcasting a distorted picture of a divided society. These fissures are specifically targeted at a number of levels of operation. At the lowest level, they target the multifaceted layers of the social fabric of a country, which in the case of the 2016 US election interference, targeted Muslims, Christians, Blacks, Whites, Veterans, Republicans, Democrats, Parents, Southerners and LGBTQ+ communities. At the next level, they aim to increase friction and reduce cooperation between countries, such as Russia's focus on its narrative about Poland, from around 2016 to 2018, which subsequently switched to a more focused narrative on Hungary, from 2018 to 2020, all aimed at destabilising efforts by the EU as a body politic, and by individual EU member states, to work with Ukraine as a partner. At the upper end of the scale, the aim is to create schisms between major alliances or international bodies, such as NATO and the United Nations, to mute criticism and blunt intervention regarding Russia's seizure of Ukrainian territory, an act described by the United Nations Secretary General as a violation of the UN Charter [54].

Deny

On 24 February, many global newspapers and media outlets led with a photograph of an injured Ukrainian woman, Olena Kurilo, who was the victim of a Russian artillery strike against a residential building in Chuhuiv, close to Kharkiv [55]. She was photographed by an Anadolu Agency photographer, Wolfgang Schwan [56]. The Russian Federation's Deputy Permanent Representative to the United Nations in Geneva, General Alexander Alimov, used his official Twitter account to deny that the woman had been injured, saying that the photo was staged using fake blood, even accusing her of being a member of a Ukrainian military PSYOPS Unit. He added additional photos claiming that the woman had been photographed uninjured two days after the attack, all of which were debunked as fake [57; 58]. Similar tactics were used to obfuscate the details of a Russian air strike on a maternity hospital in Mariupol, which Russia falsely claimed had been shelled by the Ukrainians, then said it was a staged attack, before finally admitting that the hospital was attacked by Russian forces, but claiming that it was being used as a Ukrainian military installation [59–62].

Dislocate expectations

Disinformation and its careful use in cognitive warfare can help to dislocate the expectations of one's opponent in exactly the same way that a diversionary attack can achieve a similar outcome in a kinetic battlespace. In the final days before the Russian invasion of Ukraine began in February 2022, President Putin and Russia's national media outlets were broadcasting a torrent of reassurances that the Russia had no intentions of invading Ukraine, all while putting the final touches to the plan for Russian forces to move across the border and seize large swathes of Ukrainian territory [63–66].

Destroy from within

All of the cognitive warfare tools can be combined to encourage and engineer the destruction of the opponent from within, thus potentially achieving victory without having to resort to kinetic warfare. The examples discussed previously, especially the campaign embarked upon by Russian Intelligence to create social discord in the USA's social media, prior to the Presidential elections, show how easily people can be fooled by high-volume disinformation, delivered at pace across a broad range of topics, with relevant adverts hitting precisely targeted groups or individuals. Writing about the use of disinformation and cognitive methods to turn social media use back upon protestors, Pomerantsev muses: *"What if a cleverer sort of ruler could find other ways to undermine dissidents, rid them of a clear* *enemy to fight, climb inside the images, ideas, stories of the great people-power protests and suck them dry from the inside, until they were devoid of meaning?"* [67, p. 57].

The Ethics of Foreign Targeting in Active Measures

Active measures, and the wider discussion of cognitive warfare, raise a range of ethical issues. First, however, the conceptual and normative space needs to be delineated. At issue here is the concept of "war", and its ethical significance. One particular school of thought considers that, in warfare, ethics don't apply. As Michael Walzer wrote in his pivotal text *"Just And Unjust Wars"*: *"For as long as men and women have talked about war, they have talked about it in terms of right and wrong. And for almost as long, some among them have derided such talk, called it a charade, insisted that war lies beyond (or beneath) moral judgment. War is a world apart, where life itself is at stake, where human nature is reduced to its elemental forms, where self-interest and necessity prevail. Here, men and women do what they must to save themselves and their communities, and morality and law have no place. Inter arma silent leges: in time of war, the law is silent"* [68, p. 3].

This view that war is simply justified by reference to self-interest, however, is the subject of significant criticism. The basic idea captured in the just war tradition is that many wars cannot be justified, but others can, and while certain activities in war might be not justified, others can be. A war of genocide would not be permissible, yet a war that prevents genocide *might* be. The point here is that, even in times of war, we can ethically criticise the war, and what is done in its name. Some types of cognitive warfare are going to be unjustified, while others might be more justifiable.

This leads us to the next point of clarification: do active measures count as warfare? Here we want to make an important distinction, between disinformation efforts pursued as part of an ongoing military conflict, and the wider idea of cognitive warfare. Where active measures form part of an ongoing military conflict, the ethical permissions will differ from that of cognitive warfare more generally. The principle here is that, because the norms around warfare (ethical, legal, political, and social) are of a particularly unique kind, the ethical norms around which active measures are permissible in warfare are going to be different from more general cognitive warfare. For instance, it is standard that in times of warfare there are different expectations on what a nation's media can and cannot report on, compared to peacetime restrictions. Here, insofar as the military conflict actually represents a significant threat to the survival of the state and/or its political community, the existential risk *might* offer a justification to more actively censor certain politically dangerous information, or even justify political communications aimed at giving the political community hope and a sense of optimism. In contrast, these permissions might be different in peacetime. However, there are two very important caveats to make here. First, this idea that the media and other public communications are subject to the political circumstances is a controversial one. Second, this does not necessarily mean that political leaders or the media can forgo a commitment to truth, a point we return to below.

The relevance of this distinction is that, if we accept that some particular information and activities are permitted in the exceptional circumstances of war, those permissions do not necessarily or easily carry to peacetime. That is, while we might see that certain active measures might be potentially justified in war, the permissions for cognitive warfare more generally are going to be quite different. Winston Churchill made the same point rather more succinctly during an allied conference in Tehran in 1943, when he remarked to Josef Stalin that *"in war-time, truth is so precious she should always be attended by a bodyguard of lies"* [69, sec. Prologue].

To follow this, a final point needs to be recognised: if we are comparing active measures in warfare with the use of information operations during peacetime cognitive war, it is easy to assume that cognitive warfare is permissible, as it is far less damaging than using bombs and bullets. In many ethical analyses, including in the just war tradition, proportionality calculations figure as one main way of determining if a particular course of action is permissible. If, for example, I have two options, and option A would cause 500 deaths, and option B would be a disinformation campaign that kills no-one, then on a simple proportionality calculation, option B would seem to be permissible. However, proportionality calculations are much more complicated, especially when comparing across different kinds of harm or damage, as the following highlights: *"If my life was at risk, and your only option to save me was to punch me in the face, then the punch (relevant harm) would be proportional to saving my life (relevant benefit). However, if I was being annoyed by a fly and you punched me in the face in order to get rid of the fly, then the punch (relevant harm) would be in excess to getting rid of the fly (relevant benefit); the punch is disproportional"* [70, p. 244].

While information-based operations might be far less damaging than a hot war, such cognitive warfare might actually be far more damaging than other forms of soft power such as aid and capacity building. The point here is that we must not only keep active measures used in warfare distinct from information-based operations used during peacetime (or in periods lacking sustained armed conflict), we must also be careful to compare cognitive warfare against the appropriate range and set of options available. If, at the end of its invasion of Ukraine, Russia withdraws, but a large proportion of the Russian-speaking population there believe that Ukraine was the cause of the war, then Russia still stands to win a major moral victory amongst the Russophone population.

Having set the conceptual terrain somewhat, we are now in a better place to assess the use of active measures as part of the conflict in Ukraine. First, if we want to understand the permissions around the use of active measures, we are going to consider that this situation is one in which there is an ongoing and sustained, organised armed conflict. We consider that this context is either war, or so similar to war that the moral permissions around war would apply to the use of active measures here. For this situation, as per the just war tradition, we have to assess whether the two main forces have a just cause for war or not. Russian claims about the conflict being to protect against NATO aggression, NATO expansion, Ukrainian neo-Nazi aggression, or the need to protect the Russian diaspora in the border regions are simply not valid and have been condemned by the United Nations and by the majority of the international community.

In contrast, Ukraine's case is that it is acting in self-defence against an invading and aggressive enemy. On this simple point, we can argue that the Russian use of active measures is not justified by reference to the military conflict. That is, their use of active measures forms a part of an unjustified act of invasion. The special exceptions for use of information operations that might be granted in times of conflict cannot be extended to the Russian use of active measures here, because they simply lack the just cause for warfare in the first place.

We can then consider the use of information-based operations in the more general and less permissive context of cognitive warfare. Here, there are two aspects of cognitive warfare that provide a basis for ethical criticism. In the definition offered by Dzerzhinsky at the start of this paper, active measures involve the instigator *"imposing the will to act on [their target]"* [4, pp. 161–162]. As noted previously, Kalugin stated that active measures were *"subversion. Not intelligence collection, but subversion"* [5]. These two complementary points draw out a major ethical concern with active measures, and also with cognitive warfare. The purpose, the very motivation for these operations is to subvert the will of the target. Whether this is an individual or a population more generally, active measures are intended to interfere with the will of the targets. This is ethically problematic as it does not show moral respect for people, an idea drawn from the work of Immanuel Kant. *"Central to Kant's ethical theory is the claim that all persons, regardless of personal qualities or achievements, social position, or moral track-record, are owed respect just because they are persons, that is, beings with rational and autonomous wills. To be a person is to have a status and worth unlike that of any other kind of being: it is to be an end in itself with dignity"* [71].

The key part of Kant's ethical theory here is that we need to treat people as autonomous self-directing agents. To be an end in themselves, a person's own decisions about their life, are what matters. We are bound to treat each other as having the capacity for free will, it is part of what we are as people. *"Such beings must never be used as if they were merely means, <u>as if they were nothing more than tools</u> that we may use however we want to advance our ends"* (Emphasis ours) [71]. The particular moral problem with active measures, is that they reduce the people who are the targets of the operation, to mere tools. They are not viewed as autonomous agents, but simply things to be used to achieve the military and/or political ends. In Dzerzhinsky's original formulation, we see this as the person behind the active measure imposing their will on the target. This raises an obvious counter-argument: in many normal social interactions, and especially in times of competition or conflict, we do use people for our own ends. In that case, what makes active measures especially problematic? *"Note, however, that it is not wrong to treat persons as means to our ends; indeed, we could not get along in life if we could not make use of the talents, abilities, service, and labour of other people. What we should not do is treat persons as <u>mere</u> means to our ends, to treat them as if the only value they have is what derives from their usefulness to us. Rather, we must always treat them "as the same time as an end"* (Emphasis Original) [71].

Given that the purpose of active measures, in Kalugin's terms, is intended to subvert people, they are not being treated as ends in themselves. On a Kantian approach, lies subvert a person's reason. *"Your reason is worked, like a machine: the deceiver tries to determine what levers to pull to get the desired results from you. Physical coercion treats someone's person as a tool; lying treats someone's reason as a tool. This is why Kant finds it so horrifying; it is a direct violation of autonomy"* [72, p. 334].

Putting this directly in the context of the ongoing conflict in Ukraine, we can see that the use of active measures here are simply about bending Ukrainian, and global, audiences to the will of the Russian leadership. As Rid writes: *"all active measures contain an element of disinformation"* [2, p. 9]. Whether the disinformation is the entirety of a story, a lie inserted into a mostly true story, or a narrowly true story but presented in a way that uses the truth to push a wider lie, the point of active measures is to lie, to misrepresent, or to twist the truth, in order to get the target to believe what the instigator wants the target to believe. This shows a fundamental disrespect for individuals as, by denying them proper and full information, they are being treated merely as a tool, as a means to political ends, and not making decisions of their own.

A second set of ethical concerns lifts the focus from the individual to a wider set of social harms. One of the hallmarks of Russian disinformation operations is the simple desire to cause chaos. Certain active measures, such as the use of compromising information about a political leader to blackmail them into taking a desired stance on a specific policy issue, are quite focused and targeted. There is a specific target in mind, and the information is being used to force that person to make a decision that the blackmailer wants. What we are observing in the current conflict in Ukraine, and in modern active measures more widely, does not take this form. In short, rather than specifically trying to bring about a particular outcome, the purpose itself is to sow chaos and promote social disunity. *"Sowing chaos and confusion is thus essentially operational preparation of the information battlefield – shaping actions that make the information environment more favorable for actual operations should they become necessary"* [73, p. 253].

One of the main purposes of current active measures may not necessarily be to bring about a specific political outcome, rather, the purpose is to exploit and expand existing social fissures, or to create them where none exist.

The ethical problems here are, at least, twofold. The first draws from the basic respect for individuals, discussed above. In short, when society is in chaos, individuals have less ability to determine their own paths in life. One of the reasons for individuals to form societies is the stability which that brings. In Thomas Hobbes' classic description of the state of nature in Leviathan, such a state is one in which we are in *"continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short"* [74, Chapter XIII, para. 9]. In order to avoid this nasty brutish and short life, we form societies. *"Put simply, it is in people's self-interest to collectivise certain aspects of their life, as there are particular goods that are either only achieved or secured collectively, or are better achieved collectively"* [75, p. 79]. Efforts to create chaos are essentially efforts to destroy the stability that comes from social organisation, and to return us to the dangerous state of nature.

One of the defining features of this sort of chaos is that it is hard to predict what the outcomes will be. Going back to the just war tradition, two of the criteria of whether it is permissible to go to war are whether the war itself is proportionate to other options at hand, and if there is a probability of success. Active measures and wider disinformation campaigns, even if they could be justified by reference to a justified military conflict, must be predictable to some degree. However, active measures that simply seek to unleash and amplify chaos fail these conditions.

It should also be noted that that cognitive warfare, i.e. sustained disinformation campaigns that occur in the absence of war that has chaos as the desired end-state, is extremely difficult, if not impossible, to justify. Any such efforts undertaken in Ukraine at the moment, including active measures that might continue to be used even if active conflict ceases, would be unjustified. Further to this, certain forms of chaos are explicitly about degrading the capacity of, and citizens' trust in, democratic institutions. Institutions, particularly democratic institutions, are a key point of vulnerability for interference operations [76]. Not only do such operations violate the political sovereignty of a target state, but they also violate the political will of the citizens in those states. Active measures that seek to create and sow political chaos are thus ethically impermissible.

Conclusions

Our final conclusions are twofold. First, active measures are playing an increasingly important role in the conflict in Ukraine. We suggest here that this trend is something that will be repeated and extended to other conflicts. Whether this is in reference to large-scale physical conflicts, such as Russia's invasion of Ukraine, or the wider notion of cognitive warfare, disinformation needs to be recognised, understood, and mitigated against.

Our second conclusion concerns the ethical aspects of cognitive warfare. We have argued that many of the features of active measures, as used in the lead up to, and throughout, the invasion of Ukraine, are morally problematic and/or morally impermissible. This is an important point to highlight, as it provides a basis to criticise the use of active measures in modern conflict and statecraft. Further to this, our analysis also provides the foundations of a set of guidelines that should apply to the behaviour of liberal democratic states.

While cognitive warfare may be less kinetically destructive than physical warfare, we draw attention to the fact that this alone does not mean that any and all uses of cognitive warfare are permissible. While much more needs to be said on the point about permissions and constraints in the use of information and disinformation for military and political ends, we hope to have drawn attention to some of the ethical issues in this rapidly developing space and we plan further research in this area. As the US Manual for Operations ADP 3-0 states: *"War is a human endeavor – a fundamentally human clash of wills often fought among populations. It is not a mechanical process that can be controlled precisely, or even mostly, by machines, statistics, or laws that cover operations in carefully controlled and predictable environments. Fundamentally, all war is about changing human behavior"* [77].

References

1. Burke, P., Elnakhala, D., & Miller, S. (Eds.). (2021). *Global Jihadist Terrorism: Terrorist groups, zones of armed conflict and national counter-terrorism strategies.* Edward Elgar Publishing.
2. Rid, T. (2021). *Active measures: the secret history of disinformation and political warfare.* Profile Books.
3. Sipher, J. (2018). *Russian 'Active Measures'.* CHACR Global Analysis Programme Briefing, 14.
4. KGB Felix Dzerzhinsky Higher School. (1972). К*онтрразведывательный словарь (Counter-Intelligence Dictionary).* KGB Felix Dzerzhinsky Higher School.
5. CNN. (1998). *Inside the KGB: An interview with retired KGB Maj. Gen. Oleg Kalugin*. In CNN.
6. Clausewitz, K. von. (1837). *On War* (M. E. Howard, & P. Paret (eds.); 1st ed.). Princeton University Press.
7. Waxman, O. B. (2022, March 03). What Putin Gets Wrong About 'Denazification' in Ukraine. *Time Magazine.* https://time.com/6154493/denazification-putin-ukraine-history-context/
8. United Nations. (2022, October 20). *The UN and the war in Ukraine: key information.* UN Website. https://unric.org/en/the-un-and-the-war-in-ukraine-key-information/
9. Sanger, D. E., & Perlroth, N. (2021, July 20). Attempted Hack of R.N.C. and Russian Ransomware Attack Test Biden. *New York Times.* https://www.nytimes.com/2021/07/06/technology/rnc-hacked-cyberattack-russia.html
10. Andrew, C. M., & Mitrokhin, V. (2001). *The sword and the shield: the Mitrokhin archive and the secret history of the KGB.* Basic Books.
11. Unknown. (1989). *The Trust.* The Security and Intelligence Foundation.
12. Grant, N. (1986). Deception on a grand scale. *International Journal of Intelligence and CounterIntelligence, 1*(4), 51–77. https://doi.org/10.1080/08850608608435036
13. Selvage, D., & Nehring, C. (2019, July 22). *Operation "Denver": KGB and Stasi Disinformation regarding AIDS.* Wilson Center. https://doi.org/10.1162/jcws_a_00907
14. Geissler, E. (2016). The AIDS Myth at 30. *International Journal of Virology and AIDS, 3*(1), 16–18. https://doi.org/10.23937/2469-567x/1510017
15. Sputnik. (2014, October 09). *US Links to Bio-Warfare Labs in Ebola Zone.* Sputnik International News. https://sputniknews.com/20141009/US-Links-to-Bio-Warfare-Labs-in-Ebola-Zone-Scholar-193837038.html
16. Pebody, R. (2015). *African American people's AIDS conspiracy beliefs best understood in terms of social anxiety and distrust, not ignorance.* AIDSMAP. https://www.aidsmap.com/news/jan-2015/african-american-peoples-aids-conspiracy-beliefs-best-understood-terms-social-anxiety
17. Sputnik Africa. (2018, February 02). *Les bases militaires que les USA préféreraient garder secrètes.* Sputnik News Africa. https://fr.sputniknews.africa/amp/20180202/bases-militaires-usa-images-satellite-1034989265.html
18. Dwoskin, E. (2021, May 27). Facebook will no longer remove content saying covid-19 is manmade. *Washington Post*. https://www.washingtonpost.com/technology/2021/05/27/facebook-covid-man-made/
19. Hern, A. (2021, May 27). Facebook lifts ban on posts claiming Covid-19 was man-made. *The Guardian.* https://www.theguardian.com/technology/2021/may/27/facebook-lifts-ban-on-posts-claiming-covid-19-was-man-made
20. Owens, W. A. (1996). The Emerging U.S. Systems of Systems. *Strategic Forum*, *63*, 1–6. Institute for National Strategic Studies (INSS). https://apps.dtic.mil/sti/pdfs/ADA394313.pdf
21. Stein, F. P., Garska, J. J., & Alberts, D. S. (1999). Network-centric warfare: Developing and Leveraging Information Superiority. In *IEEE/AFCEA – EUROCOMM 2000: Information Systems for Enhanced Public Safety and Security* (2nd ed.). Command and Control Research Program (CCRP). https://doi.org/10.1109/EURCOM.2000.874819
22. Department of the Army. (1996). *FM 100-6 Information operations*. Department of the Army. https://www.hsdl.org/c/view?docid=437397
23. NATO. (2022). *What is information warfare?* NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf
24. Applebaum, A. (2020). *Twilight of Democracy: The Seductive Lure of Authoritarianism*. Doubleday.
25. Hung, T. C., & Hung, T. W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies, 7*(4), 1–18. https://doi.org/10.1093/jogss/ogac016
26. Mackiewicz, D. (2019). Cognitive Warfare: Hamas & Hezbollah and their insidious efforts. In *Course: Islamic Jihadi-Salafi Terrorism as an Ongoing Challenge Institute of National Security Studies* (Issue November).

27. Rosner, Y., & Siman-Tov, D. (2018, March 08). *Russian Intervention in the US Presidential Elections: The New Threat of Cognitive Subversion*. Institute for National Security Studies. https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/

28. Ottewell, P. (2020, December 07). *Defining the Cognitive Domain*. Over the Horizon (OTH). https://othjournal.com/2020/12/07/defining-the-cognitive-domain/

29. Backes, O., & Swab, A. (2019, November). *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states

30. Bernal, A., Carter, C., Singh, I., Cao, K., & Madreperla, O. (2020). *Cognitive Warfare: An Attack on Truth and Thought*. NATO & Johns Hopkins University: Baltimore MD, USA. https://www.innovationhub-act.org/sites/default/files/2021-03/Cognitive%20 Warfare.pdf

31. Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. RAND. https://doi.org/10.7249/pe198

32. Peterson, A. (2015, January 06). Local news outlets' social media accounts get hijacked by hackers claiming to support ISIS. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2015/01/06/local-news-outlets-social-media-accounts-get-hijacked-by-hackers-claiming-to-support-isis/

33. Ingram, H. J. (2017). An Analysis of Inspire and Dabiq: Lessons from AQAP and Islamic State's Propaganda War. *Studies in Conflict & Terrorism, 40*(5), 357–375. https://doi.org/10.1080/1057610X.2016.1212551

34. Reed, A. (2015). *Al Qaeda in the Indian Subcontinent: A New Frontline in the Global Jihadist Movement?* International Centre for Counter-Terrorism (ICCT). https://doi.org/10.19165/2016.2.02

35. Schindler, J. R. (2016, June 18). False Flags: The Kremlin's Hidden Cyber Hand. *The Observer*. https://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/

36. CFR. (2015). *Compromise of TV5 Monde – Suspected to be the work of APT28*. CFR Website. https://www.cfr.org/cyber-operations/compromise-tv5-monde

37. Corera, G. (2016). *How France's TV5 was almost destroyed by "Russian hackers"*. BBC News. https://www.bbc.com/news/technology-37590375

38. France24. (2015, June 10). *Russian hackers likely behind 'IS group cyber attack' on French TV network*. France24. https://www.france24.com/en/20150610-france-cyberattack-tv5-television-network-russia-hackers

39. Weissman, C. G. (2015). *New Discovery Indicates That Russian Hackers APT28 Are Behind the TV5 Monde Hack*. Business Insider. https://www.businessinsider.com/new-discovery-indicates-that-russian-hackers-apt28-are-behind-the-tv5-monde-hack-2015-6?international=true&r=US&IR=T

40. TASS. (2022a, February 28). *Russian aviation gains air superiority over entire Ukraine*. TASS. https://tass.com/politics/1412963

41. U.S. Air University. (2017, April). *Doctrine Advisory: Control of the Air*. U.S. Air University. https://www.doctrine.af.mil/Portals/61/documents/doctrine_updates/du_17_01.pdf?ver=2017-09-17-113839-373

42. Traynor, I. (2013, November 22). Russia "blackmailed Ukraine to ditch EU pact". *The Guardian*. https://www.theguardian.com/world/2013/nov/22/russia-ukraine-eu-pact-lithuania

43. France24. (2013, December 17). *Russia woos Ukraine with $15 bn bailout and cut in gas price*. France24. https://www.france24.com/en/20131217-russia-ukraine-15-billion-bailout-cut-gas-price

44. BBC. (2013, December 11). *Kiev riot police retreat after storming protest bastions*. BBC News. https://www.bbc.com/news/world-europe-25328311

45. Chiacu, D., & Mohammed, A. (2014, February 07). *Leaked audio reveals embarrassing U.S. exchange on Ukraine, EU*. Reuters. https://www.reuters.com/article/us-usa-ukraine-tape-idUSBREA1601G20140207

46. Crowley, P. J. (2014). *Victoria Nuland gaffe shows diplomats can trash-talk too.* BBC News. https://www.bbc.com/news/world-us-canada-26085432

47. Rettman, A. (2014, February 06). *Ukraine leak designed to 'split' EU-US diplomacy*. EU Observer. https://euobserver.com/world/123036

48. Liddell-Hart, B. H. (1954). *Strategy*. Penguin Books.

49. TASS. (2022b). *Zelensky hastily fled Kiev, Russian State Duma Speaker claims – Russian Politics & Diplomacy*. TASS. https://tass.com/politics/1411855

50. Soundarajan, D. (2022, February 26). *Ukraine's Volodymyr Zelensky offered US evacuation flight but refuses to leave Kyiv: 'I need ammunition, not a ride.'* The Independent. https://www.independent.co.uk/news/world/europe/ukraine-volodymyr-zelensky-evacuation-russia-b2023838.html

51. US Senate Select Committee on Intelligence. (2018). *New Reports Shed Light on Internet Research Agency's Social Media Tactics*. US Senate Select Committee on Intelligence Website. https://www.intelligence.senate.gov/press/new-reports-shed-light-internet-research-agency's-social-media-tactics
52. Parlapiano, A., & Lee, J. C. (2018, February 16). The Propaganda Tools Used by Russians to Influence the 2016 Election. *The New York Times*. https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html
53. US Senate Permanent Select Committee on Intelligence. (2018). *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements*. US Senate Permanent Select Committee on Intelligence Website.
54. UNSDG. (2020). *Russia's invasion of Ukraine is a violation of the UN Charter, UN Chief tells Security Council*. UN Sustainable Development Group (UNSDG). https://unsdg.un.org/latest/announcements/russias-invasion-ukraine-violation-un-charter-un-chief-tells-security-council
55. Middleton, J. (2022). *Ukrainian teacher soaked in blood after surviving Russian missile strike thanks 'guardian angel'*. The Independent. https://www.independent.co.uk/news/world/europe/ukraine-teacher-invasion-russia-video-b2022739.html
56. Schwan, W. (2022, February 24). *A wounded woman, named locally as Olena Kurilo, is seen after an airstrike hits Kharkiv, Ukraine*. GettyImages. https://www.gettyimages.fr/detail/photo-d%27actualité/wounded-woman-named-locally-as-olena-kurilo-is-seen-photo-dactualité/1238718222
57. HKBU. (2022). *[FALSE] Did The Guardian use an old photo to report a Russian air strike amid the Russia-Ukraine war?* HKBU Fact Check. https://factcheck.hkbu.edu.hk/home/en/fc_report_eng/the-guardian/
58. Timberg, C., & Romm, T. (2018, December 16). New report on Russian disinformation, prepared for the Senate, shows the operation's scale and sweep. *The Washington Post*. https://www.washingtonpost.com/technology/2018/12/16/new-report-russian-disinformation-prepared-senate-shows-operations-scale-sweep/
59. de Abreu, C. M. (2022, April 05). *Debunking Russian claims that attack on Mariupol maternity hospital was staged*. France24. https://www.france24.com/en/tv-shows/truth-or-fake/20220405-debunking-russian-claims-attack-mariupol-maternity-hospital-staged
60. Musumeci, N. (2022, March 10). *Russia Makes Wild, Baseless Claims About Maternity Hospital It Bombed*. Business Insider. https://www.businessinsider.com/russia-baseless-claims-maternity-hospital-bombing-Ukraine-Mariupol-2022-3?r=US&IR=T
61. Polglase, K., Mezzoflore, G., & Doherty, L. (2022, March 17). *Anatomy of the Mariupol hospital attack: Examining how Russian forces hit a Ukraine maternity and children's hospital*. CNN. https://edition.cnn.com/interactive/2022/03/europe/mariupol-maternity-hospital-attack/index.html
62. Sadeghi, M. (2022, March 15). *Fact check: Russian attack on Mariupol hospital was not "staged".* US Today. https://eu.usatoday.com/story/news/factcheck/2022/03/15/fact-check-russian-attack-mariupol-hospital-not-staged/7041649001/
63. Kiely, E., & Farley, R. (2022). *Russian Rhetoric Ahead of Attack Against Ukraine: Deny, Deflect, Mislead*. The Annenberg Public Policy Center (FactCheck.Org). https://www.factcheck.org/2022/02/russian-rhetoric-ahead-of-attack-against-ukraine-deny-deflect-mislead/
64. Kuznetsov, V., & Cook, N. (2022, February 17). *Russia Tells U.S. No Ukraine Invasion Planned, Tass Reports*. Bloomberg. https://www.bloomberg.com/news/articles/2022-02-17/russia-tells-u-s-no-ukraine-invasion-planned-tass-says
65. Mills, C. (2022). *Ukraine crisis*. House of Commons Library. https://commonslibrary.parliament.uk/research-briefings/cbp-9455/
66. Reuters. (2022, February 04). *Russia denies allegations of fabricating pretext to invade Ukraine*. Reuters. https://www.reuters.com/world/europe/russia-denies-allegations-fabricating-pretext-invade-ukraine-2022-02-04/
67. Pomerantsev, P. (2019). *This Is Not Propaganda: Adventures in the War Against Reality*. Faber & Faber.
68. Walzer, M. (2006). *Just and unjust wars: a moral argument with historical illustrations* (4th ed.). Basic Books.
69. Brown, A. C. (1975). *Bodyguard of lies*. Harper & Row.
70. Henschke, A. (2018). Conceptualising proportionality and its relation to metadata. In Baldino (Ed.). *Intelligence and the function of government* (pp. 221–242). University of Melbourne Press.
71. Dillon, R. S. (2022). Respect. In E. N. Zalta & U. Nodelman (Eds.), *Stanford encyclopedia of philosophy*. Stanford University.
72. Korsgaard, C. M. (1986). The right to lie: Kant on dealing with evil. *Philosophy and Public Affairs, 15*(4), 325–349. https://doi.org/10.1017/cbo9781139174503.006

73. Lin, H., & Kerr, J. (2022). On Cyber-Enabled Information Warfare and Information Operations. In P. Cornish (Ed.). *The Oxford Handbook of Cyber Security* (1st ed.). Oxford University Press.
74. Hobbes, T. (1909). *Leviathan*. Collier & Son.
75. Henschke, A. (2022). Ethics And National Security: A Case For Reasons In Decision-Making. In A. Henschke, M. Clarke, M. Sussex, & T. LeGrand (Eds.). *The Palgrave handbook of national security* (pp. 1–415). Palgrave Macmillan, UK.
76. Henschke, A., Sussex, M., & O'Connor, C. (2020). Countering foreign interference: election integrity lessons for liberal democracies. *Journal of Cyber Policy, 5*(2), 180–198. https://doi.org/10.1080/23738871.2020.1797136
77. HQ Department of the Army. (2017). *ADP 3-0 Operations* (Vol. 23). HQ Department of the Army. https://irp.fas.org/doddir/army/adrp3_0.pdf