Six Inches to Victory: Digital Disinformation and War Time Support

The most important 6 inches on the battlefield is between your ears.

~ Secretary of Defense Jim Mattis

Winning in war depends on many things including resources (weapons, logistics, manpower), combat skill, and information. The informational aspects of war are frequently the subject of histories that focus on strategic and tactical intelligence that carry the day on the battlefield. Occasionally, histories focus on the disinformation activities that helped obfuscate military movements, intended objectives, or true resources available for the fight. Much of the discussion on information in war focuses on the active combatants, those who command or those who are called to arms. In the above quote former U.S. Secretary of Defense Jim Mattis is referencing the minds of those combatants actively engaged in combat. Yet, equally important to the minds of the men and women who fight are the minds of the populations that stand behind them. War is a battle of wills not solely between those with guns but also those without them. The contest for the minds of populations is a pernicious and ongoing battle. In recent years this battlefront has extended beyond airwaves, media broadcasts, and newspapers, to reside in powerful information communications devices that serve a steady stream of information to users. This stream of information is far more difficult to control and regulate than the mass broadcasts and information channels that predate the Internet.

Ukraine has been at war with the Russian Federation since the end of the Revolution of Dignity and the ouster of Russian backed President Viktor Yanukovych in early 2014. The war between Ukraine and the Russian Federation resembles many other wars that have come before, it has been bloody, contentious, defined by shifting battle lines, and filled with propaganda and disinformation. The war has also been defined by what has become known as hybrid or asymmetric operations that include information warfare, assassination, cyber-attacks, and economic warfare. Russian use of the information warfare has been particularly pronounced in Ukraine and has consistently sought to undermine the political, social, cultural, historical, and economic stability of the state. Many early narratives in 2014 and 2015 included preposterous stories of crucifixion, child rape, and more that were little more than repeated disinformation stories from prior conflicts conducted by Russia in Georgia and Estonia.

The information war in Ukraine has arisen as social networking and multimedia technologies have made enormous strides and became increasingly pervasive around the world. This information war is a war over the six inches of space between the ears of Ukrainian citizens and their global support network. It is a war that challenges the very nature of who Ukrainians consider

themselves to be and the perceptions that the world has of Ukrainians. This war is networked, integrated, and augmented by artificial intelligence and machine learning. Moreover, this war is 24 hours a day, seven days a week, and extends to the pockets of users (targets) around the world. Understanding the terrain of this conflict requires understanding how and where people access information and how information influences and alters human behavior.

In late 2013 Ukrainian President Viktor Yanukovych canceled a planned deal with the European Union in favor of a deal with the Russian Federation. The shift away from the European Union back towards Russia sparked nationwide protests that extended into online spaces.[1] At the time Internet penetration in Ukraine was still below 50%. Even fewer people used social media. In 2013 social media use was diversified across multiple platforms including Russian Social Media platforms Odnaklassniki, and V Kontakte, and U.S. based platforms Facebook and Twitter. Most citizens still relied on traditional media sources for news. Yet these platforms served as a starting point for substantial social mobilization.[2] Within these platforms and geographically over the various regions of Ukraine there remained substantial variation in support for regime change, but general societal sentiment towards a European orientation was high.

As protestors filled the streets of Kyiv a steady stream of online content began to emerge portraying the demographically diverse protest movement as neo-Nazi affiliated.[3] This narrative did not align with reality.[4] As the protests climaxed and ended in regime change, narratives of disinformation and propaganda seeking to undermine the fledgling Ukrainian state only gained momentum. In response over a period of several years the Ukrainian state sought to develop a robust national and civil society effort to combat disinformation.[5] Among the civil society actors combating disinformation were two prominent and organizations. StopFake.org was started at the Mohyla School of Journalism at the National University KyviMohyla Academy. StopFake.org took a journalistic approach to countering disinformation. As disinformation stories about Ukraine were propagated StopFake.org would take a one-by-one approach of documenting and correcting narratives. This approach could not and did not proport to address all disinformation activities targeting Ukraine, but rather sought to counter only those activities of significance with documented information providing factual counter narratives. By contrast another organization Inform Napalm took a crowdsourced approach that built a community of national and international volunteers to document and counter disinformation. Both organizations proved to be extremely successful at countering Russia's disinformation narratives in Ukraine. Both organizations also built robust multi-lingual websites to reach international audiences and enhance support for domestic concerns over disinformation narratives.

Further efforts to counter disinformation arose through the creation of an emergent open-source intelligence collective founded by former British journalist Elliot Higgins. Higgins began to apply new techniques in data mining, and imagery analysis to challenge disinformation narratives.

Countering disinformation was critical to societal resilience, stability, and the maintenance of international support. All three organizations faced one of the most prominent challenges when on July 17, 2014, Malaysian Airlines Flight 117 was shot down over Eastern Ukraine killing 283 passengers and 15 crew members. In the aftermath of the disaster, the Russia sought to portray Ukraine as responsible for the disaster and produced falsified images and documents proporting to implicate the Ukrainian state in its crash. Bellingcat, leveraging data mining, video and imaging analysis was able to develop a robust report on the events leading up to the destruction of MH117. The evidence collected placed responsibility on the Russian Federation and Russian backed separatists. Bellingcat's findings were later reiterated in a formal report by the Dutch government which investigated incident.

Each piece of disinformation put forward by the Russian Federation in Ukraine sought to undermine the validity and credibility of the fledgling state. By undermining its rival, Russia sought to weaken domestic and international support for the new government. By weakening support, Russia hoped to strengthen the position of its annexation of Crimea and its control over portions of Eastern Ukraine known as the Donbas. By fostering doubt in Ukraine, it was hoping to undermine societal cohesion and delay or weaken attempts to support Ukraine in its efforts to remain a sovereign state.

StopFake.org, InformNapalm, and BellingCat were effective at countering the Russian narrative and providing timely and accurate information in the early phases of the conflict. Yet as the conflict wore on from 2014 onward and eventually exploded into a far wider war in February 2022 it became increasingly evident that Russia's battle for the mind was beginning to expand and incorporate new technologies. Starting in late 2015 and early 2016 Russia began to leverage bots disseminate disinformation more efficiently through social media networks. Bots are autonomous programs on the internet or other systems which interact with users. Bots can be difficult to detect and are often used as tools of amplification. U.S. intelligence agencies identified as early as 2016 Russian tactics incorporating a combination of human generated content and bots to disseminate disinformation and to sow discord in advance of the 2016 U.S presidential elections.

These same tactics were visible in the run up to the Russian invasion of Ukraine in 2022. Large volumes of information were disseminated between 2014 and 2022 indicating that Ukraine was a fascist state run by neo-Nazis. Manufactured content was subsequently disseminated through numerous automated accounts on social media platforms. The intent of this dissemination through automated means was to saturate the Internet with a counter narrative and undermine the ability of viewers to decipher fact from fiction. In truth this content has had the effect of slowing or delaying the support of some major western powers, creating pro-Russian blocs within various allied states, and building support for Russian activities in Ukraine in various countries

around the world. Some Russian disinformation, initiated in 2014 and consistently cultivated and disseminated through automated networks sought to undermine the position of Ukraine to retain its status as a sovereign state. Disinformation on particular units of the Ukrainian military led to allies placing strong constraints on the provision of defensive weapon systems. Disinformation on Ukrainian military units and populations also sought to dehumanize them within international public opinion and within Russian domestic opinion.

In the buildup to the February 2022 Russian disinformation using traditional human and automated - bot-based dissemination fostered a Russian narrative of victimization and sought the obfuscation of true intentions. The narratives disseminated by the Russian Federation beginning in fall 2021 created what Winston Churchill once referred to as a "Bodyguard of lies" meant to obfuscate the truth that a dramatic escalation and expansion of 2014 war aims was imminent. This bodyguard of lies built and disseminated through social media platforms attempted to portray the massive buildup of Russian military force on Ukraine's borders as a training exercise. Large numbers of Russian bots and affiliated accounts pushed out information that any war was likely to be instigated by Ukrainian provocations all while building a narrative that Russia sought peace and stability. Reporting on the lead up to the conflict indicated that the impact of the sustained and partially automated disinformation campaigns likely undermined necessary Ukrainian military readiness and unity within allied coalitions seeking to avoid war and support Ukraine.[6] This sustained disinformation campaign weakened the psychological and material readiness of Ukraine and its allies and likely impacted the initial conduct of military operations resulting in Russian forces taking large swaths of the country early in the conflict.

While strategically and tactically information operations helped facilitate the initial escalation of the invasion of Ukraine they also served to control and weaken the dissemination of fact-based narratives of human rights violations perpetrated by Russian soldiers against the civilian populations of Ukraine. Using information networks, the Russian Federation attempted to disseminate disinformation claiming that civilian casualties were the result of indiscriminate Ukrainian military operations. Russian information operators attempted to hide evidence of rape, genocide, theft, and other activities. Often leveraging state affiliated social media accounts and affiliated bot networks, the Kremlin was able to amplify its voice and generate additional confusion. Organizations such as StopFake, InformNapalm, Human Rights Watch, the United States Department of State, dozens of news organizations were forced to not only write on the facts transpiring in Ukraine but also to address and correct deliberately falsified narratives of events. Social media firms were forced to increase network vigilance to identify and deactivate bot networks. Often the response of social media networks swung too far in correcting for Russian disinformation and led to the suspension of legitimate Ukrainian or western fact-based accounts. The battle for minds was constant and pervasive. It touched every platform in Ukraine

and beyond in Western allied nations. These automated amplifiers preyed on the free speech protections within liberal democratic societies.

By contrast within the Russian Federation new laws were adopted in advance of and at the beginning of the conflict that banned Western media and social media from the country. These laws made it illegal to disseminate information countering Russian official narratives and threatened users and firms with criminal prosecution. Individuals posting factual war-related information on Russian social media accounts had their accounts suspended and deactivated within a couple hours of making posts. Others who posted to Russian social media platforms were arrested and sentenced to lengthy prison terms or fined.

More than 9 months into the conflict the information environment is as contested as ever. The use of bots to control and shape narratives is ongoing. A combined effort of Ukrainian and Western Nations seems to have minimized but not eliminated the impact of information operations. Daily, numerous bot accounts are used to spread disinformation and undermine fact-based reporting. As amplification volumes increase so too does the need to counter disinformation narratives. Countering narratives is a time-consuming process that limits reporting on other issues of importance. Bellingcat and others have developed increasingly robust methods of identifying and countering misinformation, yet it is an uphill battle and efforts are often overwhelmed by a cascade of new narratives constantly being released. Integrating into the information environment a synergy of human and automated actors' Russian disinformation seeks to undermine and subvert the rational thought processes of its targets. It is waging a battle for the 6 inches between the ears of a global audience. It does this so that it can weaken resolve and undermine the unity among opposing nations. Automated disinformation reaches social media feeds wherever users are. Through obfuscation automated accounts attempt to sway the cognitive processes of its victims by pretending to be human or from reputable sources.

Discussion Question #1
Automated bots are programs designed to disseminate and amplify information via social media channels. Often these programs operate in violation of platform terms of service agreements and are subsequently removed. How should platforms address bots? What legitimate benefits might bots have in the present information society? Do the benefits of bots outweigh their costs?

Discussion Question #2
Social media has been a powerful supplement to free speech around the world and has been credited with facilitating democracy, civil rights, and human rights movements. How have social media, bots, and algorithms changed the way people receive and process information? Does the

combination of technologies listed in the previous question strengthen or undermine the decision processes of individuals?

Discussion Question #3
The Russian Federation has leveraged disinformation in many forms for decades. Its expansion into digital spaces began in the early 2000s and continued with its invasion of the Republic of Georgia in 2008, the initial invasion of Ukraine in 2014, the expansion of the conflict in 2022. Has the use of disinformation by the Russian Federation been an effective tool of state? Has it influenced the strategic, tactical, or operational actions of its own military, the militaries it is facing, or third parties? If so, where has this impact been most felt? What can be done to meaningfully counter any impact it has?

Discussion Question #4
Organizations such as StopFake.org and Inform Napalm have fought back against disinformation by providing counter narratives that debunk facts. There efforts are limited in scope and typically focus on countering one story at a time. Is this an effective way to combat disinformation? What other ways might organizations such as these counter disinformation campaigns? Does it matter that the campaigns they are countering are augmented by amplification bots?

Discussion Question #5
This case examines the impact of automated disinformation on the mental processes targeted individuals in a conflict situation. Does disinformation truly influence the minds of its targets? What are the implications of this influence? Have you been on the receiving end of disinformation? If so, how did you process that disinformation? Could you tell it was disinformation? Do you know if the disinformation was transmitted by a human user or by a bot?

Discussion Question #6
Many scholars and professionals discuss the need to foster critical thinking skills within populations as a mechanism to combat disinformation. Social media networks prey on how humans identify and assess the veracity of information by disseminating it through networks of friends and acquaintances whose opinions and thoughts we often value more strongly than those of strangers. How can you as an individual better prepare yourself for automated disinformation? How can you help others understand and assess information more critically?

Reflecting on 6 Inches to Victory

"The point of modern propaganda isn't only to misinform or push an agenda. It is to exhaust your critical thinking, to annihilate truth."
— Garry Kasparov

Gary Kasparov, former world chess champion and noted Russian dissident has consistently spoked out about Russian actions in Ukraine and elsewhere. In the above quote he identifies the power and danger resident within the propagation of disinformation. Disinformation attacks the most important attribute of the warfighter and the society behind them, the mind. It degrades and undermines the ability to process facts. Disinformation is not a new phenomenon. Evidence of disinformation in politics and war date back millennia. What is new are the means by which disinformation is disseminated. The use of bots to game and manipulate users and the algorithms that control the platforms through which they receive information pushes disinformation beyond the active engagement in media platforms, to a total and encompassing deluge penetrating social and informational interactions at all hours of the day and night and everywhere a person goes. The confluence of events including the increasing importance of mobile devices, the rise of social, media, and the development of bots that function in and through social media platforms creates a pervasive challenge to objective truth and rational, critical thought.

Among scholars, policymakers, and firms, there is concern that AI and ML bots combined with disinformation threaten the social cohesion of liberal democracies and the associated relationships of citizens and the state, and states in alliances. Disinformation absent automation has and is likely to also remain a problem. Automation leading to unconstrained amplification undermines the accountability individuals and actors disseminating information, it dehumanizes the targets by undermining their ability to process timely and accurate information, it undermines the integrity and legitimacy of interpersonal and social interactions in digital spaces.

Accountability: The automation of information dissemination through bots undermines basic notions of accountability. If information disseminated by an individual is demonstrably false such an individual can be held accountable for their actions through civil, criminal, and social constraints leading tangible penalties. Individuals who knowingly and repeatedly lie can be held liable libel law violations in many countries. Libel laws seek to protect potential victims from the deliberate dissemination of false information. Although libel laws can have a chilling effect on free speech, they also constrain the information space and dissuade disseminators from distributing knowingly false information. Within the United States the use of libel law to constrain certain forms of information is generally considered to be rare. Only in limited instances where material or psychological harm can be demonstrated are cases brought to trial. In such cases there must be a perpetrator and victim. A perpetrator can be a business, organization, institution, or even an individual. The law seeks to hold actors who knowingly disseminate false information

accountable within the constitutionally accepted bounds of the first amendment. Adjudication of responsibility once brought to trial is determined by a jury.

Accountability challenges become complicated as authorship becomes obfuscated through fake or falsified accounts, and when accounts comprise bots. Although many of the same principles of accountability and libel law are applicable to these types of accounts, especially if such accounts are able to be resolved back to a responsible party (individual, firm, etc.) the reality is that it is extremely difficult to trace many of these accounts. The inability to trace accounts limits their practical accountability. If a given bot generates content that is demonstrably false without direct human involvement neither the bot nor its human creator is likely to be held accountable. It is now possible for AIs to create bots which create content. This also further distances the responsible party (a software engineer) from the ultimate product that produces disinformation.

Further compounding the problem of automated disinformation is the time gap between the dissemination of information, its impact, and the time it takes to hold a disseminating party accountable. In the intervening months or years, the any accountable party has likely already exhausted the impact of a given disinformation campaign. Moreover, proving the impact of a disinformation campaign under libel law is difficult.

Dehumanization: Overwhelming individuals with deliberately false information undermines distorts and undermines human rights. Disinformation manipulates many of the core cognitive functions that underpin the exercise of rights in the Universal Declaration of Human Rights (UNDHR). Automated disinformation undermines article 19 of the UNDHR which states:

> *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

Through amplification via non-human bots the voices and opinions of those protected by article 19 are drowned in a cacophony of noise. Moreover, disinformation disseminated through bots distorts the opinion and expressions of individuals. This distortion skews the information space and undermines how individuals can receive, seek, and impart information. As fidelity is undermined it has a cascading impact on other critical articles of the UNHDR including *the right to free and fair elections* (Article 25) and *the right to health* (Article 12). In a corrupted information space individuals are unable to make decisions that advance their best interests. They are thereby dehumanized and provided only a simulacra rights.

Integrity and Legitimacy: It should come as no surprise that disinformation is a direct attack on information integrity and legitimacy. Integrity of information is vital for a range of human activities. As examined above in dehumanization, information that lacks integrity can undermine the right to health. Information disseminated pertaining to health care decisions such as vaccines, consumption of medications, or even basic care decisions including prophylactics that is knowingly false can have life or death consequences. Disinformation on vaccines can lead to global pandemics such as the Covid-19 pandemic that killed millions world-wide, or it can lead to individuals taking medications or substances that have severe side effects. In the case above on Ukraine a undermining the integrity of information can undermine efforts to document human rights violations, provide military support to an ally, or weaken a coalition of partners who might otherwise have rallied to the defense of a partner nation.

A large volume of information that lacks integrity can quickly overwhelm a small volume of information with high fidelity to reality. Additionally, information with low levels of integrity often draws substantially more attention than information with higher levels of integrity. Once bots are included in the mix, finding information with high levels of integrity can be the equivalent of finding a needle in a haystack. Pair with that information tailored to manipulate the way in which social media platform algorithms serve information and it is possible that many users will never see truthful information and instead be served a steady diet of disinformation.

A core attribute of disinformation campaigns is a desire to reduce the aggregate level of legitimacy among all sources of information. Through the process disinformation dissemination individuals becomes increasingly uncertain as to which sources are legitimate and which are not. This breaks down social trust among and within groups and societies. A breakdown in legitimacy undermines responses to problems across levels. It sows distrust that makes collective actions within communities and beyond nearly impossible.

There is a battle for the minds of individuals that is reshaping national and global politics. It can win wars and undermine alliances. This battle is often undertaken through dishonest automated and amplified technological means in expansive social networks. Winning this, the battle of the mind, constitutes that most important 6 inches in ensuring victory in war, social and political stability, and human rights.

---

[1] Aaron Brantly, "From Cyberspace to Independence Square: Understanding the Impact of Social Media on Physical Protest Mobilization During Ukraine's Euromaidan Revolution," *Journal of Information Technology & Politics*, 2019, 1–19, doi:10.1080/19331681.2019.1657047.
[2] Ibid.

[3] Chad W. Fitzgerald and Aaron F. Brantly, "Subverting Reality: The Role of Propaganda in 21st Century Intelligence," *International Journal of Intelligence and CounterIntelligence* 30, no. 2 (2017): 215–40, doi:10.1080/08850607.2017.1263528.
[4] Olga Onuch, "Who Were the Protesters?," *Journal of Democracy* 25, no. 3 (2014): 44 51, doi:10.1353/jod.2014.0045; Olga Onuch and Gwendolyn Sasse, "The Maidan in Movement: Diversity and the Cycles of Protest," *Europe-Asia Studies* 68, no. 4 (June 3, 2016): 556 587, doi:10.1080/09668136.2016.1159665.
[5] Aaron Brantly, "Battling the Bear: Ukraine's Approach to National Cyber and Information Security," in *Cybersecurity Politics*, ed. Myriam Dunn Cavelty and Andreas Wenger (London, UK: Routledge, 2022), 157–71, doi:10.4324/9781003110224-13.
[6] Shane Harris et al., "Road to War: U.S. Struggled to Convince Allies, and Zelensky, of Risk of Invasion," *The Washington Post*, August 16, 2022, https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-to-war/.