Received: 29 April 2023 | Revised: 23 July 2023 | Accepted: 27 July 2023

DOI: 10.1111/1758-5899.13257

POLICY INSIGHTS

Hybrid warfare and disinformation: A Ukraine war perspective

Sascha-Dominik Dov Bachmann[1,2] | **Dries Putter**[2] | **Guy Duczynski**[3]

[1]University of Canberra, Bruce, Australian Capital Territory, Australia

[2]Stellenbosch University, Stellenbosch, South Africa

[3]Edith Cowan University, Joondalup, Western Australia, Australia

Correspondence
Sascha-Dominik Dov Bachmann, Business, Government & Law, University of Canberra, Building 11, Level A, Room 12, University of Canberra, 11 Kirinari Street, Bruce, ACT 2617, Australia.
Email: sascha.bachmann@canberra.edu.au

Abstract

Misinformation, disinformation and mal information are part of the information disorder construct, dominating the information warfare domain. These are key enablers associated with grey zone operations, and an integral part of current adversaries' and competitors' hybrid warfare tool kit. Disinformation, in combination with influence operations, also plays an important role within the concept of hybrid warfare; both from a threat–and own resilience perspective. This article reflects on these information warfare tools and their application by Russia in the current Russo-Ukraine war, offering potentially considerable force multipliers in the information domain for the Russian aggressor. Hybrid warfare and associated threats, specifically focusing on aspects of information warfare, disinformation, deception (typically within the context of political activity or warfare so commonly associated with Russian active measures) and as part of an adversary's grey zone operations approach are all discussed raising awareness towards building resilience by means of a comprehensive approach to counter such threats to national security.

1 | THE SIAMESE TWINS OF WAR AND DISINFORMATION

Misinformation, disinformation and mal-information are currently very topical 'tools of choice' for the conduct of information warfare as witnessed in conjunction with COVID-19, Ukraine, and general elections in the Western World. These influence operations tools can be as destructive as kinetic operations, as they aim to distort, disrupt and undermine perceptions, political messaging and eventually and consequentially confidence in the Western rules-based system.

Such information warfare is not new, it had been deployed successfully and frequently as part of political warfare and propaganda approach in many conflict/competition situations, albeit with delayed propagation until the arrival of social media and other forms of mass circulation. The West, as the supposedly 'good' party in such a contest of ideas, has been using it rather successfully during preventative action against a communist takeover of Italy (1950s). From the mid-1960s propaganda seems to have become a prime Soviet Union (and its allies) influence discipline. *Disinformatjia* or reflexive control are just two of the Soviet variants of influence operations aimed at weakening Western resolve and strength—both in the operational theatre (Africa and Asia) or at home.

With the end of the Cold War, the evaporation of this 'grey zone' of war and peace (also described as operations in the cognitive information domain below the threshold of armed conflict) could have been expected. However, with the advent of both, a new Russia under Putin since 2000 primed at restoring Russian imperial 'greatness' and an increasingly assertive China under Xi, the contest in the grey zone has intensified, expanded and increased in its destructive effects.

The narrative is descriptive in nature, anchored in discussions about the manifestation of so-called hybrid warfare, associated threats and specifically focusing on disinformation in the Russo-Ukraine war during 2022, before discussing in more detail the nature of these concepts within the wider context of grey zone operations. Arguments could be offered to have three separate articles to deal with the three key aspects—the harmful nature of disinformation and its malicious intent, disinformation within the context of the Russo-Ukraine

war, and possibly a detailed unpacking of information disorder as a social science construct. However, separate articles will do little justice to the integrated nature of the three aspects. Mindful of the peculiarities of hybrid warfare, its associated threats from a grey zone perspective, a description of each of these constructs follows in this article within the context of its narrative.

2 | FALSE INFORMATION AS PART OF INFLUENCE OPERATIONS

The use of false information and by extension misinformation, disinformation and fake news as part of an adversary's influence operations are an ever-growing concern to modern democratic societies (Ahmed, Bachmann, Martin, et al., 2022: 105). It remains so due to the fact that information freedom and the freedom of expression are perceived as cornerstones for stable democratic societies.

Influence operations, both offensive and defensive in character, have a long history in the strategic competition between states. The targets of influence operations include selected decision makers and, where appropriate, the massed citizenry. These operations, due to the diversity of target audiences may involve many different domains of activity.[1] Operations targeting decision makers might focus on diplomatic, military or intelligence activities. Offensively, the practice of military deception (or generally referred to as MILDEC) is commonly used in a battlespace (Joint Chiefs of Staff 2014). Distinctively and in parallel, intelligence agencies devote considerable resources to sustaining the 'wilderness of mirrors' in espionage and counterespionage efforts (Martin, 2018; Prunckun, 2019). Defensively, intelligence sharing can be used among allies and coalitions to counter threats from adversaries and produce shared understandings between elites in the intelligence and military domains such as could recently been seen in the efforts to promote NATO (military, diplomatic and economic/financial) unity over Russian intentions in relation to Ukraine (Martin & Myre, 2022) and again as this paper was written about China's (Salama et al., 2023). Finally, influence operations directed at mass publics seek to influence the parameters of political systems by changing the levels of support for a political system, its authorities, or its policy outputs (Jensen, 1923). A large segment of hybrid warfare consists of the integration of offensive and defensive influence operations.

2.1 | Hybrid war and hybrid threats as evolving notions of warfare

Hybrid war and hybrid threats are an evolving and debated notion of warfare that emerged shortly after the end of the Cold War and magnifies the complexities of modern warfare that go beyond conventional military tactics, often involving cyberwarfare, propaganda and a fluid, non-state adversary (Bachmann, 2017). It refers to the 'use of nonconventional methods, such as cyber warfare, as part of a multidomain warfighting approach to disrupt and disable an opponent's actions without engaging in open hostilities' (Bachmann et al., 2019: 41) or in support of kinetic operations as a force multiplier as evidenced in the Russian aggression in Eastern Ukraine since 2014. Hybrid warfare and hybrid threats as 'new' concepts of warfighting and security risk management evolved since 2005 when then General Mattis coined the term at a US Naval Institute conference (Mattis & Hoffman, 2005) and Hoffman's seminal work on the rise of Hybrid Wars in 2007 (Hoffman, 2007). Hoffman using the terms hybrid war and hybrid threats interchangeably was the first to provide an early definition whereas: 'Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid Wars can be conducted by both states and a variety of nonstate actors [with or without state sponsorship]. These multimodal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict' (Hoffman, 2007: 8).

Bachmann and Brig Anthony Paphiti (UK Army, rtd) characterised hybrid warfare (HW) as a combination of warfighting methods distinctly aimed at weakening the adversary along the full DIMEFIL[2] spectrum. Russia's version of HW is commonly perceived as 'the modern application of traditional Soviet political warfare practices, such as active measures, [*maskirovka* in Russian], and disinformation' (DeBenedictis, 2022).[3]

Hybrid warfare is a comprehensive strategic approach, often combining both state and non-state threat actors in a 'broad, complex, adaptive, and often highly integrated combination of conventional and unconventional means' (Paphiti & Bachmann, 2016). It is now commonplace to associate hybrid warfare with 'covert activities, which can include military, paramilitary, irregular and civilian actors' (Paphiti & Bachmann, 2016) orchestrating geopolitical and strategic effects whilst targeting 'an adversary's vulnerabilities' (Paphiti & Bachmann, 2016). Hybrid warfare, at the operational level, aims to 'creating ambiguity and deniability' (Paphiti & Bachmann, 2016). Strategically, hybrid warfare focus on focussed on 'complicating decision-making and conducted across' (Paphiti & Bachmann, 2016) the entire DIMEFIL spectrum.

This definition reinforces NATO's new HW strategy since 2015, which adopts a similar approach *re* threats, actors and conflict domains that reflects on NATO's 2010 BI-SC Input on a new *NATO Capstone Concept*

for the Military Contribution to Countering Hybrid Threats (Bachmann, 2011; NATO ACT, 2010).[4] Briefly, hybrid war is occurring in a grey zone of war and peace: like cyber warfare and cyber operations, there exists a murky conflation of ambiguity, deniability and scarcity of attribution (Bilal, 2021). For these reasons alone, both information operations and influence operations are of particular relevance for any hybrid warfighting approach by both state and non-state actors.

Bachmann and Gunneriusson highlighted in 2017 the initial success of Russia's use of influence operations in support of its hybrid war in Russia implementing its Military Doctrine of 2010 and National Security Strategy of 2015, which combines the Soviet strategy of reflexive control with Russia's own approach to HW, namely non-linear warfare (Bachmann & Gunneriusson, 2017: 9). 'Russia is winning the Hybrid War in Ukraine: it has successfully annexed Crimea, and effectively turned Ukraine into a state on the brink of wider failure' (Bachmann & Gunneriusson, 2017: 9)—circa 2016. The annexation of Crimea—18 March 2014 (Pifer, 2020)—was distinctly grounded in a prolonged information warfare campaign occupying all corners of public media and debate. Furthermore, this complexity through ambiguity enabled Russia to successfully divide 'Western countries on how to respond to this act of aggression. Russia also successfully reactivated its Cold War disinformation mechanisms, successfully blurring reality and fiction for global observers. At that time Russia had uncovered the West's inability to find a common policy to respond to the unfolding events in Ukraine' (Bachmann & Gunneriusson, 2017: 9).

2.2 | Hybrid warfare and influence operations: The real hybrid threat in the Information-Domain

When taking an even more granular view of hybrid warfare the intent thereof can be brought into perspective. One intent of the use of hybrid warfare is the achievement of objectives without engaging in open war as long as the multi-modal warfighting approach stays below the threshold of an 'armed attack' (the prohibited use of force under Article 2 (4) UN Charter). In context, this would refer to conventional military operations, (hence the question about the use of 'warfare' to describe these activities. Such an approach aims to 'disrupt, undermine or damage the target's political system and cohesion through a combination of violence, control, subversion, manipulation and dissemination of (mis)information'. (Nilsson et al., 2021). Hence the characterisation of increasing complexity through ambiguity (Paphiti & Bachmann, 2016). Interestingly, most of these acts are also associated with covert action—operational techniques also associated closely with ambiguity and deniability. As such, political systems can be disrupted by an assassination—which is violence—and associated with covert action but also be an element of a wider hybrid warfare strategy. Waseem Qureshi describes the intent of hybrid warfare as efforts to destabilise the adversary or designated target country without engaging in direct conflict, i.e., conventional military action. The key is to influence or disrupt policy decisions and execution without the negative effects associated with 'attribution or retribution' (Qureshi, 2020: 178). This is obviously where plausible deniability plays a significant role and necessitates the use of covert action methodologies, wherein the operation may eventually be uncovered, whilst the sponsor's identity remains unknown.

Hybrid warfare is intent on providing avenues to states to influence and/or disrupt the mechanisms associated with sovereignty of other states without having to account for their activities to domestic constituencies. Democracies are considerably more vulnerable to issues of public accountability and governance than other forms of political association. Thus, when the economies of nations are affected negatively, and conventional military action is not an option or just too expensive (both economically and diplomatically) they tend to prefer deniable options such as those included in hybrid warfare and typically associated with covert action (or active measures if Russia is the threat actor). This way it also evades the international law requirements associated with the rules of (conventional) war (Dumlupınar & Erol, 2020: 172). 'These hybrid warfare tactics not only enable an aggressor to use nonmilitary forces [non-state actors] against a targeted state without being held accountable in accordance with the rules of international law [such as the Geneva Conventions and their Additional Protocols as the basis of International Humanitarian Law]; they also allow it to destabilise a target without consuming excessive resources or disturbing important diplomatic relations' (Qureshi, 2020: 158). This luxury is typically provided by phenomenon such as covert action, colour revolutions, asymmetric warfare, unconventional warfare, and irregular warfare—all included in the hybrid warfare portfolio. These forms of warfare and action utilise indirect approaches to the objective and thus evade international legal scrutiny and retribution by the target country/regime (Qureshi, 2020: 178). This speaks to the criticality of plausible deniability maintenance.

Wassem Qureshi conceptualises a more broader application of hybrid warfare by including conventional military operations as well as 'irregular tactics (rebellion, insurgency, proxies, and nonstate actors), terrorism (unpredictable violence), criminal activities (such as the smuggling of weapons, drugs and other illicit things, and the use of domestic gangs), political means (diplomacy), economic means (loans, sanctions, and wrecking of an economy), information means (propaganda,

misinformation, leaked information, and other information operations), and social means (domestic population and psychological operations)' (Qureshi, 2020: 178). A complex multi-modal preparation of the battlefield in influence of operations and adversaries during the battle—not losing sight of the advantages required for negotiations after the battle. No theory state that hybrid warfare ends as soon as conventional military capabilities enter the theatre. To the contrary, this only provides another layer of complexity that is very visible and thus mask the covert action activities even more.

Pre-invasion (24 February 2022), Russia seemed to be partly successful with its combination approach of multi-modal, low intensity, kinetic as well as non-kinetic warfare such as the use of information operations as an integral tool in its hybrid war against the people of Ukraine. The Belarussian migration crisis of late 2021 might turn out to be the turning point when the Russian engineered migration crises at the eastern border of both EU and NATO failed in light of the determination of Poland, EU and NATO to protect the borders. The migration crisis was engineered by Russia and Belarus to 'strategically put pressure on the EU and to create discord within the bloc' (Bachmann, 2021) and to force Poland to break international and EU law by returning the migrants to Belarus which qualifying as a violation of the, so-called, non-refoulment principle under international law. This form of Russian lawfare could be seen as the application of reflexive control, compelling the adversary into an action detrimental to its own interests.[5] The 2022- Russo-Ukraine invasion was orchestrated on the foundation led by information operations being used as a 'force multiplier' (Bachmann & Mosquera, 2016: 65). The information domain, and specifically the use of disinformation as an integral part of its warfighting approach were being used by the Russian aggressor to weaken Western resolve to support Ukraine.[6] As such, Russia employs a dual approach to information warfare—as a measure to avoid the necessity of using military force or as a force multiplier once military force is being used. Kofman and Rojansky (2015) formulate the doctrine as a preemptive employment of information warfare techniques and tactics aimed at gaining political (also diplomatic) leverage without having to apply the more visible and expensive conventional military force options available. Once opinions have been shaped and political ambiguity created the more subtle hybrid warfare techniques can be blended with the application of conventional military force (Kofman & Rojansky, 2015).

Bachmann and Munoz highlighted this nexus inherent in hybrid warfare already in 2016, whereas some of the non-kinetic aspects of hybrid warfare share methods with 'influence operations' by aiming to misinform world opinion (like Russia's aggression first in Crimea and later in Syria) or become a powerful 'force multiplier' (like Jihadists and Daesh in the Middle East) (Bachmann & Mosquera, 2016). These methods have a long history of successful employment. As Sun Tzu stated: '[t]o subdue the enemy without fighting is the supreme excellence' (Bachmann & Mosquera, 2016). So, the ultimate intent is not just to influence, disrupt and halt adversarial actions short of engaging in war (Weissmann et al., 2021), but also to avoid the restrictions of international rules governing war and the associated negative political and economic costs associated with conventional war. Bachmann and Mosquera (2018: 61) furthermore contend that hybrid warfare also has the potential to change future conceptualisations of war and its legal paradigms. Thus, when uncertain if an attack has taken place, decisions about response options are delayed or not taken at all—allowing the hybrid threat actor to gradually dominate all aspects of his adversary's decision-action cycle (OODA loop). Putter (2019) superimposed the OODA loop onto a dynamic continuum within the context of knowledge management (depicted in Figure 1). Putter (2019) contends that '[t]his decision-making cycle is dependent on both information and knowledge (e.g., intelligence)—but probably optimised best with a complete and real or near real-time intelligence picture' (Putter, 2019: 6–50). Considering the conceptualisation of the OODA loop and the relevance of information/intelligence (or knowledge) as depicted in Figure 1 where data and information tend to support observation and orientation and when processed into knowledge (or intelligence) supports decisions and actions—the use of information warfare can quickly deplete the advantage locked up in near real-time information as well as intelligence by continuously creating complexity in all areas at a granular level resulting in a uncontrollable OODA loop and information disorder.

Ahmed, Bachmann, Ullah, and Barnett (2022: 129) contend (based on their findings from case studies, preliminary and workshop reports) that stronger focus should be on the very nature of the emerging trends of warfare, particularly in the view of great power competition. Hybrid threats often amount to grey zone operations, taking place in the non-military domain of state-on-state competition, but is not limited to state actors alone. Below the threshold of armed conflict (and multi-modal in nature) they require additional efforts from Australia and its allies to counter such threats. Recognition and attribution as part of awareness capabilities followed by rapid assessment and decision making in preparation of an effective response are key elements of future resilience. With the focus of research on false information attacks in cyber space, further studies are needed in the researching of different remedies to identify and combat the spread of false information its effect on own and allied OODA loops and

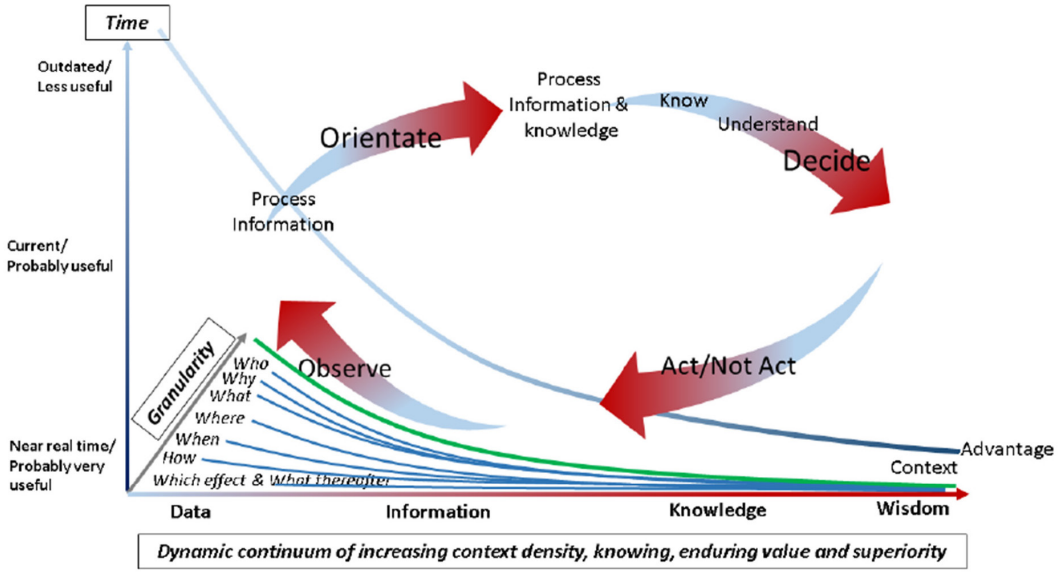

FIGURE 1 Information- and knowledge-based OODA loop superimposed on a three axis time-granularity-knowledge continuum graphic (Figure 6.4b in Putter, 2019: 6–50).

advantage in the battle space, with the added difficulty that technology that is to be used to detect such information must be improved vastly (Ahmed, Bachmann, Martin, et al., 2022: 105).

As NATO stipulates in its own approach as response to Hybrid War/Threats resilience three steps are paramount for countering such risks and threats respectively: prepare—deter—defend. Australia as a NATO Enhanced Opportunities Partner must work towards developing a whole of government ability to support vigilance and continued analysis required to respond efficiently to such emerging and identified threats in the information domain.

3 | DISINFORMATION WITHIN THE CONTEXT OF HYBRID WARFARE AND HYBRID THREAT

Hybrid warfare and the employment of disinformation, as a specific strategy or tactic, share the same conceptual space of Sun Tzu's axiom—'The greatest victory is that which requires no battle'.[7] This is why HW, and its associated threats stalk the grey zone—preparing the battlespace for future conventional warfare options.

The construct or term 'disinformation' is claimed to be the brainchild of Joseph Stalin according to Jeremy Norman's Historyofinformation.com.[8] Yet, when diving into the depths of the internet you find that the term was used as far back as 1892 in The Salt Lake Herald (Salt Lake City, Utah), (18 Aug 1892, p. 4)[9] the following clipping appeared using the term 'disinformation' (see Figure 2).

It would thus seem that disinformation as a tactic is characterised by its longevity. Without exploring the entire history of the construct, staying focussed on the aim of this article, the modern-day utilisation of disinformation within the context of hybrid warfare is fast approaching an art and science.

Before proceeding into the deployment of disinformation in the Russo-Ukraine war (2022) some closely related constructs must be clarified. Constructs such as information warfare, misinformation, disinformation, fake news and deception are more than often loosely used to describe manipulative cognitive activity within the hybrid warfare space. A UNESCO perspective[11] on these constructs differentiate between them as follows—'… misinformation is information that is false, but the person who is disseminating it believes that it is true. Disinformation is information that is false, and the person who is disseminating it knows it is false. It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors. A third category could be termed mal-information; information, that is based on reality, but used to inflict harm on a person, organisation or country' (Ireton & Posetti, 2018: 45–46). These are plotted on an 'Information Disorder' Ven diagram (Figure 3).

The UNESCO document propose an overlap between mis- and mal-information that form the outer limits of the 'information order'. This Venn-diagram propose an overlap—termed disinformation. Just like hybrid warfare and its associated threats exploit the space between peace and war, so does disinformation between mis- and mal-information. A Canadian perspective on disinformation categorise the construct as a deliberate distribution of 'false information' (Global Affairs Canada, 2022). The NATO definition for deception is the 'deliberate measures to mislead targeted decision-makers into behaving in a manner

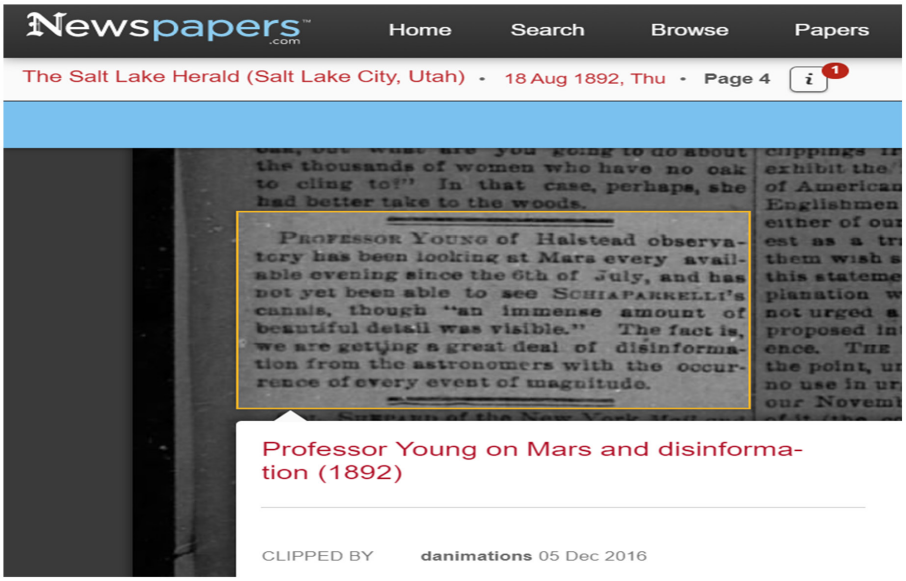

FIGURE 2 Newspaper clipping from The Salt Lake Herald (Salt Lake City, Utah), 18 August 1892, p. 4 from Newspapers.com (5 December 2016).[10]

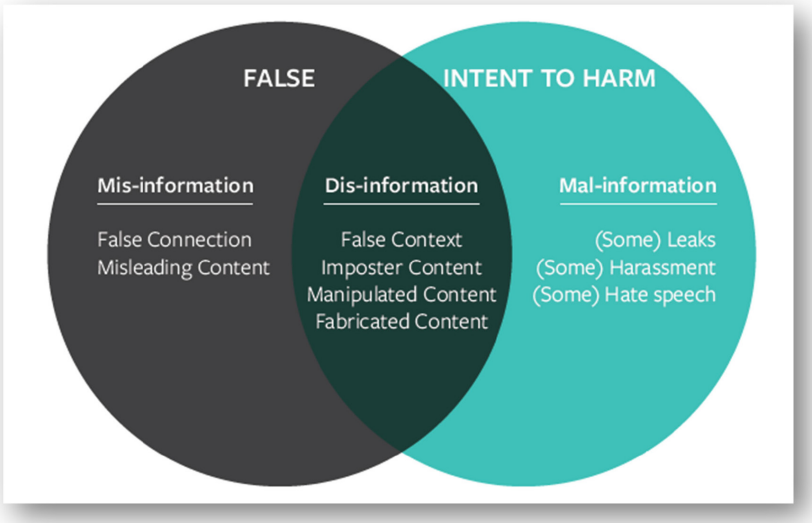

FIGURE 3 'Information Disorder' from Ireton & Posetti (2018: 46).

advantageous to the commander's intent' (NATO, n.d.). This definition places deception very close to disinformation as a construct. Deception is typically from the counterintelligence playbook to create a 'paradox of fiction' (Prunckun, 2019: 45) in which security agencies leverage what could be believed to be factual in order to gain decision advantage. (Prunckun, 2019) William Daugherty write that deception is closely related to propaganda and consists of activities that aim to confront a specific decision maker with a false reality or to 'mislead an enemy by manipulating, distorting, or falsifying evidence to induce a mistaken perception' (Daugherty, 2006: 79). Propaganda as a tool for hybrid warfare targets anybody willing to listen and not necessarily combatants (Nilsson et al., 2021: 1). This indiscriminate tool of subversion is enabled by cyber technologies to gain and sustain global reach within the rubric of information warfare. Global reach is important from a propaganda perspective due to the globalisation driven expanded expatriate and diaspora communities and their opinions and funding. Propaganda, deception and disinformation all are aimed at creating an alternate reality aligned with pre-conceived strategies to obtain advantage. Propaganda, from a covert action perspective, is the 'systematic dissemination of specific doctrines, viewpoints, or messages to a chosen audience' (Daugherty, 2006: 72). A hybrid warfare perspective on propaganda highlight the information collected

by means of espionage which is disseminated with 'information operations using domestic and international media channels and social media outlets, to shape the political discourse or to form the popular narrative of a society' (Qureshi, 2020: 176). A Russian perspective on disinformation, propaganda and active measures[12] (Darczewska & Żochowski, 2017: 12–13) are that the techniques employed by active measures utilise 'both word (disinformation and propaganda) and deed (subversion, provocation, protest actions, paramilitary actions, etc.)' (Darczewska & Żochowski, 2017: 10). As such, an oscillation between the three constructs in the Venn-diagram (Figure 3) will keep the data-knowledge continuum (Figure 1) significantly disorganised and thus leverageable to impact control over the OODA loop. Information disorder is thus an important concept within the context of hybrid warfare.

These constructs are probably used indiscriminately by the media to depict the illicit use of information to gain advantage. How is this different from information warfare? It is not, albeit as part of the information warfare portfolio of non-kinetic measures to impact the ordered dissemination of information. Information warfare techniques is also now a common tool used and mostly directed at the opponent (Gentry, 2016: 468–469). William Daugherty is of the opinion that 'The ability to clandestinely access data in computers to destroy or modify it, or even to destroy the hardware itself, is generically referred to as "information warfare", providing new operational vistas for the imaginative intelligence or counterintelligence professional' (Daugherty, 2006: 72). This would place disinformation activities within the 'modify' component of information warfare and thus make it a subset of information warfare, which itself form part of the covert action portfolio of activities richly exploited for the purposes of hybrid warfare.

John Gentry summarises covert action as a complex endeavour usually undertaken to effect change through tactics and techniques designed to influence rather than kinetically induced change. As such the 'attitudes, policies, political alignments and/or behavior' of states are targeted. This falls squarely within the manoeuvre of disinformation. Covert action, regarded as a bouquet of tactics and techniques arranged and applied to undermine the sovereignty of states, employ information warfare techniques such as disinformation campaigns. From the analysis done by Gentry, it would seem that, covert action still remains a last resort option, even for states that have considerable portfolios of foreign-based interests. However, in the case of information warfare and in particular disinformation campaigns, they seem to be the non-kinetic first choice to prepare the battlefield. Ukraine is a perfect case study in support of this thesis.

The objective of disinformation campaigns, whether they are perpetrated by state- or non-state actors, is to 'gain support for their policies and suppress criticism in their own countries and around the world; to profit from creating engaging, yet false or misleading content; or to spread their own ideology or beliefs among the public' (Global Affairs Canada, 2022). This was actively and systematically done by the Russian government since 2014 after the first invasion of Ukraine by Russia ending with the annexation of the Crimean peninsula and the installation of separatist regimes in the Donetsk and Luhansk regions of eastern Ukraine (Global Conflict Tracker, 2022).

The Russian information warfare campaign has been active against Ukraine since 2014 (Snegovaya, 2015), actively employing, among other techniques and tactics, cyberwarfare against Ukrainian targets, in preparing the future battlefield. These cyber-attacks, directed against critical infrastructure such as energy production capabilities, utility companies, government information systems and web platforms persisted till February 2022 (Snegovaya, 2015) and beyond. The more focussed motives for the 2022 Russian invasion of Ukraine were delivered with disinformation. It could be argued that the 2014 invasion of Ukraine was the pretext for a strategic campaign aimed at the disintegration of Ukraine which would provide overwhelming context, that could be manipulated with selective readings from history and current developments such as the alleged 'Nazification' of the Ukrainian state and its organs, to prepare the pre-2022 Russian aggression in the Donbas and now Russian invasion of Ukraine. This Russian disinformation campaign was strategically used to create moral ambiguity internationally with its distinct coupling to the Second World War Nazi dogma. The next section discusses the disinformation campaign fielded by Russia before and during the weeks after the kinetic invasion of Ukraine 24 February 2022 (Snegovaya, 2015).

4 | FROM THEORY TO APPLICATION: RUSSO–UKRAINIAN WAR OF 2022

Through the Cold War period Russia employed active measures such as disinformation to discredit western state and non-state actors (Darczewska & Żochowski, 2017: 14–15). Disinformation has been institutionalised in the Russian intelligence services since at least 1959 with the establishment of Department D within the 1st Main Directory (KGB) (Darczewska & Żochowski, 2017: 17). This structure has evolved over time and more so with the proliferation of cyber-related techniques and technologies. According to Anatoli Golitsyn (ex-KGB) the primary strategic thrust of Russian (Cold War era) disinformation (and the rest of the active measures portfolio) was to 'push the US out of Europe, to push the West out of Asia, Africa and South America, and to conceal the Soviet Union's own expansion' (Darczewska & Żochowski, 2017: 21). The success of this strategy is evident in the reduced size of the current Russian Federation and the reduction in influence, in

for example Africa—slowly being supplanted by China. These activities have systematically been simplified by the ubiquitous nature of information technology combined with the cyber domain. Technology also drives the increased sophistication of disinformation campaigns.

Probably the apex of Russian disinformation strategy and techniques was on display during the preparation phase for the second invasion of Ukraine during 2022. It could be argued that this campaign commenced after the 2014 invasion of Ukraine. The extent of this disinformation campaign is of such a magnitude that the US Department of State commissioned a webpage dedicated to expose the disinformation being peddled internationally by Russia (Office of the Spokesperson United Stated Department of State, 2022). At least 60 years of doctrine, tactics and technique enabled by some 20 years of continuously evolving cyber technology and techniques development came to bear on shaping the unfolding hybrid warfare as a 'special operation' (Gerdo, 2022) by Russia in February 2022. The extract from the TASS webpage on 6 March 2022 epitomise the main thrust of the Russian invasion (see Figure 4).

The Russian disinformation campaign can be tracked along various scaffolding themes in order to create 'information disorder' and to influence the international community to the point of apathy. One such theme that targeted international media was the alleged prevalence of Ukrainian neo-Nazi (Kozhurin, 2022) –possibly genocidal–tendencies against pro-Russian separatist communities in the Donbas (Eastern Ukraine). This was/is based on the culture and activity of the Azov Battalion which gained notoriety for their supra-nationalist stance. (Kozhurin, 2022) 'Most of the attention has long focused on right-wing militias and paramilitaries that have fought alongside or as part of Ukraine's armed forces—a phenomenon dating back to the start of the conflict in the Donbas in 2014' (Kozhurin, 2022). Thus, the disinformation narrative about Ukraine neo-Nazi regime started during the first invasion of Ukraine in 2014 (annexation of Crimea and war in the Donbas) and forms the basis for 'justifications' by the Russian government that the current aggression and invasion was legitimate. 'Vladimir Putin justifies his war of aggression with the "denazification" of Ukraine' (Schmid, 2022) was the headline of a *Der Spiegel* report. The US Department of State describes the disinformation theme as the Russian imperative to defend the ethnic Russians residing in Ukraine–typically those in the Donbas (Office of the Spokesperson United Stated Department of State, 2022). At the same time, the Russian Federation is known for having several neo-Nazi and white supremist groups–for example Rusich, Russian Imperial Movement and Legion (US designated terrorist group) and Wagner Group–- currently fighting in Ukraine 'in conjunction with Russia's regular armed forces or allied separatist units' as well as credibly associated with atrocities in Ukraine and Syria (Kozhurin, 2022). Dmitry Kozhurin finds that the Russian government has for an extended period focussed on the Azov group and other supra-nationalists to support their propaganda and disinformation 'often distorting or exaggerating their views and actions in support of the false assertion that Ukraine is controlled or dominated by neo-Nazis' (Kozhurin, 2022). 'Disinformation is a major threat to democracy. It makes it more difficult to access timely, relevant, and accurate information. Democracies rely on access to diverse and reliable sources of news and information. This allows members of society to form opinions, hold governments to account and take part in public debate. Disinformation undermines peace, prosperity and individual freedoms. It erodes trust in democracy. In times of crisis, disinformation can be harmful' (Global Affairs Canada, 2022). The Russian disinformation campaign against the nature of Ukraine government and society at large is a perfect example of this policy statement by Canada. Leon Aron positions that it is important to take complete cognisance of the

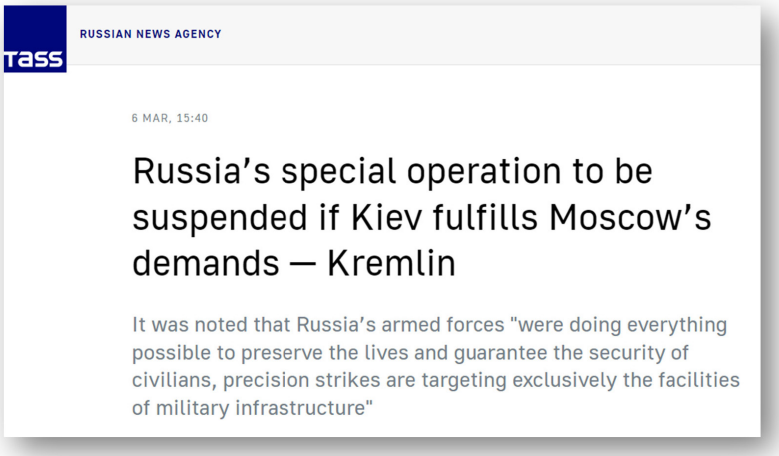

FIGURE 4 News report by TASS (Russian News Agency) (Gerdo, 2022).

fact that 'a democratic, politically stable, economically vibrant, and Western-oriented Ukraine is an existential threat to Putin's stagnant militarised dictatorship'. That threat is firmly anchored in the fact that Russian citizenry will quickly find themselves doing introspection about the fact that there does not seem to be an end to their impoverished existence—yet, to the southwest Ukraine citizens is increasingly and in a sustained manner establishing economic freedom on an individual and national scale (Aron, 2022) This is also the motivation for the Russian domestic disinformation campaign.

Another theme building on the scaffolding of fake news, propaganda, deception, and other disinformation tactical tools is the legitimacy of the Russian invasion. Here the Russian government used ancient history to spin the narrative of an once powerful (pan-) Russian Empire that was fragmented over time by Western powers and that Ukraine (as a former part of sucha pan-Russian historical empire) is now in the hands of neo-Nazi elements that seek to join NATO as part of a phased campaign to destroy Russia. In a policy statement by the Canadian government, it is claimed that the Russian government has for extended periods of time 'conducted a disinformation campaign against Ukraine by using state media and proxies' (Global Affairs Canada, 2022) to establish legitimacy for the unprovoked and illegitimate invasion of Ukraine for the second time. This disinformation campaign extends back to the illegal Crimea annexation in 2014. The disinformation campaign aims at the creation of 'information disorder', driving a wedge between Ukraine and allied partner nations and thus seeking to undermine their future support, and endeavouring support-base expansion for Russian nationalism and imperialism (Global Affairs Canada, 2022). The US government categorise these activities as 'information confrontation' and include measures such as disinformation and propaganda in a concerted effort to create a Ukraine aggressor paradox of fiction within the context of Russo-Ukraine relations (Office of the Spokesperson United States Department of State, 2022). The intention of this theme of disinformation is to sway the West that Ukraine supra-nationalism and courting of a NATO membership are the catalyst for a world war (Office of the Spokesperson United States Department of State, 2022).

Off course, Ukraine's interest in joining NATO is another key theme that is used within disinformation campaigns aimed at keeping the Russian public afraid of an impending invasion by NATO. The US Department of State capture this theme, that is the undertone in most of the other disinformation themes, as the belief that there has been a strategic, dedicated and sustained effort by NATO to dismember Russia by systematically encircling the country—by offering Ukraine membership of NATO is another (and may be final) breach of the 'neutrality' of Ukraine and as a buffer between NATO and Russia (Office of the Spokesperson United Stated Department of State, 2022). Petros Giannakouris captures this anxiety with the following statement—'The Ukrainians' supposed lack of neutrality — that is, their repudiation of pro-Moscow rulers and their tilt toward the West — was the Russian president's excuse for invading' (Aron, 2022).

A theme that impacts the Russian public is the use of disinformation to keep the Russian citizenry ill-informed about the 'successes and nature of the Russian so-called 'special operation' as a legitimate attempt to re-unify the Russian Empire. This is attempted with the control of Russian media and suppression of foreign media and social media platforms available within Russia (Global Affairs Canada, 2022). Disinformation is disseminated through official Russian government communiqués disseminated as required to 'state-funded media outlets, such as RT and Sputnik, and social media platforms […,] propaganda and disinformation channels'—typically the Telegram chat application—as well as funded programmes to influence foreign media and 'think tanks' (Global Affairs Canada, 2022).

5 | CONCLUSION—THE NEED FOR AN INTEGRATED AND COMPREHENSIVE COUNTER—APPROACH

The nature of these disinformation threats associated with influence operations, within the context of hybrid warfare, requires the adoption of a comprehensive, multi-modal, multi-stakeholder approach adding civilian actors to a whole of government approach. Such a government-plus strategy combines a governmental inter-agency approach (at both federal and state level) with key civilian stakeholders and Small and Medium Enterprises (SMEs) from cyber-intelligence, social media as well as subject matter relevant private actors from defence industries, academia, think tanks to list just some. To draw on the dividends of a comprehensive approach, successful integration is a distinct and non-negotiable requirement.

NATO's 2011 Countering the Hybrid Threat Experiment in Tallinn (2011) tested the viability of the Bi-SC Capstone Concept of Hybrid Threats (2000) not only via a MCCHT (NATO Military Contribution to Countering Hybrid Threats) approach but also a civilian outlook involving 70 civilian SMEs from academia, big pharma, cyber, major international resource multinational enterprises to formulate the essential need of formulating a comprehensive approach to counter Hybrid Threats. This approach would also be fitting for a potential Australian approach re grey zone as the so-called Hybrid Threat spectrum is mostly non kinetic and/or below the threshold and hence part of most of the grey zone threats, operations respectively. NATO worked on defining a global approach (Comprehensive Approach) in order to counter these risks. This approach envisaged involving state and non-state actors

in a comprehensive defence strategy that combines political, diplomatic, economic, military technical and scientific initiatives (Paphiti & Bachmann, 2016).

By taking a holistic approach to warfare in the grey zone as well as in the hybrid threat domain, including elements of cyber enhanced lawfare, a discussion of a resilience model (doctrinal and institutional) is a robust first step. Such must encompass a comprehensive strategy to work towards the identification, analysis, mitigation of risks and prevention of information-operation threats (in the context of information dynamics and messaging). A comprehensive strategy, to counter the effect of disinformation campaign, should aim at stopping the escalation or dissemination of hybrid threats.

Overall, influence operations with the context of 'information disorder' is not something that has an easy fix or will disappear anytime in the future. On the contrary, these operations will continuously evolve to elevated levels of sophistication that will require equal and greater sophistication and integration among all available national and international capabilities if the West and its allies are targeting resilience 2.0. Working on awareness leads to resilience. Such awareness is a distinct product of control over the OODA loop activities. From a technical perspective, new datasets must be created to be used with currently available solutions, allowing them to expand and become more effective moving forward (Paphiti & Bachmann, 2016). Australia post AUKUS agreement must utilise available private sector expertise to establish trustworthy partnership-networks as part of a comprehensive Australian approach. This should be complementary to the interagency model of a whole-of-government approach to counter the negative effects of information disorder. Israel, with its military capital approach regarding the military technology sector, can be seen as a good case study for creating a potential symbiosis between the state/civic divide (Ahmed, Bachmann, Ullah, & Barnett, 2022).

Further measures could include the adoption of new initiatives in academia and continuing adult education which would include public education and training programs. The introduction of a national influence operations—political warfare course as part of the curriculum of security focused tertiary institutions should be considered following similar US discussions.

Finally, but actually as *essentialia*—Australia requires an interagency coordination through a dedicated central coordination authority which, like a Joint Operations Centre, concentrates various expertise and capability point of contacts. Such coordination could usher in the next phase after the 'awareness', recognition, and attribution phases, namely resilience, based on counteroperations in the information domain. Australia's rather successful counter-COVID-disinformation comes here to mind as an example for such resilience as an objective. Rapid responses are absolutely critical when countering influence operations once detected. Only a dedicated coordinating central authority approach can ensure a timely and successfully targeted counter information warfare approach.

ACKNOWLEDGEMENTS

No funding was received. Open access publishing facilitated by University of Canberra, as part of the Wiley - University of Canberra agreement via the Council of Australian University Librarians.

CONFLICT OF INTEREST STATEMENT

No potential conflict of interest was reported by the author(s).

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Sascha-Dominik Dov Bachmann https://orcid.org/0000-0002-8742-0766

ENDNOTES

[1] Also, these operations may also simultaneously target both elite actors and mass publics. See, for example the discussion of Operation Neptune by Bittman (1972).

[2] Diplomatic, Information, Military, Economic, Finance, Intelligence and Law Enforcement.

[3] General David Petraeus, US Army (rtd.), former commander of the Surge in Iraq, US Central Command, and Coalition Forces in Afghanistan and former director of the CIA in DeBenedictis (2022).

[4] Remote Control Project: Interview: Sascha Dov Bachmann: Hybrid Warfare, 12 July 2017 and NATO ACT, BI-SC Input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats.

[5] On the subject of weaponization of migration, see Bachmann and Paphiti (2021).

[6] For a discussion of the Russian approach during the first phase of its aggression against Ukraine in 2014 and 2015 see Bachmann & Gunneriusson (2015 & 2017).

[7] Sun Tzu (The Art of War) in Nilsson et al. (2021: 1).

[8] "Joseph Stalin Coins the Term Desinformatsiya (Disinformation) 1923." *Jeremy Norman's History of Information*. Accessed 16 June 2022. https://www.historyofinformation.com/detail.php?id=5069.

[9] "Daminatons (2016, December 5). The Salt Lake Herald (Salt Lake City, Utah), 18 Aug 1892, p. 4 (Clipping)." Newspapers.com.

[10] Ibid.

[11] Ireton & Posetti (2018). *Journalism, Fake News & Disinformation: Handbook for Journalism Education and Training*. UNESCO Publishing, 2018.

[12] The Russian term for covert action.

REFERENCES

Ahmed, M., Bachmann, S.-D., Martin, C., Walker, T., van Rooyen, J. & Barkat, A. (2022) False information as a threat to modern society: a systematic review of false information, its impact on

society, and current remedies. *Journal of Information Warfare*, 21(2), 105–120.
Ahmed, M., Bachmann, S.-D., Ullah, A.B. & Barnett, S. (2022) Ransomware 2.0: an emerging threat to national security. *Australian Journal of Defence and Strategic Studies*, 4(1), 125–132.
Aron, L. (2022) A neutral Ukraine is a dangerous idea. *The Atlantic*. Available from: https://www.theatlantic.com/ideas/archive/2022/04/ukraine-neutrality-peace-agreement-finland/629473/ [Accessed 12 June 2022]
Bachmann, S.-D. (2011) Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management. *Amicus Curiae*, 88, 24.
Bachmann, S.-D. (2017) 'Remote control interviews Prof Sascha-Dov Bachmann' [video]. Twitter. *Hybrid Warfare*. Available from: http://remotecontrolproject.org/interview-sascha-dov-bachmann [Accessed 16 June 2022]
Bachmann, S.-D. (2021) Is the Belarus migrant crisis a new 'type of war'. *The Conversation*. Available from: https://theconversation.com/is-the-belarus-migrant-crisis-a-new-type-of-war-a-conflict-expert-explains-171,739 [Accessed 16 June 2022]
Bachmann, S.-D., Dowse, A. & Gunneriusson, H. (2019) Competition short of war – how Russia's hybrid and gray-zone warfare are a blueprint for China's global power ambitions. *Australian Journal of Defence and Strategic Studies*, 1(1), 41–56.
Bachmann, S.-D. & Gunneriusson, H. (2015) Russia's hybrid warfare in the east: the integral nature of the information sphere. *Georgetown Journal of International Affairs*, 16, 198–211.
Bachmann, S.-D. & Gunneriusson, H. (2017) Western denial and Russian control: how Russia's national security strategy threatens a western based approach to global security, the rule of law and globalization. *Polish Political Science Yearbook*, 46(1), 9–29. Available from: https://doi.org/10.15804/ppsy2017101
Bachmann, S.-D. & Mosquera, A.B.M. (2016) Lawfare in hybrid wars: the 21st century warfare. *Journal of International Humanitarian Legal Studies*, 7, 63–87. Available from: https://doi.org/10.1163/18781527-00701008
Bachmann, S.-D. & Mosquera, A.B.M. (2018) Hybrid warfare as lawfare: towards a comprehensive legal approach. In: Cusumano, E. & Corbe, M. (Eds.) *A civil – military response to hybrid threats*. Palgrave Macmillan/Springer Nature: Cham, pp. 61–76.
Bachmann, S.-D. & Paphiti, A. (2021) Mass migration as a hybrid threat? – a legal perspective. *Polish Political Science Yearbook*, 50(1), 119–145.
Bilal, A. (2021) Hybrid warfare – new threats, complexity, and trust as the antidote. *NATO Review*. Available from: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html [Accessed 16 June 2022]
Bittman, L. (1972) *The deception game: Czechoslovak intelligence in soviet political warfare*. Syracuse: Syracuse University Research Corporation.
Daminatons. (2016) The Salt Lake Herald (Salt Lake City, Utah), 18 August 1892, p. 4 (Clipping). [online] *Newspapers.com*, 5 December. Available from: https://www.newspapers.com/image/?clipping_id=7,729,235&fcfToken=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJmcmVlLXZpZXctaWQiOjgwODMyMjcxLCJpYXQiOjE2NTUzODY1NDYsImV4cCI6MTY1NTQ3Mjk0Nn0.7kId2KTmEN3_5yGYQdQm5dYDF0ZtNVQ7aybBBCaOdvQ [Accessed 16 June 2022]
Darczewska, J. & Żochowski, P. (2017) Asctive measures. Russia's key export. Ośrodek Studiów Wschodnich. *Point of View*, 64.
Daugherty, W.J. (2006) *Executive secrets: covert action and the presidency*. Lexington: University Press of Kentucky.
DeBenedictis, K. (2022) *Russian 'hybrid warfare' and the annexation of crimea: the modern application of soviet political warfare*. London: Bloomsbury Publishing (I.B. Taurus).
Dumlupınar, N. & Erol, M.S. (2020) The final state of war: hybrid war. *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, 4(2), 156–158.
Gentry, J.A. (2016) Toward a theory of non-state actors' intelligence. *Intelligence and National Security*, 31(4), 465–489. Available from: https://doi.org/10.1080/02684527.2015.1062320
Gerdo, V. (2022) Russia's special operation to Be suspended if Kiev fulfills Moscow's demands — kremlin. *Tass.com*. Available from: https://tass.com/politics/1417839?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referer=google.com [Accessed 16 June 2022]
Global Affairs Canada. (2022) *Canada's efforts to counter disinformation – Russian invasion of Ukraine*. Ottawa: Government of Canada. Available from: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng [Accessed 16 June 2022]
Global Conflict Tracker. (2022) Center for Preventive Action – conflict in Ukraine. *Council on Foreign Relations*. Available from: https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine [Accessed 16 June 2022].
Hoffman, F.G. (2007) *Conflict in the 21st century: the rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies.
Ireton, C. & Posetti, J. (2018) *Journalism, fake news & disinformation: handbook for journalism education and training*. Paris: UNESCO Publishing.
Jensen, M. (1923) *ORNET Prelim Report (embargoed Department of Defence, Canberra, Australia). Joseph Stalin Coins the Term Desinformatsiya (Disinformation) 1923*. Canberra: Jeremy Norman's History of Information. Available from: https://www.historyofinformation.com/detail.php?id=5069 [Accessed 16 June 2022]
Kofman, M. & Rojansky, M. (2015) A closer look at Russia's "hybrid war". *Kennan Cable 7*. Available from: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf [Accessed 14 June 2022]
Kozhurin, D. (2022) Who are the neo-Nazis fighting for Russia in Ukraine? *RadioFreeEurope/RadioLiberty*. Available from: https://www.rferl.org/a/russian-neo-nazis-fighting-ukraine/31871760.html [Accessed 17 June 2022]
Martin, D.C. (2018) *Wilderness of mirrors: intrigue, deception, and the secrets that destroyed two of the cold War's Most important agents*. NY: Skyhorce Publishing.
Martin, R. & Myre, G. (2022) U.S. intelligence didn't stop the invasion of Ukraine, but it had positive effects, *NPR.org*. Available from: https://www.npr.org/2022/02/25/1083003294/u-s-intelligence-didnt-stop-the-invasion-of-ukraine-but-it-had-positive-effects [Accessed 10 June 2022]
Mattis, J. & Hoffman, F.G. (2005) *Future warfare: the rise of hybrid wars*. Annapolis, MD: U.S. Naval Institute. Proceedings 131. Available from: https://www.proquest.com/docview/205977465/8D40573AC45D4F3FPQ/6?accountid=28889 [Accessed 20 June 2022]
Nato. (n.d.) *NATO Term – the Official NATO Terminology Database [online]*. Available from: https://nso.nato.int/natoterm/Web.mvc [Accessed 20 June 2022]
NATO ACT. (2010) *BISC input to a new NATO capstone concept for the military. Countering hybrid threats, 7*. Available from: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf [Accessed 16th June 2022].
Nilsson, N., Weissmann, M., Palmertz, B., Thunholm, P. & Häggström, H. (2021) Security challenges in the gray zone: hybrid threats and hybrid warfare. In: Weissmann, M., Nilsson, N., Palmertz, B. & Thunholm, P. (Eds.) *Hybrid warfare: security and asymmetric conflict in international relations*. London: I.B. Tauris, pp. 1–18. Available from: https://doi.org/10.5040/9781788317795.0025

Office of the Spokesperson United States Department of State. (2022) *Fact vs. fiction: Russian disinformation on Ukraine*. Washington, D.C.: United States Department of State. Available from: https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/ [Accessed 16 June 2022]

Paphiti, A. & Bachmann, S.-D. (2016) *Written evidence submitted by Brigadier (rtd) Anthony Paphiti, former ALS officer and Dr Sascha Dov Bachmann*. London: Associate Professor in International Law, UK Parliament, Defence Select Committee. Available from: https://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/russia-implications-for-uk-defence-and-security/written/28402.pdf [Accessed 20 June 2022]

Pifer, S. (2020) Crimea: Six Year after Illegal Annexation. *Brookings*. Available from: https://www.brookings.edu/articles/crimea-six-years-after-illegal-annexation/ [Accessed 15 July 2023]

Prunckun, H. (2019) *Counterintelligence theory and practice*. Lanham: Rowman & Littlefield.

Putter, A.P. (2019) *Knowledge management for the South African Department of Defence*. Unpublished PhD thesis. Department of Strategic Studies, Stellenbosch University.

Qureshi, W.A. (2020) The rise of hybrid warfare. *Notre Dame Journal of International & Comparative Law*, 10(2), 173–205.

Salama, V., Mauldin, W. & Youssef, N.A. (2023) U.S. considers release of intelligence on China's potential arms transfer to Russia. *The Wall Street* Journal Available from: https://www.wsj.com/articles/u-s-considers-release-of-intelligence-on-chinas-potential-arms-transfer-to-russia-8e353933 [Accessed 22 June 2022]

Schmid, F. (2022) Intelligence report: numerous neo-nazis are fighting for Russia in Ukraine. *Der Spiegel*. Available from: https://www.spiegel.de/politik/deutschland/ukraine-krieg-organisierte-neonazi-gruppen-kaempfen-fuer-russland-geheimdienstbericht-a-f1632333-6801-47b3-99b9-650d85a51a52 [Accessed 11 June 2022]

Snegovaya, M. (2015) *Russia report 1 Putin's information warfare in Ukraine – soviet origins of Russia's hybrid warfare*. Washington, D.C.: Institute for the Study of War. Available from: https://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare [Accessed 16 June 2022]

Weissmann, M., Nilsson, N. & Palmertz, B. (2021) Moving out of the blizzard: towards a comprehensive approach to hybrid threats and hybrid warfare. In: Weissmann, M., Nilsson, N., Palmertz, B. & Thunholm, P. (Eds.) *Hybrid warfare: security and asymmetric conflict in international relations*. London: I.B. Tauris, pp. 263–272. Available from: https://doi.org/10.5040/9781788317795.0025

AUTHOR BIOGRAPHIES

Professor **Sascha-Dominik Dov Bachmann**, LLM, LLD, FHEA, is a Professor in Law and Security at the University of Canberra and co-convenor of the National Security Hub. He is also an extraordinary Reader in War Studies at the Swedish Defence University and a Research Fellow SIGLA, Stellenbosch University. He is a regular contributor to NATO's Legal Advisor Web (LAWFAS) and a Fellow of NATO SHAPE - ACO Office of Legal Affairs for the Asia Pacific (Hybrid Threats and Lawfare) working on Influence operations, Grey-zone, Hybrid Warfare, Great Power competition, European Australian and Asia Pacific Security. He has been a regular visiting academic at ADF's Directorate of Joint Influence Operations and across the ADF.

Dries Putter holds a Stellenbosch University PhD in Military Science. He is a Captain in the SA Navy, a senior lecturer in Strategic Studies (Intelligence Studies), and a researcher for SIGLA, Stellenbosch University. He is an affiliated member of the National Security Hub and the University of Canberra.

Dr. **Guy Duczynski** is a national security professional with over 40 years of service with Special Operations, including two operational tours in the counter-terrorism unit of the Australian Special Air Service (SAS) and a deployment to Afghanistan. He has served in numerous appointments associated with operations, plans, training, capability development and operational analysis branches before retiring from military service in 2018. In addition to a doctorate, he holds a master's degree in Business Administration and a master's degree in Education. He continues research in influence activities, operational design, campaign planning, faction liaison, information operations, capability development, and special operations, and lectures regularly to strategic and operational-level planners. His current appointment is Adjunct Senior Lecturer at Edith Cowan University.

How to cite this article: Dov Bachmann, S.-D., Putter, D. & Duczynski, G. (2023) Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*, 14, 858–869. Available from: https://doi.org/10.1111/1758-5899.13257