THE WEAPONIZATION OF FICTION AND TRUTH: DISINFORMATION AS HYBRID WARFARE AND ITS STRATEGIC USE IN THE UNITED STATES 2024 ELECTION

DOI: https://doi.org/ 10.37458/nstf.25.2.5
Review paper
Received: October 28, 2024
Accepted: December 12, 2024

Julia Lemmon*

Abstract: This article examines the growing role of disinformation in hybrid warfare, centering on its use in social media during the 2024 United States Presidential Election. While disinformation is as old as time, the methods and its mediums have evolved rapidly since Cold-War era propaganda and towards social media infiltration. These social media campaigns, first notably observed in the 2016 United States Presidential Election, highlights a new age of conflict and foreign

* Julia Lemmon is Intern at Konrad Adenauer Stiftung, Office of Croatia and Slovenia, Master's student of International Governance and Diplomacy with a Concentration in Global Risks at Sciences Po's Paris School of International Affairs. julia.lemmon@sciencespo.fr; julia_lemmon@hotmail.com

meddling, highlighting the global shift from classical military warfare to more subversive tactics. The article argues that disinformation, as a form of hybrid warfare, that emphasizes exploiting a target's societal vulnerabilities, exacerbating them to ultimately weaken the target from the inside-out and destabilizing, eroding, or even destroying, their political systems. Via an analysis of the 2024 United States election disinformation interference, following a recapitulation of its first presence in the 2016 election, this article examines the geopolitical dimensions and draws of disinformation warfare, the motives behind the foreign actors' interference, and the destabilizing results it fosters within the general public. Additionally, it begins a discussion of how similar disinformation strategies can be and have been utilized across other democracies in Europe, Asia, and beyond, threatening the current global order of liberalism and democratic superiority. The article concludes by emphasizing the importance of nations to invest into understanding and countering these new technological warfare tactics in order to properly protect, defend, and safeguard the integrity of their democratic governance. With disinformation and information hybrid warfare, amongst social media in particular, becomes the increasingly preferred method of confrontation with adversaries due to its low-risk, high-reward quality, it poses possibly the largest threat to global stability and threatens to upend the entire system, necessitating direct and immediate attention to address this vulnerability of our global infosphere.

Keywords: disinformation, hybrid warfare, elections, social media, foreign interference

Disinformation does not mean false information. It means misleading information— misplaced, irrelevant, fragmented, or superficial information— information that creates the illusion of knowing something but which in fact leads one away from knowing. In saying this, I do not mean to imply that

> *television news deliberately aims to deprive Americans of a coherent contextual understanding of the world. I mean to say that when news is packaged as entertainment, that is the inevitable result. And in saying that the television news show entertains but does not inform, I am saying something far more serious than that we are being deprived of authentic information. I am saying we are losing our sense of what it means to be well informed. Ignorance is always correctable. But what shall we do if we take ignorance to be knowledge?*
>
> Neil Postman, *Amusing Ourselves to Death: Public Discourse in the Age of Show Business,* 1985.

Introduction

Despite being written in the latter half of the 20th century and predominantly discussing the switch from print media to television news, the main point still withstands: we are losing our sense of what it means to be well informed, and what do we do if we take ignorance as knowledge? Even in the 1980s, disinformation was a topic being discussed and in the context of Americans no less. Surely it was not the same kind of conversation or the same kind of disinformation being conversed about today, but it was there. That alone provides the understanding that disinformation, in any of its diverse potential formats, is not new, is not irrelevant, is not imagined. For decades, disinformation has slowly plagued the ability for humans to become a well-informed citizenry. For the past eight years, at least, disinformation has plagued the American political system until it is almost entirely indistinguishable from factual information for the common American.

In the United States 2016 Presidential Election between Hillary Clinton and Donald Trump, a mass amount of disinformation haunted the American public. The same thing occurred in 2020 and in 2024, as well as slowly being spread into other countries around the world. In 2016, the disinformation within the US elections predominantly rested on Russia as the perpetrator. In 2024, Russia has been joined by China and Iran. What is it about disinformation that is so attractive to these established and/or rising, powerful nations? Does this mark the beginning of the end for the American era and classical warfare strategies? Is it a new beginning of new forms of hybrid and information warfare? Does it threaten to upend the entire world system, as it stands currently, based upon liberalism and democracy?

In the 2024 United States Presidential Election, the interference from Russia, China, and Iran (Atlantic Council, 2024) largely centered on, if not predominantly, the use of disinformation inside a broader campaign of information hybrid warfare. The key goal amongst all three interfering nations was one of weakening and destabilizing the United States: exacerbating existing tendencies, sewing division amongst the public as well as between the public and its government, and denigrating its global reputation. In an age where hybrid warfare is taking over armed conflicts as the preferred method of confrontation, disrupting the sanctity of the United States elections provides warnings and lessons for future nations, a glimpse into the desires of these rising authoritarian countries, and highlights just how destructive information and social media can be if the notion of being well informed continues to decline into confusing ignorance as knowledge.

In the first part of the article, what disinformation actually is will be discussed, taking special care of distinguishing between disinformation and misinformation as well as the spreaders of misinformation versus those that spread disinformation. While many may be implicated in spreading misinformation, not all can be attributed to spreading disinformation, even if what they have shared is disinformation itself. In its second part, disinformation will be discussed as a tool of hybrid warfare: the change from classical warfare to hybrid technological warfare and how it is destructive, if not borderline lethal, to not attach disinformation to the concept of hybrid warfare.

The United States 2016 Presidential Election will follow and be discussed as, arguably, the first, large-scale and internationally-staged event in which disinformation proved to be an important and impactful weapon. Eight years removed from that, with the publication of the United States' federal investigations published (United States Senate Select Committee on Intelligence, 2020)1, gives a unique inside-look to the findings, motives, and processes of disinformation of which can be then used as a blueprint structure for what future and similar disinformation campaigns may look like. A look at the 2024 United States Presidential Election in the fourth part of this article will show the staunch increase in the weaponization of information and social media as the newest and prioritized method of imposing external and foreign political will onto the elections of the highest office in one of the most powerful nations in the world. Finally, an analysis of what this means for the future,

[1] All volumes of the full report can be found: https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures

where the world can go from here, what lessons are needing to be learned from this, and how disinformation from the same perpetrator already threatens the sanctity of other nations ensues. Every government rests on its public being portrayed factual information and every public relies on its trust for said government institutions to present truthful findings. Disinformation threatens to dissolve the entire structure of modern civilization and democracy.

Disinformation: Development, Purpose, and Format

The use of propaganda has long been a normalized form of political warfare within campaigns, societies, elections, and authoritarian regimes. In its, arguably newest, usage and formation, alongside the rise of technological advancements and emphasis on mass dissemination of information and ideology, disinformation and misinformation have appeared. Disinformation is a particularly threatening form of misinformation (Fallis, 2015). While misinformation can be denoted as purely the spread of false or misleading information for whatever purpose, the distinction between misinformation and disinformation comes with deliberate intention. Disinformation is not only false or misleading information that is spread, but it is spread with the deliberate intention to mislead and/ or deceive those that view it (Shu et al,. 2020).

The European Commission, in 2018, produced a definition of disinformation denoting it as information that is false, misleading, and/ or inaccurate being promoted with the intent to cause public harm and/ or bring the promoter some personal benefit. In this definition, the European Commission staunchly

differentiates between misinformation and disinformation with the former being misleading/ false information that may cause harm without the disseminators' knowledge and the latter including the key categories of deception, potential for harm, and an intent to harm (Freelon and Wells, 2020). In essence, it is no mistake that disinformation misleads its consumers: it is pushed and spread by one or more individuals that are actively attempting to mislead the public (Fallis, 2015). Therefore, while proving intent may be difficult enough, any organized attempts to deceive the public by those involved in political propaganda and deliberately spreading false information can be thought of as disinformation (Guess and Lyons, 2020).

Most disinformation takes the form of either information out of context, partial truths, and lies, as well as fake alarms and conspiracy theories, all of which bring some type of benefit to the perpetrator. Disinformation tends to be more "novel" or unique than what the truth is, aiding in its mass dissemination by the consumers (Shu et al., 2020). It can be forged documents, doctored photographs, or even deceptive advertising (Fallis, 2015) by which information is moved from its proper context and into a new, misleading one. Disinformation messages, therefore, are used as munition within political information warfare in an attempt to degrade adversaries or opponents, similar to other traditional and/ or classical methods (Freelon and Wells, 2020). With the increasing importance of technology and the development of social media as a place for mass dissemination and connecting with billions of individuals, it is now easier than ever before to create and disseminate this inaccurate and deceptive

information (Fallis, 2015). The malicious actors who intend to spread fabricated information, for whatever their purpose may be, then turn to social media: the communication channel for the most rapid dissemination of said articles in order to reach a wide range of audiences (Shu et al., 2020).

There appears to be two main reasons for participating in the production of "fake news," the colloquial term (largely coined by former United States President Donald Trump) for disinformation: fiscal and ideological. Fiscally, news articles that go viral and amass millions of viewers can bring in large revenue streams from advertising. Ideologically, disinformation's novelty can be used to prioritize or push in favor of a preferred candidate in elections. Both reasons seem to have practical merit. Teenagers in North Macedonia produced stories favoring both Donald Trump and Hillary Clinton during the 2016 US presidential election campaigns that then resulted in them gaining tens of thousands of dollars in revenue, while the Romanian man who created and ran the disinformation site "endingthefed.com" did so solely to help Donald Trump's campaign (Allcott and Gentzkow, 2017). Of course, this disinformation, when used as political warfare, then erodes many necessary and integral parts of political processes including public trust, public beliefs, factual evidence, and more.

Disinformation tends to come from very few sources in the larger scheme, despite the different forms it can take when being disseminated. Relatively few users actually account for most of the traffic surrounding disinformation and these are likely bots. Their strategies, however, include amplifying false content and then

connecting themselves to influential, credible sites. Some disinformation sites will even adapt names similar to a credible source, such as disinformation site denverguardian.com, in an attempt to garner more legitimacy for the fake news they then spread (Guess and Lyons, 2020; Allcott and Gentzkow, 2017). These websites, however, tend to be short-lived, especially once identified as fake and subsequently shut down. By that point, though, the fake news they spread has already infiltrated the information stream on social media and the technological infosphere, shared vastly amongst societal users, particularly due to its novelty.

Novel, new, or unique information tends to be more valuable to people from a social perspective as it portrays the users sharing the information as being knowledgeable, involved, and credible for finding information that no one else knew (Shu et al., 2020). Because individuals are more likely to trust their social media contacts as it is usually individuals, they are friends with, trust, and/ or share a common belief system, this disinformation is then solidified as trusted news via confirmation bias and the echo chambers that exist within social media circles (Oehmichen et al., 2019; Shu et al., 2020). It is particularly true within highly polarized political societies and/ or highly polarizing information as individuals existing in those societies and participating in the polarizing ecosystem tend to be more willing to rationalize novel, sometimes extreme, disinformation if they agree with it. Therefore, disinformation not only deepens the divide amongst political communities and contributes to polarization, but it also relies on it for the disinformation to grow and stick within these communities. The diffusion of disinformation tends to occur during an "attention burst"

where there is high demand for a particular topic, making it more likely to gain traction and go viral (Guess and Lyons, 2020). Similarly to the theories of confirmation bias and echo changers, people also tend to trust information that is deemed 'trendy' (Shu et al., 2020), thereby making these attention bursts the perfect occurrence for mass dissemination of disinformation.

Regardless of all of this, besides contributing to direct harm of individuals consuming and spreading fake news/ disinformation, it also erodes societal trust in one another and larger, more credible news sources and, therefore, the society's ability to effectively share accurate information (Fallis, 2015). In the United States, for example, overall confidence in the larger news media companies (CNN, Washington Post, Fox News, New York Post, New York Times, etc) and their ability to fully, fairly, and accurately report and share information has fallen consistently since the 1970s in American society. It reached an all-time low in 2016 prior to the election (Freelon and Wells, 2020). This, of course, makes sense as it was the United States' 2016 presidential election that really thrust the topic of disinformation to the forefront of primary analysis for political science, information science, and communication. However, it is important to note that, while disinformation is extremely damaging to political spheres and societal cohesion, it is usually a very small fraction of the general public that is exposed to said disinformation and it is usually those who are older, highly engaged with political news, and more conservative-leaning (Shu et al., 2020).

Disinformation as a Modern, Technological Form of Hybrid Warfare

The world has seen a global shift in preferred methods of warfare amongst adversaries. What once was a community dominated by traditional military threats and hard power is now a society with preference for other non-kinetic, but still destructive, warfare methods including soft/ economic power and hybrid warfare. Kinetic conflict is no longer the preferred and primary strategy to impose political will on adversaries (Araźna, 2015). The pre-2014 understanding of hybrid warfare was, generally speaking, warfare that was neither purely irregular nor purely conventional, including characteristics of both (Solmaz 2022). However, post-2014, the understanding of hybrid warfare expanded to encompass non-violent, disruptive actions (2022). Hybrid warfare encompasses any type of action or strategy that is designed and utilized intentionally to weaken your target whether it be economic, environmental, or cultural (Splidsboel Hansen, 2017; Coldea, 2022).

Hybrid warfare's tools are asymmetrical and can additionally utilize informational tools such as proxies, diplomacy, terrorism, and/ or any other attack that is intended to either persuade or divide societies, or both (Qureshi, 2020). In other terms, hybrid warfare can be broadly considered as a greyzone conflict by which warfare tactics are employed, particularly ones that are aggressive or coercive, but that are specifically designed to remain below the threshold of traditional military conflict (Coldea 2022). Disinformation proves itself to be an extremely effective and useful tool within the toolkit of hybrid warfare. The state or actor that engages

in waging said hybrid warfare strategically identifies and targets vulnerabilities in their target state/ society which is then used to fuel the perpetrators' own interests (Splidsboel Hansen, 2017), hence why political polarization, for example, is both a precondition for and result of information hybrid warfare. There needs to be some vulnerability within the target society that can then be exploited for the perpetrators' gain. At the same time, these perpetrators exploit the ambiguity behind social media personas/ accounts and websites, therefore affording them the ability to infiltrate society's infospheres undetected, at least at first (Qureshi, 2020). The purpose of any hybrid warfare tactic, particularly true about the use of disinformation, is that the aggressors can reach their goals without risking full-scale retaliation from their opponents. The use of disinformation affords the aggressors' a certain degree of anonymity due to the tactics' ability to be misleading of its author and, again, blurring the lines between legal and illegal, traditional and nontraditional, and, thus, peace and war time (Coldea, 2022).

While NATO has never published an official definition of hybrid warfare, via their public pronouncements, it can be assumed that their definition is some kind of warfare that includes a wide range of covert and overt measures including civilian, paramilitary, and military through which the adversary tries to influence policymakers through subversive effort (Qureshi, 2020). The subversive effort here is key to the role that disinformation plays in hybrid warfare as adversaries can infiltrate their opponents' infosphere–somewhat undetected– and weaken or undermine the state and its institutions through said disinformation. There are limited characteristics of hybrid threats and warfare that

most observers agree upon, but one of the main ones is that it predominantly targets the democratic vulnerabilities within transparent societies, resulting in seriously deteriorating and destabilizing effects on the state actors, domestic environment, international order, and the government systems (Coldea 2022).

The decline in trust in the press amongst the American society, for example, and as previously discussed, has simultaneously occurred with declines of public faith in other democratic institutions of governance (Freelon and Wells, 2020), potentially highlighting an interconnection between the infiltration by disinformation, its negative impact on media trust and perception, and the decline in trust towards other contemporary governance institutions. This opportunity of fighting in the virtual/ cyber arena has now changed the dynamics of modern conflict, allowing for a party that may be weaker in resources or traditional warfare abilities to offset this via informational games that still have a highly destructive result and influence on societies, potentially to the extremity of social and political unrest (Araźna, 2015). The advantage of hybrid warfare then ultimately becomes its ability to significanlty impact mechanisms of social change with insecurity, while absorbing limited resources, and evading the international law of war by preventing a retaliatory attack via the armed forces of their aggressor or the activation of traditional defensive mechanisms (Livaja 2021).

The list of hybrid warfare tools, therefore, includes anything from propaganda, fake news, cyberwarfare/ cyber tools, domestic and international media, to social media (Qureshi, 2020).

In 2013, the then-Chief of the Russian General Staff, General Valery Gerasminov, published a piece that touched upon the future contours and structure of warfare which includes, according to him, a use of both kinetic and non-kinetic tools, as well as the blurring of lines between the military and civilian space, and the spreading of warfare from physical spaces into information spaces (Splidsboel Hansen, 2017). This distinction between kinetic and non-kinetic operations or tools can be understood as similar to the distinction between military power and more subversive/ persuasive power.

While kinetic power is the movement of material bodies, such as a military or armed group, the non-kinetic operations are ones that seek to influence a target audience through technological and/ or more modern means including electronic or print media, information warfare, etc. (2017). In 1989, William Lind, American author in discussing the fourth generation of warfare, stated, too, that the next generation of warfare would become more decentralized and asymmetrical via nonstate actors as well as contain an emerging preference of psychological and information operations over conventional war methods (Qureshi, 2020). Contemporary armed conflicts are increasingly using images and manipulating information into disinformation. The attractiveness of the virtual environment for this is that it connects to and has the ability to transmit information that can permeate all spheres of life, thereby allowing the virtual environment to be ideal for unconscious manipulation of the target population (Araźna, 2015).

Informational warfare provides a way to destabilize an enemy without exhausting resources, while also causing minimal disturbance to political relations and circumventing or evading international law because of the specific novelty of this tactic (Qureshi, 2020). As Sun Tzu's philosophy of war proclaims, the essence of war is to defeat the enemy in the shortest period of time possible with as little use of resources as possible (Livaja 2021). It was, in fact, Russia that first coined the term disinformation, desinformatsiya, (Freelon and Wells, 2020) and broadly utilized it as a hybrid warfare tactic. Russian thinkers often view disinformation as a 'chaos button' which can be used to inflict a level of chaos on the target state, causing and feeding instability to weaken the social fabric of said state, thereby also complicating and undermining the state's institutions, authority, and decision making.

The basic tenet of the Russian disinformation strategy that is seen continuously is the claim that "all news is constructed and therefore contested," (Splidsboel Hansen, 2017). This idea alone gives way to an understanding of Russian domestic and international propaganda that often promotes varying interpretations of certain events, all of which could be considered 'reality,' when, in fact, only one (if any at all) is the reality. In fact, a retired KGB Major General, Oleg Kalugin, described in a 1998 CNN interview that Russian active intelligence measures are not necessarily about collection, but subversion: weakening the West, sowing discord among allies to particularly degrade the United States in the eyes of the other countries and continents (United States Senate Select Committee on Intelligence, 2019). As will be discussed later, it is certainly true that the Russian disinformation that aided

in the election of Donald Trump in 2016, and potentially again in 2024, degraded the global perspective of the United States and the American public. The entire idea behind this Russian strategy of disinformation, both domestically and abroad, is to weaken the social fabric of trust societies have in their institutions to report and relay truthful, factual information of events to them. If this becomes increasingly questioned, societies become destabilized and more of their vulnerabilities show: vulnerabilities that can then be used by aggressors, such as Russia, for exploitation and personal benefit (Splidsboel Hansen, 2017).

The Dawn of Hybrid Warfare: Disinformation in 2016 United States Presidential Elections

Fake news and disinformation are generally published on social media, largely due to the fact that social media does not require verification for information to be published and it holds a huge potential audience (Qureshi, 2020). Social media has created giant new venues for Americans to participate in national political discourse as well as a channel for direct engagement with media representatives, elected officials, and individuals all around the world (United States Senate Select Committee on Intelligence, 2019). It is estimated that, in the final weeks of the 2016 election campaign, 27% of adult Americans (18+) visited a fake news source with either a pro-Trump or pro-Clinton skew (Grinberg et al., 2019; Guess, Nyhan, and Reifler, 2018). While seemingly a relatively small percentage, it amounts to over 65 million people in the United States (Guess, Nyhan, and Reifler, 2018).

There is also a persistent trend of conservatives consuming more fake news, according to Grinberg et al.'s study, with 60% of the engagement with fake news coming from the top 10% most conservative Americans (based on their previous research trends) (Grinberg et al. 2019). In comparing the top 20 fake news stories circulated on social media leading up to the 2016 election with the top 20 reputable news sites in that same time period, it is found that the fake news/ disinformation stories received higher interaction from the viewing audience (Hall, 2017). All of this is meant to highlight the extreme infiltration of disinformation into the 2016 United States presidential election campaign cycle.

In one study done by Allcott and Gentskow (2017), 156 fake news articles were examined, 41 pro-Clinton and 115 pro-Trump, which were shared on Facebook a total of 7.6 million and 30.3 million times respectively. With the viral spreading of these articles, the fake news now becomes more blended in with the rest of the other news being spread around, cementing it with some credibility despite the fact that it is entirely false. It is also estimated that one in four Americans visited a fake news website from October 7- November 14, 2016 with Trump supporters visiting the most fake news websites which were overwhelmingly pro-Trump disinformation: 40% of Trump supporters are estimated to have read at least one article from a pro-Trump fake news source compared to only 15% of Clinton supporters (Guess, Nyhan, and Reifler, 2018).

In another study, it was found that more than 100 fake news sites concentrating on the 2016 US election were largely promoting Donald Trump and his campaign

(Hall, 2017). There seems to be a higher plethora of and, therefore, higher exposure to pro-Trump disinformation (Allcott and Gentskow, 2017). Despite this, President Trump is said to have introduced a 'new chapter' to this long history of propaganda and fake news due to him being an establishment or institutional figure on an international stage that continuously denounced and degraded media for stories he deemed as untrue or biased (Boyd-Barrett, 2019). The figure that touts being strongly against disinformation and 'media lies' seemingly has the most positive disinformation in the infosphere.

It is important to note that a lot of this disinformation being spread, at least beginning at its creation, came from sources outside of the United States and, therefore, can be denoted as foreign election interference. Some evidence linked thousands of fake accounts on various social media platforms, including Facebook and Twitter (now 'X'), to operations by Russian trolls and hackers as well as some connected to Russia media outlets like RT and Sputnik (Hall, 2017). Most of this interference is said to come from 'troll factories' in which Russia employs hundreds of citizens with the primary responsibility of infiltrating the online information space with praise for the Russian government and criticisms for any of its opponents. A former employee at one of these troll factories has been quoted stating that they knew 'for sure' that there was a department for the United States 2016 elections (Splidsboel Hansen, 2017).

The Russian interference in these elections, coined with the phrase 'RussiaGate' by the US media and government, included three main directions: (1) Russian interference in non-transparent ways through social

media including false websites and pages or bots; (2) Russian hacking of the Democratic National Campaign and the Democratic Congressional Campaign Committee, as well as stealing of Hillary Clinton's private emails and delivery of said material retrieved through the hacks to big whistleblowers like Julian Assange and WikiLeaks, potentially in collusion with the Trump campaign; and (3) contact between the Trump Campaign and either members of the Russian government or Russians with close ties to the government, fueling the theories and claims that Trump acted as a 'Russian asset' via trading positive influence in his election for a promise of reducing US sanctions on Russia (Boyd-Barrett, 2019).

The largest form of Russian election influence or interference into the United States in 2016 came from a Russian organization called the Internet Research Agency (or IRA). This organization conducted widespread social media operations of spreading disinformation, targeting American audiences with the desired goal of sewing further discord into the American political system (Mueller, 2019). These operatives that worked on this within the IRA masqueraded as Americans and utilized advertisements, social media platforms, self-generated content, and intentionally false news articles to interact with and deceive millions of the United States' social media and online users. These operations particularly relied upon the easy polarization of Americans on societal, racial, and ideological differences. Above all else, Russia seemed to rely on the exploitation of human biases within America as a way to spread political misinformation (Oehmichen et al., 2019). The United States' Senate Select Committee on Intelligence, upon their investigation into Russian

election interference and publication of said investigation, stated that these operations were Russia's way to covertly support their favored candidate in the elections, Donald Trump (United States Senate Select Committee on Intelligence, 2019).

As is stated previously, in hybrid warfare, the aggressors design their warfare virus in accordance with what they believe is required to penetrate the targeted nation, either pointing towards a particular candidate or just to create chaos in society (Qureshi, 2020). It is very clear, as found in the investigation done by the Senate Select Committee, that the Russian government and the IRA sustained a hybrid warfare campaign directed at the United States in the predominant form of information warfare with the aim of influencing the American citizenry's thoughts about their government, fellow Americans, and themselves. In fact, former US Secretary of State, Rex Tillerson, stated himself that Russia's meddling in the 2016 election is an act of hybrid warfare (Solmaz 2022).

When analyzing the IRA's social media activities in the post-election time period after Trump's 2016 victory, it can be further understood that the Russian disinformation campaign was about more than just harming Clinton and supporting Trump, but it was, overall, targeted to undermine public belief and faith in the American democratic process (United States Senate Selection Committee on Intelligence, 2019). Further information learned via this investigation was that, as of January 2018, over 50,000 twitter accounts were linked to Russia and tweeting election-related content during the election and that the most targeted demographic of Americans by the IRA was African-Americans. Race

and related issues were highly preferred as the issue to sow discord with over 66% of the IRA's facebook advertisement content containing race-related terminology: one of its top performing Facebook pages, Blacktivist, generated 11.2 million engagements. Five of its top 10 Instagram accounts targeted African-American audiences and issues, its Twitter content heavily focused on issues with racial undertones such as the NFL kneeling protests, and that 96% of its Youtube campaigns and activities targeted police brutality and its intersection with race issues (United States Senate Selection Committee on Intelligence, 2019). The bottom line was that Russia's goal was to further exacerbate divisions and underlying tensions that were already prevalent in the United States as a way to destabilize American democracy (ASD Team, 2024), utilizing polarizing racial and identity issues as its fuel.

Russian disinformation and interference in the elections was not solely confined to disseminating disruptions that remained within the infosphere. Parts of it also included posing as Americans online and rallying in-person results within the United States' borders. While these Russian intelligence officers masqueraded as Americans online, 'real' Americans participated in the protests that were engineered and created over social media by the Russian operatives (ASD Team, 2024). Of course, the Americans participating in these protests in person were under the fair assumption that it was an 'all-American' protest. At the same time, the media campaigns were also used to get contact with and relative information from unassuming Americans. An IRA operative was found posing as an American and spoke with a Texas grassroots organization and learned that the focus of the Russian infiltration should be on so-called 'purple

states,' or swing states, such as Virginia, Florida, and Colorado (United States Senate Select Committee on Intelligence, 2019). The United States' Department of Homeland Security also found, in their own investigation, that Russian government hackers increasingly targeted the American election infrastructure of 21 different states ahead of this 2016 election, resulting in success for penetrating a small number of them (ASD Team, 2024).

Even further, Russian Maria Butina was indicted by the United States for operating as a Russian foreign agent and attempting to establish a 'back channel' with US politicians, further showcasing the breadth of Russian interference in the 2016 election beyond solely disinformation (ASD Team, 2024). After election day, the IRA and other Russian interference avenues increased their activity immensely and thereby confirmed that their attempt to infiltrate and degrade American democracy is bigger than one individual election (United States Senate Select Committee on Intelligence, 2019). The IRA's planning for the 2016 election dates back to at least 2014, clarifying that their campaign is a long-term operational plan of slowly eroding cohesion and unification within American society as well as between the general public and its government. In addition to this, it was found in the 2018 indictment of an accountant for the Russian IRA that the IRA's budget had increased by 70% between 2016 and 2019, highlighting further that the Russian interference did not begin, nor will it end, with any particular election (ASD Team, 2024). Of course, the Russian success in degrading Hillary Clinton and promoting Donald Trump during this election, so much so that he won the election, convinced almost every single authoritarian nation that

they needed to utilize this strategy for future gains (Kirkpatrick, 2024).

Amplification of Foreign Interference: Disinformation and Hybrid Warfare Campaigns in the 2024 United States Presidential Election

This, of course, then brings us to the recent United States presidential election in which Donald Trump was running against current Vice President Kamala Harris. While it is difficult to find verifiably false news and disinformation examples this soon after the election, certain things have appeared to be evidence of foreign meddling in this election cycle. Similarly to the standoff between Clinton and Trump in 2016, the volume of disinformation against Harris was exponentially more than disinformation against Trump (Steffen, 2024). And it was no longer solely Russia that was attempting to interfere with the election and the campaigns. Russia, Iran, and China were found to have increased their English-language disinformation in the months leading up to the election, of course, with varied motives (Cassidy and Klepper, 2024).

Many state that it should come as no surprise that these countries have ramped up their influence within and infiltration of US politics as rising powers will always and consistently come into conflict with top powers (Hardesty, 2024). In this election, it seems that Russia and Iran, in particular, are working even harder at election influence than they did in any other previous election (Kirkpatrick, 2024). Regardless of motives, Russia, China, and Iran's tactics were all the same, and garnered, in part, from the lesson found in the success of Russia's interference in 2016: using fake news and/ or misleading social media accounts and websites to

disseminate mass content meant to erode confidence in American democracy and election security (Cassidy and Klepper, 2024).

Some of the clearly verifiable and false fake news stories circulating in this election cycle included a video that appeared around October 24th which depicted mail-in ballots for Donald Trump being destroyed in Pennsylvania (Atlantic Council, 2024). The video showed an individual from Bucks County in Pennsylvania— a key swing county within a key swing state— supposedly sorting through mail in ballots, tearing up the ones marked for Trump and not touching the ones for Harris (Goldin, Catalini, and Swenson, 2024). Hours after this video surfaced, the Bucks County Republican Committee, with the Republican nominee being Trump who was shown as presumably having a disadvantage in the video, issued a post on the social media platform X stating "the actions seen in this video did not occur," (Vercellone et al., 2024). This video campaign was then later discovered to be part of something the United States federal government has named 'Storm-1516.'

As one of the largest Russian election interference campaigns throughout the 2024 election cycle, it is believed that it is a response for at least 52 different disinformation narratives that appeared online between August 2023 and October 2024 (Warren and Linvill, 2024). Officials from the FBI, in response to this widely circulated video, stated that they believe the video was manufactured and disseminated by Russian actors as part of the Kremlin's broader effort to increase skepticism and questions of uncertainty surrounding the integrity of the US elections, further sewing divisions in the

American public (Goldin, Catalini, and Swenson, 2024). Even concerning the aforementioned video depicting Trump ballots' destruction, the Bucks County District Attorney's Office issued a statement that stated the video was specifically meant to "undermine confidence in the upcoming election" with the Bucks County Board of Elections also stating that "[the] video is fake. The envelope and materials depicted in [the] video are clearly not authentic materials belonging to or disturbed by the Bucks County Board of Elections," (Vercellone et al., 2024). On the weekend of November 2nd and 3rd, the FBI additionally reported that a different video claiming they apprehended three groups for ballot fraud was false as well as a second video containing disinformation about Harris' husband, Doug Emhoff (Tarinelli, 2024). It is unclear whether these, too, were related to the Storm-1516 campaign or any other Russian disinformation campaigns.

Storm-1516 was also reported as responsible for and containing another staged disinformation video with an individual accusing Kamala Harris of a hit-and-run crime while the other large Russia disinformation campaign, Storm-1679, circulated an additional viral video that depicted a fake New York billboard sharing further false claims about Harris (Kirkpatrick, 2024). A key pillar of the Storm-1516 campaign was to distribute fake news pages containing AI-generated news stories stolen from real news sources, so as to garner some legitimacy, and then intermixing completely falsified stories (Warren and Linvill, 2024) in order to make it difficult to discern what was real and what was not. Social media personnel and influencers linked to Russia were also implicated in creating and disseminating disinformation videos and articles, particularly with the

goal of undermining the legitimacy of the United States elections and suggesting violent responses from the American public against one another on the basis of political preferences and alliances (Steffan, 2024). The Office of the Director of National Intelligence stated in an assessment that Russia "remains the predominant threat to US elections," identifying that Russian propagandists and operatives are planning to use social media to also try and undermine American support for Ukraine in key swing states (Lyngaas, 2024).

Perhaps the most tangible example of voter intimidation and persuasion via Russian interference was the series of bomb threats at election poll places in five battleground states on Election Day, some of which even resulted in temporary evacuations of said polling places (Cassidy and Klepper, 2024). These emails of bomb threats were traced back to Russian email domains, though those sending those emails may not have necessarily been Russian. As seen in 2016 and discussed previously, there have been fake news dissemination into the American social media sphere from North Macedonia, Romania, etc. Nevertheless, in an election security update published in September 2024 by the United States intelligence agencies, Russia has deployed the most disinformation and conspiratorial narratives, resulting in increased division amongst Americans on high-priority topics such as immigration, in order to help Trump's campaign while damaging the Democrats (Kirkpatrick, 2024).

The largest disinformation narratives against Harris were that she was involved in the aforementioned hit-and-run, already attributed to a Russian disinformation campaign, and one where she allegedly worked as a

prostitute at some point (Steffan, 2024). Particularly concerning her running mate, Tim Walz, disinformation campaigns came out that accused him of sexual abuse of a minor and one of his ex-students during his time as a teacher at Makato West High School (Warren and Linvill, 2024), an allegation that appeared less than a month before Election Day on October 16th, 2024. While these have not been clearly linked to Russian operatives as of late, Russia had a consistent pattern of creating and disseminating videos and false information with the aim of degrading Harris and Walz, highlighting their favor towards Trump (Cassidy and Klepper, 2024). The United States intelligence community continues to assess and assert that Russia prefers said former President over Harris as the next to hold the executive office of the United States (Kirkpatrick, 2024). This proved to be fairly similar to Russia's preferences, as well as tactics, in the 2016 election where they released exorbitant amounts of false stories about Trump's opponent, Hillary Clinton, as a way to not only disparage her, but uphold Trump as the 'better' candidate.

However, a staunch difference between the 2024 and 2016 US presidential elections is that of the specific actors involved in foreign election interference and dissemination of disinformation. While 2016 largely and predominantly concerned Russian interference, the 2024 election also saw interference from Iran and China, thereby proving Kirkpatrick's previously stated claim that Russia's success in influence in 2016 encouraged other adversaries to also get involved. Not only this, but it seems as though the two additional interferences from China and Iran had a slight difference in goals than that of Russia, but similar tactics. The intelligence community within the United States concluded that,

while Russia clearly prefers a Trump victory over Harris, Iran prefers Harris and China is seemingly not seeking to influence the specific outcome of the Presidential election (Kirkpatrick, 2024). Iranian operatives have been found liable in creating disinformation/ fake news outlets targeting both liberal and conservative communities, similar to Russia, as well as facilitating a hack against one one of the presidential campaigns that remain officially unnamed (Lyngaas, 2024).

However, the Department of Justice has indicted three Iranian actors with links to the Islamic Revolutionary Guard Corps for their entanglement in and association with a 'hack and leak' attack on the Trump campaign (United States Department of Justice Office of Public Affairs, 2024). Therefore, it can be strongly assumed that the previous 'unnamed hack' of a presidential campaign was that of Trump's, showing clear preference of Harris over Trump as the next American president. This is most likely the case due to Harris' preference in diplomacy when dealing with Iran over Trump's, arguably unhinged, comments and increasing threats of military power, such as his promise in his Times Magazine interview to defend and protect Israel should Iran attack them while he is president. One of the false news sites alleged to be connected to Iran called Trump an "opioid-pilled elephant in the MAGA china shop" as well as a "raving mad litigiosaur," (Lyngaas, 2024).

Iranian operatives and/ or those connected to Iran also carried out a hacking operation against the email of Roger Stone, long-term advisor to Trump (Myers, Hsu, Fassihi, 2024). Iran's hacking operations alongside its covert social media operations and campaigns highlight their attempt to not only undercut Trump's campaign and

candidacy, but also increase social discord and sew division amongst the American public ahead of the election (Lyngaas, 2024): a goal shared with a Russia despite their differing preferences for the electoral victory. In fact, while Iran has seemingly preferred to disparage Trump and his campaign, they have not left Harris and the Biden administration alone, further highlighting the predominance of their goal in fostering internal discord and degrading the American democratic system for not only the eyes of Americans to see, but the rest of the world too (Myers, Hsu, and Fassihi, 2024). This goal, similar to the Russian tactic, utilized things that were more social issues to divide the American public such as the topics of LGTBQ, gender reassignment surgeries, and even encouraging the student organized protests surrounding the Israel-Gaza conflict, going so far as to pose as students online and provide financial assistance for said protests (Lyngaas, 2024; Myers, Hsu, and Fassihi, 2024).

Chinese interference in the electoral process and presidential campaigns has, arguably, been the mildest seen thus far. It seems that, unlike Iran and China who seemingly have a preference for the victor of the election, China's main goal is really to just interfere and create division, absent of a preferred presidential candidate (Kirkpatrick, 2024; Lyngaas, 2024; Booth, 2024; Frenkel, Hsu, and Myers, 2024). In fact, in late October 2024, mere weeks before the presidential election, Chinese hackers targeted the cell phones used by Trump, his running mate JD Vance, and some of those associated with Harris' campaign (Klepper and Tucker, 2024), further highlighting their more or less equal treatment of the candidates in the presidential election and implying a neutral Chinese stance on the

matter. Rather, Chinese-linked online personas, occupying hundreds of thousands of accounts, instigated outrage around pro-Palestinian protests at American universities as part of the large Chinese disinformation campaign, Taizi Flood (Lyngaas, 2024; Frenkel, Hsu, and Myers, 2024). Taizi Flood, along with the other main Chinese disinformation campaign entitled Spamouflage or Dragonbridge, have both predominantly focused on disseminating inflammatory messages to fuel tensions and increase divisions, spread propaganda, and discredit a wide range of politicians (Booth, 2024). China has been found liable in the use of artificial intelligence in their influence operations (Kirkpatrick, 2024) including manipulated audio files, fabricated voter polls, and damaging memes (Frenkel, Hsu, and Myers, 2024). While not having a preferred candidate, their disinformation campaigns and infiltration into the American public social media spheres allows for them to capitalize on preexisting social divisions, heighten them, and thereby weaken their dominant adversary, the United States (Thibaut, 2024). Much of this, similar to Russia and Iran, seems to target social issues such as racial justice, immigration, economic inequality, and foreign conflicts such as Israel-Gaza and Russia-Ukraine (Booth, 2024; Thibaut, 2024). Rather than preferring one candidate over another in the presidential election, China's interference seems to target anyone and everything that holds anti-Chinese policies in order to advance their own interest (Nazzaro and Vakil, 2024) and increase social unrest so as to draw the US focus away from the international realm as well as weaken their reputation in the eyes of the world.

This does not mean that China's interference lacks a significant threat to the state of the American public,

democracy, and sustainability of the nation. In fact, China's strategy and where the focus of its interference lies is not even predominantly within the American presidential elections, but in the local and state elections and 'down-ballot' candidates (Booth, 2024). Their disinformation campaigns focus on those that are specifically critical of the Chinese Communist Party (Thibaut, 2024) as well as these down-ballot candidates' position on Taiwan (Klepper and Tucker, 2024). China's use of disinformation as their primary influence tools within the US elections, as well as their focus on local and state elections more so than presidential elections, highlights their predominate aim to further facilitate a fragmented American political environment that thereby weakens national unity and resilience, as well as the Chinese understanding of the difficult level in swaying American politics at a national level especially when pertaining to their own nation (Booth, 2024; Thibaut, 2024).

This is most likely due to the bipartisan consensus within the United States that China is the United States' largest and most important adversary with both dominant American political parties having less than desirable policies towards China in China's perspective. Therefore, their focus on the 'smaller' elections could imply China's preference and tendency for the long game: building relationships with and aiding in the campaigns of politicians who could eventually benefit and advance China's interests, creating a more China-friendly political ecosystem within the United States, and to denigrate the American ability to act coherently both domestically and abroad (Booth, 2024; Lindsay, 2024). This strategy, of course, aligns with China's cognitive warfare philosophy that calls for internally

weakening the enemy from within, thereby 'affecting their will to fight' (Thibaut, 2024). With China being the United States' predominant adversary that continues to threaten the American position in the international world, the weakening from within at every level allows them a certain kind of pathway to potentially soar past the US in the global arena and overtake as the 'world hegemon.'

World War 3: The Global War on Truth and the Importance of Disinformation Alliances and Information Resilience in Safeguarding Democracy

Foreign interference, disinformation, propaganda campaigns, and alike are not new to society or the United States specifically. In fact, the United States itself has meddled in other countries' affairs frequently in the past. It should, therefore, not come as a surprise that other nations and rising powers will then attempt to repay that and get retribution, whether for themselves or just in general to increase their own power vis-a-vis their largest perceived adversary. At the same time, implications of this election interference, particularly when concerning the stark increase of it between the eight-year span of the 2016 election and the 2024 election, marks a new version of hybrid warfare facing the United States and the strength of challenges that threaten the very foundation upon which the United States rests in the global world.

Disinformation as a tool of hybrid warfare allows for the internal degradation of an enemy or adversary with less devotion of resources in comparison to other classical warfare methods like military warfare. It also is often a less polarizing version of warfare. While this may not matter as much in authoritarian regimes compared to

democracies, authoritarian rulers, particularly the modern-day ones, are still required to maintain the image of societal support so as to avoid a coup or mass uprisings. The United States continues to have the strongest, most highly funded military in the world.[2] Since no nation could see a clear-cut victory without suffering significant blows if they engaged in a military, kinetic conflict with the United States, hybrid information warfare via the use of disinformation almost levels the playing fields a bit more. It truly does allow the perpetrators to exacerbate and attack the vulnerabilities of their target without suffering significant consequences themselves. In this case, the vulnerabilities within the United States are the highly polarizing topics, mainly social ones such as immigration, foreign conflicts, and identity politics.

Russia, China, and Iran particularly targeting these things, especially during an attention burst like they did with the increasing American outrage over the Israel-Hamas situation, highlights a keen awareness and understanding of the American society and political system. Because information warfare and disinformation are significantly less explicit and detectable than kinetic conflict, it not only allows the perpetrators to engage in warfare campaigns with significantly less threat of public disapproval and fracture, but it also allows them to do so with less traceability from their targets.

It remains a highly clever and strategic tactic to attack your adversaries behind a thinly veiled curtain of ignorance. By impacting the information environment of

[2] The Fiscal Year 2025 United States Department of Defense budget is set at 849.8 billion USD (roughly 808.9 billion EUR). For an entire breakdown of the budget, more information at: https://comptroller.defense.gov/Budget-Materials/Budget2025/

the societies within your target, the aggressors are able to slowly change the tides into their preferred political outcomes. This could also explain why China does not seem to have a strong preference of Harris versus Trump, considering neither of them will provide China with preferred political outcomes.

Russia, China, and Iran all have their own distinct goals, preferential outcomes, and reasonings for interfering in the election and mass dissemination of disinformation. Russia clearly prefers a victory of Donald Trump, of which the Kremlin is likely rejoicing within their recent success. Trump has long been less of a hardliner on American policy towards Russia in comparison to the Democratic candidates: Clinton in 2016, Biden in 2020, and Harris in 2024. Therefore, the majority of their disinformation interference would surely aim at promoting Donald Trump while degrading its competition, whomever it may be depending on the race. In 2024, of course, it was Kamala Harris and her running mate Tim Walz. Iran, on the other hand, seemed to prefer a Harris victory, no doubt due to, as mentioned before, her preference for diplomacy over force when dealing with them.

China, interestingly enough but not entirely unsurprisingly, seems to remain quite neutral in presidential candidate preference, resulting in a focus on local and state campaigns that contain candidates staunchly divided on US-China relations and positions. Despite all of these different preferences, the three unite in their desire for disruption of the American political society and system. These differences and unification means a multitude of things as well as potentially signifying some future decisions requiring attention.

First, their domination in US election interference points to all three nations viewing the United States as their chief adversarie: a statement with no new implications. Prior to this article, it should have been well known that they would all share in their number one adversary. Depending on how the chips fall within the near future, this could push the already-forming authoritarian geopolitical bloc closer together. If Russia, China, and Iran can put aside their solely self-serving interests to fully align with one another in their desire to weaken the United States, it could result in an expedited demise of the 'American Era' that is currently being exhibited.

At the same time, their clear differences in aims and goals, despite using the similar tactics of disinformation, could pose a problem for a full unification and alignment amongst them. Russia is, after all, promoting a candidate that has less than friendly opinions on how to deal with Iran and vice versa. Could these countries unite temporarily under the shared desire to denigrate the United States' global leadership? Potentially, but it is unclear how long that would last and this would be a topic for another article, especially considering the political psychology that would come into play. We have already seen a rising formation of geopolitical blocs: the West versus an authoritarian bloc. These currently play out within 'middle ground' states that are towing the line in their alliances such as India, Serbia, and many African nations. The continued election interference and spread of disinformation within the American social media echo chambers and spheres done by their largest adversaries could force the United States to focus inward on reunification, potentially distracting them enough for China, Russia, and/ or Iran to win over these middleground states in allegiance.

Second, the United States' impact by said disinformation could foreshadow the eventual fate that will be extended to the rest of the West and particularly Europe.

The United Kingdom, France, and Germany have all been increasingly impacted by the Russian disinformation campaign called Doppelganger as well as Italy, but not as severely as the aforementioned European nations. Swarms of social media accounts across the EU flooded social media chambers with disinformation right before and leading up to the European Parliament elections this past June and promoted far-right political discourse particularly in France and Germany (Thomas, 2024). Reports in France uncovered Russian disinformation efforts to undermine France for their hosting of the 2024 Summer Olympic Games and President Emmanuel Macron who remains one of the most vocal Ukraine supporters in Europe (Hinnant, 2024). Russian actors have created fake websites under the guise of reputable national media outlets and government and fake accounts on social media in an attempt to spread disinformation and foster division in France (Colonna and the France Ministry of Foreign Affairs, 2023), particularly over the conflict with Israel-Gaza in which 1000 social media bots linked to Russia posted falsified photos of graffitied Stars of David in Paris (Hinnant, 2024).

In Germany, Russian disinformation campaign, Doppelganger, cloned websites, produced misleading and false social media posts that usurped the identity of European media outlets, and fabricated articles, all of which pushed pro-Russian narratives (Delcker, 2024). Tens of thousands of fake accounts on social media platform, X, pushed disinformation messages in the

German language that implied Olaf Scholz's government was neglecting German citizens and their needs, distracted by his support of Ukraine with both weapons and aid provided and allowing an influx of a million Ukrainian refugees into Germany (Connolly, 2024). The United Kingdom placed sanctions on six Russian agencies and individuals involved in a disinformation network within their borders that spread false information and rumors about the Princess of Wales (Coughlan, 2024). Since 2022, Russia has been linked to sponsoring 80 different documented disinformation campaigns in 22 different African countries (Foreign, Commonwealth and Development Office and Zainuddin, 2024).

Chinese disinformation has spread into Taiwan, particularly so during the Taiwanese elections in January 2024 where China spread false information in an attempt to discredit William Lai and/ or other political leaders that may be supportive of Taiwanese independence (Colley, 2024; Voo, 2024). With the growing alliance between the Philippines and the United States, China's disinformation has begun infiltrating them as well with the goal of promoting political figures in the Philippines that support the Chinese position in the region (Voo, 2024). With India rising exponentially in power and importance, China has expanded a misinformation warfare campaign against them, too, concerning anything from India's G20 presidency to spreading lies that fuel the tensions between Canada and India over the killing of Hardeep Singh Nijjar, a Kahlistan sympathiser (Sagar, 2023). Of course, as is expected, Iran's disinformation campaigns are also not limited to the United States with much of it also attempting to infiltrate the Israeli public and garner support and legitimacy for

the Iranian government and its actions. When Iran launched missiles at Israel in April 2024, Iranian state TV showed footage of destruction, claiming it was the damage done in Israel on behalf of Iran's efforts and missiles, when, in reality, it was footage from wildfires in Chile (Frances-Wright and Ayad, 2024; Jingnan and Joffe-Block, 2024).

All of this is meant to say that the disinformation occurring in the United States as a way to not only impact the outcomes of the American elections and electoral processes, but also as a way to exacerbate divisions and amplify weaknesses and vulnerability amongst the American public is not occurring within a vacuum. The same nations disrupting the American elections and inundating the American public with disinformation are launching disinformation campaigns into a vast majority of other countries. Should these nations achieve their goals of toppling the United States in the global world and weakening/ breaking it down, they could potentially redirect some of the resources that are currently occupied by the information warfare campaign against the United States to other target states such as the ones listed above. The rest of the world, whether American allies or fast-rising nations, could use the American election interference as a lesson or blueprint of how to best insulate their nations from future increased disinformation attacks on themselves.

Finally, the quick spread of disinformation and information hybrid warfare by these nations can be used as a blueprint for a new age of war and counter-threat fighting and tactics. The chances of geopolitics and great power competition dwindling out of importance is severely unlikely, if not impossible. While the United

States, for example, could sustain a good campaign in a kinetic (military) conflict with China, Russia, or Iran, if the fighting has switched to cyberspace and morphed into technological hybrid warfare, it would not be an equivalent retaliation. While physical damage forces funds and monetary resources to be diverted to its rebuilding, cyberspace and warfare in the information environment can and do have lingering impacts for generations after said physical damage would be rebuilt.

This, in itself, is evident in how the American people continue to view Russia in the post-Cold War era as a result of the anti-Soviet propaganda from that time. There is little to correctly dictate why the American public has been so susceptible to believing disinformation in comparison to the French public, German public, or alike. In fact, there may be no difference in the susceptibility with the difference in impact being solely due to the sheer amounts of resources being dedicated to disinformation for the United States versus other countries. Regardless, it can only be assumed that this type of hybrid warfare will become increasingly used and preferred for all nations, organizations, and/ or terrorist groups attempting to harm adversaries, therefore making it incredibly important that nations understand this implication, its potential impact, and devise effective strategies on how to counter it whether it be as drastic as an overhaul of the media system or simply creating tighter restrictions and requirements for creating a social media account.

The unfortunate thing about the disinformation world and its medium of social media is that it inherently lacks insulation: part of the purpose of social media is for vast connection across the globe and mass dissemination.

However, just like everything else, it can be weaponized for bad or utilized for good. It is time that nations devote resources to the strategic use of social media to counter this spread of disinformation and mitigate its impacts on its public population. In truth, fighting in this technological information space is the only clear way, as of right now, to fight against the rapid increase in disinformation hybrid warfare.

> *Contrary to common belief even among the educated, Huxley [the author of Brave New World] and Orwell [the author of 1984] did not prophesy the same thing. Orwell warns that we will be overcome by an externally imposed oppression. But in Huxley's vision, no Big Brother is required to deprive people of their autonomy, maturity, and history. As he saw it, people will come to love their oppression, to adore the technologies that undo their capacities to think. What Orwell feared were those who would ban books. What Huxley feared was that there would be no reason to ban a book, for there would be no one who wanted to read one. Orwell feared those who would deprive us of information. Huxley feared those who would give us so much that we would be reduced to passivity and egoism. Orwell feared that the truth would be concealed from us. Huxley feared that the truth would be drowned in a sea of irrelevance.*
>
> Neil Postman, *Amusing Ourselves to Death: Public Discourse in the Age of Show Business*, 1985.

Literature:

1.Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake News in the 2016 Election." Journal of Economic Perspectives, vol. 31, no. 2, May 2017, pp. 211–36. DOI.org (Crossref), https://doi.org/10.1257/jep.31.2.211.

2.Araźna, Marzena. “Conflicts of the 21st Century Based on Multidimensional Warfare – ‘Hybrid Warfare’, Disinformation and Manipulation.” Security and Defence Quarterly, vol. 8, no. 3, Sept. 2015, pp. 103–29. securityanddefence.pl, https://doi.org/10.5604/23008741.1189421.
3.ASD Team. “Fact Sheet: What We Know about Russia’s Interference Operations.” German Marshall Fund of the United States (GMF), 2024, https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations.
4.Atlantic Council. “Interference 2024: The 2024 Foreign Interference Attribution Tracker: A Project of the Digital Forensic Research Lab (DFRLab) of the Atlantic Council.” Atlantic Council DFR Lab, Oct. 2024, https://interference2024.org/.
5.Booth, Barbara. “China’s New Focus in U.S. Elections Interference Is Not Harris-Trump Presidential Race.” CNBC, 15 Oct. 2024, https://www.cnbc.com/2024/10/15/chinas-new-focus-election-interference-local-state-races.html.
6.Boyd-Barrett, Oliver. RussiaGate and Propaganda: Disinformation in the Age of Social Media. 1st ed., Taylor & Francis Group, 2019. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/sciences-po/detail.action?docID=5813232.
7.Cassidy, Christina, and David Klepper. “The Us Election Was Largely Trouble-Free, but a Flood of Misinformation Raises Future Concerns.” AP News, 8 Nov. 2024, https://apnews.com/article/election-2024-security-voting-cybersecurity-misinformation-5fcf17a888ac25855a9feda62d9be50a.
8.Coldea, Florian. “Intelligence Challenges in Countering Hybrid Threats.” National Security and the Future, vol. 23, no. 1, Feb. 2022, pp. 49–66. DOI.org (Crossref), https://doi.org/10.37458/nstf.23.1.2.
9.Colley, Thomas. “The Impact of Disinformation: Contrasting Lessons from the UK.” Australian Institute of International Affairs, Oct. 2024, https://www.internationalaffairs.org.au/australianoutlook/the-impact-of-disinformation-contrasting-lessons-from-the-uk/.
10. Colonna, Katherine, and France Ministry of Foreign Affairs. “Statement by Ms Catherine Colonna- Foreign Digital

Interference – France's Detection of an Information Manipulation Campaign (2023)." France Diplomacy - Ministry for Europe and Foreign Affairs, June 2023, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2023/article/statement-by-ms-catherine-colonna-foreign-digital-interference-france-s.

11. Connolly, Kate. "Germany Unearths Pro-Russia Disinformation Campaign on X." The Guardian, 26 Jan. 2024, https://www.theguardian.com/world/2024/jan/26/germany-unearths-pro-russia-disinformation-campaign-on-x.

12. Coughlan, Sean. "Sanctions for Russian Misinformation Linked to Kate Rumours." BBC, Oct. 2024, https://www.bbc.com/news/articles/c4g2x3kr6lgo.

13. Delcker, Janosch. "Russian Disinformation Is Growing in Germany – Dw – 10/15/2024." Dw.Com, Oct. 2024, https://www.dw.com/en/russian-disinformation-is-growing-in-germany/a-70506294.

14. Fallis, Don. "What Is Disinformation?" Library Trends, vol. 63, no. 3, 2015, pp. 401–26.

15. Frances-Wright, Isabelle, and Moustafa Ayad. "Misleading and Manipulated Content Goes Viral on X in Middle East Conflict." Institute for Strategic Dialogue, Apr. 2024, https://www.isdglobal.org/digital_dispatches/misleading-and-manipulated-content-goes-viral-on-x-twitter-in-middle-east-conflict-iran-israel-strikes/.

16. Freelon, Deen, and Chris Wells. "Disinformation as Political Communication." Political Communication, vol. 37, no. 2, Mar. 2020, pp. 145–56. Taylor and Francis+NEJM, https://doi.org/10.1080/10584609.2020.1723755.

17. Frenkel, Sheera, et al. "How Russia, China and Iran Are Interfering in the Presidential Election." The New York Times, 29 Oct. 2024, https://www.nytimes.com/2024/10/29/technology/election-interference-russia-china-iran.html.

18. Goldin, Melissa, et al. "Russian Actors Made Fake Video Depicting Mail-in Ballots for Trump Being Destroyed, FBI Says." AP News, 25 Oct. 2024, https://apnews.com/article/misinformation-fact-check-trump-

ballots-destroyed-pennsylvania-d75fdc56c71d77c7a48d8fca96b03288.

19. Grinberg, Nir, et al. “Fake News on Twitter during the 2016 U.S. Presidential Election.” Science, vol. 363, no. 6425, Jan. 2019, pp. 374–78. DOI.org (Crossref), https://doi.org/10.1126/science.aau2706.

20. Guess, Andrew, et al. “Selective Exposure to Misinformation: Evidence from the Consumption of Fake News During the 2016 U.s. Presidential Campaign.” European Research Council, Jan. 2018.

21. Guess, Andrew, and Benjamin Lyons. “Misinformation, Disinformation, and Online Propaganda.” Social Media and Democracy: The State of the Field and the Prospects for Reform, edited by Nathaniel Persily and Joshua Tucker, Cambridge University Press, 2021.

22. Hall, Holly Kathleen. “The New Voice of America: Countering Foreign Propaganda and Disinformation Act.” First Amendment Studies, vol. 51, no. 2, July 2017, pp. 49–61. DOI.org (Crossref), https://doi.org/10.1080/21689725.2017.1349618.

23. Hardesty, Greg. “Foreign Election Interference Has a Long History.” USC Price, 1 Nov. 2024, https://priceschool.usc.edu/news/foreign-election-interference-has-a-long-history/.

24. Hinnant, Lori. “Russian-Linked Cybercampaigns Put a Bull’s-Eye on France. Their Focus? The Olympics and Elections.” AP News, 4 July 2024, https://apnews.com/article/france-election-disinformation-russia-olympics-be18d688677240686df200096018f221.

25. Jingnan, Huo, and Jude Joffe-Block. “As Iran Attacked Israel, Old and Faked Videos and Images Got Millions of Views on X.” NPR, 16 Apr. 2024, https://www.npr.org/2024/04/16/1244920615/iran-israel-fake-social-media-disinformation.

26. Kirkpatrick, David D. “The U.S. Spies Who Sound the Alarm About Election Interference.” The New Yorker, 21 Oct. 2024. www.newyorker.com, https://www.newyorker.com/magazine/2024/10/28/the-us-spies-who-sound-the-alarm-about-election-interference.

27. Klepper, David, and Eric Tucker. “Foreign Threats to the Us Election Are on the Rise, and Officials Are Moving

Faster to Expose Them." AP News, 26 Oct. 2024, https://apnews.com/article/trump-harris-russia-iran-china-disinformation-election-6f4cb99be3facb08c58cecd11b2c5d41.

28. Lindsay, James M. "Election 2024: China's Efforts to Interfere in the U.S. Presidential Election | Council on Foreign Relations." Council on Foreign Relations, Apr. 2024, https://www.cfr.org/blog/election-2024-chinas-efforts-interfere-us-presidential-election.

29. Livaja, Jerko. "Decentralized Security Systems in Hybrid War Conditions with an Emphasis on the Security System in Bosnia and Herzegovina." National Security and the Future, vol. 22, no. 3, Dec. 2021, pp. 89–99. DOI.org (Crossref), https://doi.org/10.37458/nstf.22.3.2.

30. Lyngaas, Sean. "Iran Steps up Influence Campaign Aimed at Us Voters with Fake News Sites, Microsoft Says." CNN Politics, 9 Aug. 2024, https://www.cnn.com/2024/08/09/politics/iran-nfluence-campaign-microsoft-report/index.html.

31. Miranda Nazzaro, Caroline Vakil. "China's Alleged Interference in Us Elections Prompts Worries up and down Ballot." The Hill, 27 Oct. 2024, https://thehill.com/policy/technology/4954346-chinese-influence-us-election-meddling/.

32. Mueller III, Robert S. Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volume I of III. Investigation Report, Volume 1, U.S. Department of Justice, Mar. 2019.

33. Myers, Steven Lee, et al. "Iran Emerges as a Top Disinformation Threat in U.S. Presidential Race." The New York Times, Sept. 2024, https://www.nytimes.com/2024/09/04/business/media/iran-disinformation-us-presidential-race.html.

34. Nazzaro, Miranda, and Caroline Vakil. "Alleged Chinese Influence Campaigns Intensify Worries About U.S. Election Meddling." The Hill, 27 Oct. 2024, https://thehill.com/policy/technology/4954346-chinese-influence-us-election-meddling/.

35. Oehmichen, Axel, et al. "Not All Lies Are Equal. A Study Into the Engineering of Political Misinformation in the 2016 US Presidential Election." IEEE Access, vol. 7, Aug.

2019, pp. 126305–14. IEEE Xplore, https://doi.org/10.1109/ACCESS.2019.2938389.

36. Postman, Neil. Amusing Ourselves to Death: Public Discourse in the Age of Show Business. Viking Penguin Inc., 1985.

37. Qureshi, Waseem Ahmad. "The Rise of Hybrid Warfare." Notre Dame Journal of International & Comparative Law, vol. 10, no. 2, 2020, pp. 173–208.

38. Sagar, Pradip R. "How China Has Unleashed a Misinformation War on India." India Today, 18 Oct. 2023, https://www.indiatoday.in/india-today-insight/story/how-china-has-unleashed-a-misinformation-war-on-india-2450656-2023-10-18.

39. Shu, Kai, et al. "Combating Disinformation in a Social Media Age." WIREs Data Mining and Knowledge Discovery, vol. 10, no. 6, July 2020, p. e1385. Wiley Online Library, https://doi.org/10.1002/widm.1385.

40. Solmaz, Tarik. "'Hybrid Warfare': A Dramatic Example of Conceptual Stretching." National Security and the Future, vol. 23, no. 1, Feb. 2022, pp. 89–102. DOI.org (Crossref), https://doi.org/10.37458/nstf.23.1.5.

41. Splidsboel Hansen, Flemming. Russian Hybrid Warfare: A Study of Disinformation. Research Report, 2017:06, DIIS, Danish Institute for International Studies, 2017.

42. Steffen, Sarah. "Fact Check: Disinformation's Impact on the Us Election." DW, Nov. 2024, https://www.dw.com/en/fact-check-what-role-did-disinformation-play-in-the-us-election/a-70729575.

43. Tarinelli, Ryan. "Us Agency Warns of 'Fire Hose' of Disinformation About the Election." Roll Call, 4 Nov. 2024, https://rollcall.com/2024/11/04/us-agency-warns-of-fire-hose-of-disinformation-about-the-election/.

44. Thibaut, Kenton. "Trends in China's Us Election Interference Illustrate Its Longer Game." DFRLab, 4 Nov. 2024, https://dfrlab.org/2024/11/04/china-us-election-interference/.

45. Thomas, James. "Vast Disinformation Networks Hit Europe Ahead of EU Elections." Euronews, July 2024, https://www.euronews.com/my-europe/2024/07/18/huge-

disinformation-networks-ensnared-france-and-germany-ahead-of-eu-elections.

46. United States Senate Select Committee on Intelligence. (U) Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election; Volume 2: Russia's Use of Social Media with Additional Views. Investigation Report, 116–XX, United States Senate, Oct. 2019.

47. U.S. Department of Justice Office of Pulblic Affairs. "Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election." Office of Public Affairs U.S. Department of Justice, 27 Sept. 2024, https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us.

48. Vercellone, Chiara, et al. "2024 U.S. Election Misinformation Monitoring Center." NewsGuard, Nov. 2024, https://www.newsguardtech.com/special-reports/2024-elections-misinformation-tracker.

49. Voo, Julia. "Driving Wedges: China's Disinformation Campaigns in the Asia-Pacific." Asia-Pacific Regional Security Assessment 2024, by International Institute For Strategic Studies, 1st ed., Routledge, 2024, pp. 108–23. DOI.org (Crossref), https://doi.org/10.4324/9781003530060-6.

50. Warren, Patrick, and Darren Linvill. "Writers of the Storm: Who's Behind the Ongoing Production of Pro-Russian False Narratives." Media Forensics Hub Creative Inquiry Reports, Oct. 2024.

51. Zainuddin, Hannah, and Foreign, Commonwealth, and Development Office. "Disinformation Is Being Weaponised Against All of Us: Uk Statement at the Un Fourth Committee." GOV.UK, 6 Nov. 2024, https://www.gov.uk/government/speeches/disinformation-is-being-weaponised-against-all-of-us-uk-statement-at-the-un-fourth-committee.