Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence op…

Article *in* Defense and Security Analysis · March 2024

DOI: 10.1080/14751798.2024.2321736

CITATIONS
11

READS
1,548

5 authors, including:

Lance Y. Hunter
Augusta University
48 PUBLICATIONS **236** CITATIONS
SEE PROFILE

Craig Albert
Augusta University
35 PUBLICATIONS **163** CITATIONS
SEE PROFILE

Joshua Rutland
Augusta University
11 PUBLICATIONS **115** CITATIONS
SEE PROFILE

Defense & Security Analysis

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/cdan20

Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations

Lance Y. Hunter, Craig D. Albert, Josh Rutland, Kristen Topping & Christopher Hennigan

To cite this article: Lance Y. Hunter, Craig D. Albert, Josh Rutland, Kristen Topping & Christopher Hennigan (05 Mar 2024): Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations, Defense & Security Analysis, DOI: 10.1080/14751798.2024.2321736

To link to this article: https://doi.org/10.1080/14751798.2024.2321736

Published online: 05 Mar 2024.

DEFENSE & SECURITY ANALYSIS
https://doi.org/10.1080/14751798.2024.2321736

Routledge
Taylor & Francis Group

Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations

Lance Y. Hunter[a], Craig D. Albert[a], Josh Rutland[b], Kristen Topping[a] and Christopher Hennigan[c]

[a]Department of Social Sciences, Master of Arts in Intelligence and Security Studies (MAISS) Program, Augusta University, Augusta, GA, USA; [b]U.S. Army Cyber, Fort Eisenhower, GA, USA; [c]Department of Government and Public Service, Deloitte, Washington, DC, USA

ABSTRACT

Previous research in security studies contends that information warfare (IW) is becoming a critical element in states' overall security strategies. Additionally, many researchers posit that artificial intelligence (AI) is quickly emerging as an important component of digital communications and states' military applications worldwide. However, less is known regarding how states are incorporating AI in their information warfare and influence operations (IWIO). Thus, given the growing importance of AI and IW in global security, this paper examines how the United States, China, and Russia are incorporating AI in their IWIO strategies and tactics. We find that the US, China, and Russia are utilizing AI in their IWIO approaches in significant ways depending on each state's overall IW strategy, with important implications for international security.

KEYWORDS

Artificial intelligence (AI); information warfare (IW); information warfare and influence operations (IWIO); major power states; United States; China; Russia

Introduction

Many government officials, military leaders, and researchers acknowledge the growing importance of information warfare and influence operations (IWIO) in the realm of international security. As Khan states: "While information warfare is as old as military history, the revolution in communication sciences has changed its nature. It has become a double-edged sword equally important for the powerful states as well as technically poor states, non-state actors, and individual experts in software."[1] IWIO is critical to international security because it can shape global and domestic narratives that affect stability within states, international alliances, and the survivability of governments and leaders.[2] As military officials and researchers remark: "In current and future warfare, information superiority could be the single most decisive factor."[3] IWIO is evolving at a rapid pace due to the technological changes that have occurred in recent years that influence IWIO capabilities. One evolving technology of particular importance to IWIO is artificial intelligence (AI). AI

CONTACT Lance Y. Hunter lahunter@augusta.edu

developments have a significant impact on IWIO because they enhance the speed and effectiveness of IWIO operations, as well as shape the specific IWIO tactics that can be employed.[4] In addressing the role of AI in defence competition, Hurley remarks: "The onset of what is perceived to be the next global 'arms' race will position 'the winner' as the top superpower that could define and dictate future directions and priorities across the globe."[5]

Previous valuable IWIO scholarship has focused on the strategies and tactics behind IWIO,[6] and researchers have documented the effect AI has on military applications in major-power states.[7] However, minimal research has considered how AI is affecting the IWIO strategies of major-power states. This topic is important due to the expanding role of AI and IWIO in defence and security, and the rapidly growing influence AI is having on IWIO tactics. Perez and Nair note that "AI and its subcomponents … are serving as powerful tools for generating and amplifying disinformation about the Russia-Ukraine war, particularly on social media channels."[8] Based on the above statements, it is clear AI is already shaping the digital battlespace, and in the case of the war in Ukraine, it is also likely affecting the kinetic realm. Thus, this paper examines how the US, China, and Russia are incorporating AI in to their IWIO strategies and tactics and considers the implications for international security. In our analysis, we find that the US, China, and Russia are utilising AI in their IWIO in significant ways depending on each state's overall IWIO strategy. Additionally, we argue that the manner in which AI is being used in IWIO by the US, China, and Russia has significant effects on the stability and security of states that could be targeted in IWIO. Overall, we contend that considering the effect AI has on IWIO strategies and tactics in the major power states is a vital component of the modern security landscape (Table 1).

We focus on the US, China, and Russia due to the large amount of influence each state has in global politics and international security.[9] Even though other states could be considered major power states, we contend that the IWIO strategies employed by the US, China, and Russia significantly affect other states in their regions, as well as globally. More specifically, we argue that while other states' IWIO strategies are also important to consider, the US, China, and Russia play an outsized role in affecting international security based on their IWIO capabilities and operations.

The layout of the paper is as follows. First, we discuss our definition of AI and how it relates to IWIO. We then discuss our conceptualisation of IWIO and why it is important to global security. In this section we also highlight the distinct IWIO doctrines of the US, China, and Russia and how they motivate their IWIO strategies and tactics. Next, we analyse how surveillance capitalism, data collection processes, regime type, and grey zone activities affect the use of AI in IWIO for the US, China, and Russia. We then examine how the US, China, and Russia are incorporating AI in their specific IWIO strategies and tactics, discussing similarities and differences amongst the three states. Lastly, we discuss the ways in which the US, China, and Russia's application of AI in their IWIO strategies could affect international security.

Artificial intelligence

There are many different definitions of AI and there is much debate regarding how to define it. Based on prior scholarship, we advance a common definition of AI that has

Table 1. Artificial Intelligence (A.I.) Strategy, Development, and Integration in Major Power States.

State	Strategies and Tactics	Developers and Companies	Integration and Applications
US	Focus on information operations and the means through which the state pursues information warfare[a]	Booz Allen Hamilton[f]	Involve psychological operations, operations security, military deception, and electronic warfare[k]
	Train via complex wargame simulations generated and adapted by machine learning programmes and operational concept improvement bolstered by machine learning[b]	US Intelligence Community[g]	Monitor large streams of data to detect information patterns which can be identified as hostile information[l]
	Third Offset Strategy (TOS)[c]	National Artificial Intelligence and Initiative Office[h]	Incorporate learning machines, human-machine collaboration, assisted human operations, human-machine combat training, and network enabled autonomous weapons[m]
	Artificial Intelligence Use Case Inventory[d]	DARPA[i]	GEAR program[n]
	Pillar AI Strategy: Deliver AI-enabled capabilities that address key missions, scale AI's impact across DoD through a common foundation that enables decentralised development and experimentation, cultivate a leading AI workforce, engage with commercial, academic, and international allies and partners[e]	Joint Artificial Intelligence Center[j]	Use unmanned aerial systema (UAS) and artificial intelligence (AI)-enabled autonomy capability[o] Deepfake Detector[p] Multidimensional Anomaly Detection fusing HPC, Analytics, and Tensors (MADHAT)[q] MediFor[r]
China	Use "Asymmetric warfare" capable of offsetting technological inferiorities that might otherwise impact a state's ability to challenge geopolitical adversaries[s]	State Key Laboratory for Communication Content Cognition[y]	Invest heavily into information warfare capabilities[ab]
	Overcome superior forces by "robbing an army of its spirit" and a commander of his courage[t]	Comprehensive National Science Center[z]	Enhance population control, as well as to profile and control its ethnic minorities[ac]
	Utilise information technology in a wide variety of sectors and regions, including "disruption through trade wars, information manipulation in cyberspace and military integration of advanced technologies[u]	Academy of Military Medical Sciences (AMMS)[aa]	Strengthen specific advantages in social control and information management[ad]
	Focus on 'informatisation warfare,' or 'xinxihua,' the application of information technology to all aspects of military operations[v]		Exploit contradictions in interests and perceptions between groups and create division[ae]
	New Generation Artificial Intelligence Development Plan[w]		Use big data and artificial intelligence" to strengthen China's leadership and better understand the citizens[af]
	4 Key Sectors: Increased information-processing capabilities, rapid decision-making, the use of swarms, and cognitive warfare[x]		Co-ordinate campaigns of inauthentic posts to create the illusion of widespread grassroots support for a policy, individual, or viewpoint, when no such widespread support exists[ag]
Russia	Cover a wide swath of technology, where "jamming electronic communication and disrupting access to the electromagnetic spectrum, Cyber espionage, and distributed denial of services (DDoS) attacks are no different from (and work in tandem with) using trolls and bots to spread dis/misinformation, establishing pro-Russian media outlets, or supporting local sympathisers to propagate favourable messages[ah]	"Internet troll factory"[am]	Sow distrust in U.S. elections[ap]
	Revitalise "traditional values at the individual level and a focus on returning the glory of the Soviet Union on the national level[ai]	Russian Internet Research Agency[an]	Deepen pre-existing socio-political fault lines in Western societies[aq]
	Divide and polarise society, tear it into small pieces and fragments, and make these fragments sincerely hate each other in order to have them collide with each other thereby initiating a fight for destruction or combine their aggression into a uniform stream and direct it against the ruling government[aj]	FSB[ao]	Equip state backed propaganda facilities with AI powered Deepfake technology that can create more realistic false narratives by constructing fake images and even video clips involving key figures that support whatever narrative the "troll" is attempting to push[ar]

(*Continued*)

Table 1. Continued.

State	Strategies and Tactics	Developers and Companies	Integration and Applications
	Use internet connected technology to "undermine, manipulate, and mislead the information people consume as it believes this can advance its political and military objectives[ak] Do not differentiate between technologies and information, and instead of calling the digital-only system Cyberspace, refer to "as the 'information space,' which includes both computer and human information processing[al]		Inject dis/misinformation (partially attained through cyberattacks), and fake news stories that a majority of those exposed to believed true at the time[as] Gray Zone[at] Use AI instruments, including electronic warfare, influence operations, propaganda campaigns, and disinformation[au] Generative Adversarial Networks (GANs)[av]

[a]Army Techniques Publication 3-13.1, 2018, 1-1.
[b]McGrath, 'Twenty-first century'; Pomerleau, 'Pentagon AI Team Sets Sights on IWIO'.
[c]Work, 'The Third U.S. Offset Strategy'.
[d]US Department of State, 'AI Inventory'.
[e]CDAO, 'About the JAIC'.
[f]Booze Allen Hamilton 2022.[14]
[g]National Security Commission on Artificial Intelligence 2021, 110.
[h]National Artificial Intelligence and Initiative Office 2022; Subcommittee on Networking and Information Technology Research and Development Committee on Science and Technology Enterprise 2021, 18.
[i]NSTC 2019.
[j]CDAO, 'About the JAIC'.
[k]Theohary, 'IWIO: Issues for congress'.
[l]McGrath, 'Twenty-first century'; Pomerleau, 'Pentagon AI Team Sets Sights on IWIO'.
[m]Hilner, 'The Third Offset Strategy and the Army Modernization Priorities'.
[n]Pimentel 2022.[15]
[o]CDAO Public Affairs 2022.
[p]US Department of State, 'AI Inventory'.
[q]C4ISRNET, 'Pentagon AI team sets sights on IWIO'.
[r]Sybert, 'DARPA Launches New Programs to Detect Falsified Media'.
[s]Wang, 'Asymmetric war?'.
[t]Tzu, 'The Art of War', 108.
[u]Saalman, 'China and its hybrid warfare spectrum', 95.
[v]Buck, 'China in the Asia-Pacific Cyber Domain', 1.
[w]Kania, 'The Strategic Support Force and the Future of Chinese Information Operations', 3.
[x]Takagi, 'The Future of China's Cognitive Warfare'.
[y]Pollpeter and Kerrigan, 'The China AI and Autonomy Report', 5.
[z]Towey, 'Researchers in China claim they have developed 'mind-reading' AI'.
[aa]Bureau of Industry and Security, Commerce, 'Addition of Certain Entities'.
[ab]Cheng, *Cyber Dragon*.
[ac]Daniels and Chang, 'National Power After AI', 12.
[ad]Buck, 'China in the Asia-Pacific Cyber Domain', 4.
[ae]Pollpeter and Kerrigan, 'The China AI and Autonomy Report', 3.
[af]Ibid., 5.
[ag]US Department of State 2022.[16]
[ah]Bolton, 'Targeting Ontological Security', 130.
[ai]Ajir and Vailliant, 'Russian IWIO', 70.
[aj]Manoilo, 'Modern-Day IWIO and Hybrid War Operations', 3.
[ak]Topor and Tabachnik, 'Russian Cyber IWIO', 115.
[al]Ajir and Vailliant, 'Russian IWIO', 74.
[am]Wilde and Sherman, 2023, 34.[17]
[an]O'Donnell, 'Have We No Decency? Section 230 and the Liability of Social Media Companies for Deepfake Videos', 710.
[ao]Polyakova, 'Weapons of the weak: Russia and AI-driven asymmetric warfare'.
[ap]Wojnowski, *Russian Interference in the U.S. Presidential Elections in 2016 and 2020 as an Attempt to Implement a Revolution-like IWIO Scheme. Part II*.
[aq]Cunningham, 'A Russian Federation IWIO Primer'.
[ar]Marks and Bendett, 'Russia Is Systematically Copying U.S. Military AI Robotics'.
[as]Bolton, 'Targeting Ontological Security: IWIO in the Modern Age', 136.
[at]Morgan et al., *Military applications of AI: ethical concerns in an uncertain world*, 83.
[au]Ibid.
[av]Ibrahim, '"We are not prepared": Russia uses AI, deep fakes in propaganda warfare.'

been used by many previous researchers. We define AI as the ability of machines or computer programmes to execute tasks in a similar manner as humans in areas such as visual and spatial perception, audio, text, language, and speech recognition, decision-making, data collection and data analysis, and learning.[10] Within this definition, it is important to acknowledge that many of the functions we discuss are forms of machine-learning, which is a subset of AI.[11] As Kumar et al. remark, "Machine learning is a branch of artificial intelligence that aims at enabling machines to perform their jobs skilfully by using intelligent software."[12] These machine learning functions include, but are not limited to: algorithmic content moderation, algorithmic classification, machine-learning enabled content generation (including image, text, and algorithmic feeds), regression analysis, and clustering.[13] Thus, when using the term AI, we are referring to many types of machine-learning functions. We use the phrase AI because it encompasses these functions as well as additional activities that fall outside traditional machine-learning functions, or that are extensions of machine learning functions including but not limited to: symbolic AI, natural language processing, and expert systems.[18]

Information warfare and influence operations (IWIO)

This paper focuses on how states apply AI in their IWIO strategies and tactics. A large portion of the paper examines how states use AI in what would be considered information warfare (IW) operations in the digital space, specifically through social media sites, such as attempting to influence specific populations through purposeful narratives digitally. However, within this context, we also examine Cyber-operations (to a lesser degree) as they can be linked with broader IW campaigns. Typically, this is referred to as Cyber-enabled influence operations (CEIO) and is an example of IW in Cyberspace. We understand CEIO as "information operations that leverage means and dynamics unique to Cyberspace – with a particular focus on operations targeting social media."[19] CEIO is the cognitive hacking that occurs through digital media and is generally combined, or can work in unison with, physical Cyber-attacks, thus fitting within the larger framework of information warfare and the more specific terminology of IWIO. For example, a Cyber-attack that targets an adversary state to acquire data to use in a digital IW operation is also considered in the study since the two separate actions (i.e. the Cyber-attack and subsequent use of the data from the Cyber-attack to form propaganda narratives online) are part of a larger IW strategy. Thus, we use the term Information Warfare and Influence Operations (IWIO), which includes both Cyber-enabled influence operations (e.g. spreading propaganda narratives on social media), and Cyber activities, to account for the Cyber-component of the study. We elaborate on our conceptualisation of IW and IWIO below.

IW is a complex phenomenon that academics and military professionals have struggled to define. Researchers have conceptualised IW as "the deliberate manipulation or use of information by one party on an adversary to influence the choices and decisions the adversary makes in order for military or strategic gain."[20] Whilst broad, this definition highlights the fundamental elements of IW, namely the targeted and intentional desire to influence an adversary's decision-making through information.[21] US military doctrine tends to focus on information operations, the means through which the state pursues IW,[22] and these operations can fall within the realms of psychological

operations, operations security, military deception, and electronic warfare.[23] By IWIO, we rely on Lin's definition, which is the "deliberate use of information (whether true of false) by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes."[24] Additionally, IWIO describes the integration of multiple aspects of IW (electronic warfare, Cyber-warfare, and psychological warfare) to achieve strategic objectives.[25] As mentioned, the focus of the paper is on how AI is being used in IW strategies and tactics as it pertains primarily to CEIO. However, we also discuss Cyber-attacks within the analysis. Thus, as previously mentioned, we use the term IWIO that incorporates the more broadly considered, full range of activities from CEIO, Cyber-attacks, and IW.

IWIO is considered significant in the context of modern great power competition for its ability to act as both a force multiplier and an alternative to traditional kinetic means of persuasion. China describes its value as a means of "asymmetric warfare" capable of offsetting technological inferiorities that might otherwise impact a state's ability to challenge geopolitical adversaries.[26] This is embodied in Sun Tzu's teachings on how to overcome superior forces by "robbing an army of its spirit" and a commander of his courage.[27] Russia has recognised the potential power IWIO offers as well, notably in its own efforts to sow distrust in U.S. elections via meddling[28] and attempting to deepen pre-existing socio-political fault lines in Western societies, notably within the US.[29] In essence, the capability of IWIO lies in its ability to redistribute power and negate the need for rapid advancements in military capabilities.[30]

It should be noted that as of this writing, each of these three states (US, China, and Russia) advance very different approaches to IWIO. The acronym DIME (Diplomatic, Informational, Military, and Economic) often refers to instruments of national power,[31] and unlike China and Russia, the US does not have an entity responsible for the informational component of DIME.[32] In fact, it can be argued that the three states view the IWIO domains through fundamentally distinct lenses. The US views IWIO as largely taking place in the Cyberspace domain. Russia views it through the information domain, and China uses a mixed domain preference.[33] Furthermore, the US generally separates peacetime from wartime activities in the information domain. In other words, the US limits its IWIO capabilities when it is not engaged in conflict with another state.[34] This places the US at a disadvantage when compared with Russia and China, who constantly engage in offensive IWIO activities as a matter of strategy and policy in the information domain. The US, however, considers IW activities as force multipliers within an already defined strategic conflict; in other words, the US only engages in IW activities during conflict, whereas China and Russia see IW as perpetual and persistent activities. Additionally, the US conducts IWIO through the military and DoD broadly while China and Russia employ IWIO through a whole of society approach. Russia's official stance is there is no distinction in their IWIO strategies and tactics in peacetime and wartime.[35] In other words, Russia is permanently in a state of conflict within the information environment, specifically against the United States, but also as a general strategy in the international arena. China also pursues IWIO differently than the US, but more akin to the Russian approach. As with Russia, China's Cyber-enabled influence operations revolve around the operational imperative of "peacetime wartime integration."[36] These differences are important to acknowledge when considering how each state applies AI to

their IWIO strategies. We expand on each state's IWIO strategies and tactics in the later sections of the paper.

Throughout the paper, we refer to states' IWIO strategies and tactics. Strategies refer to broad, long-term goals or plans that are advanced to achieve the desired political and military objectives of a state. Tactics are more detailed, immediate actions that are guided by strategies and are designed to accomplish shorter-term goals within the context of a given strategy and can vary based on circumstance.[37] Thus, IWIO tactics are the specific actions that are carried out based on the IWIO strategies of each state.

Governance structures, AI, and data collection

Before examining how the US, China, and Russia are using AI in their IWIO, it is important to consider how the type of government institution of each state affects their data collection processes, IWIO strategies, and how they apply AI within these strategies. First, while the US obtains a large amount of data on potential security threats domestically, China and Russia can collect data on their domestic populations to a greater extent through more aggressive methods due to the non-democratic nature of their governments. In other words, China and Russia can surveil their populations more freely without privacy, or civil liberty concerns, and use the data to train AI algorithms that can be used in IWIO.[38]

The authoritarian and centralised nature of the Chinese and Russian governments allow both states greater ability to collect data domestically and internationally compared with democracies such as the US. These data can be deployed to train AI algorithms to use in IWIO and grey zone activities.[39] In contrast, the US faces more difficulty in collecting and utilising large-scale data in the same manner due to its democratic principles that include some protection of privacy rights, as well as political and bureaucratic oversight regarding the decision-making processes that govern the collection and use of domestic surveillance data. This is also a component of the US' strategy regarding not employing IW more broadly outside of wartime, including against its strategic adversaries. This is not to argue that western democracies do not collect security data domestically, or that US multinational corporations (MNCs) do not collect large amounts of domestic data through surveillance capitalism frameworks. Rather, it is to argue that democracies such as the US cannot collect data and wield it in IWIO to the same degree as authoritarian states such as China and Russia based on the democratic and decentralised nature of US governance. Relatedly, an important point to highlight within the context of regime type, AI, and IWIO is how surveillance capitalism affects data collection, AI algorithms, and IWIO.

Surveillance capitalism and data collection

Surveillance capitalism refers to the practice of technology companies collecting and selling data and personal information while employing specifically tailored algorithms to predict and affect individual behaviour. Surveillance capitalism is based on the idea that consumer data is a driving force within the digital economy. Consumer data is often used by corporations in conjunction with algorithmic programmes to target individuals to affect their buying habits, as well as by political actors to influence individuals' political viewpoints. Some of the potentially negative effects

of surveillance capitalism are that it can harm privacy, erode confidence in governmental systems, increase polarisation within societies, and exacerbate various forms of discrimination.[40] Surveillance capitalism is important to discuss regarding AI and IWIO because states such as China and Russia can more easily deploy AI algorithms to sow division and divide populations based on the data gathered through companies operating within the surveillance capitalist framework compared with western democracies.[41] The reason is that the data collected can allow the AI algorithms to identify and target individuals for IWIO based on their shopping and social habits and political viewpoints. As Dawson states: "governments must recognise microtargeting – data informed individualised targeted advertising – and the current advertising economy as enabling and profiting from foreign and domestic information warfare being waged on its citizens."[42] China and Russia can use data collected through the surveillance capitalism framework to a greater extent than democracies such as the US because their state identities and authoritarian governance structures allow for more aggressive data collection programmes, which drive AI algorithms that are useful for IWIO.

China is employing surveillance capitalism methods to collect large amounts of data to power AI algorithms that could be used for numerous purposes including, but not limited to: increasing domestic surveillance and population control of Chinese citizens, targeting Uighur minorities in Xinjiang for re-education purposes, and conducting IWIO to divide and polarise societies within democracies such as the US.[43] Through Chinese security forces, Chinese companies, and the Belt and Road Initiative (BRI), China is collecting massive amounts of data that can be used to tailor AI algorithms that can help China achieve its larger IW goals of controlling domestic populations, spreading the PRC's political narratives internationally, and increasing division within western democracies to undermine confidence in their governments.[44]

One example of how China exerts control over its domestic population through data collection and AI is through the application WeChat. WeChat is a Chinese social media application that can be used for a range of functions including instant messaging and mobile phone payment and fund transfers. WeChat was developed by the Chinese company Tencent. It is estimated that over 60% of transactions in China are conducted through WeChat.[45] The data from these transactions are used by the PRC to monitor and control Chinese citizens. China has identified 75 behavioural characteristics to identify if someone is considered susceptible to radicalisation,[46] and WeChat is the ideal platform to monitor and track individuals' behaviour to measure the extent they conform with PRC standards. Additionally, the issue is not limited to the domestic use of AI to monitor and control individuals. Researchers and policy-makers have raised concerns that companies such as Tencent, Byte Dance, and Zoom collect large amounts of data on citizens around the globe through online gaming, social media, and video conferencing platforms that could be potentially used for AI algorithms for targeted IWIO.[47] As Dawson states, "While Chinese data collection is perceived as a national security threat, domestic data collection is viewed as a digital privacy issue – these are not separate issues. Domestic digital privacy is fundamentally linked to national security."[48]

Russian influence operations have also used the surveillance capitalism framework to deploy specifically tailored algorithms to increase political polarisation within the

US. One example is Russia's use of data collection processes and AI algorithms to target military veterans and individuals more prone to support the military for propaganda campaigns.[49] It is also estimated that leading up to the 2016 election Russian IWIO efforts were likely designed to motivate some voters to turn out to the polls, whilst discouraging others.[50] The bipartisan US Senate investigation discovered that during the 2016 US Presidential elections, Russia conducted IWIO targeting US infrastructure using Facebook-targeted advertising and used social media to intensify social divisions in the US.[51] Additionally, Russian AI algorithms have been employed to encourage some individuals to attend protests, whilst encouraging others to attend counter-protests, thereby amplifying polarisation.[52] An important feature of the PRC and Russian IWIO efforts described above is the data collection efforts conducted within the surveillance capitalism framework significantly empowered the AI algorithms that were used to target particular individuals and groups for IWIO. Within this context, it is also important to examine each state's identity in considering grey zone activities and IWIO, and why democracies such as the US are likely to distinguish between wartime and peace time regarding IWIO while authoritarian states such as China and Russia are more prone to view IWIO within the framework of continuous conflict.[53]

State identity and grey zone activities

Grey-zone actions are those that are below the threshold of armed kinetic conflict and are designed to achieve specific goals. They often include, but are not limited, to Cyber-attacks, information warfare, economic coercion, and the use of proxy forces.[54] As Tiwari remarks: "The grey zone has been defined as the space between peace and war, characterised by the ambiguity of objectives, the participants involved, and the role of military force in response that remains below the level of war."[55] Whilst the US has focused much of its efforts on protecting vital infrastructure, China and Russia have viewed the US (and much of the West) as a threat to their security and geopolitical ambitions, thus prompting both states to take more aggressive actions in the grey zone compared with the US. In this way, China and Russia view IWIO within the grey zone in the context of a broader, ongoing conflict with the US and West where there is no distinction made between wartime and peacetime activities.[56]

Examples of Chinese grey-zone activities include using IWIO to disseminate propaganda regarding territorial disputes in the South China Sea and Taiwan reunification, incorporating psychological warfare into military operations, and controlling digital information and spreading online disinformation to decrease morale and increase polarisation in Western democracies.[57] Russia has employed similar IWIO strategies in the grey zone, as evidenced through its 2014 doctrine which prioritises the use of Cyber and IWIO, to assist its military as well as Russia's use of the Internet Research Agency (IRA) to employ wide-spread disinformation campaigns through social media. Specific examples include Russian IWIO in the 2016 US Presidential elections and attempted IWIO in the 2018 US mid-term elections along with numerous IWIO in Ukraine leading up to the invasion and during the conflict.[58]

Overall, the nature of China and Russia's political regimes allow for more aggressive data collection domestically and internationally compared with the US. The data can be

used in AI algorithms for IWIO that spreads disinformation, propagates PRC and Russian narratives, and seeks to undermine the confidence in democratic governments. These activities can be incorporated in grey-zone operations across numerous fronts. Thus, China and Russia's state identities consider IWIO within the context of continual conflict with the west, and the authoritarian nature of the Chinese and Russian regimes leads to more aggressive use of AI in data collection efforts, IWIO, and grey-zone activities compared with the US. In contrast, the US' identity and democratic institutions place more restrictions on its ability to gather data to use for AI algorithms for IWIO. Thus, the US places more emphasis on developing AI programmes to detect and counter IWIO and adversarial grey-zone actions. Having examined how regime type and state identify affect data collection, AI algorithms, and grey-zone activities, along with the role of surveillance capitalism in IWIO, we now turn to analysing how each state is applying AI within their IWIO strategies and tactics.

US

IW background information

The origins of US IW can be dated to World War II. During World War II, President Franklin Roosevelt established the Office of War Information (OWI) to organise US propaganda. In addition, the Office of Strategic Services (under the Joint Chiefs of Staff) employed psychological warfare techniques in concert with overseas military operations. The Supreme Headquarters Allied Expeditionary Forces in Europe was also active in the IW space as was evinced by the successful subterfuge involved in concealing the actual location of the D-Day invasion.[59] In 1942, the US launched the Voice of America (VOA) to disseminate news to states in German occupied territory. The VOA was also used to spread American values and attempt to counter communist propaganda during the cold war.[60] During this era, the US also employed IW in the form of psychological and disinformation tactics in attempting to obtain a narrative advantage over the Soviet Union.[61] In later years, US Air Force Colonel John Boyd helped develop and solidify the notion of "information warfare" and argued that IW was not simply a way to spread disinformation or propaganda, but could also be used to a greater extent to assist the US in military and political activities due to the inherent value that emerged from utilising information in a particular manner.[62] In the 1960s and 1970s, the US employed information warfare tactics (psychological warfare specifically) in the Vietnam conflict.[63] In the 1980s, the US military, intelligence community, and US State Department began using computers and satellites as part of the US' IW efforts. In the 1990s, the US employed IW tactics against Saddam Hussein's regime in the Gulf War.[64]

The US and AI military application: information warfare

Current experts contend that the US does not have a clearly defined strategy regarding IWIO.[65] Part of this is related to the lack of a clear definition of IW by the US government, or single agency responsible for conducting IW for strategic advantage.[66] The US military is responsible for the US' IWIO. IWIO is gaining increasing recognition in the

US as an important and inter-related aspect of war. The US Department of Defense (DoD) published the Joint Publication (JP) 3-13, Information Operations in 2012 (i.e. Joint Doctrine), and updated it again in 2014. Though lacking a unified definition and doctrine regarding IWIO across the government, military, and civilian populations, the acknowledgment that "operations in and across land, sea, air, space, and the electro-magnetic spectrum … depend on … [and] create information" is becoming more widely recognised.[67] Regarding US military strategy and IWIO, there is one operational environment and three dimensions within it: the physical, informational, and human.[68] The US Army describes the physical as "connective infrastructure that supports the transmission, reception, and storage of information," and the cognitive as "the minds of those who are affected by and act upon information."[69] Taken as a whole, the US Army views IWIO as using information collected from the physical environment to influence an adversary's decisions. Similarly, the US Marine Corps manual describes it as "leveraging the power of information to influence the behaviour of others."[70] It should be noted that the US Army is currently out of line with the joint doctrine, because joint doctrine recognises the distinction of the information environment where the US Army does not.

The most recent publicly available doctrine guiding US IWIO is the US Army's ATP 3-13.1 Conduct of Information Operations document, published in 2018.[71] Regarding the US' IWIO strategy, or lack thereof, though there is doctrinal recognition that IWIO can be used offensively to influence others, the US appears more hesitant than states such as Russia or China to use such tactics against individuals. Thus, the US seems to approach IWIO from a more defensive posture seeking to protect itself from IWIO and respond to adversarial IWIO when targeted.[72] The US has traditionally viewed IWIO in military terms while attempting to differentiate between acceptable and unacceptable activities.[73]

Recently, the US Army has shifted from operating within the standard academic definitions of IW and has moved into what is being called Information Advantage and Decision Dominance (IA & DD).[74] Within this realm information advantage activities (IAA) are conceptualised as the condition of holding the information advantage over a relevant actor's behaviour, situational understanding, and decision-making by using all military capabilities.[75]

Within the US' IWIO strategy, one issue that places it at a disadvantage compared with states such as China is the lack of a centralised approach to data collection.[76] Outdated data collection directives, different agencies having disparate approaches to data collection processes, and the lack of inter-agency communication often produces redundant data collection efforts and unnecessary resource expenditures. In simpler terms, due to the lack of a centralised data collection process, US agencies often expend valuable resources collecting identical data, and unco-ordinated data collection processes can lead to difficulty analysing the data and producing actionable intelligence for IWIO.[77]

The US is applying AI in several areas related to IWIO. China and Russia's recent investments in IWIO operations have driven the US to prioritise AI research to bolster its own defensive and offensive IWIO capabilities. The focus appears to be on using AI for weapons systems, training purposes, and protecting networks and digital information from other states' IWIO attacks.[78] It should be noted that China has invested heavily in IWIO in lieu of AI technology to offset some of its military technological disadvantages compared to the US.[79]

Currently, AI is being applied by the US in a defensive standpoint to monitor large streams of data to detect information patterns which can be identified as hostile information campaigns and potentially countered.[80] McGrath and others believe the US can improve its own information operations through training via complex wargame simulations generated and adapted by machine learning programmes, and operational concept improvement bolstered by machine learning.[81] As McGrath[82] argues, this might help the US realise the goals of its Third Offset Strategy (TOS), which was adopted in 2015 with the aim of shifting the US military's mentality towards innovation and direct competition with other great power states in hopes of overcoming adversarial technologies in Russia and China. The TOS was announced in 2015 by Robert Work, Deputy Secretary of Defense.[83] The top technological priorities listed in TOS focused on: learning machines, human-machine collaboration, assisted human operations, human-machine combat training, and network-enabled autonomous weapons.[84]

The importance of expanding and utilising AI to protect against IWIO attacks is exemplified by the 2023 National Defense Authorization Act (NDAA). The NDAA "outlines the Pentagon's spending priorities" with "a $20 billion increase from the 2022 NDAA" going toward research and development for AI.[85] According to the 2023 NDAA, there is a five-year plan to apply AI to "warfighting cyber missions within DoD."[86] Department of the Navy CISO Tony Plater describes how "AI will impact vulnerability management, threat hunting, and boost network security … so [it] is highly sought after to help … secure … cloud services."[87] In this way, the DoD seeks to bolster its network defences against outside informational threats by increasing the areas in which AI is employed, as well as update how it is utilised to protect the information sphere. By expanding the use of AI in the IWIO space, the US seeks to protect itself from manipulation, privatise and compartmentalise its information, and secure its intellectual property from theft.

The US and AI diplomatic application against information warfare

The US Department of State (DoS) utilises AI in a multitude of ways both to inform diplomacy and protect the American public from IWIO tactics employed by other states. Recognising the issues posed within the information sphere, the DoS acknowledges that "competing strategically on a global stage demand[s] that data not only be produced, used, or stored, but leveraged as a strategic asset."[88] In a departmental first, an AI Use Case Inventory has been released. In it, the DoS reveals the multitude of ways AI contributes to national security regarding IWIO from "accessing and analysing large amounts of text data from Department reporting" to "countering disinformation."[89] The AI Inventory reveals that the Global Engagement Centre (GEC) is at the heart of many AI uses for operating against IWIO. For Disinformation Topic Modelling, the GEC uses "text clustering and topic modelling of documents and social media to determine possible disinformation subjects and topics" whilst image clustering is used to "identify similar images in order to predict likely disinformation."[90] Another way the DoS is using AI to combat disinformation is via a Deepfake Detector. This tool examines an image of a face "and classifies the image as either being real … or fake (synthetically generated face …) to predict disinformation activities."[91] Such programmes and tools could potentially help the American government recognise attempts to sow disinformation within the public more expediently, and

adversarial IWIO tactics may be revealed in a timelier manner, thus increasing the likelihood of countering offensive information campaigns.

The pentagon and US cyber command's use of artificial intelligence for information warfare

In 2018, the Joint AI Centre (JAIC) was established by the Department of Defense to make use of AI and its potential as a valuable tool in the sphere of IWIO.[92] The DoD has five pillars of AI strategy: to "deliver AI-enabled capabilities that address key missions, scale AI's impact across DoD through a common foundation that enables decentralised development and experimentation, cultivate a leading AI workforce, engage with commercial, academic, and international allies and partners" whilst maintaining ethics and safety precautions.[93] One mission of the JAIC was to use AI to enhance joint warfighting efforts. In 2020, JAIC placed greater emphasis on ways to incorporate AI in the IWIO space.

By incorporating AI, the JAIC aimed to give the Department of Defense "an information advantage" by first refining its ability to combine commercial AI capabilities with government AI and then "improving the standardization of foundational DoD data needed to field high-performing AI-enabled capabilities to support operations in the information environment."[94] One programme the JAIC was using is the Multidimensional Anomaly Detection fusing HPC, Analytics, and Tensors (MADHAT). MADHAT "allows for the exploration of network data as a way of enabling more effective detection of nuanced adversarial threats."[95] By combining MADHAT's capabilities with established AI technology such as NLP and speech-to-text functions, the DoD aims to reduce the signal-to-noise ratio. When successful, using AI in this way allows analysts to devote their limited human resources to issues which require more nuanced interpretation rather than sifting through immeasurable data. JAIC was merged into the Chief Digital and Artificial Intelligence Office (CDAO) in 2022. Two of the primary goals of the newly formed CDAO are to: "1-Review and more tightly integrate the Department's policy, strategy, and governance of data, analytics, and AI, to include an integrated Data, Analytics and AI Strategy. 2-Provide the enterprise-level infrastructure and services that enable efforts to advance adoption of data, analytics, and AI, to include an expanded and more accessible enterprise data repository and data catalogue with designated authoritative data sources, common data models for enterprise and joint use cases, as well associated coding and algorithms to serve as a 'public good' as Department stakeholders put data on the offensive."[96]

In 2023, the CDAO reinstated experiments known as Global Information Dominance Experiments (GIDE) in collaboration with the Joint Chiefs of Staff (JCS). Members of the US military from all branches and civilian personnel made up the teams. The large-scale integration was made possible, in part, due to data and analytics connected to CDAO AI programmes. The most recent version of the GIDE (fifth iteration) included participation from combatant commands, the Pentagon, and international duty stations. The purpose of the GIDE was to provide information regarding Joint All-Domain Command and Control (JADC2) solutions pertaining to Joint data integration and AI and machine learning technology.[97] As Chief Digital and AI Officer Dr. Craig Martell stated, "We want to rapidly improve access to data across the Joint force – from the strategic level to our tactical warfighters. The intended outcome of these experiments is two-fold. First, we want to identify where we may have barriers in policy, security, connectivity,

user-interface, or other areas that prohibit data sharing across the Joint force. Second, we want to show how data, analytics, and AI can improve Joint workflows in a variety of missions from global integrated deterrence through targeting and fires."[98]

Defense advanced research projects agency, artificial intelligence, and information warfare

The Defense Advanced Research Projects Agency (DARPA) aims "to a singular and enduring mission: to make pivotal investments in breakthrough technologies for national security."[99] DARPA is a collaborative effort between government employees and civilians with a storied connection to advancements across arenas from stealth technology to the Internet.[100] In April 2022, DARPA's Director Dr. Stefanie Tompkins stated the Department "is pursuing more than 39 programs that are exploring ways to advance the state-of-the-art in AI, pushing towards third wave contextual reasoning capabilities" while over "60 active programmes are applying AI in some capacity."[101] DARPA focuses on identifying and countering malicious deepfake technology, which uses AI to substitute one person's likeness for another in media such as photographs or videos. MediFor, DARPA's Media Forensics programme, "builds algorithms to detect manipulated images or videos, then produces a quantitative measure of integrity, which enables filtering and prioritization of media at scale."[102] The programme "uses detection algorithms, which analyse media content to determine if manipulation has occurred," as well as "fusion algorithms, which combine information across multiple detectors."[103] These algorithms contribute to an integrity score for each piece of data the programme analyses. A low score means the media was likely manipulated and is thus flagged for review by analysts – resulting in large volumes of media being analysed by AI, allowing analysts to concentrate their efforts when and where they are most needed. Though the MediFor programme is in its final stages, DARPA has a new programme called semantic forensics (SemaFor). Unlike MediFor, which focused on detecting discrepancies and anomalies in media, SemaFor aims to attribute and characterise these deepfakes.[104] SemaFor's semantic technologies "automatically analyse modal media assets to defend against large-scale, automated disinformation attacks" while its "attribution algorithms will infer if digital media originates from a particular organization or individual" and its "characterization algorithms determine whether media was generated or manipulated for malicious purposes."[105] These models may help bolster their deepfake defensive models which preserve individuals' facial expressions and how they move their head.[106] The defensive model would illuminate whether a video of a President, or dictator were legitimate while SemaFor could indicate who may be responsible for the particular deepfake episode. In this scenario, a deepfake (for example, a video of a world leader ordering the release of a nuclear, or biological weapon) could have serious ramifications for national security and international relations around the globe. Thus, the deepfake identification technology may play an important role in US AI-enabled IWIO defence.

The US, artificial intelligence, and information warfare overview

The US is employing AI in its overall IWIO strategy in numerous ways. The US is primarily focused on applying AI defensively rather than through offensive IWIO

operations. This mirrors the US' overall IWIO strategy that is defensive in nature. Through collaborations with US technology companies and numerous government and military sectors, the US is using AI to identify, categorise, and counter a wide array of potential international IWIO threats. Examples include utilising AI technology designed to sift through large amounts of data to identify misinformation, propaganda, and intentionally divisive content that is intended to sow discord within the US domestically through social media and online content. Additional emphasis is being placed on using AI technology to counter AI-driven deepfake technology that could be used by adversaries for IWIO operations directed at the US. Furthermore, AI is being used to protect critical infrastructure from Cyber-attacks. This is being accomplished by employing machine learning programmes to sift through large amounts of data for indicators of possible attacks and generating AI programmes to defend against Cyber-attacks.

China

IW background information

Influenced by Sun Tzu and Mao Zedong, psychology is a central component of Chinese IW and is often employed as a key weapon rather than simply a support instrument.[107] Chinese IW is often conceptualised as consisting of "three warfares" that entail legal, psychological, and media operations. The aim of the warfares is to manipulate international legal regimes, affect public opinion, and undercut the morale of potential enemies. Within this framework, China employs IW operations pre-emptively. China often combines its IWIO tactics to include electronic warfare, precision-strikes, and Cyber-warfare with the goal being to injure the information capacity of its opponents.[108]

In engaging in IW, China incorporates Mao's notion of the "People's War" which consists of employing large amounts of Cyber-attacks combined with online disinformation. IWIO is a central component of China's military strategy given that China concedes it cannot match US military spending. China has placed significant emphasis on IW beginning as early as the 1950s, which has evolved into the current Strategic Support Force (SSF) and is a main component of China's IW capacity.[109] Numerous academies have been designed by China to expand China's IW capabilities, which include the Academy of Military Sciences Military Strategy Research Centre, the PLA Academy of Electronic Technologies, and the Xian Politics Academy. The Xian Politics Academy places a unique emphasis on psychological warfare training.[110] Researchers contend that China has employed IW simulation training for over a decade and IW units specialising in psychological warfare are embedded within the army.[111] Additionally, it is important to note that an important component of China's IW strategy includes operations in Cyber-space.[112] An example is the interconnected network of Chinese online influencers who reinforce Chinese narratives in countries that are targeted in Chinese IWIO.[113]

China actively employs its IWIO on social media. China utilises IWIO in its operations to attempt to weaken the perception of an enemy's leaders and its citizenry.[114] In a similar strategy as Russia, China employs psychological warfare to divide populations. This occurs through social media and by PRC agents purposely placed on social media platforms to propagate PRC narratives. Many of the programmes used by

PRC agents are AI-assisted. One example is China's use of the United Front, which is a sophisticated network of operators that carry out co-ordinated IWIO against specific individuals and institutions.[115] These actions allow the PRC to manipulate public narratives that are favourable to the party, domestically and internationally. China also controls online and social media content domestically to shape narratives and to ensure that it does not become the target of the type of influence campaigns it directs at adversary states.[116]

China and artificial intelligence military application: information warfare

China seeks to utilise information technology in a wide variety of sectors and regions, including "disruption through trade wars, information manipulation in cyberspace, and military integration of advanced technologies."[117] China created the Strategic Support Force (SSF) in 2015 with the aim of generating strategic advantages in the areas of space, Cyber-space, and the electromagnetic spectrum.[118] As Kania and Constello remark, "the SSF has integrated the PLA's capabilities for cyber, electronic, and psychological warfare into a single force within its Network Systems Department, which could enable it to take advantage of key synergies among operations in these domains."[119] China aims to implement an IWIO strategy that "focuses on 'informatization warfare,' or 'xinxihua,' the application of information technology to all aspects of military operations."[120] Daniels and Chang state that the government of China is actively "using AI technologies to enhance population control, as well as to profile and control its ethnic minorities."[121] They continue, stating that "China will likely export versions of these capabilities to authoritarian governments globally in the 2020s and 2030s, as it has already begun to do."[122] If social influencing can be altered and if "mass opinion can be decisively influenced by the clash between AI influence systems, for example, China may determine its best option for reabsorbing Taiwan is heavy investment in AI-empowered propaganda."[123] The integration of AI with nearly every facet of China's technology allows for specific advantages in social control and information management and is "enhanced with its 2017 Cyber-law that delivers unlimited avenues to virtually every network and piece of hardware operating in the Asia-Pacific."[124]

China has been accused of engaging in "cognitive warfare" against Taiwanese citizens by a Taipei think-tank and other observers in Taiwan.[125] As Taiwanese citizens, particularly the younger generation, have increasingly shifted away from China amid arguments that they have no connections to the mainland, China has engaged in "tactics ranging from military intimidation and propaganda to misinformation spread by its army of online trolls in a bid to manipulate public opinion."[126] Ultimately, this tactic is aimed at trying to coerce a reunification of Taiwan with mainland China without risking armed conflict.[127] This type of cognitive warfare falls within the realm of IWIO, particularly as the efforts seek to manipulate Taiwan's decision-making capacity.[128,129]

It has also been alleged that China has adopted the Kremlin's IWIO tactics "to highlight America's faults and weaponize the culture wars and identity politics currently buffeting the West,"[130] which some have alleged is a move "to distract away from Beijing's own rights abuses, including the internment of more than a million ethnic Muslim Uyghurs."[131] This marks a notable shift from China's previous methods of defending itself from accusations of human rights abuses, most of which involved

pressuring foreign states to refrain from involvement in China's "internal affairs."[132] These new offensive tactics bare the hallmarks of an IWIO campaign, and the increasing incorporation of AI technology could intensity China's IWIO operations.

China recognises the potential AI holds as a facilitator for growth, disruption, and control in the information space. In 2017, China's "New Generation AI Development Plan elevated AI as a core priority, catalysing what has become a whole-of-nation strategic initiative."[128] AI falls under China's military strategy of "'intelligentised' warfare," which "is characterised by four key features: increased information-processing capabilities, rapid decision-making, the use of swarms, and cognitive warfare."[133] According to Chinese strategists, human cognition is the main battlefield in intelligentised warfare. A former deputy chief of staff of the PLA, Qi Jianguo, "stated that those who gain the upper hand in developing new-generation AI technologies will be able to control the lifeline of national security."[134]

The official paper of the PLA, the *PLA Daily*, published an article discussing how cognitive warfare could be employed to influence the PLA's opponents. First and foremost, "cognitive warfare is directed at human emotion" and "should focus on the use of … AI … to strike at 'cognitive gaps' between social groups, especially the alliance system of the 'strong power' (a euphemism for the US), to exploit contradictions in interests and perceptions between groups, and create division."[135] The US saw many cultural conflicts intensify in recent years between protests, heated election cycles, and dichotomous stances on Covid vaccines. The PLA is utilising AI to identify and target these fractures that could have significant ramifications for such intelligentised warfare. However, China does not singularly focus on using AI in its IWIO tactics directed against the US. China also plans to employ AI to monitor and control the information space as it pertains to Chinese citizens.

The 2022 China Internet Civilisation Conference was meant to bolster and encourage the People's Republic of China's ability to implement and increase internet authority and control within its borders. The Party secretary, Ye Zhenzhen, shared "that the State Key Laboratory for Communication Content Cognition … is working to develop cognitive computing applications to guide political direction, public opinion guidance, and values orientation into a 'national weapon in the digital era.'"[136] Zhenzhen implicates "the use of big data and AI" as a means to strengthen China's leadership and better understand the citizens.[137] Though the report and accompanying video were quickly deleted following massive public backlash and condemnation, China's Comprehensive National Science Centre in Hefei's researchers "claimed to have developed 'mind-reading' AI capable of measuring citizens' loyalty to the Chinese Communist Party."[138] According to the researchers, AI analysed facial expressions and brain waves, thus measuring viewers' reactions – both positive and negative – to political information.[139] Though this specific publication was deleted, the US Department of Commerce did add the Academy of Military Medical Sciences (AMMS) in China, along with nearly a dozen of its research institutes, to its Entity List "based on the body of information that AMMS and its eleven research institutes use biotechnology processes to support Chinese military end uses and end users, to include purported brain-control weaponry."[140] The Entity List, though originally focusing on items relating to WMDs, now also serves to notify the public of "activities contrary to U.S. national security and/or foreign policy interests." Thus,

the AMMS's inclusion on a list for potential cognitive-monitoring and control tactics, and the potential to achieve its stated cognitive warfare goals, is concerning to many observers.[141]

China: artificial intelligence, information warfare, and the Uyghurs

Analysing China's manipulation of the information circulating regarding the treatment of Uyghurs in the Xinjiang region reveals a myriad of ways the state is utilising AI for IWIO purposes. It is alleged that China has detained "more than one million Uyghurs against their will" whilst many others in this majority Muslim community have been imprisoned.[142] In August 2022, the US Department of State released a report stating that "the People's Republic of China (PRC) actively attempts to manipulate and dominate global discourse on Xinjiang" in multiple ways via the internet and social media.[143] Of particular interest is their means of downplaying negative reports on the treatment of the Uyghur population while magnifying more positive, fabricated stories.

The Department of State report explains that "the PRC floods conversations to drown out messages it perceives as unfavourable to its interests on search engines and social media feeds."[144] Researchers analysed how often Chinese state media appeared in search results for key terms relating to Xinjiang and Covid over a four-month period for Google Search, Google News, YouTube, Bing Search, and Bing News.[145] They found that over the course of one hundred and twenty days, "Chinese state media featured prominently" in search engine results with "21.5% of the top results on Google News and Bing News" and a quarter of YouTube's results featuring state-backed media and accounts.[146] Simply searching a neutral term such as "Xinjiang … returned Chinese-state media in top results in 88% of News searches and 98% of YouTube searches."[147] By matching text and headlines word-for-word, nearly three dozen additional sources regurgitated Chinese state media reports – their inclusion in the report would have increased Chinese state influence by almost ten percent while YouTube videos posted by confirmed Beijing-supported users would add an additional twenty-seven percent of search results.[148] With "AI power[ing] almost every part of a search engine" and every single search result produced being "a direct result of decisions made by AI," some researchers contend that China's use of AI to manipulate information in the international arena must be examined more closely.[149]

Additionally, supporters of the PRC's IWIO mission also engage in astroturfing to promote more positive stories of what is happening to the Uyghurs in Xinjiang.[150] The term astroturfing describes "coordinated campaigns of inauthentic posts to create the illusion of widespread grassroots support for a policy, individual, or viewpoint, when no such widespread support exists."[151] The PRC accomplished this by using bots to spread quickly videos of content, such as the portrayal of happy Uyghur citizens on social media. When the *New York Times* and *ProPublica* analysed thousands of videos in 2021, they discovered numerous signs of astroturfing. Though "most of the clips carry no logos or other signs that they are official propaganda," analysis of over three thousand videos "found evidence of an influence campaign orchestrated by the Chinese government."[152] Most of the videos were shared on Chinese apps, but then began appearing other apps such as Twitter and YouTube – with English subtitles. All the videos possess similar or identical messaging, words, and phrases claiming that the Uyghur

citizens being filmed were happy, prosperous, and free. In over one thousand of the videos, the people "say they have recently come across [Former Secretary of State Mike] Pompeo's remarks" regarding their treatment and that his declarations they are oppressed, and genocide is taking place, are "complete nonsense."[153] Numerous aspects of the videos indicate their scope and reach was propelled by Chinese AI technology. *ProPublica* and *The Times* discovered "the clips were shared by more than 300 accounts whose posts strongly suggested they were no ordinary users" due to the identical messaging save "for a random string of characters at the end with no obvious meaning."[154] The random characters being generated were meant to circumvent anti-spam filters employed by Twitter to identify such bots. The random characters were found in seventy-five percent of the tweets. Additionally, every account had been recently created, did not follow other accounts, had few – if any – followers, and most of the tweeting occurred during the daytime in Beijing.[155] Of particular importance is the fact that "the text of several of the accounts' tweets contained traces of computer code, indicating that they had been posted, sloppily, by software."[156]

The CCP has also used popular, female, minority social media influencers to spread CCP propaganda in Xinjiang, Tibet, and Inner Mongolia. When examining 1,741 videos published on 18 popular YouTube Accounts researchers found that the influencers propagated the CCP narrative that political, economic, and social conditions were ideal in these regions and rejected or ignored any human rights concerns.[157] Researchers contend that the influencers were likely manipulated by 'professional user-generated content,' or content that's produced with the help of special influencer-management agencies known as 'multi-channel networks (MCNs).'[158] These MCNs are directly controlled and funded by the CCP and are designed to propagate the CCP's narrative. These videos are often prioritised on search engines because the users generate a large amount of reoccurring posts and AI search-engine algorithms prioritise users that post frequently. Thus, posts from non-CCP affiliated users in these regions, which often raise genuine human rights concerns, are given lower priority by AI-search engine algorithms and the posts are viewed less often because the users are not able to post with the same volume and frequency as the MCN-assisted creators. Additionally, since YouTube is blocked in China, non-CCP affiliated social media creators cannot monetise social media content on platforms like YouTube where the MCNs can, due to their special agreements with China, thus providing the CCP with greater means to disseminate its propaganda.[159]

China: artificial intelligence, information warfare, and Hong Kong

Following a wave of protests and demonstrations in Hong Kong opposing China's new extradition law, the PRC media began to spread false narratives to attempt to delegitimise the Hong Kong protestors and portray them as participating in an independence, or separatist movement. It was discovered that numerous fake accounts were generated by the PRC to amplify the PRC's narrative that the demonstrators were violent separatists. The fake accounts produced large amounts of misleading information across numerous social media platforms including Twitter, Facebook, and YouTube. In August 2019, Facebook suspended 7 pages (with approximately 15,500 account followers) and 3 groups (with approximately 2,200 account followers). Additionally, Twitter suspended 200,000 accounts and You Tube suspended 210 channels related to

PRC misinformation efforts regarding the Hong Kong demonstrators. Furthermore, in 2020, Twitter suspended 23,750 main accounts and discovered that approximately 150,000 social media accounts were created to amplify the misleading content of the main accounts.[160] The suspicious accounts were identified due to the accounts reinforcing pro-PRC narratives and the activity of the accounts surged at the same time as the PRC began its propaganda campaign against the Hong Kong demonstrators. Additionally, many of the accounts did not have any followers and many account users claimed to be located in Hong Kong, but the account locations were set in other countries. After removing the suspicious accounts, Twitter announced that the suspended accounts were attempting to "sow political discord in Hong Kong" by "undermining the legitimacy and political positions of the protest movement on the ground."[161] As with the IWIO tactics employed by China regarding Taiwan and the Xinjiang region, AI algorithms were likely involved in the bot activity pertaining to the Hong Kong protests in respect to the content shared, the frequency of postings, and attempts to evade spam detection protocols.

China, artificial intelligence, and information warfare overview

China is using AI in the area of IWIO through multiple channels. China has incorporated AI into its offensive IWIO strategy by attempting to increase social and political tensions and divisions in the US through social media. China has also used AI to attempt to manipulate public sentiment in Taiwan, international opinion regarding the Hong Kong demonstrations, and the international community's perception of the treatment of the Uyghurs in Xinjiang. To accomplish these objectives, China has appeared to use AI to eliminate negative press while manipulating information by filming propaganda videos, disseminating the videos globally, and employing AI to circumvent spam detectors while flooding social media platforms with misinformation. These tactics indicate that China is willing to take aggressive actions to control political narratives and utilise AI to achieve its IWIO goals. China has also increasingly used AI to surveil its domestic population and spread political propaganda that is favourable to the PRC within its borders.

Russia

IW background information

Russia, since the fall of the Berlin Wall, has sought to revitalise "traditional values at the individual level and a focus on returning the glory of the Soviet Union on the national level."[162] To do so, Russia has used information and technology as part of its IW approach, where the purpose of such warfare when directed at adversary states is "to divide and polarise society, tear it into small pieces and fragments, and make these fragments sincerely hate each other in order to have them collide with each other thereby initiating a fight for destruction or combine their aggression into a uniform stream and direct it against the ruling government."[163] As Wilde and Sherman remark, "its core tenet might well be that regime security has historically been indivisible from information warfare in Russian strategic thought. Rather than an aggressive, or expansionist,

expression of Moscow's foreign policy, the Kremlin's so-called information war should primarily be viewed through a domestic and regime security prism – it's as much a counterinsurgency as an expeditionary strategy, less an escalation than a projection."[164] Some of the common IW techniques employed by Russia include disinformation, propaganda, and psychological operations. Among the more well-known Russia IW operations, Russia has allegedly employed IW to influence elections in the US, France, and Germany, and has been accused of deploying IW to aid the Russian military in Syria and Ukraine.[165]

Topor and Tabachnik explain that the focus of Russia's IWIO strategy is to use internet connected technology to "undermine, manipulate, and mislead the information people consume as it believes this can advance its political and military objectives."[166] The key to this style of warfare is the creation of unsecured or permissive information spaces, "wherein discourse or debate lines favourable to Moscow permeate a targeted society."[167] Ajit and Vailliant state that the use of IWIO is nothing new to Russia, where the "first known use of the words 'active measures' was in a Bolshevik document in 1919."[168] The use of manipulating, influencing, and controlling information has been a constant tool used by all versions of Russia throughout the most recent century.

From a constructivist viewpoint, Russia perceives itself as a disrupter. Since the 1970s, Russia strategists have been considering how the Digital Age would affect warfare and society. Russia has long considered the digital information age as a new type of battlefield where information can be wielded as a weapon. However, Russia has realised it cannot compete commercially in the digital space with other western states such as the US. Thus, it has employed a strategy of disruption, denial, and delay regarding IWIO. This strategy has included Cyber-warfare and influence operations, especially disinformation. The ultimate aim of the strategy is to undermine public confidence in the US and western political systems through the surveillance capitalism model.[169]

An important element to consider in relation to Russia, AI, and IWIO, is how technologies such as AI, as well as globalisation and changing economic landscapes, affect cultural backlash in western democracies, and how the configuration of these factors impacts the types of IWIO Russia employs as well as the ultimate success of Russia's IWIO strategies. One aspect of cultural backlash theory is based on how some individuals in western states may become disenchanted with the erosion of traditional ideals and beliefs and the emergence of more progressive and secular trends, thereby increasing their political grievances and support for populism.[170] A second aspect is centred on possible grievances that emerge in western states due to rising economic inequality tied to changes that transform economic patterns and labour markets, which could also increase grievance formation and support for populism.[171] In considering these potential economic changes, researchers have noted that technologies such as AI can affect labour markets[172] leading to possible increases in social, economic, and political divisions and potentially greater instability and support for populist movements.[173] A potential effect of cultural backlash, whether driven by social, economic, or technological factors, is that states such as Russia can more easily deploy AI driven IWIO campaigns to target individuals and groups that are discontent, leading to greater societal divisions, polarisation, and support for populist movements. Having examined how historical factors and Russia's state identity affect its IWIO, we now turn to examining how Russia is applying AI in its IWIO strategies and tactics.

Russia and artificial intelligence military application: information warfare

Despite Russia's AI developments, Russia is currently lagging behind the United States and China in terms of incorporating AI technology into its military overall.[174] However, Russia has demonstrated an intense focus on further developing its already advanced IWIO tactics with the assistance of AI technologies. This is likely due to Russia's strategic focus on IWIO as a primary security strategy. Russia's internet sponsored propaganda manufacturing facilities, or "troll farms," are now equipped with AI powered Deepfake technology that can create more realistic false narratives by constructing fake images and even video clips involving key figures that support whatever narrative the "troll" is attempting to push.[175] This software has made it possible to create ultrarealistic depictions of events that never happened. Experts have stressed the massive risk posed if Russia begins doctoring images and videos for political gain.[176]

Russia's view of IWIO covers a wide swath of technology, where "jamming electronic communication and disrupting access to the electromagnetic spectrum, Cyber-espionage, and distributed denial of services (DDoS) attacks are no different from (and work in tandem with) using trolls and bots to spread dis/misinformation, establishing pro-Russian media outlets, or supporting local sympathisers to propagate favourable messages."[177] Russia exploits information ecosystems by "interjecting dis/misinformation (partially attained through Cyber-attacks), and fake news stories that a majority of those exposed to believed true at the time."[178] Faking and altering digital materials can be used in many scenarios, including political ones, as shown when "during the 2017 French election, Russia stole documents from the Macron campaign and edited them to include fake, damaging information."[179] Botnets, trolls, and deepfakes are tools often utilised in the information space with decent success rates, so much so that "Russian authorities have set up the so-called 'Internet troll factory' in St. Petersburg – young people who pretend to be real members of the Internet, widely concentrating and disseminating provocative and outrageous information."[180] O'Donnell provides another example of Russian disinformation, stating that the "Russian Internet Research Agency has launched sophisticated campaigns to create the appearance of a chemical disaster in Louisiana and an Ebola outbreak in Atlanta."[181] The nature of AI-assisted deep fake technology has "accentuated perceived differences between the realities of partisan groups and accelerated the prevalence of, and discussion on, 'fake news.'"[182] The use of AI-assisted deep fake technology can even create physical, real-world events, as seen when Russia "successfully organised a fake protest prior to the 2016 election that was attended by thousands of people in New York and another in Florida."[183]

In present times, unlike competitors, Russia does not differentiate between technologies and information, and instead of calling the digital-only system Cyber-space, refers to it "as the 'information space,' which includes both computer and human information processing."[184] This integrated viewpoint allows Russia to command a hybrid information and digital technology suite with real-world applications such as "the recycling and spreading of a YouTube video of Russian soldiers with the title 'Punitive Ukrainian National Guard Mission' throwing dead bodies near Kramatorsk (Donetsk region) on 3 May 2014."[185] Not just regulated to using combat footage to influence viewers on the World Wide Web, Russia has used social influencing and communications to sway public opinion when Russian agents tweeted "pundits call on @Theresa_May to disrupt possible Russia-US

thaw. No trust in Britain's best friend and ally?"[186] Further IWIO tactics involve stories shared on social media, where prior to the Netherland's 2016 trade deal referendum with Ukraine, Russia subjected Dutch citizens to online articles consisting of "Ukrainian soldiers crucifying a child and reports from individuals, purporting to be experts, portraying Ukraine as a 'bloodthirsty kleptocracy, unworthy of Dutch support.'"[187] By using various AI-assisted methods and tools in the information space, Russia can influence consumers of web-connected systems, public figures, and private citizens alike.

Russia has been flexible with its AI applications, often deploying the technology "in situations that may not constitute either war or peace," commonly referred to as the "grey zone."[188] Cyber-warfare, electronic warfare, influence operations, propaganda campaigns, and disinformation are prime examples of instruments that fit the Russian models of AI.[189] Russia has increased the use of AI in the digital world and "cyberwarfare, electronic warfare (EW), influence operations, propaganda campaigns, and disinformation are prime examples of instruments that fit the Russian modus operandi and are ripe to be integrated with AI."[190]

Though there are reports that Russia is lagging behind the US in military-AI integration, it is important to note that "unconventional tools – Cyber-attacks, disinformation campaigns, political influence, and illicit finance – have become a central tenet of Russia's strategy toward the West and one with which Russia has been able to project power and influence beyond its immediate neighbourhood."[191] By using AI in the information sphere, Russia can significantly improve the scope of their IWIO campaigns. Polyakova's assertion that "unlike in the conventional military space, the United States and Europe are ill-equipped to respond to AI-driven asymmetric warfare (ADAW) in the information space" requires serious consideration by policymakers (Polyakova 2018). With Russia trailing the US in integrating AI into the military, it is understandable that Russia would focus on ADAW as asymmetric warfare involves "conflicts between nations or groups that have disparate military capabilities and strategies."[192] Additionally, the Russian state utilises its AI IWIO capabilities at home as much as they do abroad.

In 2016, the Yarovaya amendments were instituted. These Russian laws "required telecom providers, social media platforms, and messaging services to store user data for three years and allow the FSB access to users' metadata and encrypted communications."[193] Although there is no consensus or knowledge about what Russia wants with such data, "their very collection suggests that the Kremlin is experimenting with AI-driven analysis to identify potential political dissenters."[194] Additionally, in Moscow, officials are using AI facial recognition systems called Sfera to target and surveil journalists.[195,196] By utilising such surveillance and biometric data, "the system has seen the preventative detention of dozens that the regime suspects to be potential instigators of public unrest." If IWIO is evaluated according to an entity using capabilities "to influence, disrupt, corrupt, or usurp the decision making of [target audiences]," then Russia's detention and intimidation of journalists from independent outlets can influence and disrupt the information Russian citizens obtain from independent journalists.[197]

Russia, artificial intelligence, information warfare, and Ukraine

Russia uses AI to conduct influence campaigns against citizens to sow civil discord or garner support for their own actions (such as the war in Ukraine). On February 15th

and 16th, nine days prior to the Ukrainian invasion, it is alleged that Russia carried out Distributed Denial-of-Service (DDoS) attacks targeting Ukrainian banks, government websites, and the Ukrainian Ministry of Defence and Foreign ministry. In conjunction with the DDOS attacks, Ukrainians began receiving SMS spam messages containing disinformation that indicated Ukrainians could not withdraw funds from ATMs due to technical issues.[198] In addition, numerous Russian disinformation campaigns have been identified and reported by social media companies since the Ukrainian invasion began. The Russian social media disinformation campaigns have directed inauthentic behaviour on social media platforms, temporarily seized control of social media channels, and sought to compromise the integrity of social media accounts.[199] A specific example was in September 2022 in which Meta removed a large network of fake accounts impersonating major news outlets publishing pro-Kremlin articles. These articles "[accused] the Ukrainian government and military of corruption and warning of dire consequences from European sanctions on Russia."[200] The report indicates "many of the fake accounts used profile pictures generated by AI."[201] Twenty-three hundred accounts were removed. These accounts, their pictures, and the websites created for the fake news stories, may have been the result of generative adversarial networks (GANs). This "branch of AI can be trained to produce realistic-looking data … [and] can disseminate that disinformation like rapid fire, while at the same time tracking its performance online by counting clicks and engagement."[202] GAN is the same software that can produce deepfakes and is a concerning area for those seeking to combat AI-enabled IWIO tactics employed by states such as Russia.

Russia uses GANs in its IWIO tactic in many areas as the Kremlin's Internet Research Agency (IRA) "is becoming increasingly decentralised and is gaining 'incredible traction' on TikTok with misinformation aimed at sowing doubt over events in Ukraine."[203] The IRA has a history of using trolls to post online and/or create bots that can spam social media sites with repetitive messaging. In May 2022, officials with the United Kingdom's government revealed that recent "research suggested Moscow's operation was 'designed to manipulate international public opinion' in favour of its military campaign in Ukraine."[204] Social media sites such as TikTok, Facebook, and Instagram attempt to remove accounts posting inconsistently with legitimate, non-bot users, but it can be difficult to keep up.[205] Though Twitter reports removing 100,000 accounts "for violations of its platform manipulation and spam policy" between February to May 2022, these types of information operations are becoming more common, gaining momentum, and appear more authentic than ever before.[206] The Ukrainian Secret Service confirmed in March 2022 that it had neutralised five different bot farms that were spreading disinformation on more than 100,00 active social media accounts.[207]

Russia, artificial intelligence, and information warfare overview

Russia, similar to China, utilises AI in its IWIO tactics to increase domestic tensions in the US and other Western states, as well as to divide and confuse antagonistic agencies and organisations. The overarching view of IWIO by Russia is "that information is the most important object of operations, independent of the channel through which it is transmitted."[208] As analysis and co-ordination of information and data from disparate channels requires exponential effort from IWIO analysts, Russia is researching the application of AI to IWIO data streams. Bendett explains that the focus of Russia is on

merging separate sectors into a unified front, stating that "many public efforts originate from the Russian Ministry of Defence (MOD), which is dedicating financial, human, and material resources toward AI development across its vast technical, academic, and industrial infrastructure."[209] Additionally, many technology events have been hosted by Russia over the past few years as they seek to merge AI research and application with existing IWIO implementations. These IWIO and AI events include "the 2018 Intellectual Systems in Information Warfare symposium" as well as workshops held on a regular basis by the "Russian AI Association."[210]

In summary, Russia has pursued aggressive IWIO operations targeting the US and other democracies ranging from seeking to manipulate elections, to spreading politically motivated deepfake videos, to attempting to increase political and societal polarisation within states. Russia has devoted more of its energy and resources to utilising AI in its overall IWIO strategy compared with the US and China. This may be an extension of Russia's overall military doctrine that places greater emphasis on offensive IWIO tactics compared with the US.

Discussion

AI can play a significant role in affecting IWIO strategies and tactics. AI can significantly enhance capabilities for automating IWIO operations, especially in reaching mass audiences and influencing public perceptions. AI can affect IWIO by increasing the speed of IWIO operations and it can be applied to a wide range of IWIO applications. As AI technology continues to evolve, its influence on IW tactics and techniques will undoubtedly grow and affect the landscape of modern security competition. This study has found that the US, China, and Russia are applying AI in their IWIO strategies and tactics in unique and impactful ways.

The United States is applying AI in its overall defensive IWIO strategy through numerous techniques. The US is utilising AI in many governmental and military areas the better to identify and counter IWIO threats pertaining to disinformation spread over social media and through other online channels. Specific AI applications seek to identify particular texts, themes, images, and videos that are part of foreign governments' IWIO operations. The aim is to reduce threats that seek to spread misinformation, propaganda, intensify polarisation and division within the population, and increase discontent with the government. While the US is incorporating AI in many different sectors within its defensive IWIO framework, frequent discussions within the government are centring around whether the US should continue to approach IWIO from a defensive posture, or advance a more offensive approach, as illustrated in the new doctrine of IA & DD.[211] If the US decides to adopt a more offensive-minded IWIO strategy, it possesses the technical sophistication to incorporate AI in its operations in several potentially effective ways based on pre-existing technology that can be adapted for offensive tactics. The decision by government leaders to pursue a more aggressive IWIO strategy may ultimately be determined by whether, and to what degree, Russia and China continue to target the US and its allies in future IWIO operations.

China is incorporating AI in its offensive IWIO operations through multiple avenues. China is using AI algorithms to spread information on social media to highlight divisions and political tensions in democracies as part of its overall "divide and conquer" strategy.

In addition, China is using AI in its cognitive warfare tactics to attempt to manipulate public opinion in Taiwan regarding reunification. This is being done in part through AI-powered programmes and bots that target Taiwanese citizens through the spread of misinformation and propaganda on social media. China is employing similar strategies internationally in its efforts to manipulate global opinion regarding the Uyghur situation in the Xinjiang region. China has mounted significant international IWIO operations ranging from AI bots generating misleading content on social media, to altered videos depicting the treatment of Uyghurs in China, to the manipulation of propaganda information posted on social media to evade AI misinformation and spam detectors on social media platforms. China is also advancing initiatives to further incorporate AI into the monitoring and control of its domestic population through expanding surveillance techniques and propaganda messaging. Concerns exist that China will export these AI technologies, designed to control and manipulate domestic populations, to other authoritarian regimes in the coming years.

Russia, employing a similar strategy as China, has used AI in its IWIO in attempting to sow political discord in several democratic states. Russia has relied on many different AI technologies to spread disinformation against its perceived adversaries in hopes of internally weakening those states. AI algorithms, bots, and deepfake technology have been employed to undermine the functioning of targeted governments. AI has also assisted Russian IWIO in identifying targets (e.g. specific citizens and groups) within democracies for precisely tailored propaganda messaging. Russia is also actively incorporating AI in its IWIO operations regarding Ukraine by attempting to manipulate international public opinion on the Ukrainian invasion using misinformation, bots, and altered videos that are AI driven. Lastly, Russia is likely to be employing AI technology to monitor journalists and potential opposition groups in Russia in a larger effort to minimise public dissent regarding the Ukrainian invasion and Putin administration.

In summary, AI is playing a pivotal role in affecting the IWIO tactics employed by the US, China, and Russia. Each state's overarching IW strategy is guiding the types of IWIO deployed. AI is providing states with a greater spectrum of possible tactics ranging from more complex IWIO detection software, to more powerful misinformation techniques (e.g. social media propaganda, deep fake videos, and bot proliferation), and increased capacity to conduct domestic surveillance and manipulate public opinion, both domestically and internationally. AI is significantly expanding the types of IWIO states can employ and altering the existing IWIO landscape. Given the growing sophistication of AI-supported IWIO tools, states will have to decide what types of IWIO strategies and tactics most appropriately match their values and maximise their security.

Notes

1. K. Khan, 'Understanding IWIO and Its Relevance to Pakistan', *Strategic Studies* 32 (2012): 138–159, p. 138.
2. W. R. Gery, S. Lee, and J. Ninas. 'Information Warfare in an Information Age', *Joint Force Quarterly* 85, no. 2 (2017): 22–9, p. 24.
3. Ibid., 24.
4. G. Yan, 'The Impact of AI on Hybrid Warfare', *Small Wars & Insurgencies* 31, no 4 (2020): 898–917.

5. J. S. Hurley. 'Enabling Successful AI Implementation in the Department of Defense', *Journal of IWIO* 17, no. 2 (2018): 65–82, p. 65.
6. M. Bishop and E. Goldman, 'The Strategy and Tactics of IWIO', *Contemporary Security Policy* 24, no. 1 (2003): 113–39.
7. L. Y. Hunter, C. D. Albert, C. Hennigan, and J. Rutland, 'The Military Application of AI Technology in the United States, China, and Russia and the Implications for Global Security', *Defense and Security Analysis* 39, no. 2 (2023): 207-232.
8. C. Perez and A. Nair, 'Information Warfare in Russia's War in Ukraine: The Role of Social Media and Artificial Intelligence in Shaping Global Narratives', *Foreign Policy* (August 2022). https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/
9. Congressional Research Service (CRS) Renewed Great Power Competition: Implications for Defense – Issues for Congress (2022); A. Radin et al., 'China-Russia Cooperation. Determining Factors, Future Trajectories, Implications for the United States', *RAND Corporation* (2021).
10. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning* (Cambridge: Massachusetts, MIT Press, 2016); I. A. Joiner, *Emerging Library Technologies: It's Not Just for Geeks* (Chandos Publishing, 2018).
11. Y. Kumar, K. Kaur, and G. Singh, 'Machine Learning Aspects and Its Applications Towards Different Research Areas', (2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2020), 150–6.
12. Ibid., 150.
13. A. Alimadadi and others, 'Artificial Intelligence and Machine Learning to Fight COVID-19', *Physiological Genomics* 52, no. 4 (2020): 200–2; Murphy, K. P. Murphy, *Probabilistic Machine Learning: An Introduction* (Cambridge: MA, MIT Press, 2022).
14. Booz Allen Hamilton, 'AI for National Security'. (2022). https://www.boozallen.com/markets/intelligence/ai-for-national-security.html (accessed September 27, 2022).
15. Pimentel, Elias, '2nd MAW Marines Train Using Video Games'. US Government: Marines. (2022). https://www.2ndmaw.marines.mil/News/Article-View/Article/3125552/2nd-maw-marines-train-using-video-games/
16. US Department of State, 'AI Inventory' (2022), https://www.state.gov/data-strategy/ai_inventory/ (accessed September 15, 2022).
17. G. Wilde and J. Sherman, 'No Water's Edge: Russia's Information War and Regime Security'. Carnegie Endowment for International Peace. (2023). https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644
18. M. Harré, T. Bossomaier, and A. Snyder, 'The Development of Human Expertise in a Complex Environment', *Minds and Machines*, 21 (2011): 449–64; H. Honda and M. Hagara, 'Question Answering Systems with Deep Learning-Based Symbolic Processing', *IEEE Access* 7 (2019): 152368–78.
19. B. Nakayama, 'Democracies and the Future of Offensive (Cyber-Enabled) Information Operations', *Cyber Defense Review* 7, no. 3 (2022): 49–65, p. 50.
20. C. A. Whyte, T. Thrall, and B. M. Mazanec, *IWIO in the Age of Cyber Conflict* (Oxfordshire: UK, Routledge, 2020, 344).
21. Ibid.
22. US Army, U.S. Army Techniques Publication No. 3-13.1: *The Conduct of Information Operations*. Headquarters, Department of the Army (2018), p. 1–1.
23. C. A. Theohary, 'IWIO: Issues for Congress', *Congressional Research Service* (2018): 7–5700.
24. H. Lin, 'Russian Cyber Operations in the Invasion of Ukraine', *The Cyber Defense Review* 7, no. 4 (2022): 31-46, p. 166.
25. CRS, Renewed Great Power Competition: Implications for Defense—Issues for Congress (2022)
26. V. W. Wang, 'Asymmetric War? Implications for China's IWIO Strategies', *American Asian Review* 20 (2002): 167–207.

27. S. Tzu, *The Art of War*, trans. Sammeul Griffith (London: Duncan Baird Publishers, 2005), 108. (Original work published 5th century BC).
28. M. Wojnowski, *Russian Interference in the U.S. Presidential Elections in 2016 and 2020 as an Attempt to Implement a Revolution-like IWIO Scheme. Part II* (Warsaw Institute, 2021).
29. C. Cunningham, 'A Russian Federation IWIO Primer', The Henry M. Jackson School of International Studies, University of Washington (2020). https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/ (accessed March 5, 2022).
30. Cunningham, 'A Russian Federation IWIO Primer'; Wang, 'Asymmetric War? Implications for China's IWIO Strategies'.
31. US Army, U.S. Army Techniques Publication No. 3-13.1
32. Cybersecurity and Infrastructure Security Agency (CISA), 'Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity', (2020), https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-258a; G. Wilde and J. Sherman, 'No Water's Edge: Russia's Information War and Regime Security'. Carnegie Endowment for International Peace (2023), https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644
33. B. Nakayama, 'Democracies and the Future of Offensive (Cyber-Enabled) Information Operations'.
34. C. D. Albert and others, 'Weaponizing Words: Using Technology to Proliferate Information Warfare', *Cyber Defense Review* (2023); D. Morabito, 'National Security and the Third-Road Threat: Toward a Comprehensive Theory of Information Warfare', *Air & Space Power Journal* 35, no. 3 (2021): 19–39.
35. M. Ajir and B. Vailliant, 'Russian IWIO: Implications for Deterrence Theory', *Strategic Studies Quarterly* 12, no. 3 (2018): 70–89; C. Francois and H. Lin. 'The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot', *Journal of Cyber Policy* 6, no. 1 (2021): 9–30.
36. E. B. Kania and J. K. Costello, 'The Strategic Support Force and the Future of Chinese Information Operations', *The Cyber Defense Review* 3 no. 1 (2018): 105–21; R. Diresta and others, *Telling 'China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives* (Stanford International Observatory. Cyber Policy Center: Hoover Institution, 2020).
37. C. Botan, 'Grand Strategy, Strategy, and Tactics in Public Relations', *Public relations Theory II* (Oxfordshire, Routledge, 2006).
38. J. Dawson, 'Who Controls the Code, Controls the System: Algorithmically Amplified Bullshit, Social Inequality, and the Ubiquitous Surveillance of Everyday Life', *Sociological Forum* (2023); J. Dawson and T. Wheeler, *How to Tackle the Data Collection Behind China's AI Ambitions* (Brookings, 2022). https://www.brookings.edu/techstream/how-to-tackle-the-data-collection-behind-chinas-ai-ambitions/
39. See Note 34; S. Tiwari, 'The Reality of Cyber Operations in The Grey Zone – The Emerging Geopolitics', *The Defense Horizon Journal* (2022).
40. S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (New York: NY, Public Affairs, 2020).
41. J. Dawson, 'Microtargeting as Information Warfare', *Cyber Defense Review* (2021), https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2537110/microtargeting-as-information-warfare/; Dawson, 'Who Controls the Code'.
42. Dawson, 'Microtargeting as Information Warfare', 63.
43. See Note 34.
44. Ibid.
45. K. Strittmatter, *We have been Harmonized: Life in China's surveillance state* (New York: NY, HarperCollins, 2020).
46. See Note 37; Strittmatter, *We have been Harmonized: Life in China's Surveillance State.*
47. Dawson, 'Microtargeting as Information Warfare'; J. Leonard, S. Mohsin, and D. McLaughlin, 'Tencent's Gaming Stakes Draw U.S. National Security Scrutiny', (Bloomberg, 2020). https://www.bloomberg.com/news/articles/2020-09-17/tencent-s-game-investments-draw-u-s-national-security-scrutiny#xj4y7vzkg

48. Dawson, 'Microtargeting as Information Warfare', 69.
49. Dawson, 'Who Controls the Code'; K. Goldsmith, 'An Investigation into Foreign Entities Who Are Targeting Service members and Veterans Online', *Vietnam Veterans of America* (2019).
50. See Note 34.
51. 116th Congress, Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Senate Report. 116–XX (Washington, DC: United States Senate Intelligence Committee, 2017); Dawson, 'Microtargeting as Information Warfare'.
52. 116th Congress, Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election; Dawson, 'Who Controls the Code'.
53. See Note 30.
54. Tiwari, 'The Reality of Cyber Operations in The Grey Zone – The Emerging Geopolitics'.
55. Ibid.
56. See Note 30; Tiwari, 'The Reality of Cyber Operations in The Grey Zone – The Emerging Geopolitics'.
57. J. Costello and J. McReynolds, 'China's Strategic Support Force: A Force for a New Era', *China Strategic Perspectives* 13 (2018); Tiwari, 'The Reality of Cyber Operations in The Grey Zone – The Emerging Geopolitics'.
58. M. Kaminska, 'Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks', *Journal of Cybersecurity* 7, no. 1 (2021). https://doi.org/10.1093/cybsec/tyab008; Tiwari, 'The Reality of Cyber Operations in The Grey Zone – The Emerging Geopolitics'.
59. Thomas Cripps and David H. Culbert. *Information Control and Propaganda: Records of the Office of War Information* (University Publications of America, 1986).
60. Voice of America, 'History of VAO', (2023), https://www.insidevoa.com/p/5829.html
61. See Note 55.
62. B.R. Price, 'Colonel John Boyd's Thoughts on Disruption', Marine Corps University Press. *MCU Journal, JAMS* 14 no. 1 (2023). https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-14-no-1/Colonel-John-Boyds-Thoughts-on-Disruption/
63. J. Whitaker, 'Psychological Warfare in Vietnam', *Political Psychology* 18, no. 1 (1997): 165–79; Whyte Jeffrey, 2018. 'Psychological War in Vietnam: Governmentality at The United States Information Agency', *Geopolitics* 23, no. 3 (2018): 661–89.
64. R. Bouchard, 'Information Operations in Iraq', *Defense Technical Information Center. Access Number*: ADA363160 (1999).
65. See Note 30; Tiwari, 'The Reality of Cyber Operations In The Grey Zone – The Emerging Geopolitics'.
66. H. Lin, 'Russian Cyber Operations in the Invasion of Ukraine'.
67. M. D. Phillips and T. A. Drohan, 'Informatizing Operations: The Other Half of All-Domain Warfare', *Small Wars Journal* March 03 (2020). https://smallwarsjournal.com/index.php/jrnl/art/informatizing-operations-other-half-all-domain-warfare
68. R. Stenson, US Army Training and Doctrine Command updates Army capstone doctrine, codifying shift to multidomain operations. U.S. Army (2022). https://www.army.mil/article/260943/us_army_training_and_doctrine_command_updates_army_capstone_doctrine_codifying_shift_to_multidomain_operations
69. Department of the Army, *FM 3-13: Information Operations*, 1–2, 2016.
70. USMC. *Information Doctrine*, 4–2, 2022.
71. US Army, U.S. Army Techniques Publication No. 3-13.1: The Conduct of Information Operations (Headquarters, Department of the Army, 2018).
72. See Note 30; Tiwari, 'The Reality of Cyber Operations in The Grey Zone – The Emerging Geopolitics'.

73. A. Wanless and J. Pamment, 'How Do You Define a Problem Like Influence?', *Journal of Information Warfare* 18, no. 3 (2019): 7.
74. R. J. Ross, 'Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations', *The Cyber Defense Review* 6, no. 4 (2021): 63–74.
75. Ibid.
76. T. Blagovest, M. Purcell, and B. McLaughlin, 'Russia's Information Warfare: Exploring the Cognitive Dimension', *MCU Journal* 10, no. 2 (2019): 133.
77. See Note 30; S. Tiwari, 'The Reality of Cyber Operations in The Grey Zone – The Emerging Geopolitics'; T. Blagovest, M. Purcell, and B. McLaughlin, 'Russia's Information Warfare: Exploring the Cognitive Dimension'.
78. J. R. McGrath, 'Twenty-First Century IWIO and the Third Offset Strategy', *Joint Force Quarterly* 82, no. 3 (2016): 16–23.
79. D. Cheng, *Cyber Dragon: Inside China's IWIO and Cyber Operations: Inside China's IWIO and Cyber Operations* (ABC-CLIO, 2016).
80. McGrath, 'Twenty-First Century IWIO and the Third Offset Strategy'; M. Pomerleau, 'Pentagon AI Team Sets Sights on IWIO', *CYISRNET* (2020).
81. Ibid.
82. McGrath, 'Twenty-First Century'.
83. R. Work, 'The Third U.S. Offset Strategy and its Implications for Partners and Allies', As Delivered by Deputy Secretary of Defense Bob Work, January 28, 2015. https://dod.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/
84. E. P. Hilner 'The Third Offset Strategy and the Army Modernization Priorities. Director's Action Group', *Center for Army Lessons Learned* (2019).
85. A. Obis and K. Macri, 'The 2023 NDAA Emphasizes AI Investment for Cybersecurity, JADC2', *Government CIO Media*. December 2022. https://governmentciomedia.com/2023-ndaa-emphasizes-ai-investment-cybersecurity-jadc2
86. Ibid.
87. Ibid.
88. US Department of State, 'Data Informed Diplomacy' (2022), https://www.state.gov/data-strategy/
89. US Department of State, 'AI Inventory' (2022), https://www.state.gov/data-strategy/ai_inventory/
90. Ibid.
91. Ibid.
92. CDAO, 'About the JAIC: The JAIC Story', (2022) https://www.ai.mil/about.html
93. Ibid.
94. C4ISRNET, 'Pentagon AI team sets sights on IWIO', July 22, 2020 https://www.c4isrnet.com/smr/information-warfare/2020/07/22/pentagon-ai-team-sets-sights-on-information-warfare/
95. Ibid.
96. CDAO, 'Chief Digital and Artificial Intelligence Office', (2023) https://www.ai.mil/
97. US Department of Defense, 'DoD Chief Digital and Artificial Intelligence Office Hosts Global Information Dominance Experiments' (2023). https://www.defense.gov/News/Releases/Release/Article/3282376/dod-chief-digital-and-artificial-intelligence-office-hosts-global-information-d/
98. Ibid.
99. DARPA, 'About DARPA', (2022) https://www.darpa.mil/about-us/about-darpa
100. Ibid.
101. S. Tompkins, Accelerating Innovation for the Warfighter: Statement Submitted to the U.S. Senate Armed Services Committee – Subcommittee on Emerging Threats and Capabilities, 117th Cong. (2022) (statement by Dr. Stefanie Tompkins, Director, Defense Advanced Research Projects Agency (DARPA)). https://www.armed-services.senate.gov/imo/media/

doc/PASSBACK%20DARPA_%20Tompkins%20SASC-ETC%20testimony%206%20Apr%202022_DARPA_FIINAL%200031.pdf
102. S. Sybert, 'DARPA Launches New Programs to Detect Falsified Media', *GovCIO Media & Research* September 16, 2021. https://governmentciomedia.com/darpa-launches-new-programs-detect-falsified-media
103. Ibid.
104. Ibid.
105. Ibid.
106. Ibid.
107. J. Yin and P.M. Taylor, 'Information Operations from an Asian Perspective: A Comparative Analysis', *Journal of Information Warfare* 7, no. 1 (2008): 3.
108. L. Wortzel, 'The Chinese People's Liberation Army and Information Warfare', *US Army War College, Monographs, Books, and Publications* 30 (2014): https://press.armywarcollege.edu/monographs/506
109. See Note 30.
110. Yin and Taylor, 'Information Operations from an Asian Perspective: A Comparative Analysis', 1–23.
111. T. Thomas, 'The Chinese Way of War: How Has it Changed?' *The MITRE Corporation*. US Army Futures and Concepts Center 47 (2020).
112. Kania and Costello, 'The Strategic Support Force and the Future of Chinese Information Operations'.
113. L. Turner and N. Hinkis, 'Chinese State Media's Global Influencer Operation', Miburo (2022) (currently part of the Digital Threat Analysis Center), https://miburo.substack.com/p/csm-influencer-ops-1
114. (Harold, Beauchamp-Mustafaga, and Hornung 2021) Harold, Scott W., Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung. *Chinese Disinformation Efforts* (RAND, 2021).
115. Diresta et al., *Telling 'China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives'*.
116. See Note 30.
117. L. Saalman, 'China and Its Hybrid Warfare Spectrum', in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, eds. M. Weissmann, N. Nilsson, B. Palmertz, and P. Thunholm (London: I.B. Tauris, 2021), 95–112. Bloomsbury Collections. p. 95.
118. E. B. Kania and J. K. Costello. 'The Strategic Support Force and the Future of Chinese Information Operations', *The Cyber Defense Review* 3, no. 1 (2018): 105–21.
119. Ibid, p. 105.
120. D. Buck, 'China in the Asia-Pacific Cyber Domain', *Marine Corps Gazette* 105, no. 4 (2021): 1–5, p. 1.
121. M. Daniels and B. Chang, 'National Power After AI', *Center for Security and Emerging Technology* (2021): 1–30, p. 12
122. Ibid, p. 13.
123. Ibid, p. 14.
124. D. Buck, 'China in the Asia-Pacific Cyber Domain', *Marine Corps Gazette* 105, no. 4 (2021), p. 4.
125. J. Huang, 'China Using 'Cognitive Warfare' Against Taiwan, Observers Say', Voanews.com (2021), para. 1.
126. Ibid, para. 3.
127. Ibid.
128. C. A. Theohary, 'IWIO: Issues for Congress', *Congressional Research Service* (2018): 7–5700.
129. J. Dettmer, 'China Adopts Kremlin's 'IWIO' Tactics', Voanews.com (April 5, 2021), https://www.voanews.com/a/east-asia-pacific_china-adopts-kremlins-information-war-tactics/6204171.html, para. 1.
130. Ibid, para. 2.
131. Ibid, para. 11.

132. E.B. Kania, 'Chinese Military Innovation in AI', *Testimony before the U.S-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion* (2019), 3.
133. K. Takagi, 'The Future of China's Cognitive Warfare: Lessons from the War in Ukraine', *Hudson Institute* (July 2022), https://www.hudson.org/research/17991-the-future-of-china-s-cognitive-warfare-lessons-from-the-war-in-ukraine
134. Ibid.
135. K. Pollpeter and A. Kerrigan, 'The China AI and Autonomy Report', *CNA* 22 (2022): 1–9, p. 3.
136. Ibid., 5.
137. Ibid., 5.
138. H. Towey, 'Researchers in China Claim they have Developed 'Mind-Reading' AI that can Measure Loyalty to the Chinese Communist Party, Reports Say', *Business Insider*, (July 10, 2022): https://www.businessinsider.com/china-says-mind-reading-ai-can-gauge-political-loyalty-reports-2022-7
139. Ibid.
140. Bureau of Industry and Security, Commerce, 'Addition of Certain Entities to the Entity List and Revision of an Entry on the Entity List', *Federal Register* (December 07, 2021), https://www.federalregister.gov/documents/2021/12/17/2021-27406/addition-of-certain-entities-to-the-entity-list-and-revision-of-an-entry-on-the-entity-list
141. Bureau of Industry and Security, 'Entity List' (2022), https://www.bis.doc.gov/index.php/policyguidance/lists-of-parties-of-concern/entity-list
142. BBC, 'Who are the Uyghurs and why is China being accused of genocide?' *BBC News* (May 24, 2022), https://www.bbc.com/news/world-asia-china-22278037
143. US Department of State, 'PRC Efforts to Manipulate Global Public Opinion on Xinjiang', August 24 (2022) https://www.state.gov/prc-efforts-to-manipulate-global-public-opinion-on-xinjiang/
144. Ibid.
145. J. Brandt and V. Wirtschafter, 'How China Uses Search Engines to Spread Propaganda', *Brookings* (July 6 2022): https://www.brookings.edu/techstream/how-china-uses-search-engines-to-spread-propaganda/
146. Ibid.
147. Ibid.
148. Ibid.
149. M. Kaput, 'AI in Search Engines: Everything You Need to Know', *Marketing AI Institute* (March 7, 2022): https://www.marketingaiinstitute.com/blog/how-search-engines-use-artificial-intelligence
150. US Department of State, 'PRC Efforts to Manipulate Global Public Opinion on Xinjiang'.
151. J. Kao and others, 'How China is Using Social Media Propaganda to Whitewash the Repression of the Uyghurs', *Scroll.in* (June 25, 2021) https://scroll.in/article/998385/how-china-is-using-social-media-propaganda-to-whitewash-the-repression-of-the-uyghurs
152. Ibid.
153. Ibid.
154. Ibid.
155. Ibid.
156. F. Ryan, D. Impiombato, and H. Pai, 'China is Using Ethnic-Minority Influencers to Spread Its Xinjiang Narrative on Social Media', *Australian Strategic Policy* (2022).
157. Ibid.
158. Ibid.; P. Mozur and others, 'How Beijing Influences the Influencers', *The New York Times* (2021) https://www.nytimes.com/interactive/2021/12/13/technology/china-propaganda-youtube-influencers.html; Ryan et al., 'China is Using Ethnic-Minority Influencers to Spread Its Xinjiang Narrative on Social Media'.
159. Mozur et al., 'How Beijing Influences the Influencers'; Ryan et al., 'China is Using Ethnic-Minority Influencers to Spread Its Xinjiang Narrative on Social Media'.

160. Diresta et al., *Telling 'China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives'*.
161. Ibid., 20.
162. Ajir, Media, and Bethany Vailliant, 'Russian Information Warfare: Implications for Deterrence Theory', *Strategic Studies Quarterly* 12, no. 3 (2018): 70–89.
163. A. Manoilo, 'Modern-Day IWIO and Hybrid War Operations', *Analytical Dossier* 1 (2021): 1–69, p. 3.
164. G. Wilde and J. Sherman, 'No Water's Edge: Russia's Information War and Regime Security', Carnegie Endowment for International Peace (2023), https://carnegieendowment.org/2023/01/04/no-water-s-edge-russia-s-information-war-and-regime-security-pub-88644
165. C. Cunningham, 'A Russian Federation IWIO Primer', The Henry M. Jackson School of International Studies, University of Washington (2020), https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/; B. Lilly, 'Russian Information Warfare: Assault on Democracies in the Cyber Wild West', *Naval Institute Press* (2022).
166. Topor, Lev, and Alexander Tabachnik, 'Russian Cyber IWIO: International Distribution and Domestic Control', *Journal of Advanced Military Studies* 12, no. 1 (2021): 112–27, p. 115.
167. D. Bolton, 'Targeting Ontological Security: IWIO in the Modern Age', *Political Psychology* 42, no. 1 (2021): 127–42, p. 130.
168. See note 158, 72.
169. Z. Rogers, 'The Geopolitics of Surveillance Capitalism', Chesterfield Strategy (2019), https://chesterfieldstrategy.com/2019/09/16/the-geopolitics-of-surveillance-capitalism/
170. Norris, Pippa, and Ronald Inglehart, 'Trump, Brexit, and the Rise of Populism: Economic Have-Nots and Cultural Backlash', *Harvard JFK School of Government Faculty Working Papers Series* (2016): 1–52.
171. Ibid.
172. A. Agrawal, J. Gans, and A. Goldfarb, 'Economic Policy for Artificial Intelligence', *Innovation Policy and the Economy* 19, no. 1 (2016): 139–159.
173. See Note 7.
174. See Note 7; S. Petrella, C. Miller, and B. Cooper, *Russia's AI Strategy: The Role of State-Owned Firms* (Foreign Policy Research Institute, 2020).
175. R. J. Marks and S. Bendett, 'Russia is Systematically Copying U.S. Military AI Robotics', *Mind Matters* (2020), https://mindmatters.ai/2020/10/russia-is-systematically-copying-u-s-military-ai-robotics/.
176. F. E. Morgan and others, *Military Applications of AI: Ethical Concerns in An Uncertain world* (Santa Monica, CA: Rand Project Air Force, 2020), 89.
177. D. Bolton, 'Targeting Ontological Security', 130.
178. Ibid., 136.
179. Ibid., 136.
180. O. S. Sheremet, 'Political and Legal Aspects of the IWIO', *Revista Amazonia Investiga* 10, no. 45 (2021): 31–41, p. 34.
181. N. O'Donnell, 'Have We No Decency? Section 230 and the Liability of Social Media Companies for Deepfake Videos', *University of Illinois Law Review* 3 (2021): 701–40, p. 710.
182. Bolton, 'Targeting Ontological Security', 137.
183. O'Donnell, 'Have We No Decency? Section 230 and the Liability of Social Media Companies for Deepfake Videos', 710.
184. See note 158, 74.
185. Ibid., 75.
186. Ibid., 76.
187. Bolton, 'Targeting Ontological Security', 135.
188. Morgan et al., *Military Applications of AI: Ethical Concerns in an Uncertain World*, 83.
189. Ibid., 83.
190. Ibid., 88.

191. A. Polyakova, 'Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare', *Brookings Institute*, (November 15, 2018): https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/. https://www.rand.org/topics/asymmetric-warfare.html
192. The RAND Corporation, 'Asymmetric Warfare'.
193. Polyakova, 'Weapons of the Weak: Russia and AI-Driven Asymmetric Warfare'.
194. Ibid.
195. D. Salaru, 'Russia: Facial Recognition Software used to Target Journalists', *International Press Institute* (June 23, 2022): https://ipi.media/russia-facial-recognition-software-used-to-target-journalists/
196. Ibid.
197. Joint Staff, *Joint Publication 3-13: Information Operations,* (2012), II-1
198. James Andrew Lewis, 'Cyber War and Ukraine', CSIS (2022); NOTE: The 2/15-2/16 DDOS attacks were attributed to Russia by Australian, US, and UK. The 2/15 disinformation attack remains unattributed.
199. H. Lin, 'Russian Cyber Operations in the Invasion of Ukraine', *The Cyber Defense Review* 7, no. 4 (2022): 31-46.
200. S. Bond, 'Facebook takes down Russian network impersonating European news outlets', *NPR* (September 27, 2022): https://www.npr.org/2022/09/27/1125217316/facebook-takes-down-russian-network-impersonating-european-news-outlets
201. Ibid.
202. N. Ibrahim, '"We Are Not Prepared": Russia Uses AI, Deep Fakes in Propaganda Warfare', *Global News* (March 30, 2022), https://globalnews.ca/news/8716443/russia-artificial-intelligence-deep-fakes-propaganda-war/
203. R. Booth, 'Russia's Trolling on Ukraine Gets 'Incredible Traction' on TikTok', *The Guardian* (May 01, 2022), https://www.theguardian.com/world/2022/may/01/russia-trolling-ukraine-traction-tiktok
204. Ibid.
205. Ibid.
206. Ibid.
207. Lin, 'Russian Cyber Operations in the Invasion of Ukraine'.
208. V. Akimenko and K. Giles, 'Russia's Cyber and Information Warfare', *Asia Policy* 15, no. 2 (2020): 67–75
209. S. Bendett, 'The Development of Artificial Intelligence in Russia', *Air University Press* 1, (2019): 168–77, 168.
210. Ibid.
211. Ross, Robert J., 'Information Advantage Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations', *The Cyber Defense Review* 6, no. 4 (2021): 63–74.

Disclosure statement

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

Notes on contributors

Lance Y. Hunter, PhD, is a Professor of International Relations in the Department of Social Sciences and Master of Arts in Intelligence and Security Studies programs at Augusta University located in Augusta, GA, USA. His expertise is in security studies and democratization. His research focuses on the causes and effects of terrorism and conflict, democratization, and the relationship between evolving technology and conflict.

Dr. Craig D. Albert, PhD, is Professor and Director of the Master of Arts in Intelligence and Security Studies at Augusta University. He received his PhD from the University of Connecticut in 2009. His areas of concentration include international security studies, ethnic conflict, cyberterrorism, and cyberwar.

Josh Rutland is a graduate of Augusta University's Master of Arts in Intelligence and Security Studies program. He is an Information Technology Specialist at the U.S. Army Cyber Command. His research focuses on information warfare, cybersecurity, terrorism, and biosecurity.

Kristen Topping is a recent graduate of Augusta University's Master of Arts in Intelligence and Security Studies program. Her research focuses on information warfare, social influence, and how in-depth cross-cultural understanding and language acquisition affect intelligence analysis.

Christopher Hennigan is an AI and Data Operations consultant in Deloitte's Government & Public Services group. He is a graduate of Augusta University's Master in Intelligence and Security Studies program. His expertise is in Six Sigma, business risks and mitigation, data and process analysis, and ML process automation. His research focuses on machine learning, cybersecurity, terrorism, and AI game modeling theory.