Towards a Theory of Defence Against Information Warfare:

A Case Study of Russian and Chinese Information Operations in the United States of America

Ethan Clow

Department of Political Science

McGill University, Montreal

August 2024

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Master of Arts.

Table of Contents

Abstract

Human beings make decisions according to the information available to them. In recent years, authoritarian governments have adapted long-existing strategies of information manipulation to the digital age. This thesis examines the information operations used by Russia and China to target the United States and evaluates them in relation to existing strategies of defence and deterrence. Variations between Russian and Chinese strategies are highlighted and investigated, along with the differences in each country's relationship with the United States. Russia has utilized a caustic approach, fomenting division within the social sphere as a method of undermining America's image. China, until very recently, had neglected to use the same practices, instead focusing softer efforts on the Chinese diaspora and citizens of key American allies. Interdependence between China and the United States makes possible a strategy of deterrence by entanglement that affects the tactics used by the aggressor. Other forms of deterrence are seriously challenged in relation to asymmetrical information warfare. Methods to build social resilience vis-a-vis information warfare remain promising but may be difficult to implement successfully in the American context. A process of manipulating the aggressor's cost-benefit analysis through interdependence remains the best path forward for the United States.

Les êtres humains prennent des décisions en fonction des informations dont ils disposent. Ces dernières années, les gouvernements autoritaires ont adapté à l'ère numérique des stratégies de manipulation de l'information qui existaient depuis longtemps. Cette thèse examine les opérations d'information utilisées par la Russie et la Chine pour cibler les États-Unis et les évalue par rapport aux stratégies de défense et de dissuasion existantes. Les variations entre les stratégies russes et chinoises sont mises en évidence et étudiées, ainsi que les différences dans les relations de chaque pays avec les États-Unis. La Russie a utilisé une approche caustique, fomentant des divisions au sein de la sphère sociale comme méthode pour saper l'image de l'Amérique. La Chine, jusqu'à très récemment, avait négligé d'utiliser les mêmes pratiques, concentrant plutôt ses efforts sur la diaspora chinoise et les citoyens des principaux alliés des États-Unis. L'interdépendance entre la Chine et les États-Unis rend possible une stratégie de dissuasion par enchevêtrement qui affecte les tactiques utilisées par l'agresseur. Les autres formes de dissuasion sont sérieusement remises en question par rapport à la guerre asymétrique de l'information. Les méthodes visant à renforcer la résilience sociale face à la guerre de l'information restent prometteuses, mais pourraient être difficiles à mettre en œuvre avec succès dans le contexte américain. Un processus de manipulation de l'analyse coût-bénéfice de l'agresseur par le biais de l'interdépendance reste la meilleure voie à suivre pour les États-Unis.

Acknowledgements

This project would not have been possible without the gracious support of many individuals. Thank you to my friends who helped make my time at McGill a life-defining experience. Classmates, especially those from the POLI 618 course in Fall 2023, helped me keep my head above water during an intellectually challenging first semester. Students at the Centre for the Study of Democratic Citizenship further aided in this process. Professor Elissa Berwick played an enormous role in helping me learn the foundations of quantitative analysis, a subject with which I was largely unfamiliar at the time.

Professor Alexander Moens, Hannah Christensen, and Amy Topshee, along with the rest of the staff and students from the NATO Field School course I attended in the summer of 2023, all played key roles in establishing the direction of my research. Professors Fernando Nuñez-Mietz and Rex Brynan were among the finest teachers I have had the pleasure of learning from.

Professor Dietlind Stolle was integral during my first year at McGill, providing insights I will carry with me throughout my career. I remain bewildered by her knowledge and work ethic and will be forever appreciative of the support she provided me. I thank her immensely.

Professor T.V. Paul, as my supervisor, was integral to the development of this project and as a purveyor of knowledge in international relations. His brilliance and direction were fundamental to my time at McGill. I am beyond honoured to have had the opportunity to work with him.

Finally, I thank the undergraduate students for whom I had the pleasure of being a teaching assistant for being so inquisitive and focused. Their determination gives me hope for the future, and working alongside them was my greatest experience at McGill.

Preface

At my most simple, I am a translation machine. In the most reductive sense, human behaviour is a process of receiving external data through the senses, interpreting it, and acting according to it to produce a desired result; — input — comprehension — output. In the evolutionary context, it is beneficial for individuals to act pursuant to the information they receive from the external, translating it internally to introduce a beneficial action back into the outside world. This process is simple under simple circumstances - in a storm, we seek shelter; if there is a threat in our environment, we act accordingly to ensure our security. We can trust, in the aggregate, that our senses do not deceive us. Indeed, this is a helpful tool in the natural environment, one in which the majority of problems facing human beings are those at the bottom of Maslow's hierarchy.

Today, however, the world is more complex. The sources from which we gather information are not solely in the natural environment, nor are they the relatively uncomplicated social bonds defining the period when humans interacted on a local scale. Rather, since roughly the turn of the 20th century, and the advent of the radio and other mass media devices, the information around us has become convoluted, fast-paced and rapidly changing, often unnecessary and always overwhelming. This is worsened by social media and its *algorithm*. Young and old people alike, today, often spend a significant portion of their waking hours online; the external sources from which we gather much of our sensory information are fundamentally different from those of the past. This thesis will go on to argue the ease by which actors can access and pollute this information environment. If this assertion holds, then the information we now translate can be deliberately manipulated by far-away actors on a large scale, affecting our understanding of the world and therefore our tangible actions.

In a simpler world, Individual X could inform me that my neighbour had stolen from me, inciting me to exact some form of retribution, regardless of whether the theft had actually occurred. If it is in Individual X's interest to produce discontent between myself and the neighbour, then his statement allows him to acquire benefits from the subsequent dispute.

Today, unlike in the past, Individual X can be omnipresent and invisible, operating like a ghost in the shadows. He can introduce caustic rhetoric to my information environment at a mass scale. He need not even know who I am. Taking the metaphor into today's world, Individual X can be a nation-state, and I am the abstract concept of a foreign citizen. Individual X need not be proximate to me but can be a distant state apparatus with a vested interest in producing resentment between two or more neighbours. And every time I engage with the online information environment, I have a reasonable chance of encountering his rhetoric. My actual neighbours, those around me, he may say, are not to be trusted. Their ideas about the world are not only incorrect but they are dangerous. I should be scared of what they have in store for my community. If I am not careful, their ideas and actions will dissolve my chance of living in the world in which I wish to live.

Thus, a problem exists. A brain evolved in a simpler time is not well equipped to deal with today's complex information environment. The inherent biases and thought processes that may have been helpful in nature can be abused to produce destructive results in a globalized society. This project aims to describe the mechanisms by which the external information environment can be hijacked and twisted to produce desired outcomes. It explores established theories of security and defence and highlights their deficiencies regarding this type of adversarial conduct. It seeks, despite the challenges, to elucidate the best path forward. It is a process of uncovering, explaining, and defending against the fabricated ghosts in our machine (4th PSYOP Group, 2022).

Introduction

Democracy dies in division. The political system underlying today's liberal international order requires trust and understanding between neighbours and tacit confidence in the institutions of the democratic state. Illiberal nations have keenly noted this condition as a vulnerability in the fabric of democracy as a system and have sought to exploit it accordingly. Russia and China, in particular, have rehashed age-old strategies devised to influence foreign societies and have combined them with the twenty-first-century information environment to create a powerful attack vector that democracies may struggle to counter effectively. These two countries have put particular effort into disrupting the American information sphere. The United States, as the foremost democratic state and the strongest geopolitical challenger to the two attackers, faces consistent efforts from abroad to obstruct its information environment. By introducing carefully designed rhetoric into the American information sphere, Russia and China influence American citizens through the shaping of public discourse. This may include fostering chaos, a hallmark of contemporary Russian information strategy, or influencing political opinions to achieve a set of specific and predetermined goals, a softer policy used notably by China.

But is the introduction of manipulated information from abroad truly a challenge for the United States? Traditional defence scholarship notes that altering an attacker's cost-benefit analysis can prevent unwanted action through a process of deterrence. As such, deterrence forms a fundamental part of existing American strategy in both the material and immaterial realms (Department of Defense, 2023, 9). It is argued that deterrence against attacks based in cyberspace is not difficult in practice, implying that disruption efforts waged via social media may be prevented (Goodman, 2010, 102; Jasper, 2017, 10). The application of fact-checking and policies intended to minimize the sharing of damaging narratives and preserve social harmony have been proposed as solutions to counter foreign information interference (Lanoszka, 2019, 237; Roozenbeek & Van der Linden, 2021, 8). Under the guise of deterrence theory, effective social resilience towards manipulated information should remove the benefit of engaging in information warfare. Furthermore, democracies are defined by their abundance of ideas, and the diversity of opinion present within them should provide citizens with the opportunity to analyze and subsequently select the information they deem to be trustworthy. In this view, the populace of a democratic state should be able to resist efforts of indoctrination and foreign obstruction.

And yet, states like Russia and China continue to attack the American information sphere, implying that the benefits are tangible and are still exceeding any costs (De Luce & Grumbach, 2024**)**. Through an assessment of the characteristics (qualities, elements, attributes, features, etc.) of Russian and Chinese obstruction campaigns, this project examines why the United States has been unable to successfully prevent the use or undermine the effectiveness of concerted attacks against its information environment. It further seeks to explain if and why there are differences in the campaigns stemming from Russia and China and whether these differences shed light on potential defence strategies against this sort of warfare.

I argue that the majority of established defence strategies are ill-equipped to deal with the immaterial nature of information warfare. I further argue that the differing political circumstances of China and Russia affect their choice of information strategy, resulting in unique characteristics for each that impact their resistance to American counter-efforts. By analyzing both Russian and Chinese efforts to attack the American information sphere, the project aims to show that an independent variable (the nature and characteristics of a particular information obstruction campaign) affects the dependent variable (the effectiveness of a specific defence strategy).

In Chapter 1, I evaluate an underappreciated aspect of information warfare: the role of *cognition* in shaping our perceptions and determining our beliefs. If hostile obstruction campaigns targeting the United States are not comprised solely of false information, and our capacity to determine what is true is inherently constrained, the prospects of a defence policy focused on presenting factual evidence about the world will be largely insufficient. This section is the most theoretical portion of the project but is essential for establishing the groundwork of the following chapters.

In Chapter 2, I examine Russian and Chinese political circumstances and information strategies, highlighting the divergence in their approaches. This consists of a brief analysis of their relational power deficiency vis-a-vis the United States, illustrating their necessary dependence on asymmetrical strategies that provide opportunity in the context of an unbalanced rivalry. I show that Russia focuses primarily on destabilizing the American social fabric, while China has sought to shape policy and public opinion in a more constructive manner. In examining the differences present between the Russian and Chinese approaches to information warfare, I explore the nature of their relationships with the United States, with particular focus on their economic associations. I also highlight the variance in their international image and how this may affect the reputational costs each is willing to bear.

In Chapter 3, I assess the use and feasibility of existing defence strategies against information warfare. Building on the arguments established in the first two chapters, I show how the basic use of information obstruction is difficult for the United States to prevent through a process of altering an adversary's cost-benefit analysis. This includes traditional methods of deterrence but also efforts focused mainly on strengthening social cohesion. These two approaches encompass the majority of scholarship on defence within the context. In general, I demonstrate the challenges the United States faces in *denying* adversaries the ability to effectively manipulate their information environment and the *difficulty in imposing credible threats of retaliatory punishment* against authoritarian regimes. I proceed, however, to demonstrate how the cost-benefit analysis can be used to alter *how* a state wages information warfare. To do so, I further analyze how the approaches used by each adversary may be influenced by their relationship and level of economic interdependence with the United States. In a close examination of the costs and benefits of manipulating the American information environment, this project demonstrates the inadequacies of traditional defence policies in the information realm and the need for rethinking how we deal with obstruction from abroad.

This project offers a new approach to the study of information warfare, analyzing the variation in approaches from Russia and China and exploring how existing relationships can alter chosen strategies. Further, the beginning of Chapter 1 addresses some factors that are known by academics and policymakers but are underappreciated. In particular, *truth* and its relationship to belief are known in the abstract but not adequately dealt with in existing scholarship and policy. The effect of this consideration is likely to be multiplied as technology improves and artificial intelligence becomes a greater concern, an issue dealt with in the implications section of the project.

In particular, assessing economic integration with the United States as a mitigating factor is an original approach to investigating information strategy. In cases where states have little economic interdependence with their target, information obstruction campaigns can take on a shape that is highly resilient to existing defence strategies and unlikely to incur significant punitive costs. In these cases, the prospects of deterring information warfare by denial and punishment are significantly challenged. Strategies may also take on a more damaging format, as the benefit of affecting the target's social sphere does not produce the downsides that would occur with significant economic integration. In cases where interdependence is present between states, a strategy of deterring by entanglement is theoretically promising (albeit challenging), with heavy costs resulting from certain forms of damaging information manipulation. Thus, the existing relationship between states can alter an adversary's strategy, determining the policies it chooses to use.

Through comparative analysis of the strategies used by America's biggest geopolitical challengers, the project aims to make two things clear. First, the characteristics that define information warfare in the twenty-first century necessitate new approaches to defence. Many of these qualities are known to scholars and policymakers, but their impact on defence strategy is often underappreciated. Second, the existing relationship between the attacker and the target can influence the characteristics of a strategy of information warfare.

Literature Review

The History of Information Warfare

The value of manipulating the information available to an enemy has been appreciated since antiquity. Biblical narratives provide accounts of religious armies using torches and trumpets in the night to appear as a force larger in size than they truly were (New International Version, 2023, Judges 7:19). These accounts typically end with the enemy descending into chaos and turning their swords against each other (New International Version, 2023, Judges 7:22). The authors of these stories understood the psychological nature of warfare, and so described armies of hundreds emerging victorious against much larger forces in some of history's first asymmetrical conflicts. The Mongols used similar tactics, manufacturing rumours regarding the size of their army (Martin, 1943, 59). They further forged letters to look like the correspondence of soldiers planning to execute a coup against the target sovereign and ensured that these fell into the hands of leadership (Martin, 1943, 59). The success of these deceptive tactics resulted in division within the ranks of the target, allowing for an easier invasion and subsequent seizure of territory (Martin, 1943, 59).

Kauṭilya, in the third century B.C.E., highlighted the advantages of manipulating the emotions of those living in key confederacies by providing conciliation and gifts to those favourable to you and promoting dissension and quarrels between those who are not (Kauṭilya, 2013, 389). "Secret agents operating nearby should out the grounds for mutual abuse, hatred, enmity, and quarrels among members of confederacies, and sow dissension in anyone whose confidence they have gradually won, saying, 'That person defames you.' When ill will has thus been built up among adherents of both sides, agents posing as teachers should provoke quarrels among their young boys with respect to their knowledge, skill, gambling, and sports" (Kauṭilya, 2013, 389). These writings demonstrated the power of manipulating sectors of foreign populations that were particularly exploitable, fomenting division amongst the youth over issues related to their pride.

By the twentieth century, the fundamental principles that underlie previous examples of psychological warfare began to be assembled into recognizable forms of modern information manipulation. Coordinated efforts to distribute specific narratives to enemy populations during the First World War demonstrate the shift from psychological tactics employed mainly against hostile military forces towards the inclusion of foreign publics as a target. An early example of this is the British Report of the Committee on Alleged German Outrages, a government document published in 1915 which describes purported German atrocities in Belgium. In detail, the report delineates instances of German troops slaughtering innocent civilians and burning villages to the ground (Great Britain, 1915, 10). The vivid descriptions of the crimes of Britain's enemy have been noted as *atrocity-mongering* by academics and increased both military recruitment and violence against German-speaking residents of the country (Wilson, 1979, 369). Notably, the British took the step of shipping forty-one thousand copies to the United States, resulting in the mass publication of the anti-German narrative amongst the media and acceptance by the American public (Quinn, 2001, 39). With the Great War resulting in an Entente victory and harsh treaties levied against the German nation, actors within Germany took lessons from British propaganda efforts and turned them inwards. Adolf Hitler cited British efforts in Mein Kampf, noting their success as a "gradual seduction" of the minds of the general public (Cull et al., 2003, xvii). The German government went on to engage in their own mass propaganda efforts during the Second World War, with a specific focus on dividing allies like Britain and France (Rhodes & Margolin, 1983, 31).

Throughout the Cold War, both the United States and the Soviet Union engaged in information operations against each other's public. In 1950, the Central Intelligence Agency funded the National Committee for a Free Europe, which began a campaign of radio broadcasting to countries beyond the Iron Curtain (Encyclopedia Britannica, 2018). The Radio Free Europe project served as a dissemination tool for American anti-Communist propaganda, aiming to influence the beliefs of those living behind the Curtain. Notably, however, broadcasting policy shifted over time. More control was placed into the hands of émigrés from the regions in question, allowing for a tailored approach to dissemination dictated by those who had a substantial understanding of how the target populations thought and lived (Byrne, 2012, 213). Soviet agents from the Committee for State Security sought to inflame racial tensions within the domestic sphere of the United States. Agents worked to promote the idea that the American government was involved in the assassination of civil rights leader Martin Luther King Jr. and authored fake letters from the Ku Klux Klan, sending them to citizens around the United States (Johnson 2019, 210). Soviet forces attempted to paint the United States as a fundamentally racist nation, working to undermine the moral position of the country (Johnson, 2019, 211).

With the rise of social media, the power and ease of manipulating information has multiplied. Literature on the nature of contemporary obstruction efforts shows remarkable similarity to historical examples. Emotional narratives achieve a greater level of virality on social media platforms, reaching a broad audience and subsequently influencing more people than impersonal alternatives (Brady et al. 2017, 7314). Taking advantage of pre-existing schisms in democracies, such as those between political affiliations, these messages can increase societal polarization (Hartman et al. 2022, 5). Analysis of Russian obstruction, in particular, highlights their use of emotionally poignant messaging directed at the civilian population of their adversaries. Russia's Internet Research Agency pursued a strategy of inciting anger among Americans during the 2016 presidential election campaign (Linvill et al., 2019, 292). On Twitter, the common theme portrayed by the Agency was one which sought to foment anger in America's right-wing and direct it toward the left (Linvill et al., 2019, 295). Obstructive narratives are often presented with emotional language (Alvarez et al. 2020, 3028). They are frequently used to foment mistrust in democratic institutions, such as elections, government agencies, and even political parties (Giusti, 2021, 68).

Deterrence

Deterrence is perhaps the greatest tool available to policymakers to ensure the security of their nation. Deterrence theory notes how actors may issue threats to others to prevent unwanted actions from taking place (Morgan, 1977, 17; Snyder, 2015, 3). The goal is to imply to the other that their actions will cost more than they will benefit, a process of manipulating intentions and provoking second thoughts (Morgan, 2003, 12; Schelling, 1963, 531; Snyder, 2015, 11). Debate abounds over whether deterrence is a process between unique actors, each with distinctive qualities, or whether general trends of human behaviour can be deciphered and used to standardize methods of deterrence (Morgan, 1977, 50). Taking Jervis' view on the common misperceptions of actors (1968, 455), we can generalize trends among leaders to understand deterrence as effective and feasible (Morgan, 1977, 56). But if individual variations in thinking and perception do constitute an important element, then this view of deterrence is incompatible with reality. Instead, policymakers tend to downplay irrationality and focus on others as rational actors attempting to operate in their own best interests (Achen & Snidal, 1989, 151; Mercer, 2005, 78; Morgan, 1977, 57). This gives us a convenient lens through which to analyze deterrence within the context of information warfare. The defender must convince the attacker that their actions will detract from their overall goals. This is relatively simple in the material realm, especially concerning nuclear weapons. The tacit understanding of the immense danger posed by nuclear weapons simplifies the concept of deterrence, as the threat of destruction is clear and tangible (Morgan, 1977, 58). This is a major reason for the purported success of deterrence throughout the twentieth century. Information, however, is immaterial. Its effects are not immediate, especially those related to the provocation of caustic rhetoric within the domestic sphere. Information obstruction is a slow-burning phenomenon, with the totality of its effects delayed and impossible to judge in full.

Many in the discipline downplay the difficulties of deterring information attacks. Often, information warfare is conflated with cyber warfare. In assessing deterrence in cyberspace, authors like Will Goodman assert that as cyber actors operate in the real world, it is possible to assign responsibility (even if doing so requires time and effort) [2010, 112]. Scott Jasper notes that a strategy of *active cyber defence* which focuses on real-time detection, analysis, and mitigation provides opportunities to counter twenty-first-century cyber warfare effectively and rapidly (2017, 165). In this, defenders may deny benefits through system durability and inflict costs by disrupting actions. Other strategies include norm-based approaches, such as the proposal for a *no-first-use* policy, where states demonstrate their refusal to utilize cyber warfare unless provoked through cyberspace by adversaries (Mazanec & Thayer, 2015, 46). It remains unclear, however, whether adversaries who benefit from the inherently asymmetric nature of the battlespace will be willing to give up such a powerful tool (Mazanec & Thayer, 2015, 47). More importantly, these strategies deal exclusively with attacks on infrastructure. The functionality of information warfare stems from its effects on the immaterial realm of the human processes of thinking and feeling.

Broadly, information warfare is the use of manipulative policies to divide the civilian population of rival states, to influence through propaganda, or to grow support for the attacker's interests (Ventre, 2016, xiv). It is employed to influence targets to make decisions against their interests (Glenn & Florescu, 2017, 2). The concept of using information to manipulate an enemy goes back far longer than our technological age. Dropping propaganda leaflets from the air or sending an individual to parrot messages from a soapbox in the town square achieves the same outcome as contemporary online campaigns. While cyberspace is a convenient vehicle through which countries may employ this power, it is merely a modern and faster delivery mechanism through which long-used tactics are executed. In the literature, most research on cyber conflict regards attacks on infrastructure (Winterfield & Andress, 2012, 3; Springer, 2020, xv; Whyte & Mazanec, 2023, 84). Distinguishing this activity from the psychological manipulation that defines our topic demonstrates cyber deterrence's challenges in being applied to information warfare and highlights that existing theorizing in this realm may not apply to the subject at hand.

Looking more specifically at deterrence in the information environment, the American government notes China and Russia as two of the largest threats, and the Department of Defence observes that these adversaries are continually expanding and refining their abilities (2023, 3). The noted aim of the present American information deterrence strategy is to shape the behaviour of foreign states, organizations and individuals to reflect that which is favourable to American interests (Department of Defense, 2023, 8). The designation of success for these efforts is dependent on observing a change of behaviour in those actors listed (Department of Defense, 2023, 8). Ignoring the difficulties associated with actually determining whether deterrence is successful, effectiveness here relies on the adversary appreciating threats as credible (Snyder, 2015, 10). Challenges arise when analyzing the sort of threat that may be implemented. While this is discussed further below, democratic states may face challenges of attribution and in penetrating authoritarian information spaces to apply equivalent punishment. The inherent qualities and status attributed to democracies may further hinder their willingness to engage in similar forms of information manipulation in their strategic communications. In the available documentation on American information strategy, most focus is dedicated to funding allocation, the integration and collaboration of departments and teams, and the future expansion of capability (Department of Defense, 2023, 10). Beyond noting three broad approaches of integrated deterrence, campaigning, and building enduring advantages, few specifics are emphasized (Department of Defense, 2023, 9). There is good reason for this, as revealing the scope of deterrence strategy informs the adversary of your capabilities and intentions. However, this highlights a further problem: governments may be hesitant to employ clandestine operations at the risk of revealing them and undermining their continued usefulness. Regardless, evaluating the intricacies of confidential government strategy is not feasible. Importantly, these strategies have yet to prevent adversaries from manipulating the American information environment. American policy has not adequately deterred information warfare to the degree that it has deterred material warfare, revealing the information environment as a battlespace in which weaker actors can achieve some level of parity with greater ones.

Social Resilience

Efforts aiming to increase social resilience to information obstruction are prevalent. Researchers have emphasized the importance of moral framing when disseminating messages which seek to counter foreign narratives (Hassain, 2022, 8). Creating a catchy 'hook' to describe a message has shown to be successful when governments attempt to spread their counter-narratives to mass audiences (Hassain, 2022, 11). Efforts that frame messages in a manner suited to achieve end goals can be considered *strategic communication*. The NATO Strategic Communications Centre of Excellence defines the field as a "holistic approach to communication, based on values and interests, that encompasses everything an actor does to achieve objectives in a contested environment" (n.d.). While it is clear that domestic spheres have become a *contested environment* in recent years, states must be cautious in the art of persuading their citizens. Trust in the government of the United States, for example, has reached historic lows, complicating the task of influencing the masses (Pew Research Center, 2023). An environment with low trust in government benefits the attacker and hinders the defender.

Democratic governments have put significant effort into providing their own interpretation of events to the public. A notable example is the Communications Security Establishment, which routinely publishes updates on threats to Canadian democracy (Canadian Centre for Cyber Security, 2023). Government agencies make great efforts to communicate clearly and openly to citizens. The problem of public trust remains, however, with CSE themselves noting that confidence in their agency has declined in recent years (2020, 13). Perhaps an even larger problem is the lack of public knowledge of these reports. The Canadian Center for Cyber Security, the author of the report on threats to Canadian democracy, is unknown by more than nine in ten Canadians (Communications Security Establishment, 2020, 3). While findings may be shared more broadly through legacy media, Canadians have demonstrated a remarkable lack of trust in these sources (Statistics Canada, 2024). Worse still, while the openness of information spheres is a paramount factor in democracy, it creates the inevitable drawback that sources become somewhat equivalized even when they should not be. Trust in expert opinion declines as the number of arguments present in an information environment increases (Flanigan & Metzger, 2013, 1628). Hostile actors take advantage of these democratic qualities, using information attacks that are “high-volume and multichannel” and “rapid, continuous, and repetitive” (Paul & Matthews, 2016). Government reports that seek to counter foreign narratives, (often long and written in academic jargon) must compete in an environment of fast headlines, social media, and memes. Presenting counter-narratives to the public is a well-intentioned idea, but the challenges that must be overcome are immense. Integrating these efforts with a strategic communications strategy, however, may provide a feasible path forward.

Inoculation theory and *prebunking* have also gained attention in recent years. Here, actors seek to develop a psychological *vaccine* to prepare targets for impending exposure to manipulated information (Roozenbeek & Van der Linden, 2021, 8). Doing so involves introducing targets to a weaker version of existing hostile narratives to prepare them for future exposure to stronger ones (Roozenbeek & Van der Linden, 2021, 8). However, it has been made clear that even when individuals know information has been discredited, they will continue to be informed by and rely upon it (Rapp, 2016, 282). Even if a small group of individuals may be inoculated or a government can successfully create effective counter-narratives, these efforts are unlikely to reach all target audiences. There is sufficient reason to doubt that they will work even in the majority of cases. Therefore, it is unlikely these endeavours will sufficiently alter an attacker's cost-benefit analysis.

Numerous problems can be identified in the existing research related to this domain. Information warfare targets the mind and takes advantage of inherent cognitive biases to become accepted by targets, to spread quickly, and to reach mass audiences. Deterrence theory works well in material domains but may struggle to counter the psychological elements of information obstruction. Theorizing on cyber deterrence is prevalent and well-established but centers largely around attacks on infrastructure. Strategies to counter the effects of information obstruction have been proposed but may not be effective in preventing adverse consequences in a society. Given the continued use of these campaigns, adversaries have calculated that the benefits still exceed the costs. Thus, while certain elements of the existing literature demonstrate some promise, they have yet to be implemented effectively.

Based on the above theoretical framework, I make the following propositions:

1. The prospects of deterrence are significantly challenged by information warfare.
2. Social resilience approaches are beneficial but may be lacklustre in their actual effects.

Methodology and Case Selection

To explore the propositions, the project will investigate and analyze the cases of Russia and China vis-a-vis the United States. The two cases differ in both the strategies employed by the attacker and the amount of leverage and interdependence between the attacker and defender. In both cases, I aim to show that an independent variable (the nature and qualities of a particular information obstruction campaign) affects the dependent variable (the prospects of a successful defence policy).

The Russian case will be the main focus of the thesis. It demonstrates the policies used by an authoritarian state against a democratic one with little to no leverage over the attacker. Russia has also demonstrated little regard for its image in the international system. The case illustrates the challenges deterrence faces in the context of information warfare. The Kremlin heavily controls the Russian information sphere. Russia has demonstrated that it is willing to bear high costs for its actions. Further, it has little more to lose in terms of economic access to the United States. Its strategy of chaos also plays a large role in analyzing the usefulness of social resilience approaches.

The Chinese case further allows for an analysis of how economic interdependence and trade linkages may affect a state's ability to deter an aggressor. It also demonstrates the different strategies employed by China compared to Russia. While Russia has aimed to foster chaos within the United States (Hamilton, 2019, 334), China has historically been more selective in its targeting (Fitzgerald, 2018, 59; Cohen, 2021, 8). Rather than aim to stimulate general chaos between American social groups, it has focused largely on influencing its diaspora and, more recently, introducing narratives that blame the United States for the COVID-19 pandemic. China benefitted little from the chaos surrounding the 2016 American election. The election of Donald Trump to the White House hurt their interests. While Russia gains when the paramount liberal state falters, China may have more interest in a stable and predictable American policy.

Comparing and contrasting these two cases allows for an assessment of how the circumstances of each may dictate their strategic choices. The political and economic relationship with the target may shape an attacker's choices. Tying circumstances to strategy allows for a tailored approach to defence and deterrence, something generally absent from contemporary literature and government policy. However, using two cases with the same target limits the generalizability of the findings. As such, the findings only apply to the American case but may be generalizable to some degree regarding other democracies.

Chapter 1: Cognition and Objectivity

Information manipulation is the process of shaping the premises from which you want your target to reason. The Russian term for this process is *reflexive control*. We see this in practice regarding Ukraine, where the goal is to "minimize the West's perception of its own leverage over Russia" (Bugayova et al., 2024, 4). Russia seeks to achieve this objective by shaping American perceptions of the likelihood and cost of a Ukrainian victory. But why are these perceptions so vulnerable to manipulation? Intuition tells us that we are complex creatures, able to interpret the world and its truths. This conception of our abilities, however, arises from comparison. We are complex in relation to other organisms around us but are imperfect in our own assessments. Through this lens, the cognitive processes that guide us through the world should be understood as fallible, subject to misinterpretation, and consisting of inherent rules shaped by natural selection. It is the weaknesses of our cognition that make information warfare possible.

Each of us has the ability to narrow our focus and select helpful information out of the chaotic environment, shaping it into a meaningful interpretation of the world. Scottish philosopher David Hume argued for our dependence on custom and habit, noting that our knowledge of repeated occurrences of events allows us to form predictions about the future and the past (Hume, 2019, 35). Merging Hume's skepticism with Cartesian rationalism, Immanuel Kant postulated that what lies beyond the senses is unknowable to the human mind (Kant et al., 2007, 28). Rather, we are subject to a set of *a priori* intuitions and concepts that give rise to the possibility of interpreting the outside world uniformly, where all empirical knowledge about the environment must conform to an inherent structure of thinking that guides human behaviour in an adaptive manner (Kant et al., 2007, 59). Kant's transcendental idealism frames cognition as a translating apparatus, filtering Hume's raw experience through the mind's inner workings to produce an ordered and workable interpretation of the external world.

The state of our cognitive toolset is the result of evolution. Successful reproduction is the result of adaptive behaviour. A hypothetical ancestor who could not determine and subsequently focus upon a threat in their environment was not long for their world. We are the descendants of those most adept at minimizing noise and tuning into important signals. To fail in this regard meant unfitness, and those unable to succeed were unlikely to pass on their genes. Under this assumption, the development of efficient and rapid perceptual shortcuts would improve fitness in the environment. Hoffman and Singh note that the need for fitness over all else opens the possibility that sensory tools do not provide an accurate assessment of the external world but rather a highly selective assortment of the information needed to survive (2012, 1087). Under this model, gaining objective truth about the outside world is less beneficial to us than perceptual shortcuts that make survival and reproduction more likely. Indeed, evolutionary simulations demonstrate that accurate perception of reality goes extinct within a handful of generations in favour of environmental fitness. “Natural selection tunes perception to payoffs, not to truth” (Hoffman et al., 2015, 1486). The long and arduous process of achieving an exact interpretation of the environment is outcompeted by rapid and unconscious processes that deliver desirable ends. Intuitional shortcuts influence our beliefs to a greater degree than a thorough examination of the external world. The universe should by all accounts appear to us as overwhelming and disorganized madness. And yet, we are able to pull disparate shapes, colours, sounds, movements, and events into a comprehensible structure to operate within. Human dominance over the environment is not so much a result of more accurate perceptions, but a keen ability to pull order out of chaos and organize it into a workable schema, and more importantly, communicate our intentions towards it with others.

Communication is the mechanism by which one's conceptions can influence others. Human beings are social creatures. The ability to transmit complex ideas through sounds and symbols sets us apart from the rest of the animal kingdom. One of the manifestations of natural selection in this realm is the proclivity to view social relations as consisting of *in-groups* and *out-groups*. There was a benefit in ancient and hostile environments to keeping associative bodies relatively small and tightly knit (Efferson et al. 2008, 1847). This allowed for the sharing of resources among trusted peers, and cooperation against external threats. Overall, the odds of surviving in an integrated group setting were superior to those when living alone. Social groups also allow individuals to create an identity for themselves, providing an opportunity to enhance self-esteem, a trait beneficial to both the individual and the group overall (Tajfel &Turner, 2004, 16). To maintain this, members of groups will often supplement their social identity by comparing their group to others around them. Discrimination arises against individuals in an outgroup as an unfortunate consequence of establishing comparisons that enhance a group's worth, and therefore the worth of an individual member (Crocker & Luhtanen, 1990, 60).

Emotions also play a significant role in governing human behaviour. Environmental stimuli are introduced to the senses in distinct circumstances, "but to be reacted to by decision-making algorithms, they must be assigned a meaning in the terms that these algorithms use" (Tooby & Cosmides, 1990, 409). To do so, humans take cues from others around them. One largely learns what constitutes a threat by observing what stimuli prompt peers to act with fear (Tooby & Cosmides, 1990, 409). Inserting carefully selected premises into this process can influence how we act. Successfully stoking fear in the mind of an individual member of a social group inevitably influences other members. For example, if a Russian goal in the United States vis-a-vis Ukraine is to prevent monetary support, narratives that play on the in-group and out-group dichotomy and use emotion to prompt fear toward others can be used as a vehicle to achieve the desired outcome. Indeed, Russian narratives in this context highlight supposed rising crime levels and a decline in funding for police, or immigration through the southern border, to evoke fear and questions about whether the United States can afford to support a far-away conflict. These narratives provoke conversations over the meaning of 'national security', aiming to turn America's focus inwards. This, in turn, prompts the election of leaders who trade in fear and attacks against their political opponents. An elected leader's actions may prompt fear amongst allies of America's commitment to Europe and other causes around the world.

Information operations seek to fill the chaotic environment with carefully selected themes and depend on inherent and predictable cognitive patterns to seize on these themes to shape explanations, eliciting the actions and worldview desired by the aggressor.

Given uniform cognitive traits, it may be expected that our interpretations be uniform as well. This is not the case. Although we may share the traits that allow us to simplify the surrounding environment, we order this information into differing interpretations. Our tools are the same, but the reality we construct varies. Out of our cognitive and social processes arise differing ideologies, discourses, and interpretive bubbles. These differences are what constitute our politics. When Russia claims that the United States is heading in the wrong moral direction, the truth of the matter lies in the eye of the beholder, influenced by their own subjective considerations. Information obstruction campaigns targeting the United States build upon these differing interpretations, taking advantage of our preexisting beliefs and seeking to enhance or shape them in ways that benefit the attacker. The lack of objective truth underlying our moral interpretations is what makes this exercise possible.

Considering our dependence on cognitive shortcuts, and the resulting subjectivity of our interpretations, a strategy focused on presenting the "truth" to democratic audiences is certain to face difficulties. Perhaps we may rely upon our basic cognitive tools to acquire strong evidence regarding specific events. We can review actions in the Donbas and find no evidence to support the Russian claim of a genocide perpetrated by the Ukrainian government (RFI, 2021). Ukraine requested the International Court of Justice to do so, and asked that the court "adjudge and declare that, contrary to what the Russian Federation claims, no acts of genocide, as defined by Article III of the Genocide Convention, have been committed in the Luhansk and Donetsk oblasts of Ukraine", and that "the 'special military operation' declared and carried out by the

Russian Federation on and after 24 February 2022 is based on a false claim of genocide and therefore has no basis in the Genocide Convention" (International Court of Justice, 2022, 2). The court fulfilled its duty and found that Russian claims of genocide in the Donbas were unfounded (International Court of Justice, 2022, 13) and that Russia has no legal basis in continuing its invasion to prevent the purported genocide (International Court of Justice, 2022, 17). This narrative is as close as one can get to *objectively* untrue.

Consider another narrative regarding the crisis, concerning the role of NATO and the EU purportedly spreading their values and military capabilities into the Russian sphere of influence. Stephen Walt argues that states balance against perceived threats in the international system. What constitutes a threat is determined by aggregate power, geographic proximity, offensive capability, and perception of intention (Walt, 1985, 36). As a capable military alliance moving ever closer to the Russian border, NATO fulfills the first three of these factors. Russia appears to perceive Western intentions as hostile. To its credit, NATO has made it explicitly clear that the alliance does not intend to threaten Russia and is merely allowing citizens in prospective member states to exercise their right to self-determination (2016). Russia has not been convinced by these statements or the clearly established definition of NATO as a purely defensive alliance.

John Mearsheimer relates the situation to the following example: if Canada were to independently decide to allow Chinese interests to gain a foothold in their sovereign territory, and stage military exercises proximate to the American border, does this pose a security threat to the United States (2014, 82)? Even if Canada and China state in no uncertain terms that their intentions are benign, and Canadian citizens have chosen of their own volition to pursue this policy, it is unlikely that the American state apparatus will view this initiative in a positive or neutral light. The conception of threat presents differently to different sides. The subjective nature of this narrative is readily apparent, especially to the significant number of lauded experts in the field of political science we call *realists*.

Specifically, Russia uses an operational method called the *firehose of falsehood* technique. Contrary to its name, the underlying strategy involves no commitment to truth or falsity, but rather a focus on flooding the target information environment to overwhelm individuals and tire the brain (Paul & Matthews, 2016). The result is a chaotic American social sphere in which what is true and false becomes so difficult to determine that the concepts lose their importance (Aminulloh et al., 2023, 250). Jonathan Haidt notes that in such chaos, “the social construction of reality turns into a million tiny fragments on social media” (Novicoff, 2024). When Russia fills social media with mass amounts of false, subjective, and biased information, they overload our cognitive system, and people begin to doubt all that they see which does not easily fit into their pre-existing schemas. When a Russian information agent engages in subjective criticism of America’s shifting values, Americans who feel threatened by the shift in values are largely impervious to any contending opinions and are likely to dismiss them in favour of the simpler approach. High-volume information attacks exhaust the mind and cause people to resort to the easier path, damaging the likelihood of individuals taking the effort to view these issues from different perspectives.

A supercut of a politician’s gaffes may have the power to undermine confidence in a government in much the same way that an unsubstantiated story would. Further, the effects of pushing uncited and non-credible speculation regarding neo-Nazi ideology within the Ukrainian state apparatus are multiplied when presented alongside a decontextualized video of the Canadian House of Commons and Volodymyr Zelensky applauding a former member of the Waffen-SS Galicia Division. While the content of manipulated information can be labelled by democratic sources as untrue, it does not *need* to be false. For this reason, the term *disinformation*, often used as a catch-all for information warfare by the general public, is often misapplied. Further, some academics and agencies have resorted to using the three separate terms of *disinformation*, *misinformation*, and *malinformation* to capture deliberately shared falsehoods, accidentally shared falsehoods, and misleading truth or opinion, respectively (Cybersecurity and Infrastructure Security Agency, n.d.). The concept of *obstruction* or *manipulation* ties these notions together neatly. Focusing heavily on what we determine to be false information, a tendency of public, academic and media circles, is well-intentioned but neglectful of subjective or partly true information that can be just as damaging, and ignores the underlying differences of interpretation present within our societies.

This establishes a new sort of problem. In the case of the Russian invasion of Ukraine, explanations provided by the Kremlin are often cited as *disinformation* by Western governments (Global Affairs Canada, 2023). Rather, some Kremlin-backed narratives are better understood as framing decisions that provide either legal or moral justification for the unacceptable waging of conventional war against a sovereign state. One can witness similar narrative decisions throughout history, including the case of the American invasion of Iraq in 2003. To this day, the existence of Saddam Hussein's nuclear stockpile is questioned, and it is acknowledged that the United States and its allies formulated their reasoning for invasion upon non-tangible evidence (Chang et al., 2013, 32). Regardless, the American insistence on this arms program as a threat to world peace provided a convenient *casus belli* for their invasion. Information obstruction employed by American adversaries is used for similar reasons. Russia's decision to invade Ukraine, for example, is made more acceptable in the eyes of both its public and the international community if it is done for perceived *just* reasoning.

As such, the strategic shaping of information is not the prerogative of authoritarian states. Every individual and government uses narrative to convey information to others, with democratic politicians being prime examples. Presidential elections in the United States demonstrate candidates interacting with the public through stories, using ad hominem attacks against their rival nominees, and succeeding primarily as a result of their personability. Debates rarely consist purely of policy discussion, and the moments that viewers remember are the witty ones. Donald Trump has proven remarkably successful at using the power of narrative and humour more broadly in politics, but he is not the only one. It is the ability to translate complex political topics into engaging rhetoric that is the mark of a good politician, whether their statements are truthful or not. This is even more true in societies that select leaders by free and open votes than in authoritarian ones. Recall the earlier point, that adversaries utilize carefully selected themes to shape our perceptions, prompting desired thinking and actions. This is the same vehicle by which our politicians secure their votes. When done by a democratic actor, we call this political communication, or at worst, the skillful manipulation of information to achieve desired ends. When conducted by an adversary, we call this information warfare.

We are all influenced by narrative. In the realm of geopolitics, Russia and China have proven more adept at employing narrative than their democratic rivals. Democracies like the United States face challenges, described in later sections, that detract from their ability to match the authoritarian toolset. Even if democracies can successfully outcompete authoritarian narratives with their own, this would simply be the result of being the better storyteller. Democracies pride themselves on being the arbiters of truth, but determining that truth is often an insurmountable challenge, especially concerning the subjective arguments that make up the majority of foreign information operations. Even in cases where the truth of the matter can be somewhat *objectively* determined, and an International Court of Justice ruling regarding Russian claims may be cited as an end-all-be-all representation of fact, the same deference may not be afforded when it concerns the actions of an American ally (Singh, 2024). The United States and other democracies face the challenge of foreign narratives eroding social politics, but the efforts required to counter this challenge may involve the use of their own, more palatable narratives. Doing so would lean into the criticisms of their enemies, who note the hypocrisy of America's use of subversive tactics while maligning their use by others. For such reasons, this thesis deals with deterrence as a primary goal and riskier social resilience measures as a secondary strategy to be used if others fail.

There is a tendency to view information warfare as a battle between truth and falsity. This is a false dichotomy. Our perceptions do not seek objectivity, and the evolution of our sociality has been bolstered by subjectivity. Critics of this argument will note that, in such circumstances, it would be expected that both the author and reader would fall prey to what we term "disinformation", and that we should be in great difficulty when seeking to evaluate any given situation objectively. They are correct. The strategies of American enemies do not inherently depend on presenting falsities but rather on manipulating the subjective nature of our interpretations of information. They take advantage of our shortcomings. They manipulate our worldview and amplify our worst tendencies. Whether false, true, or more likely, subjective, engineered information can influence in desired ways. The truth of the matter is unimportant to the problem at hand. The primary elements that determine our beliefs are our preconceptions, the result of consistent evolutionary processes that deliver inconsistent evaluations. Regardless, the mere act of introducing mass amounts of conflicting information into an environment overwhelms the public and challenges our already diverse interpretations of reality. Democracy requires citizens to be at their best and willing to seek and engage with each other to the greatest extent possible. But foreign adversaries have found democracy's Achilles heel, understanding that a divided, confused and inundated citizenry provides the grounding to influence in calculated ways.

Chapter 2: Information Strategies and Political Circumstances: The Cases of Russia and China vis-a-vis the United States of America

A. **Information Strategies**

Russian Information Manipulation

"My cousin is studying sociology in university. Last week her and her classmates polled 1,000 conservative Christians. 'What would you do if you discovered that your child is a homo sapiens?' 55% said they would disown them and ask them to leave their home."
@PoliteMelanie, 2018 (~90,000 retweets, ~300,000 likes).

This tweet was posted by a Russian information agent in 2018. It serves as a convenient demonstration of the methods used by Russia. This piece of media seems to target left-leaning individuals, implying to them that right-leaning Christians are not intelligent enough to know the term "homo sapiens". It presents the reader with a clear divide between an *in-group* (framed as a rational, educated, and forward-thinking left-leaning segment of society) and an *out-group* (framed as a hateful, unknowledgeable, and backward-thinking religious right). It is effortless to digest such media and even easier to share it far and wide. It provokes, to a degree, an emotional feeling of superiority in the targeted reader. Even better if it makes them wonder about the intelligence or morals of the out-group in question. The supposed poll discussed in the tweet does not exist, but three hundred thousand individuals online did not bother to check. This type of thinking contributes to polarization within the American domestic sphere. The focus need not solely be on other individuals. Similar reactions can be provoked when using emotional information to foment mistrust in democratic institutions, such as elections, government agencies, and even political parties (Giusti 2021, 68).

A prime set of examples come to light through the 2019 Mueller Report. After a prolonged period of significant criticism for her mishandling of classified documents, Hillary Clinton and her campaign were subjected to a large release of stolen correspondence and related files (Mueller, 2019, 41). Emails stemming from the Democratic National Committee that discussed strategies to undermine the presidential campaign of Vermont Senator Bernie Sanders were given significant attention (Stein, 2016). Further, leaked emails from campaign manager John Podesta referred to Sanders as a 'doofus' (Stein, 2016). Other Democratic National Committee staffers had their conversations about using the Senator's religious faith against him released by Russia (Boorstein & Zauzmer, 2016). Clinton, already seen as relatively untrustworthy by the American public, was blindsided and hurt critically by the release of this information.

Further leaked correspondence also regarded debate questions being preemptively shared with the campaign and personal information about Clinton's Wall Street speeches, an already contentious subject at the time (Stein, 2016). The general theme of this particular campaign seemed to be an effort to paint Clinton as an entrenched politician, *elitist* and supported by the political establishment. It sought to incite the feeling that she was disconnected from the average American citizen. The issue of the elitist political class has become a common theme in American politics. Fundamentally populist, complaints regarding a 'deep state' or 'the one percent' having undue influence over American politics demonstrate the perception of a divide between the average middle and lower classes and those who benefit from their losses. Tied inherently to economic issues of the day, such as the relocation of manufacturing jobs overseas, it links legitimate economic concerns to the idea that an out-group is taking advantage of Americans facing financial challenges. This particular campaign also helped birth the Pizzagate conspiracy theory, further reinforcing a perceived (and in this case, blatantly fabricated) divide between the lifestyles of the rich and the poor (Robb, 2017).

Conspiracy theories are key in Russian information strategy (Yablokov, 2022, 767). Taking advantage of a trend of political disillusionment among the public, Russia is quick to provide Americans with manufactured explanations for the source of their problems. In the wake of the 2008 financial crisis and into the present, economically struggling Americans are inundated with narratives blaming the elite and the process of globalization for their troubles. Russia provides the names of people who have benefited during times of struggle, granting individuals a convenient face to blame, often those in positions of power within the United States (Yablokov, 2022, 767). The general process is one of creating doubt by "asking reasonable questions without making any evidence-based conclusions" (Yablokov, 2022, 767).

Building on the process of sowing doubt, Russia proceeds to explicitly attack the social fabric of American society. The totality of Russia's goals can be best described as fabricating chaos (Polyakova & Boulègue, 2022). For example, in early 2017, trolls employed by Russia's Chief Intelligence Office took special aim at a heavily publicized women's rights march in Washington D.C. Understanding the existing rifts within the American feminist movement, the trolls posed as "black women critical of white feminism, conservative women who felt excluded, and men who mocked participants as hairy-legged whiners" (Barry, 2022). The movement inevitably fractured, being labelled as racist by many onlookers, including other feminists (Stockman, 2018).

Exposing and utilizing existing rifts in the American socio-political fabric is a standard tactic used by Russia. These rifts not only provide ready controversy but also a number of willing participants. The use of proxy messengers, whether unofficial news outlets or everyday American citizens, is a hallmark of Russian strategy (Global Engagement Center, 2020, 8). Indeed, the dependence on American citizens to play an important role in the propagation of narratives is one of the largest challenges posed by this sort of warfare. As made evident in the coming chapter, the exponential spread of manipulated information can make it difficult to trace its source and successfully camouflages foreign interference within the existing social environment. The breakers of the 2017 Women's March were not Russians, but Americans ready and willing to hitch themselves to narratives presented to them, especially those that suited their cognitive disposition. The primary agents of chaos are Americans themselves, unknowingly acting in cooperation with foreign governments.

The overall process fits neatly with both historical and contemporary Russian international strategy. In 1997, Russian grand strategist and political theorist Aleksander Dugin wrote that the country's foreign policy in the post-Soviet era should focus on undermining Atlantic influence in Eurasia. To do so, he noted that Russia should use a "fairly sophisticated program of subversion, destabilization, and disinformation spearheaded by the special services" (Dunlop 2004, 47). Vis-a-vis the United States, Russia should instigate forms of instability (Dunlop 2004, 50). "It is especially important to introduce geopolitical disorder into internal American activity, encouraging all kinds of separatism and ethnic, social and racial conflicts, actively supporting all dissident movements-- extremist, racist, and sectarian groups, thus destabilizing internal political processes in the U.S. It would also make sense simultaneously to support isolationist tendencies in American politics" (Dunlop 2004, 50). Chaos within the liberal world's foremost nation produces many benefits for Russia. Most importantly, it harms the image of the United States and helps facilitate a political turn towards dysfunction, populism and, subsequently, authoritarianism. American allies around the globe are growing concerned by American social division (de Graaf 2021, 923). Growing skepticism towards multilateral institutions like NATO, led primarily by Donald Trump, also harms American relationships with allies.

Russia's modus operandi is the weaponization of ideology (Dawson and Innes, 2019, 251). They recognize existing divides between the rich and the poor, racial and ethnic groups, protest movements, and other social schisms, exploiting them to create chaos within a rival's domestic political sphere. They sow discord and rupture trust in the spirit and institutions of the United States (United States Department of Justice, 2021). They use humour and short-form messaging to reach broad audiences. While their attempts to divide Clinton's potential electoral base and their interference in the women's rights movement are two particularly salient examples, their efforts continue to this day and spread far beyond these two communities. With a specific focus on fear-mongering and alienation, they are likely to continue their efforts until they perceive a shift in the cost-benefit analysis.

This form of information warfare should be of particular concern to the United States. It threatens the public's ability to reach informed conclusions and deepens polarization (Colomina et al., 2021, 13). Its deliberate abuse of existing social divides multiplies these problems. Russia puts relatively little effort into shaping American minds to fit its policies and visions for the world, instead focusing on undermining the basic functions of liberal democracy. Russia's strategy of information warfare within the United States is less about the construction of a story and more about the destruction of the political system.

Chinese Information Manipulation

Interestingly, China's strategy of information obstruction has, at times, looked remarkably different. Although their policies are beginning to converge with Russia's, their efforts during the 2010s and early 2020s were relatively constrained. Rather than divide the broad populace of the target, China tends to focus heavily on their diaspora. They strategically influence students by using Confucius Institutes, a network of institutions existing on foreign university campuses. Located across every populated continent, including over one hundred in the United States, "they provide Chinese-language instruction and various cultural offerings through a presence on university campuses in dozens of democracies" (Walker, 2018, 13). The Confucius Institutes are a mechanism by which the government can directly influence their citizens abroad. The group has blocked academic speakers who are critical of Chinese policy from speaking on campuses (Walker, 2018, 13). Through channels like these, China influences overseas students to manipulate academic coverage of China (Allen-Ebrahimian, 2018). Student groups worldwide took action in response to the protests in Hong Kong. At McMaster University in Hamilton, Ontario, the Chinese Students and Scholars Association was briefly banned from campus in response to their alleged ties to the Chinese government (Mowat, 2019). Pro-Hong Kong protests around the globe have been met by opposition from similar groups in recent years as China works hard to cement its sovereignty over the city. Confucius Institutes provide cultural information in a way that might be described as similar to other methods of exercising soft power. China sees it as important to keep its diaspora in line and understands that loyal Chinese citizens abroad can act as unique messengers, presenting China's ideal image to the world.

The diaspora is both an agent and a target (Taehwan, 2018). The Chinese government depends heavily on the diaspora to echo government narratives and defend core Chinese interests and expects those in privileged positions to help facilitate technology transfer in China's favour (Schäfer, 2022, 6). They are expected to be purveyors of soft power and public diplomacy. This dependency is both a strength and a weakness of Chinese information strategy, given individual members of the diaspora's heterogeneous opinions of the Chinese state. Indeed, most individuals of Chinese descent living outside of China are unwilling to align themselves with Beijing's policies (Schäfer, 2022, 6). China relies on both incentives and coercion to shape the actions of the diaspora (Wong, 2022, 608). Their policies range from surveillance and the issuing of threats to the promise of political connections and economic rewards (Wong, 2022, 617). WeChat is a popular tool for Chinese information agents targeting the diaspora. However, Chinese WeChat penetration into the American information sphere is limited, especially in comparison to similar Russian efforts (Harold et al., 2021, 44). Given the scarce use of the app amongst the broader American population, the Chinese diaspora is the most significant user base of the app in the United States (Harold et al., 2021, 44). It is likely that when China does seek to influence high-level actors in the American sphere through social media applications, it focuses on members of the Armed Forces, aiming to affect their disposition toward any operations China deems unfavourable (Harold et al., 2021, 120).

Moreover, China has invested significantly in the capture of foreign media and further uses its state media enterprises to improve its image abroad. The Chinese government has found it beneficial to be the architect behind the stories that people see. John Fitzgerald emphasizes

China's comprehension that control over foreign media allows them to achieve their foreign policy goals more efficiently (2018, 59). He presents the case of Australia, a relatively close neighbour to China and home to a significant portion of the Chinese diaspora. The Australian Broadcasting Corporation stands as a central source of information for those living in Australia and has worked to provide Chinese language programs to reach the large population of Mandarin and Cantonese speakers that reside within the country. The Chinese language content broadcasted by the network was deemed to be unacceptable by the Chinese government (Fitzgerald, 2018, 62). In light of this, China worked to reach a lucrative sponsorship deal with the network that hinged on removing the content in question (Fitzgerald, 2018, 62). After introducing the new rules, the broadcaster frequently censored coverage in favour of the Chinese demands (Fitzgerald, 2018, 62). We can identify the same pattern in New Zealand, where several formerly independent media institutions came under partial control of the Chinese government (Brady, 2018, 71). In general, China aims to construct an international media network of loyal broadcasters, all united in their positive coverage of the country and its government. The Chinese state media companies "have used mergers and partnerships to claim niches in foreign markets for radio, television, and online content", giving them immense control over how their image might be displayed to the outside world (Brady, 2018, 69). Importantly, both Australia and New Zealand serve as staunch American allies in the South Pacific, both members of the Five Eyes intelligence sharing alliance and fundamental to American strategy in the region.

Capturing media in America, however, has proven to be more difficult than in the South Pacific. Chinese influence is thus perpetuated largely by social media, including through applications like TikTok and WhatsApp. Much of China's focus in recent years has been directed at countering conspiracy theories regarding the origins of the COVID-19 virus. Early in the crisis, this included a strategy of undermining conspiracy theories and supporting the argument that the virus originated in wildlife rather than a military research lab (Consentino, 2021, 62). Later in the crisis, the focus shifted towards manufacturing a narrative that the virus was genetically engineered by American bioweapons laboratories and introduced into China as a means of harming their international image (Consentino, 2021, 63). This narrative, importantly, was less about damaging America's image and more about defending China's. The narrative did not begin until after the mass spread of anti-China narratives, which mostly gained traction in the United States through media sources such as Fox News (Consentino, 2021, 64). Thus, it operated more as a counter-narrative than as an original attempt at undermining America. Overall, China's efforts to manipulate the American domestic sphere are far more restrained than Russia's. Rather, China seeks to undermine American influence in other populations around the world, particularly in regions within East Asia.

One of the few instances where Chinese information manipulation has historically appeared similar to Russia's is in Taiwan (Cohen, 2021, 13). Their goal is to cultivate support for reunification from the ground up and use narratives to shape Taiwanese political opinions (Hille, 2018). Focusing on the individual, they target small groups and hope to entice them to support China-friendly policies (Hille, 2018). They seek to undermine anti-Chinese political parties and work to grow a new generation of supporters for mainland China in Taiwan. They do so by using *zhuangjiao*, or grassroots operators that participate in anything from "friendly neighbourhood chats, to backroom deals, to mobilization and outright vote-buying" (Hille, 2018). Institutions like the United Front further work to build support for Beijing in areas like Taiwan, Hong Kong, and Macau (Kynge et al., 2017).

Chinese information campaigns that indirectly target the United States can be seen in Singapore. Taking advantage of the city-state's ethnic ties to China, the government of Singapore is particularly concerned about Chinese influence operations that seek to undermine social cohesion and make the country ungovernable, making it difficult for the United States to operate from the island (Harold et al., 2021, 81). The Philippines, with a population wavering in trust towards the United States, is another potential target. There is no evidence, however, that China is involved in any caustic information campaigns targeting the country as of yet (Harold et al., 2021, 92). Rather, they focus on soft power influence initiatives through the Chinese language press (Harold et al., 2021, 96). Further potential to take advantage of anti-American sentiments exists in Japan, especially concerning the presence of American military bases in the country. Similarly to the Philippines, however, there is little evidence of significant Chinese information operations targeting the nation. Subtle exercises on the island of Okinawa, home to an American military base, were conducted in 2015 (Hsiao, 2019). These efforts aimed to foment questions about Japanese sovereignty over the island, exploiting existing opposition towards the Japanese government (Hsiao, 2019).

In general, Chinese information strategy has thus far focused little on creating chaos within the American social sphere. Rather, the Chinese approach is more constructive, seeking to achieve palpable improvements to their image, and at worst, influencing elections in a manner that benefits their economy or relationship with the American government. In the cases where China has taken a harder approach, they dedicate their attention to American allies in their geographic region rather than targeting American citizens directly.

Experts worry that China's modus operandi is beginning to shift. Subtle changes to strategy that aligned more with the Russian playbook appeared during the 2022 midterm elections, with China using TikTok to target politicians from both political parties (De Luce & Grumbach, 2024). The 2024 presidential election will be a major demonstration of the policies China intends to use in the future. Already, reports of Chinese interference based on strategies of division are being detected in the American information environment (Hsu & Myers, 2024). Two possible explanations may be proposed for the shift in policy. It is possible that China has improved its capabilities in the past handful of years and has recognized the advantages of the Russian strategy. However, the capabilities required to engage in caustic information warfare are not particularly advanced. Russia's Internet Research Agency comprised a small group of agents who used a relatively simple network of troll accounts to spread their narratives. As previously discussed, policymakers have long understood the advantages of fomenting division in foreign societies. It is also possible that China's relationship vis-a-vis the United States has changed, with evidence for this argument supported by their use of these forms of manipulation arising in the post-Trump era, alongside a trend of decreasing trade (Brown & Wang, 2023). If the status of bilateral relationships can affect information strategy, this opens the door to interdependence as a defence mechanism.

The theoretical benefits of engaging in anti-American information campaigns are as valuable to China as they are to Russia. Authoritarian regimes, with interests fundamentally different from those of the West, gain from the erosion of liberal democratic values (Hinšt, 2021, 96). Increased polarization within the United States, the world's foremost democracy, can depreciate its status. For an attacking state, the degradation of America's image as a functioning democracy undermines its moral authority and leadership amongst Western countries. This can deliver significant benefits to a state seeking to subvert liberal order. But China has been historically hesitant to engage in the type of divisive rhetoric used by Russia, and they have previously avoided targeting the United States directly. Thus, a difference in strategies is present, deserving further scrutiny.

B. Political Circumstances

Why have China and Russia chosen to engage heavily in information manipulation, and why have their strategies varied so much? Understanding these questions requires closely examining the political and economic circumstances in which the two states find themselves. Information obstruction campaigns can provide significant benefits to states that choose to use them. This is particularly true for states on the weaker side of an asymmetrical conflict. Propagating information is far cheaper than investing in military armaments. The defending state in our case study is the United States, and neither Russia nor China can yet match their conventional military power. Given the power gap between the two aggressors and their target, it is prudent for them to engage in other means of challenging American prowess beyond military strength. Of course, information strategy is supplementary to traditional internal balancing. Still, the material reality plaguing Russia and China requires them to utilize a multi-pronged approach to gain relative power vis-a-vis the United States.

Russian Political Circumstances

Russia's geopolitical position has weakened since the end of the Cold War. Much of their military power was dismantled in the wake of the dissolution of the Soviet Union. In the collapse of communism, Russia lost the identity it had been working to spread throughout most of the twentieth century. The country was weakened both militarily (Meyer, 1995, 322) and in its image (Rutland & Kazantsev, 2016, 395). In particular, Russia's manpower decreased to a quarter of the size it was during the height of the Soviet Union (Meyer, 1995, 323). In light of this, the state has had to rebuild and find new ways to exercise power. Bohdan Harasymiw contextualizes the condition of Russian internal affairs by explaining how the country fell into a state of rapid political change and transition following the Cold War (2011, 401). While it seemed Russia was on the road to democratization, the country fell short of achieving this goal (Harasymiw, 2011, 401). Instead, Russia has stabilized as an authoritarian regime. With the rise of Vladimir Putin, Russia found a new strongman to begin challenging the West, but still lacked relative power regarding the country's political rivals. Russia is in a unique situation, weakened by its past but eager to maintain its position in the global hierarchy of states. This has paved the way for its contemporary methods of power projection.

While Russia has returned to conducting military operations, it has mostly refrained from involving itself in far-off global conflicts. The country has instead chosen to focus almost exclusively on asymmetrical wars close to its borders or internal disputes. Unlike the United States, it has refrained from large-scale overseas military operations. While their involvement in Syria and their use of paramilitary groups in Africa both stand as recent exceptions, the majority of Russian conflicts since the fall of the Soviet Union have been relatively local. Even their forays into traditional soft power have failed. "It is hard for a country facing economic stagnation to project a positive international image" (Rutland & Kazantsev, 2016, 395). Hosting the 2014 Olympic Games in Sochi resulted in significant negative press coverage, culminating in the uncovering of a massive state-sponsored doping program (Rutland & Kazantsev, 2016, 404). This conspiracy has only damaged Russia's international image. Russia has fallen far behind in the battle for international status and failed in its few overt attempts to establish soft power. They have less to work with in terms of traditional sources of power in comparison to their rivals. And yet, Russia has been at the center of geopolitical crises in recent years and has carved a role for itself in the contemporary international system. This is a result of their adaptation and usage of alternative forms of power.

Chinese Political Circumstances

China has also faced a tumultuous recent past, and immense challenges related to its massive population. They face the unique struggle of needing to keep more than one billion people under the control of an authoritarian political system and uninfluenced by negative coverage of the Chinese Communist Party arising from external sources. This is a matter of existential importance to the Chinese government. Especially in the wake of the Tiananmen Square massacre, the government has worked hard to keep public dissatisfaction with the regime under wraps (Sarotte, 2012, 156). China has seen former great powers, including those with authoritarian-style governments like the Soviet Union, completely collapse, and has stood by while much of the world faced a wave of democratization. This was a major concern to the Chinese Communist Party (Sarotte, 2012, 166). In a world facing major changes, the Chinese government has been forced to use a heavy hand in domestic affairs to maintain its hold over the country. It is in this reality that Chinese information initiatives have come to life.

Although not as weak in terms of relative soft power as Russia, China still faces a scenario that traditional strategies are hard-pressed to solve. Hard power cannot stop citizens from going overseas and becoming accustomed to the ways of a free society. Although China maintains a stronger level of soft power than Russia, authoritarian regimes tend to be weaker on this front than free societies like the United States (Robert, 2018, 41). They have found that the best course of action has been to couple their cultural abilities with contemporary information strategy. Notably, China spent roughly ten billion dollars in 2015 on external propaganda efforts, paling in comparison to America’s public diplomacy budget of roughly six hundred million dollars (Shambaugh, 2015, 100). If China seeks to continue its rise to the top of the international hierarchy, it must find strategies to realistically achieve its foreign policy goals. Against a rival as powerful as the West, China is not prepared to undergo major military operations (Roberts, 2018, 44). The price to pay is too high, and the odds of winning are too low. However, China does not immediately need to face the West through military initiatives. China understands that exercising power and gaining leverage over rivals can be achieved through alternative means. “Even if China does not seek to conquer foreign lands, many people fear that it seeks to conquer foreign minds” (National Endowment for Democracy, 2017). Beijing has determined that ideational influence and the obstruction of foreign information spheres suit its needs.

The material realities facing Russia and China have required them to seek alternative strategies to improve their geopolitical standing. But how does information obstruction relate to relative power? Take the example of contemporary Russia. There is an ongoing draft of young citizens to fight in a terrible war, a stagnating economy, and a largely decaying authoritarian government based on a cult of personality around one individual, all of which challenge their ability to present a soft power-based argument regarding the prestige of their nation. Russia, however, has determined that it does not need to put significant focus on improving its own image. Key here is the importance of relativity to the concept of power (including soft power, and international status). Russia has determined that while it may struggle to improve its own image, it can instead make Western democracy and values appear less enticing (National Endowment for Democracy, 2017, 9). Damaging the image of the United States lowers its relative superiority over the authoritarian world. The strategy is a concerted effort to erode the prestige of liberal democracy as an institution.

Economic Relationships and the Threat of Pariahdom: A Mitigating Factor?

Both the existing economic relationship with the United States and the country's international image may serve as mitigating variables in the attacker's choice of information strategy. Russian interdependence with the West has been minimized in recent years. This can be seen most notably in the oil and gas industry. Russia faces sanctions from the United States aiming to disrupt its long-term production capabilities (Brown, 2020, 2). Sanctions have been central to American policy vis-a-vis Russian aggression. Focus has been put on punishing specific key individuals in the Russian regime (Rennack et al., 2021, 2). Notably, Russian behaviour has not changed despite increasing pressure from the West. Sanctions are a crucial part of the broader decline in relations between Russia and the United States. Total combined imports and exports between the two nations have only accounted for two-hundred and sixty-four million dollars thus far in 2024, a meagre number compared to other countries of similar size and influence (International Trade Data, 2024, 16).

The general trend for Russia is one of increasing isolation. With their removal from the international SWIFT banking system, and their ongoing war against Ukraine, this trend will continue. Russia, for its part, has shown resistance and a general lack of concern towards their increasingly isolated position. Western sanctions have had a limited impact on Russian finances (Rennack et al., 2021, 2). Their economy has continued to grow at a modest rate, and they suffered more from economic crises related to COVID-19 than from sanctions (Rennack et al., 2021, 2). In totality, Russia has little remaining economic connection with the United States.

They have repeatedly demonstrated that they are willing to bear the burden of being considered a pariah state in the international community, likely calculating that the benefits of being viewed as powerful outweigh the costs of being perceived as immoral.

China's relationship with the United States is distinct from Russia's. While China also faces sanctions, their level of trade with the United States is significant. Thus far in 2024, nearly fifty billion dollars worth of imports and exports have been exchanged between the two countries (International Trade Data, 2024, 16). In recent history, China helped stabilize the collapsing American banking sector during the 2009 economic crisis (Gou et al., 2010, 17). China's significant holdings in American dollars leave them relatively exposed to the American financial market (Thompson, 2010, 127). Nonetheless, much of China's growth over the past decades has been a result of its economic policies, and foreign direct investment has been key in accessing foreign technology sectors (He, 2009, 27). China is also the second largest state holder of American debt, totalling roughly nine hundred billion dollars (Labonte & Leubsdorf, 2023, 2). China and the United States are deeply intertwined with one another. Their relationship extends far deeper than the American-Russian relationship.

China has also invested significantly in constructing a positive image of itself abroad. Elements of this campaign include the Belt and Road Initiative, a concerted grand strategy aimed at superseding the United States as the global hegemon (Weil & Munteanu, 2020, 2). The Chinese government stresses these economic programs as a method of strengthening global ties and fostering positive approval ratings of China amongst global citizens (Economy, 2018, 223). This stands in stark contrast to how Russia has operated in recent years, showing little care for its growing identity as an international outcast. China, on the other hand, has been far less extreme in its actions, with the notable exceptions being its continued stance against Taiwanese sovereignty and its operations in the South China Sea. Nonetheless, they have not engaged in material warfare on the same scale that Russia is presently waging in Ukraine. Both China and Russia aim to raise their positions in the global hierarchy. China has sought to achieve this through economic and soft power strategies, while Russia has resorted to using hard power in its geographic neighbourhood and divisive rhetoric to subvert its enemies.

Chapter 3: Evaluating Defence Strategies

A. Deterrence

Deterrence and social resilience are the basis for contemporary American information defence. Deterrence, at its best, aims to prevent hostile information obstruction from being waged in the first place. A secondary possibility afforded by deterrence is to alter the attacker's choice of strategy, potentially influencing them to choose less damaging options. Deterrence traces its history to material warfare. When costs and benefits are readily apparent, the process of manipulating an opponent's calculations is easier to achieve. This process may be more difficult to accomplish in the immaterial information environment. To the attacker, benefits are often delivered slowly over a long period and are far less tangible than material alternatives. For the defender, instituting equivalent costs for adverse behaviour may be difficult for several reasons, including the difficulty of attribution, the question of whether attacks meet the threshold for response, and asymmetry between information spheres.

Nonetheless, the basic process of prevention via the manipulation of an actor's cost-benefit analysis is still theoretically reasonable within the context. Rather, the question becomes *how* targets like the United States may implement the concept. Indeed, American policymakers have tried to formulate deterrent measures against information obstruction

(Department of Defense, 2023, 9). Despite these efforts, however, Russia and China have continued to obstruct information **(**De Luce & Grumbach, 2024**)**. As such, it is important to evaluate the theoretical underpinnings of different forms of deterrence to determine potentially functional practices. The ultimate goal of democracies like the United States should be to develop feasible deterrence in response to information obstruction, as the practice serves as a strong first line of defence. Even partial deterrence that is effective in shaping strategy may help prevent more damaging forms of foreign interference.

Deterrence by Denial

A concept drawn from the literature on military strategy, deterrence by denial seeks to reduce the likelihood of an unwanted action succeeding (Snyder, 2015, 15). Within the context of information warfare, it appears theoretically promising at first glance. The example of Russia dividing the Clinton campaign's potential voter base relied heavily on correspondence stolen through a cyber attack. As noted, scholars are relatively convinced of the feasibility of cyber deterrence, where democratic states can attribute actions to states, deny in real-time, and be norm entrepreneurs in the online realm (Goodman, 2010, 112; Jasper, 2017, 165; Mazanec & Thayer, 2015, 47). Furthermore, in theory, the diversity of opinion and beliefs within democracies like the United States should provide citizens with the opportunity to analyze and subsequently select the information they deem to be trustworthy. Well-established and rigorous news sources should drown out falsity within an open system, and provide citizens with the opportunity to correct misguided beliefs (Humprecht et. al, 2020, 500). As such, the populace of a democratic state should be able to resist less-than-accurate information. With this assumption, opinions regarding reality should trend closer to factual evidence, allowing citizens to refute what they perceive as false information easily. These citizens of open information systems are perceived as followers of experts. In the United States, the news media may play an important role as a trustworthy information provider and, in theory, will present objective facts regarding particular topics. Scoring high in media openness, the United States is defined by its diversity of opinion and the concept of freedom of expression (Stier, 2015, 1288).

The public square in the United States, however, has moved online. With social media allowing for the mass propagation of a near-infinite amount of narratives, citizens can search for content that suits their pre-existing biases and lessens cognitive dissonance. Further, the general process of using social media to spread manipulated information requires no concerted cyber attack, leaving elements of cyber deterrence concerning strikes on physical or digital infrastructure useless within the context. America's open information sphere allows individuals to receive information in the format and predisposition that suits them. The presence of diverse opinions can foster unintended consequences. As an evolutionary tool, the human brain simplifies its surroundings into a workable schema. It works to dampen cognitive dissonance (Jervis, 2017, 382). It formulates a worldview and seeks to incorporate any information it receives into this existing map (Jervis, 2017, 143). People will often ignore information that does not fit into their preconceived notions of things (Jervis, 2017, 143). Furthermore, research has established that people tend to be most accepting of the first information they receive, and refer to it when faced with contradictory evidence (Paul & Matthews, 2016). This is the reality that has been used by Russia and China to formulate approaches to information obstruction. Russia's firehose of falsehood technique takes particular advantage of these circumstances: information attacks are high-volume and multichannel, they are rapid, continuous, and repetitive, they lack a commitment to objective reality, and they lack a commitment to consistency (Paul & Matthews, 2016). This high-volume broadcasting of opinionated and often inflammatory information can engulf the American media environment and undermine the importance of evidence. Combined with the human tendency to seek knowledge that conforms to an existing worldview, the strategy can be enormously effective in producing division and confusion within a society. Furthermore, trust in expert opinion declines as the number of arguments increases (Flanigan & Metzger, 2013, 1628). The search for truth becomes even less important and more difficult with a large variety of available information. Peer influence becomes significant in a high-volume environment as well.

The diversity of opinion in media and online within open systems may counter the state's ability to quell the spread of damaging information. As citizens will have access to a broader set of opinions, they may be more willing to accept and be affected by alternative explanations. As people tend to seek evidence that conforms to their worldview, simplifies explanations, and lessens cognitive dissonance, America's information environment is particularly weak towards polluted information from abroad and false or biased narratives concerning contentious subject matter. Furthermore, the fundamental tenet of free speech that is unassailable in the United States poses a challenge to a government's ability to counter unwanted narratives from taking hold and spreading within society. "Purposeful deception and accidental misleading statements have all at one time or another had their day in court and, to a certain extent, won the protection of the First Amendment " (Spicer, 2018, 47). While open media systems present citizens with the opportunity to find accurate information, this is dependent on people choosing to seize the opportunity. If they instead fall into cognitive shortcuts and simplified explanations that fit their worldview, then the inherent diversity of information present within the system may lower the degree to which people attempt to seek objective or benign information.

Denial is only feasible if states can create defences that impede the likelihood of an unwanted action succeeding (Snyder, 2015, 15). Here, it is often argued that social media corporations can play a large role in countering manipulated information through the identification of bot accounts, banning of individuals trafficking in hate speech, and being overall heavy-handed with the enforcement of their terms of service. However, social media companies may be hesitant to ban individuals at risk of losing profit, and scholars have noted that mass banning induces individuals to migrate to platforms more accepting of their views, resulting in the creation of echo chambers (Cinelli et al. 2022, 3). This only delays the problem, as users subjected to information spread by bot accounts on less popular and less moderated platforms may return to established social media sites to repeat what they have previously encountered. Furthermore, fact-checking measures on Twitter are characterized by a time lag of thirteen hours between the sharing of false information and correction (Shao et al., 2016, 3). So while deterrence by denial is cited as a paramount strategy regarding cyber conflict (Nye, 2016, 56), it is far more difficult to apply to intangible information obstruction.

The democratic values of openness and freedom of speech are paramount, and information within the United States flows more or less freely. To prevent these values would be paradoxical to democracy as a system. In this way, the United States, and democratic countries in general, are caught in a catch-22. To interfere with the flow of information, which may be necessary to stop targeted information obstruction campaigns, they must commit to inherently undemocratic policies. Furthermore, they will certainly face pushback from society at large, further increasing polarization and dissatisfaction with the government. However, allowing the continuance of such media attacks puts the country at risk of greater internal fracture. While democracies may be able to prevent adversaries from gaining access to damaging information through cyber attacks, they will remain hard-pressed to prevent obstruction that does not depend on material means.

Deterrence by Punishment

Deterrence by punishment, another concept drawn from military strategy, is similarly challenged. Here, the subject matter of a specific obstruction campaign is of particular importance. When attempting to signal the threat of punishment, does the mere amplification of pre-existing caustic rhetoric or the purveying of soft propaganda meet the threshold needed to validate retribution? What kind? In countering information obstruction campaigns, the United States must be wary that much of the manipulated content has some basis in subjectivity or involves the repetition of narratives already shared by citizens. The problem is multiplied vis-a-vis Chinese efforts, which are thus far more subtle and can often be described as advocacy or promotion of their own ideals. In cases where China takes a harder approach, it is often targeted at American allies rather than the United States.

Attribution remains key to deterrence (Clark & Landau, 2010, 25), but the attribution of information campaigns is not as simple as tracing a cyberattack on infrastructure. Nefarious actors take advantage of willing citizens to spread manipulated information on their behalf. One message delivered to one individual can be spread exponentially. Imagine a piece of disinformation reaching one sole individual, who then shares it with family around the dinner table. This process continues onwards at other dinner tables amongst family and friends, spreading quickly. One friend three instances down the line can post the narrative online, where it can go viral. Tracing the source of a claim is incredibly difficult. Often, a polarizing opinion pushed by a foreign adversary is not their construction, but rather the amplification of existing narratives. Adversaries are not inventing the divisions seen within democracies around the world, but are stoking the flames of a fire that has been burning for decades or longer.

Even if the United States can correctly attribute and chooses to engage in retribution, perceiving the totality of information efforts from Russia or China to be worth responding to, the credibility of an adequate and equivalent retaliation is threatened. Media environments differ between states. One of the key variables that defines the distinction between open and closed information environments is the number of accepted views within a society. As stated, the United States is characterized by its tolerance of diverse viewpoints, and the state can not prevent people from believing or voicing opinions. Authoritarian states like Russia and China, however, are defined by their non-acceptance of information diversity. Citizens are not only prevented from voicing opinions divergent from those accepted by the state but may also have less access to diverse information in general. In particular, authoritarian states tend to censor politically symbolic messages (Han & Shao, 2022, 1355). The use of censorship may result in more uniform views across the population of closed systems. By this logic, countries with less media freedom may have a lower diversity of beliefs, and the population is more likely to follow the narrative provided by the state apparatus.

Government control over information provides the closed regime with distinct advantages to quell obstruction or unwanted narratives in a way that the United States cannot realistically match. While democracies depend, by definition, on the free flow of information, authoritarian governments have an enormous ability to shape narratives. Under this assumption, we can expect that any counter-narratives pushed by the United States as a method of deterrence by punishment will have difficulty gaining a foothold within closed societies that do not wish for these narratives to be present. In line with the discussion on cognitive tendencies, closed systems should also dampen the effect of the firehose of falsehood technique. The United States will face challenges in flooding an information system that is unwelcome to its influence. While individuals still aim to simplify information into pre-existing schemas, the lack of diversity in information may limit a person's ability to deviate from the state's established story.

Given these factors, it is apparent that while democratic information spheres are theoretically weak toward information warfare, authoritarian information spheres are relatively closed and thus far more secure within the context. Any attempt to deter through punishment should be reasonable, proportionate, and credible. As made evident by the asymmetry in information spheres, responding in a tit-for-tat manner can be a difficult task for the United States vis-a-vis its authoritarian adversaries.

Deterrence by Entanglement

A third option, deterrence by entanglement, may prove more feasible. Interdependence between two states can reduce the probability of conflict (Russett & Oneal, 2001, 126). The goal is to alter an adversary's cost-benefit analysis by giving them a stake in the game (Brantly, 2018, 9). If the adversary risks suffering from attempts to destabilize a society, they may be deterred from engaging in these types of strategies.

Here, the case study of China vis-a-vis the United States becomes important. The desired economic goals of the United States are not necessarily mutually exclusive from Chinese economic goals. Both countries are among the other's largest trading partners, and the prospect of economic growth is an enticement for each. If it is the case that both countries perceive this interdependence as beneficial, then we can consider this an example of Keohane's concept of harmony (2005, 53). Under this assumption, it is in the interest of the Chinese government to seek a stable United States with a predictable set of policies. However, as populism rises in the United States, the positive perception of the Chinese relationship is declining. Perhaps small adjustments can be made in American policy to produce an approach that is palatable to the populace, in which case the potential for cooperation remains (Keohane, 2005, 53), but increasing discord in American politics, the growing realization that the countries are peer competitors, and the overall rise of nationalism within each challenges this possibility. Nonetheless, if China perceives a stable and predictable America as favourable, there are no benefits to creating social discord within their domestic sphere. This does not preclude the use of information warfare to achieve other goals (a recent and notable example of which revolves around the origin of COVID-19) but does demonstrate that interdependence can influence a state's cost-benefit analysis. This provides a challenging, but theoretically feasible method of deterring specific forms of information warfare.

The potential costs of destabilizing the United States are clear to China. In 2017, the United States imposed a ban that prohibited American companies from selling to Chinese technology giant ZTE, claiming they had provided American technology to North Korea and Iran (Yong, 2019, 114). Almost immediately, ZTE agreed to pay a billion-dollar fine and allow American compliance teams to survey the company, avoiding the potential loss of over seventy thousand jobs in China (Yong, 2019, 115). Generally, in the realm of technology, China has been willing to provide concessions to the West to maintain a valuable trading relationship (Yong, 2019, 115). Certain groups within the United States have a similar understanding of how trade between the two countries can be beneficial. Edwin Lai notes that American corporations that export or import products to or from China, highly educated voters, and traditional Republicans all tend to have an aversion to policies that hurt interdependence (2019, 173). Importantly, these three categories were not highly represented among those who voted for populist candidates like Donald Trump in 2016. Blue-collar workers, who showed significant support for Trump in the elections, were those who tended to prefer policies that affected the Chinese-American trade relationship (Lai, 2019, 172). This was the inevitable result of an unemployment crisis and stagnating wages that could all be traced to bilateral trade between the two countries to some degree (Autor et al., 2013, 2121). Indeed, these crises help grow populist tendencies among the American populace (Nelson, 2019, 33).

When bilateral trade between the two countries came under scrutiny during the Trump administration, the United States lost more than nineteen billion dollars as a result of Chinese retaliatory tariffs (Zheng et al., 2023, 225). China, on the other hand, lost more than thirty-four billion dollars in 2019 as a result of the initial American tariffs (Zheng et al., 2023, 228). The Trump-China trade war demonstrated very clearly that each country took on net losses when performing actions that threatened the other. China in particular is poised to lose heavily in the short term, with economic warfare threatening to slow GDP growth and lower the standard of living for the Chinese middle class (Lai, 2019, 176).

Nonetheless, hostilities continue to grow. Rhetoric has taken an antagonistic turn, and much of the American population blame the country for the COVID-19 pandemic (Hass, 2021, 1). This hostility, combined with each country's fear of being dependent on the other for key resources, has begun a slow process of uncoupling. Deterrence by entanglement may become as difficult as deterrence by denial or punishment if the gap between the two nations widens. A rapprochement between the two superpowers is still possible, however. The two worked together in the face of Soviet expansionism during the Cold War (Hass, 2021, 156). Realists would note that China and the United States may find common ground on the subject of constraining

Russian imperialism. Still, China's conception of the United States as the larger threat is made evident by its positive rhetoric regarding its relationship with Russia. Regardless, China has shown a willingness to engage with other powers on points of friction, including Japan, India, and the European Union (Hass, 2021, 160). China is somewhat dependent on foreign imports and would be hard-pressed to cease trading with the United States. In terms of allowing for a process of deterrence of caustic information warfare via entanglement, the United States should continue to find common ground and be cognizant of the risks that arise from deteriorating relations. It will come down to a cost-benefit analysis, with the American government weighing the pros of becoming less dependent on Chinese goods and services and the cons of a China unconstrained by the costs of harmful actions. Given Russia's willingness to engage in destructive behaviour, it should be clear to American policymakers that each decision on this issue will have major implications on Chinese calculations.

China is left with a puzzle. They should avoid using policies that help grow populist movements in the United States. Importantly, as long as China remains heavily intertwined with the American economy, it should not engage in information obstruction campaigns that seek to foster a chaotic American politics. Rather, if they are to manipulate the American information sphere, they should do so in a manner that strengthens liberal free trade ideology and avoids deepening the divide between the rich and the poor in the United States. They should also seek to shift the blame for the poor state of the American economy off of their shoulders and onto other scapegoats. Importantly, this scapegoat should not create an unpredictable, hostile, or isolationist American public. Thus, existing interdependence has the power to restrain China from seeking to erode the domestic American political sphere. This may help explain why their obstruction campaigns have been relatively moderate compared to Russia, which loses little from the degradation of American politics. Interdependence does not preclude information warfare from China's arsenal but may shape it in a manner that is less damaging than the alternative. Regardless, given the potential shift in Chinese strategy, the United States must be prepared to use methods beyond deterrence to prevent serious damage from information warfare.

B. <u>The Challenges and Advantages of Approaches to Build Social Resilience</u>

A government trying to influence a citizen who is untrusting of the establishment is much like a person trying to reach their ex-partner through the phone. You have already tried to make it work, they have already given you a second chance (at which you failed miserably); they are not going to pick up. You shall forever proceed straight to the answering machine, they have blocked your number.

The above metaphor is an unorthodox way to open a section of a thesis. It is colourful but unprofessional. It is a *bathos*, a vulgar turn of style used to capture the reader's attention. It also conveniently demonstrates three factors that are critical to the content discussed in this chapter. This opening metaphor very simply introduces a central issue undermining the feasibility of building social resilience: in a society plagued by both conspiracy theories and legitimate grievances towards the practices of the state, a central government attempting to publish what it deems to be 'correct' is certain to face pushback and reach only a negligible audience. Those who lack trust in their democratic institutions are difficult to influence, and they are among the most susceptible to information obstruction campaigns.

Furthermore, the paragraph stands out from the rest of the thesis. For the reader, especially one who is not an expert in the dull and monotonous intricacies of political science, it may be the one part of the paper that they remember. Successful information campaigns, especially those stemming from Russia, are shaped by the same guiding philosophy. They are short and often humorous chunks of text, images, or videos. They seek to capture an onlooker's attention above all else. They are constructed out of emotionally provocative stories and old folk tales about the generalized traits of others.

Finally, the metaphor is written in an unprofessional manner. Given the rigid structures of academia, it may very well induce some pushback from the supervisors and second readers responsible for ensuring I meet the very official and occasionally inflexible guidelines for scholastic research. But I ask the reader to question whether the official publications of democratic governments may be subject to the same guidelines. In 2019, during a bizarre internet fad about a citizen-led raid on the Area 51 Air Force base, the United States Department of Defense tweeted out a photo of a squadron of soldiers standing in front of a B2 Spirit bomber. They captioned the tweet with the following text: "the last thing #Millenials will see if they attempt the #area51raid today…" (Pickrell, 2019). This tweet was clearly in jest and an example of the American government leaning into an *in-joke* that was rapidly taking society by storm. They were immediately put under fire by citizens and officials alike and were forced to issue an apology the following day (Pickrell, 2019).

Democratic governments face immense challenges in reaching the most vulnerable sectors of society. They face an intangible threat that often leans into humour and unprofessional narrative structure while being significantly constrained by the ethical and moral guidelines that are expected from a democratic state. Authoritarian adversaries, especially when operating in foreign information spheres, do not face the same restrictions. They can, for lack of a better term, do all in their power to burn the system down without regard for what is *right* and *wrong* in the field of public communications. Asymmetry is not only present between the structures of information spheres but also in the ways democracies and authoritarian states can act within them.

Trust

To build social resilience against information obstruction, a democratic state requires a strong level of *trust* between itself and its citizens. Here, both interpersonal and institutional trust are relevant. Interpersonal trust relates to the expectancy that others can be relied upon (Rotenberg, 2020, 17). Since the 1960s, the United States has undergone a significant decline in what researchers term *social capital* (Putnam, 1995, 71). Robert Putnam defines social capital as the 'features of social organizations, such as networks, norms and trust that facilitate action and cooperation for mutual benefit' within a society, and notes its importance in the functioning of social groups (Putnam, 1993, 35). Overall, trust in others within the United States is split roughly evenly, with nearly half of Americans stating that others cannot be trusted (Pew Research Center, 2019). Such a high level of skepticism poses challenges to the improvement of social resilience. Obstruction campaigns often seek to target existing divides within a society, pushing different social groups apart and highlighting the flaws in others (Barry, 2022). Lack of trust is both a weakness to be exploited *by* and a symptom *of* information manipulation. Institutional trust is also in decline within the United States (Pew Research Center, 2023, 24). In particular, a historically low 16% of Americans have trust in their federal government (Pew Research Center, 2023, 27). This inherently complicates the process of governments becoming the dependable relayers of truth. Rather, the significant portion of Americans who lack confidence in the government may be likely to search for other sources of information.

Once again, the open media environment of the United States may hamper the challenge of building trust between citizens. Americans who lack trust in their government do not have to search hard to find narratives that suit their pre-existing understanding of the world. This is compounded by the aforementioned issue of how trust in expert opinion declines as the number of arguments available to an individual increases (Flanigan & Metzger, 2013, 1628). In traditional media, the wide variety of news channels presenting coverage from perspectives across the political spectrum provides ample opportunity to remain within an ideological echo chamber. The diversity of news sources is even more prevalent online. Any number of Twitter accounts, Facebook pages, or alternative media websites offer the reader the narrative framing they desire. And if they wish to see what the *other side* is saying, they can find that too, often conveniently collected by anti-*other side* accounts that trade in mockery and the ensuing emotions their examples produce. This was particularly prevalent on YouTube during the 2016 presidential election season, where right-leaning individuals skeptical of the left could watch twenty-minute supercuts labelled as "SJW (Social Justice Warrior) Cringe Compilations". Of course, the opposite was readily available to the left, often in the form of Late Night comedy hosts capturing footage of Trump supporters failing to answer basic questions about subjects like geography, quickly shared in online video format and going viral.

Somewhere amid all the content were foreign trolls hiding in plain sight, indistinguishable from their surroundings. They also relied heavily on making different groups appear 'cringeworthy' or 'stupid'. Russia, simultaneously supporting and undermining both sides of the political spectrum, helped foment the increasing divide between the American left and right. Their tactics did not stop there. They sought to inflame racial, religious, gender, sexual orientation, generational, and economic tensions as well. They were not the only ones. The SJW compilations, compiled by American citizens, were full of clips from different social movements and protests. Videos concerning the moral reprehensibility of the right were defined by instances of right-leaning individuals saying unacceptable things. Throughout the chaos that defined this era of online communication, one was hard pressed to determine what came from where, and the ulterior motives behind each example of emotionally provocative media.

The effect of the divided but dogma-reinforcing media sphere contributed to a social crisis. Accordingly, trust between American citizens remains at historic lows (Pew Research Center, 2019**)**. On both sides of the political aisle, trust in institutions is similarly unhealthy (Pew Research Center, 2023, 24**)**. Attempts to engage in *prebunking*, the undermining of expected hostile information attacks before they occur, require the audience to have faith in the provider. Similarly, efforts by democratic governments to provide their narrative to the population will be challenged.

Prebunking, one of the foremost information defence strategies being researched today, aims to expose citizens to weaker versions of expected hostile narratives before they are introduced, along with corrected information (Roozenbeek & Van der Linden, 2021, 8). Inoculating citizens before they are exposed to hostile information is important, given our tendency to be continually affected by the first information we receive even when it is later corrected (Walter & Tukachinsky, 2019, 156). As such, prebunking functions as a sort of information *vaccine*, preparing the mind for any contact with unwanted narratives. By dealing with the fundamental shortcoming that is our dependence on our first experience with a narrative, prebunking has shown remarkable success in making people resilient to distorted information (Vivion et al., 2022, 239). However, most studies on this practice occur in a controlled laboratory setting. The process of scaling the tactic up to the broader societal level will be impacted by the issues of institutional trust and the challenges that will arise in prebunking narratives that are not objectively false. Reaching those most susceptible to polluted information attacks will be difficult for a state to accomplish, and presenting subjective refutations of subjective arguments leaves the American government open to criticism by individuals from across the political aisle.

Fact-checking measures that deal with objectively false information face challenges as well. For example, Twitter suffers from an average delay of thirteen hours before false information is corrected (Shao et al., 2016, 3). These corrections are useless to those interacting with manipulated information in its early stages. These measures have also been shown to be far more effective on people who do not carry pre-existing beliefs about the subject in question, a challenge when dealing with American political narratives witnessed by American citizens (Fazio et al., 2022, 16). Furthermore, obvious corrections or refutations of false information can suffer from a *backfire* effect, where the notoriety bestowed on a claim via its refutation causes it to spread further and be remembered to a greater degree than it would have otherwise been (Lewandowsky et al., 2012, 115).

Regardless, the American government has endeavoured to present refutations of hostile narratives. Examples include highlighting Russia's historical revisionism, and noting that concepts like family values, tradition, and spirituality (all used heavily by Russia to note a decline in Western morality) are ill-defined (U.S. Embassy and Consulates in Russia, 2022). They also provide brief rebuttals to the claim that the United States was responsible for fomenting the Color Revolutions in states bordering Russia (U.S. Embassy and Consulates in Russia, 2022). Each of these refutations functions only if the audience has confidence that the government is consistently truthful. Augmenting this issue is the American history of engaging in revolutions abroad, and other actions of which they now accuse Russia (Morley & Smith, 1977, 209; Gasiorowski, 2013, 4; Fraser, 2005, 486). In short, there is a perception among many citizens that the United States is throwing stones from a glass house. Furthermore, a person who genuinely values traditional roles and concepts and perceives them as being eroded in favour of progressive ideology is unlikely to be convinced that the Russian argument regarding the collapse of the moral foundations of the West is without merit. Indeed, a sizable portion of the public is pessimistic about subjects such as the future of the American family (Pew Research Center, 2023, 10).

There is promising research that governments can begin the process of increasing trust within society. This can include the improvement of political representation and grassroots movements (Poertner, 2023, 554), and increasing the scope and membership of civic organizations (Howard, 2002, 165). Scholars further note that social trust is affected by institutional trust (Peter et al., 2014, 562), demonstrating that the amelioration of institutional trust issues should be of significant focus. Increasing interpersonal and institutional trust is a theoretically reasonable way to hinder the effects of information obstruction, but the process of rebuilding societal confidence is an uphill battle. Furthermore, it is of no harm to provide citizens with information sources that highlight the discrepancies in foreign obstruction campaigns. While they may not reach wide audiences, they are a useful tool for those who trust their government and are willing to be vigilant in their research. Thus, governments should not shy away from these efforts but should be realistic about what they are likely to achieve.

Strategic Communications

Governments, facing a lack of trust, should be calculated in their engagement with citizens. In general, the “synchronization of crucial themes, messages, and images” is important in reaching key audiences (United States Joint Forces Command Norfolk Va., 2010, xii). The goal is to engage people in a manner that sticks and influences them according to national goals. The process of communicating strategically can include public diplomacy, which seeks to inform individuals of policy, and psychological operations that use communications and other means to influence perceptions and behaviour (NATO Strategic Communications Centre of Excellence, n.d.; Falkheimer & Heide, 2022, 2). Issues arise, however, when noting that the intended target of strategic communications in this context will be American citizens. Compounded by the issue of trust, the act of ‘influencing’ a government's own citizens is certain to provoke strong reactions. Further, note that information obstruction campaigns are often catchy, short, and pithy. It is difficult to compete with sensational and bias-confirming rhetoric if one is taking the safe route, ensuring legal and moral obligations are fulfilled. Thus appears the moral action asymmetry: authoritarian adversaries do not need to comply with norms and ethical standards that constrain democratic governments. It is a monumental task to create communications that are effective but also legal, moral, and based on the values that the public expects from their elected government. As such, democratic states are at a disadvantage in their quest to strategically communicate their messages to citizens. This does not mean, however, that it is an impossible undertaking. Nations should seek to formulate their counter-information in a manner that will be noticed, and move beyond the presentation of narrative in lengthy government documents or through the legacy media.

To lay the groundwork for effective strategic communications policy, democratic governments must encourage an appreciation for other points of view, and commit to the idealistic view that this can help reduce conflict between opposing movements (Pike, 2021, 241). When shaping hearts and minds, building bridges that link adversaries and address points of contention is key (United States Advisory Commission, 2003, 14). Emphasizing any shared values that exist is fundamental. Using positive and memorable framing in an attempt to match adversarial campaigns can allow messages to be spread further than if they are framed generically and officially (Hassain, 2022, 11). Doing so from official sources may generate hostility or an unwillingness to listen in key sectors of the public. Thus, if they choose to take this step, democratic governments should engage in their strategic communications through unaffiliated channels. This may include the use of social media *influencers*, who are required to share their sponsorships by law but have greater freedom in their style of messaging. Additionally, decentralized groups of online activists driven by ideological beliefs have demonstrated success in undermining Russian efforts to spread disinformation about Ukraine (Scott, 2022). Without state affiliation, these groups are able to engage in memetic warfare in a manner that governments cannot. The capacity for a decentralized and unregulated community to operate effectively may be democracy’s greatest asset in this context, and deserves particular attention. It can and should be argued that the information war will not be won through bureaucracy, but through an army of youth raised in the information space with a keen grasp of the operational environment and a knack for the absurdism that defines many foreign information operations. Finally, while democratic governments may be constrained in influencing their own citizens, they have allies with the necessary skills who are not. The example of the Five Eyes intelligence-sharing alliance demonstrates previous examples of friendly countries engaging in espionage on behalf of other members (Watt, 2013). Ukraine has proven their ability to successfully engage in psychological influence operations (Munk, 2024, 6).

Perceptions are influenced by expectations, and more information is needed to discern an unexpected occurrence than an expected one (Heuer, 1981, 315). To prepare citizens for foreign obstruction, strategic communications strategies should seek to provide the public consciousness with a set of expectations that both undermine the incoming obstruction and strengthen social cohesion. For example, if the public has a positive view of a particular social group, and subsequently witnesses information attacks that demonize the group, the attacks will not fit neatly into their preconceived set of expectations. Despite the unpopularity of the 2003 Iraq War, support amongst the American public for veterans of the conflict remains very high (Pew Research Center, 2019, 6). Support for individual veterans is prevalent among the American people despite reports of war crimes and human rights abuses. This is likely due to the status afforded to veterans as a social group, and the public understanding that all individuals are not responsible for the mistakes of a few. There is an established public comprehension of veterans as both heroes and victims of terrible conflict. Attempts to slander them face immediate pushback. A policy of strategic communications that seeks to build the same level of public support for groups likely to be the target of information obstruction is one worth exploring. Of course, given the propensity for these attacks to focus on groups who face existing discrimination, this is a difficult challenge to overcome. But, in theory, building a narrative that constructs positive preconceived notions regarding different groups is a feasible method of defence against divisive information obstruction.

Generating status for social groups can be achieved through many different methods. Previous American military operations utilized strategies like the provision of medical supplies to struggling communities, and the gifting of toys and sweets to local children (Tuck, 2023, 809). Religious drives that feed the impoverished and support their community, protest movements that practice peacefully, and moderated and respectful discussions between opposing political sides may all afford positive status to their according social groups by those who witness these activities. Democratic governments can support such instances of good press, and slowly build goodwill between portions of the public and the social group in question. Although this appears promising in the abstract, it is nevertheless a very difficult and slow process that is unlikely to materialize at a large scale. So while strategically enforcing positive interactions between groups can help, successfully implementing such practices to the extent needed to induce change is improbable. This is compounded by existing expectations, which must be overcome before the construction of new ones.

Findings, Implications, and the Future

Human behaviour is oriented by the information we take in. Active distortion of the information environment allows actors to manipulate our thinking and our actions. Democracy inherently depends on the open sharing of information between individuals. It only thrives when citizens share a common understanding of rules and norms and are willing to see the best in each other. Russia and China have aimed at the world's foremost democratic state, disrupting these fundamental tenets of the American system.

A fascinating distinction can be made between the strategies used by Russia and China. Russia takes a destructive approach, seeking to undermine American social cohesion and fostering a contentious form of politics. To do this, they explicitly target American citizens with emotionally charged information, with little care about its truth or falsity. They seek to overwhelm the American information environment, understanding that massive amounts of disparate narratives impede constructive conversation. They take advantage of existing divides within the American social sphere and work to widen the gap between opposing groups. They simultaneously undermine and support every movement with the potential to disturb domestic stability with no regard for the moral implications of the philosophies they reinforce. Indeed, chaos within America fits neatly with established Russian geopolitical goals, as they seek to damage the country's image and its relationships with allies worldwide. Their approach takes advantage of cognitive biases and is constructed out of short-form writing styles, humour, and adages about specific social groups. Through historical lessons and concerted effort, Russia has crafted what may be best described as mind viruses, able to spread rapidly and be shared far and wide. They take advantage of social media algorithms and cognitive shortcuts to undermine the fabric of American social life.

China has thus far taken a softer approach. They seek to construct a positive image of themselves and have largely avoided targeting American citizens to the degree that Russia has. Rather, when they do interfere with the United States, it tends to be on a small scale and focused on either the Chinese diaspora or citizens of American-allied states. They use students to echo government talking points and work to capture foreign media to formulate a network of pro-Beijing messengers. They have relied less on social media than their Russian counterparts, favouring a grassroots approach. With less dependence on algorithms and socially damaging messaging, their hitherto strategies can be considered far less destructive than the Russian alternative.

This divergence in strategy is both interesting and academically valuable. While foreign political interference should be prevented in general, the caustic Russian strategy has helped grow the worst elements of American society. By attacking interpersonal trust and fundamental American institutions, the Russian modus operandi strikes directly at the heart of democracy. China, while a major competitor with the capacity to engage in similar tactics, has instead focused on achieving far less (but still) damaging outcomes. While growing distrust of America within key allied states and discourse interference are problematic for the United States, they are not existential to the political system.

Russia and China differ in their international image and their relationship with the United States. Russia is a pariah state with little remaining economic connection with the West. China and the United States are heavily intertwined, with their economic success depending on each other to a great degree. While Russia loses little with the rise of a chaotic American political sphere, China may suffer greatly. With significant economic ties to the United States, it is in China's interest to have a stable and predictable American politics.

Analyzing differences in strategies combined with assessing relations between the attacker and the target is a new approach to the subject. Interdependence serves as a potential mitigating variable and has implications for American defence against information warfare. The United States has primarily sought to establish a policy of deterrence against foreign information obstruction. This is well-intentioned, as there is no reason the basic psychological tenets of deterrence that focus on manipulating the enemy's cost-benefit analysis should not be translatable to the immaterial realm. However, other underlying pillars of the theory are challenged by the asymmetrical nature of the American information sphere vis-a-vis its rivals. For example, credible threats of equivalent retribution may be difficult to establish against closed authoritarian information spaces. Given the difficulty of tracing the source of narratives, attribution is also challenged. Further, the feasibility of deterrence by denial is deeply challenged by the core values of democracy, preventing the government from effectively stifling communication.

With China's economic relationship with the United States, they have a stake in the stability of American politics. Unpredictability leaves them vulnerable, and the rise of nationalistic and populist leaders that tend to accompany social discord threatens their continued security. Given the presence of a large sector of the American public affected by the outsourcing of jobs to countries like China and their rise as the obvious challenger to American hegemony, they are likely to be a primary target for political attacks from such leaders. Through the lens of deterrence theory, China faces a high cost for disruptive actions.

This in no way precludes China from general information interference. Indeed, the same factors that challenge traditional deterrence make the United States a soft target. China still seeks to drive policy that aids its goals and will likely target the diaspora with communications to foster support for specific political candidates. They will likely continue to undermine the American image in key regions of East Asia. Rather, China's stake in American stability has shaped its strategy, and the resulting challenges are likely easier to deal with than the ones posed by Russia's concerted attack against the foundation of American social life.

If interdependence continues to decline and China begins to utilize caustic narratives to create social division, the United States must supplement their deterrence policies with defence strategies that seek to strengthen social resilience. These are theoretically promising but face major obstacles. The method of prebunking, for example, depends on the preferred narrative reaching the right audiences. The American government's reach is affected by the level of trust that its citizens have in them, a variable that continues to decline. To effectively shape hearts and minds, the United States must produce narratives that match or outperform those from abroad. Russia's abuse of human cognition and catchy narrative structure will be particularly difficult to match. Democracies like the United States may be morally constrained from constructing messages in the same effective and far-reaching manner.

Continued improvements in technology will likely amplify the issues highlighted in this thesis. Artificial intelligence, especially, poses grave dangers to the process of determining reality and the basic cognitive functions of the human brain. Given the relative unimportance of truth associated with information manipulation, *deepfaked* images and videos will be a major challenge. Two outcomes are likely: a significant number of individuals will not put effort into determining whether a piece of information is real or fake, and a general tendency to be untrusting of any and all information will take hold of the public consciousness. Neither of these outcomes are beneficial to democracy. The term *post-truth era* is likely to become a fitting expression. Plausible deniability will be easily afforded to any politician who claims that damaging photographs, videos, or audio clips are not real. A voter base caught off guard by unbecoming evidence against their preferred candidate will latch on to the explanation that fosters the least cognitive dissonance. The greatest damage from deepfaked material will not be the falsity of its content, but its mere existence serving as a coup de grace against our ability to trust what we perceive.

Decreasing interdependence and increasing divergence between the United States and China will remove one of America’s few tools that affect China’s cost-benefit calculation regarding information warfare. The present trend of isolationism in the United States makes this a possible, if not likely, outcome. The famed *Thucydides trap*, however, is not a foregone conclusion. Great powers may accommodate rising ones (Paul, 2016, 16). Regardless, information warfare will be one of the most pressing challenges facing the United States in the coming years and decades.

Conclusion

Democracy dies in division. Given the citizen's role in determining the policies of the state, their access to unpolluted, accurate, and unbiased information is paramount. Authoritarian governments have noted this dependency and have sought to exploit it. Targeting the world's premier democratic country, the United States, Russia and China have put significant efforts into manipulating the information space. These countries perceive several benefits from doing so, ranging from the undermining of the American image via social chaos or the betterment of their own image and political ambitions. Russia has utilized a destructive strategy of chaos, seeking to foment division within the American domestic sphere. Historically, China has been less disruptive; instead, it seeks to bolster its global perception and influence policy in a manner that is helpful to its goals. This may be due to the differences in each of their relationships with the United States, with Russia being a pariah state and China being heavily intertwined with the American economy. As the American-Chinese relationship heads through rocky waters, decreasing cooperation and trade between the two nations may provoke China to take a harder approach and face fewer costs in return. Indeed, it seems likely that China is in the process of shifting its strategy. Given the challenges facing deterrence by denial and punishment, deterrence by entanglement through interdependence may be the United States' best option of defence against caustic and damaging information warfare. Other defence strategies seeking to bolster social resilience to damaging information attacks are theoretically feasible but face numerous challenges in the American domestic context. These include issues of reach, where the federal government may have difficulty influencing the citizens most likely to be affected by foreign obstruction. While the soft information manipulation stemming from China in previous years was not helpful for the United States, it was comparatively less of a threat than the divisive narrative techniques practiced by Russia. Given the existing cleavages in the American social sphere, further damage to interpersonal and institutional trust and understanding are significant threats to the continued success of the American political system. Democracy dies in division, and its funeral is one we should not wish to witness in our lifetimes.

References

4th PSYOP Group. (2022, May 2). *Ghosts in the machine*. YouTube. https://www.youtube.com/watch?v=VA4e0NqyYMw

Achen, C. H., & Snidal, D. (1989). Rational deterrence theory and comparative case studies. *World Politics, 41*(2), 143–169. https://doi.org/10.2307/2010405

Allen-Ebrahimian, B. (2018, March 7). *China's long arm reaches into American campuses*. Foreign Policy. https://foreignpolicy.com/2018/03/07/chinas-long-arm-reaches-into-american-campuses-chinese- students-scholars-association-university-communist-party/

Alvarez, G., Choi, J., & Strover, S. (2020). Good news, bad news: A sentiment analysis of the 2016 election Russian Facebook ads. *International Journal Of Communication, 14*(27). https://ijoc.org/index.php/ijoc/article/view/11518/3108

Aminulloh, A., Artaria, M. D., Surya, Y. W. I., Qorib, F., & Hakim, L. (2023). Firehose of falsehood propaganda model in the 2019 Indonesian presidential election. *MediaTor*, *15*(2), 249–263. https://doi.org/10.29313/mediator.v15i2.10573

Autor, D. H., Dorn, D., & Hanson, G. H. (2013). The China syndrome: Local labor market effects of import competition in the United States. *American Economic Review, 103*(6), 2121–2168. https://doi.org/10.1257/aer.103.6.2121

Barry, E. (2022, September 18). *How Russian trolls helped keep the women's march out of lock step*. The New York Times. https://www.nytimes.com/2022/09/18/us/womens-march-russia-trump.html

Boorstein , M., & Zauzmer, J. (2016, July 22). *Wikileaks: Democratic party officials appear to discuss using Sanders's faith against him*. https://www.washingtonpost.com/news/acts-of-faith/wp/2016/07/22/wikileaks-democratic-party-officials-appear-to-discuss-using-sanderss-faith-against-him/

Brady, A. (2018). New Zealand and the CCP's magic weapons. *Journal of Democracy, 29*(2), 68-75.

Brady, W. J., Julian A. W., Jost, J. T., Tucker, J, A., & Bavel. J. J., (2017). Emotion shapes the diffusion of moralized content in social networks. *Proceedings of the National Academy of Sciences 114*(28), 7313–18. https://doi.org/10.1073/pnas.1618923114.

Brantly, A. F., (2018). Conceptualizing cyber deterrence by entanglement. *Social Science Research Network*: http://dx.doi.org/10.2139/ssrn.2624926

Brantly, A. F., (2020). Entanglement in cyberspace: Minding the deterrence gap. *Democracy and Security, 16*(3), 210–233. https://doi.org/10.1080/17419166.2020.1773807

Brown, P., & Library of Congress Congressional Research Service. (2020). *Oil market effects from U.S. economic sanctions: Iran, Russia, Venezuela*. Congressional Research Service. https://soton.idm.oclc.org/login?url=https://www.heinonline.org/HOL/Index?index=crs/govcakv&collection=forrel

Brown, C., & Wang, Y. (2023, March 16). *Five years into the trade war, China continues its slow decoupling from US exports*. Peterson Institute for International Economics. https://www.piie.com/blogs/realtime-economics/five-years-trade-war-china-continues-its-slow-decoupling-us-exports

Bugayova, N., Kagan, F. W., & Stepanenko, K. (2024). *Denying Russia's only strategy for success*. Institute for the Study of War.

https://www.understandingwar.org/backgrounder/denying-russia%E2%80%99s-only-strategy-success

Byrne, M. (2012). Review of Radio Free Europe and Radio Liberty: The CIA years and beyond. *Journal of Cold War Studies, 14*(3), 213-215. muse.jhu.edu/article/490189.

Canadian Centre for Cyber Security. (2023, December 6). *Cyber threats to Canada's democratic process: 2023 update - Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2023-update

Chang, G. C., Lueck, K., & Mehan, H. B. (2013). Evidencing international threat: Examining Iraq Survey Group's post-invasion verification of Iraq's WMD threat. *Journal of Language and Politics, 12*(1), 29–58. https://doi.org/10.1075/jlp.12.1.02cha

Cinelli, M., Etta, G., Avalle, M., Quattrociocchi, A., Di Marco, N., Valensise, C., Galeazzi, A., & Quattrociocchi, W. (2022). Conspiracy theories and social media platforms. *Current Opinion in Psychology*, *47*, 101407. https://doi.org/10.1016/j.copsyc.2022.101407

Clark, D. D., & Landau, S. (2010). Untangling attribution. Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy. *National Research Council*, 25–40.

Cohen, R. S., Rand Corporation, & Project Air Force (U.S.). (2021). *Combating foreign disinformation on social media: Study overview and conclusions*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR4373z1.html

Colomina, C., Margalef, H. S., Youngs, R., & Jones, K. (2021). The impact of disinformation on democratic processes and human rights in the world. *Brussels: European Parliament*, 1-19.

Communications Security Establishment. (2020). *Attitudes towards the Communications Security Establishment – Tracking study*. https://publications.gc.ca/site/archivee-archived.html?url=https://publications.gc.ca/collections/collection_2020/cstc-csec/D96-16-2020-eng.pdf

Convention on the Prevention and Punishment of the Crime of Genocide. (1948). United Nations. https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf

Cosentino, G. (2021). *Infodemic: Disinformation, geopolitics and the COVID-19 pandemic (First edition)*. Bloomsbury. https://doi.org/10.5040/9780755640775

Crocker, J., Luhtanen, R. (1990). Collective self-esteem and ingroup bias. *Journal of Personality and Social Psychology, 58*(1), 60–67. https://doi.org/10.1037/0022-3514.58.1.60

Cull, N. J., Culbert, D. H., & Welch, D. (2003). *Propaganda and mass persuasion: A historical encyclopedia, 1500 to the present*. ABC-CLIO.

Cybersecurity and Infrastructure Security Agency. (n.d.). *Foreign influence operations and disinformation*. Foreign Influence Operations and Disinformation. |https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation#:~:text=Misinformation%20is%20false%2C%20but%20not,mislead%2C%20harm%2C%20or%20manipulate.

Dawson, A., & Innes, M. (2019). How Russia's internet research agency built its disinformation campaign. *The Political Quarterly*, *90*(2), 245–256. https://doi.org/10.1111/1467-923X.12690

de Graaf, B. (2021). How contagious were the Capitol riots in Europe – In praxis and in perception? *Terrorism and Political Violence, 33*(5), 922-925, DOI: 10.1080/09546553.2021.1932346

De Luce, D., & Grumbach, G. (2024, March 11). *AI gives Russia, China new tools to sow division in the U.S., undermine America's image, intel agencies say*. NBC News. https://www.nbcnews.com/politics/national-security/china-russia-ai-divide-us-society-undermine-us-elections-power-rcna142880

Department of Defense. (2023, November 17). *Strategy for operations in the information environment*. https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-department-of-defense-strategy-for-operations-in-the-information-environment.pdf

Dickinson, P. (2023, April 12). *NATO poses a threat to Russian imperialism not Russian security*. Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/nato-poses-a-threat-to-russian-imperialism-not-russian-security/

Dunlop, J. B., (2004). Aleksandr Dugin's foundations of geopolitics. *Demokratizatsiya-Washington- 12*(41), 58.

Economy, E. (2018). *The third revolution: Xi Jinping and the new Chinese state*. Oxford University Press. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=173781512864837-1001

Encyclopedia Britannica. (2018, May 16). *Radio Free Europe*. Encyclopedia Britannica. https://www.britannica.com/topic/Radio-Free-Europe.

Falkheimer, J., & Heide, M. (2022). *Research handbook on strategic communication*. Edward Elgar Publishing. https://doi.org/10.4337/9781800379893

Fazio, L. K., Hong, M. K., & Pillai, R. M. (2023). Combatting rumors around the French election: the memorability and effectiveness of fact-checking articles. *Cognitive Research: Principles and Implications, 8*(1). https://doi.org/10.1186/s41235-023-00500-2

Fitzgerald, J. (2018). Overstepping down under. *Journal of Democracy, 29*(2), 59-67.

Flanagin, A. J., & Metzger, M. J. (2013). Trusting expert- versus user-generated ratings online: The role of information volume, valence, and consumer characteristics. *Computers in Human Behavior, 29*(4), 1626–1634. https://doi.org/10.1016/j.chb.2013.02.001

Fraser, A. (2005). Architecture of a broken dream: the CIA and Guatemala, 1952-54. *Intelligence and National Security, 20*(3), 486–508. https://doi.org/10.1080/02684520500269010

Gasiorowski, M. J. (2013). The CIA's TPBEDAMN operation and the 1953 coup in Iran. *Journal of Cold War Studies, 15*(4), 4–24. https://doi.org/10.1162/JCWS_a_00393

Giusti, S. & Piras, E. (2021). *Democracy and fake news: Information manipulation and post-truth politics. Politics, media and political communication*. Abingdon, Oxon: Routledge.

https://www.taylorfrancis.com/books/oa-edit/10.4324/9781003037385/democracy-fake-news-serena-giusti-elisa-piras

Glenn, J. & Florescu, E. (2017). *State of the future v. 19.0*. The Millenium Project. https://millennium-project.org/wp-content/uploads/2017/10/SOF2017-ExecSumm-front_matter.pdf

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice? *Strategic Studies Quarterly*, *4*(3), 102–135. http://www.jstor.org/stable/26269789

Global Affairs Canada. (2023, March 22). *Countering disinformation with facts - Russian invasion of Ukraine*. Global Affairs Canada. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng

Global Engagement Center. (2020). *GEC special report: Pillars of Russia's disinformation and propaganda ecosystem*. https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

Great Britain. (1915). *Report of the Committee on Alleged German Outrages: Appointed by His Britannic Majesty's Government and presided over by the Right Hon. Viscount Bryce.* http://nla.gov.au/nla.obj-52678421

Guo, S., Guo, B., Devuyst, Y., Flick, K. E., Hickey, D., Huang, K., Ji, Y., Kang, L., Kao, D.-Y., Kao, P.-s., Kim, Y., Lee, J.-Y., Lim, Y.-H., Liu, G., Men, J., Mierzejewski, D., Mingjiang, L., Yee, A. S., QuanshengZhao, et al. (2010). *Thirty years of China - U.S. relations: Analytical approaches and contemporary issues*. Lexington Books. http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=1032045

Hamilton, R. (2019). Russia's attempts to undermine democracy in the West: Effects and causes. *Orbis, 63*(3), 334-348.

Han, R., & Shao, L. (2022). Scaling authoritarian information control: How China adjusts the level of online censorship. *Political Research Quarterly, 75*(4), 1345–1359.

Harasymiw, B. (2011). In search of post-communism: Stalking Russia's political trajectory.

Canadian Slavonic Papers, 53(2-4), 401-VII.

Harold, S., Beauchamp-Mustafaga, N., Hornung, J. W., Rand Corporation, & Project Air Force (U.S.). (2021). *Chinese disinformation efforts on social media. Combating foreign disinformation on social media series*. RAND Corporation.

Hartman, R., Hester, N., Gray, K. (2022). People see political opponents as more stupid than evil. *Personality and Social Psychology Bulletin*, *2022*(04), 28. https://doi.org/10.1177/01461672221089451.

Hass, R. (2021). *Stronger: Adapting America's China strategy in an age of competitive interdependence*. New Haven: Yale University Press. https://doi-org.proxy3.library.mcgill.ca/10.12987/9780300258479

Hassain, J. (2022). *Disinformation in democracies: Improving societal resilience to disinformation*. NATO Strategic Communications Centre of Excellence

He, K. (2009). *Institutional balancing in the Asia Pacific: Economic interdependence and China's rise*. Routledge. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=248386

Heuer, R. J. (1981). Strategic deception and counterdeception: A cognitive process approach. *International Studies Quarterly, 25*(2), 294–327. https://doi.org/10.2307/2600359

Hille, K. (2018). *China's 'sharp power' play in Taiwan*. Financial Times. https://www.ft.com/content/5c272b90-ec12-11e8-89c8-d36339d835c0

Hinšt, D. (2021). Disinformation as geopolitical risk for transatlantic institutions. *Međunarodne Studije, Xxi*(2), 89–111. https://doi.org/10.46672/ms.21.2.4

Hoffman, D. D., & Singh, M. (2012). Computational evolutionary perception. *Perception*, *41*(9), 1073–91.

Hoffman, D. D., Singh, M., & Prakash, C. (2015). The interface theory of perception. *Psychonomic Bulletin & Review*, *22*(6), 1480–1506. https://doi.org/10.3758/s13423-015-0890-8

Howard, M. (2002). The weakness of postcommunist civil society. *Journal of Democracy, 13*(1), 157–169.

Hsiao, R. (2019, June 26). *A preliminary survey of CCP influence operations in Japan*. Jamestown. https://jamestown.org/program/a-preliminary-survey-of-ccp-influence-operations-in-japan/

Hsu, T., & Myers, S. L. (2024, April 1). *China's advancing efforts to influence the U.S. election raise alarms*. The New York Times. https://www.nytimes.com/2024/04/01/business/media/china-online-disinformation-us-election.html

Hume, D. (2019). *An enquiry concerning human understanding*. Electric Book. https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=5302411

Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. *The International Journal of Press/Politics, 25*(3), 493-516. https://doi.org/10.1177/1940161219900126

International Court of Justice. (2022). *Allegations of genocide under the Convention on the Prevention And Punishment Of The Crime Of Genocide (Ukraine V. Russian Federation*). International Court of Justice. https://www.icj-cij.org/case/182

International Trade Data Main Page. (2024, March 7). United States Census Bureau. https://www.census.gov/foreign-trade/data/index.html

Jasper, S. (2017). *Strategic cyber deterrence: the active cyber defense option*. Rowman & Littlefield.

Jervis, R. (1968). Hypotheses on misperception. *World Politics, 20*(3), 454–479. https://doi.org/10.2307/2009777

Jervis, R. (2017). *Perception and misperception in international politics*. Princeton University Press.

Johnson, D. E.W. (2019). Russian election interference and race-baiting". *Columbia Journal of Race and Law*, *9*(2), 191-264. https://doi.org/10.7916/cjrl.v9i2.3409.

Kakutani, M. (2018). *The death of truth*. William Collins.

Kant, I., Weigelt, M., & Müller F. Max. (2007). *Critique of pure reason (Ser. Penguin Classics)*. Penguin.

Kauṭilya. (2013). *King, governance, and law in ancient India: Kauṭilya's arthaśāstra (P. Olivelle, Trans.)*. Oxford University Press.

Keohane, R. O. (2005). *After hegemony: Cooperation and discord in the world political economy (1st Princeton classic, Ser. A Princeton Classic Edition)*. Princeton University Press.

Kynge, J., Hornby, L., & Anderlini, J. (2017). *Inside China's secret 'magic weapon' for worldwide influence*. Financial Times. https://www.ft.com/content/fb2b3934-b004-11e7-beba-5521c713abf4

Lanoszka, A. (2019). Disinformation in international politics. *European Journal of International Security, 4*(2), 227–248. http://doi.org.proxy3.library.mcgill.ca/10.1017/eis.2019.6

Lai, E. L.-C. (2019). The US-China trade war, the American public opinions and its effects on China. *Economic and Political Studies, 7*(2), 169–184. https://doi.org/10.1080/20954816.2019.1595330

Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and its correction: Continued influence and successful debiasing. *Psychological Science in the Public Interest*, *13*(3), 106-131. https://doi.org/10.1177/1529100612451018

Linvill, D. L., Boatwright, B. C., Grant, W. J., & Warren, P. L. (2019). "The Russians are hacking my brain!" Investigating Russia's Internet Research Agency Twitter tactics during the 2016 United States presidential campaign. *Computers in Human Behavior, 99*, 292-300. https://doi.org/10.1016/j.chb.2019.05.027

Martin, H. D. (1943). The Mongol army. *Journal of the Royal Asiatic Society of Great Britain and Ireland*, *1*, 46–85. http://www.jstor.org/stable/25221891

Mazanec, B. M., & Thayer, B. A. (2015). *Deterring cyber warfare: Bolstering strategic stability in cyberspace*. Palgrave Macmillan. https://doi.org/10.1057/9781137476180

Mearsheimer, J. J. (2014). Why the Ukraine crisis is the West's fault: The liberal delusions that provoked Putin. *Foreign Affairs, 93*(5), 77–89. http://www.jstor.org/stable/24483306

Meyer, S. (1995). The devolution of Russian military power. *Current History*, *94*(594), 322-328.

Morgan, P. M. (1977). *Deterrence: A conceptual analysis*. Sage Publications.

Morgan, P. M. (2003). *Deterrence now*. Cambridge University Press.

Morley, M., & Smith, S. (1977). Imperial "reach": U.S. policy and the CIA in Chile. *Journal of Political & Military Sociology, 5*(2), 203–216. https://doi.org/10.2307/45293026

Mowat, J. (2019). *McMaster student government bans Chinese students' group from campus*. CBC News. https://www.cbc.ca/news/canada/hamilton/mcmaster-china-student-association-ban-1.5298882

Mueller, R. S. (2019). *Report on the investigation into Russian interference in the 2016 presidential election*: S*ubmitted pursuant to 28 c.f.r. §600.8(c)*. United States Department of Justice: Special Counsel's Office.

Munk, T. (2024). *Memetic war: Online resistance in Ukraine (Ser. Routledge studies in crime and society)*. Routledge.

National Endowment for Democracy. (2017). *Sharp power: Rising authoritarian influence: New forum report.* National Endowment for Democracy. https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/

NATO. (2016, July 9). *Russia relations: The facts.* NATO. https://www.nato.int/cps/en/natohq/topics_111767.html

NATO Strategic Communications Centre of Excellence. (n.d.). *About strategic communications*. StratCom. https://stratcomcoe.org/about_us/about-strategic-communications/1

Nelson, L. (2019). Are trade unions and their members "populist"? *Ideas*, *14*. https://doi.org/10.4000/ideas.6089

Nesse, R. M. (1990). Evolutionary explanations of emotions. *Human Nature, 1*(3), 261–289. https://doi.org/10.1007/BF02733986

New international version: Holy bible. (2023). Zondervan.

Novicoff, M. (2024, March 24). *"It's causing them to drop out of life": How phones warped Gen Z.* https://www.politico.com/news/magazine/2024/03/24/the-anxious-generation-qa-00147880

Nye, J. S. (2016). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.

Paul, C., & Matthews, M. (2016, July 11). *Russia's "firehose of falsehood" propaganda model.* RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html#fn13

Paul, T. V. (2016). *Accommodating rising powers past, present, and future*. Cambridge University Press. https://doi.org/10.1017/CBO9781316460191

Paul, T. V., Morgan, P. M., & Wirtz, J. J. (2009). *Complex deterrence: Strategy in the global age*. University of Chicago Press.

Peter, N., Gert, T. S., Peter, T. D., & Kim, M. S. (2014). Do institutions or culture determine the level of social trust? The natural experiment of migration from non-Western to Western countries. *Journal of Ethnic and Migration Studies, 40*(4), 544–565. https://doi.org/10.1080/1369183X.2013.830499

Pew Research Center. (2019). *The American Veteran Experience and the Post-9/11 Generation.*

Pew Research Center, (2019). *Trust and Distrust in America.*

Pew Research Center, (2023). *Americans' Dismal Views of the Nation's Politics.*

Pew Research Center, (2023). *Public Has Mixed Views on the Modern American Family.*

Pickrell, R. (2019, September 22). *DOD apologizes for tweet suggesting millennials would be bombed if they stormed Area 51*. Air Force Times. https://www.airforcetimes.com/news/your-air-force/2019/09/23/dod-apologizes-for-tweet-suggesting-millennials-would-be-bombed-if-they-stormed-area-51/

Pike, S. L. (2021). Using q methodology to augment evaluation of public diplomacy programs. *Place Branding and Public Diplomacy, 18*(3), 240–253. https://doi.org/10.1057/s41254-021-00229-z

Poertner, M. (2023). Does political representation increase participation? Evidence from party candidate lotteries in Mexico. *American Political Science Review, 117*(2), 537-556. doi:10.1017/S0003055422000533

Polyakova, A., & Boulègue, M. (2022, October 21). *The evolution of Russian hybrid warfare: Executive summary*. CEPA. https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-executive-summary/

Putnam, R. D. (1993). The prosperous community social capital and public life. *The American Prospect*, 35–42.

Putnam, R. D. (1995). Bowling alone: America's declining social capital. *Democracy*, 65–78.

Quinn, P. J. (2001). *The conning of America: The Great War and American popular literature (Ser. Costerus, new ser. 136)*. Rodopi.

Rapp, D. N. (2016). The consequences of reading inaccurate information. *Current Directions in Psychological Science, 25*(4), 281–285. https://doi.org/10.1177/0963721416649347

Rennack, D. E., Welt, C., & Library of Congress Congressional Research Service. (2021). *U.S. sanctions on Russia: An overview*. Congressional Research Service.

Reuters. (2022, November 7). *Russia's Prigozhin admits interfering in U.S. elections*. https://www.reuters.com/world/us/russias-prigozhin-admits-interfering-us-elections-2022-11-07/ https://soton.idm.oclc.org/login?url=https://heinonline.org/HOL/Page?handle=hein.crs/govedoj0001&id=1&size=2&collection=forrel&index=alpha/U_forrelcrs

RFI. (2021, December 9). *Putin says conflict in eastern Ukraine 'looks like genocide'*. RFI. https://www.rfi.fr/en/putin-says-conflict-in-eastern-ukraine-looks-like-genocide

Rhodes, A. R. E., & Margolin, V. (1983). *Propaganda: the art of persuasion, World War II (2nd-vol. ed.)*. Chelsea House.

Robb, A. (2017). *Pizzagate: Anatomy of a fake news scandal.* Rolling Stone. https://www.rollingstone.com/politics/politics-news/anatomy-of-a-fake-news-scandal-125877/

Robert, Ł. (2018). U.S. and China: Hard and soft Power potential. *International Studies: Interdisciplinary Political and Cultural Journal, 22*(1), 39-50.

Roozenbeek, J., Van der Linden, S. (2021). *Inoculation theory and misinformation*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/inoculation-theory-and-misinformation/217

Rotenberg, K. J. (2020). *The psychology of interpersonal trust: Theory and research*. Routledge. https://doi.org/10.4324/9781351035743

Russett, B. M., & Oneal, J. R. (2001). *Triangulating peace: Democracy, interdependence, and international organizations (Ser. Norton Series in World Politics)*. Norton.

Rutland, P., & Kazantsev, A. (2016). The limits of Russia's 'soft power'. *Journal of Political Power, 9*(3), 395-413.

Sarotte, M. (2012). China's fear of contagion: Tiananmen Square and the power of the European example. *International Security, 37*(2), 156-182.

Schäfer, C. (2022). *China's diaspora policy under Xi Jinping: Content, limits and challenges*. Stiftung Wissenschaft und Politik (SWP). https://doi.org/10.18449/2022RP10

Schelling, T. C. (1963). Deterrence: Military diplomacy in the nuclear age. *The Virginia Quarterly Review, 39*(4), 531–547.

Scott, M. (2022, September 1). *The shit-posting, Twitter-trolling, dog-deploying social media army taking on Putin one meme at a time*. Politico. https://www.politico.eu/article/nafo-doge-shiba-russia-putin-ukraine-twitter-trolling-social-media-meme/

Shambaugh, D. (2015). China's soft-power push the search for respect. Foreign Affairs, *94*(4), 99–107.

Shao, C., Ciampaglia, G. L., Flammini, A., & Menczer, F. (2016). Hoaxy: A platform for tracking online misinformation. *ArXiv*. https://doi.org/10.1145/2872518.2890098

Singh, K. (2024, July 21). *US criticizes ICJ opinion on Israeli occupation of Palestinian Territories*. Reuters. https://www.reuters.com/world/us-criticizes-icj-opinion-israeli-occupation-palestinian-territories-2024-07-20/.

Snyder, G. H. (2015). *Deterrence and defense (Ser. Princeton Legacy Library)*. Princeton University Press.

Spicer, R. N. (2018). *Free speech and false speech: Political deception and its legal limits (or lack thereof) (Ser. Palgrave Pivot)*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-69820-5.

Springer, P. J. (2020). *Cyber warfare (Ser. Documentary and Reference Guides)*. ABC-CLIO, LLC. http://public.eblib.com/choice/PublicFullRecord.aspx?p=6181609.

Statistics Canada. (2024, May 16). *Trust in news or information from media by gender and province*. Statistics Canada. https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=4510009601

Stein, J. (2016). *What 20,000 pages of hacked WikiLeaks emails teach us about Hillary Clinton.* Vox. https://www.vox.com/policy-and-politics/2016/10/20/13308108/wikileaks-podesta-hillary-clinton

Stier, S. (2015). Democracy, autocracy and the news: The impact of regime type on media freedom. *Democratization, 22*(7), 1273–1295. https://doi.org/10.1080/13510347.2014.964643

Stockman, F. (2018, December 23). *Women's March roiled by accusations of Anti-Semitism*. The New York Times. https://www.nytimes.com/2018/12/23/us/womens-march-anti-semitism.html

Sun, T., & Sawyer, R. D. (1994). *Art of war (Ser. History & Warfare)*. Basic Books. March 16, 2024.

Taehwan, K. (2018). *Authoritarian sharp power: Comparing China and Russia*. The Asan Forum. http://www.theasanforum.org/authoritarian-sharp-power-comparing-china-and-russia/

Tajfel, H., & Turner, J. C. (2004). The social identity theory of intergroup behavior. In J. T. Jost & J. Sidanius (Eds.), *political psychology: Key readings* (pp. 276–293). Psychology Press. https://doi.org/10.4324/9780203505984-16

The Economist. (2017, December 16). *Sharp power; China and the West*. The Economist, 425, 11. https://proxy.library.mcgill.ca/login?url=https://www.proquest.com/magazines/sharp-power-china-west/docview/1977459770/se-2

The Moscow Times. (2017, October 16). *Kremlin troll tells all about influencing U.S. elections*. The Moscow Times. https://www.themoscowtimes.com/2017/10/16/kremlin-troll-tells-all-about-influencing-us-elections-a59274.

Thompson, H. (2010). *China and the mortgaging of America: Economic interdependence and domestic politics*. Palgrave Macmillan.

Tooby, J., Cosmides, L. (1990). The past explains the present: Emotional adaptations and the structure of ancestral environments. *Ethology and Sociobiology, 11*(4), 375–424. https://doi.org/10.1016/0162-3095(90)90017-Z

Tuck, C. (2023). Shaping hearts and minds: Claret operations in Borneo, 1965–1966. *Small Wars & Insurgencies, 34*(4), 803–827.

United States Advisory Commission on Public Diplomacy. Advisory Group on Public Diplomacy for the Arab and Muslim World, & United States. Congress. House. Committee on Appropriations. (2003). *Changing minds, winning peace: A new strategic direction for U.S. public diplomacy in the Arab & Muslim world: Report of the advisory group on public diplomacy for the Arab and Muslim world*. U.S. Dept. of State.

United States Department of Justice. (2021, August 10). Russian national charged with interfering in U.S. political system. Office of Public Affairs. United States Department of

Justice. https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system

United States Joint Forces Command Norfolk Va. (2010, June 24). *Commander's handbook for strategic communication and communication Strategy*. DTIC. https://apps.dtic.mil/sti/citations/ADA525371

U.S. Embassy and Consulates in Russia. (2022, January 22). *Russia's top five persistent disinformation narratives*. https://ru.usembassy.gov/russias-top-five-persistent-disinformation-narratives/

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

Ventre, D. (2016). *Information warfare (Revised and Updated 2nd, Ser. Information Systems, Web and Pervasive Computing Series)*. ISTE Ltd.

Vivion, M., Anassour Laouan Sidi, E., Betsch, C., Dionne, M., Dubé, E., Driedger, S. M., Gagnon, D., Graham, J., Greyson, D., Hamel, D., Lewandowsky, S., MacDonald, N., Malo, B., Meyer, S. B., Schmid, P., Steenbeek, A., van der Linden, S., Verger, P., Witteman, H. O., & Yesilada, M. (2022). Prebunking messaging to inoculate against COVID-19 vaccine misinformation: An effective strategy for public health. *Journal of Communication in Healthcare, 15*(3)*,* 232–242. https://doi.org/10.1080/17538068.2022.2044606

Walker, C. (2018). What Is "sharp power"? *Journal of Democracy, 29*(3), 9-23.

Walt, S. M. (1985). Alliance formation and the balance of world power. *International Security 9*(4). 3–43. https://doi.org/10.2307/2538540.

Walter N., & Tukachinsky R. (2019). A meta-analytic examination of the continued influence of misinformation in the face of correction: How powerful is it, why does it happen, and how to stop it? *Communication Research*. https://doi.org/10.1177/0093650219854600

Watt, N. (2013, June 10). *NSA offers intelligence to British counterparts to skirt UK law*. The Guardian. https://www.theguardian.com/politics/2013/jun/10/nsa-offers-intelligence-british-counterparts-blunkett

Whyte, C., & Mazanec, B. M. (2023). *Understanding cyber warfare: Politics, policy and strategy (Second)*. Routledge, Taylor & Francis Group.

Wijermars Mariëlle, & Lehtisaari, K. (Eds.). (2020). *Freedom of expression in Russia's new mediasphere (Ser. Basees/Routledge series on Russian and East European Studies, 133).* Routledge, Taylor & Francis Group.

Winterfeld, S., & Andress, J. (2012). *The basics of cyber warfare: Understanding the fundamentals of cyber warfare in theory and practice (Ser. The Basics)*. Syngress.

Wong, A. (2022). *The diaspora and China's foreign influence activities*. Wilson Center. https://www.wilsoncenter.org/publication/diaspora-and-chinas-foreign-influence-activities

Yablokov, I. (2022). Russian disinformation finds fertile ground in the West. *Natural Human Behavior 6,* 766–767. https://doi.org/10.1038/s41562-022-01399-3

Yong, W. (2019). Interpreting US-China trade war background, negotiations and consequences. *China International Strategy Review, 1*(1), 111–125. https://doi.org/10.1007/s42533-019-00019-6

Zheng, J., Zhou, S., Li, X., Padula, A. D., & Martin, W. (2023). Effects of eliminating the US-China trade dispute tariffs. *World Trade Review, 22*(2), 212–231. https://doi.org/10.1017/S1474745622000271