The Art of "iWar": Disinformation Campaign as a Strategy of Informational Autocracy Promotion[*]

Ming-Chiao Chang [a], Chun-Chih Chang [b] and Thung-Hong Lin [c]

[a] *National Taiwan University, School of Medicine*

[b] *Department of Political Science, Xiamen University, Xiamen, China. Email: stoicchang@gmail.com;*

[c] *Institute of Sociology, Academia Sinica, Taipei, Taiwan. Email: zoo42@gate.sinica.edu.tw*

Abstract

This study aims to investigate the global pattern of social media disinformation dissemination among regimes. We assume that autocracies adopting Internet censorship and spreading disinformation online to domestic population are more probable to apply Internet disinformation to attack their neighboring democracies than neighboring autocracies for their geopolitical interests. The autocracy promotion hypothesis is confirmed by the database integrated from the Varieties of Democracy (V-Dem) Digital Society Project (DSP) dataset (2000~2018) released in 2019. We also integrated socio-economic variables from different data sources from 137 countries to test the other hypotheses of domestic conditions facilitating the spread of Internet disinformation. Our empirical evidences show that democracies with a neighboring autocracy that adopted higher degree of Internet capacity would expose to higher risk suffering from foreign disinformation than other countries. In addition, the lower educational level of population, and the greater Internet coverage increase the possibility of disinformation campaign from abroad.

Keywords: autocracy promotion; fake news; internet censorship;
internet disinformation; iWar

[*] This paper is submitted to the 116th American Political Science Association's Annual Meeting & Exhibition, September 10-13, 2020.

Introduction

In the 2016 U.S. president election, Donald Trump's victory was inferred as a consequence of Russia's attacks of fake news and disinformation. Following evidences revealed that Russia's fake news did not only attempt to intervene into the U.S. president election but also target many elections and referenda in European countries (Davis 2018). During crucial events and political crises, disinformation and fake news grows to interrupt normal politics and cause appreciable damage. For example, in the 2019 Hong Kong demonstration, internet giants, such as Twitter, Facebook, and Google, recognized massive disinformation sources. When Coronavirus (COVID-19) has posed a medical crisis all over the world, the World Health Organization warned the risk of disinformation as "infodemic" which enhances interstate hostility and prevents global medical collaboration .

Disinformation, defined as false information spread deliberately to deceive people, had been applied to politics far before the digital age (Pacepa and Rychlak 2013). After the internet become a necessity in human life, disinformation spreading widely on social media lessens the effective communication in real politics, and manipulates the political behavior of the citizens via feeding them biased information (Fallis 2015). Furthermore, under the surrounding of "information overload", fake news containing extreme and emotional information perform more attractive and influential than the truth to the public (Deibert 2019). Therefore, studies of communication and internet politics mostly focused on the political and social mechanisms applying the micro-level surveys or mining the "big data" in the domestic cyberspaces (Guess 2019).

Since the internet facilitates dissemination of digital information across the border and at less cost, disinformation and digital technology may become a state's tool to manipulate domestic public opinion and intervene into foreign politics. As Guriev and Treisman (2020) argued, "informational autocrats" could apply censorship and disinformation to manipulate citizens' preference in order to sustain their political survival and to reduce the risk applying costly violent repression. A recent study uncovered that in contrast to democracies, autocracies tend to apply Internet censorship to reduce the strength of civil society effectively (Chang and Lin 2020). Furthermore, "internet warfare" (or iWar) has performed as a new diplomatic and security strategy for international conflicts and (Ryan 2007). Lutscher et al. (2020) found, during election periods, authoritarian states used the tool of denial-of-service to censor information from websites abroad. Given vivid cases and evidences revealed the existence of "iWar", however, some experts argue that internet conflicts should not be exaggerated as another kind of international warfare. Valeriano and Maness (2014) claimed that there are only limited, low-end, and regional cyber disputes and conflicts. Bradshaw and Howard (2018b; also see 2018a; 2019) found, either in democratic or authoritarian regimes, disinformation campaigns mostly focus on domestic audiences, and only a small number of autocracies use the weapon of disinformation to attack foreign adversaries.

Based on these academic studies, we like to elucidate the following questions: which state does commit to launch attacks of disinformation campaigns? Who are more likely to become targets of disinformation campaigns? We offer a comprehensive theoretical framework, underlying initiators and receptors of global disinformation campaigns. Our comprehensive database integrated from the Varieties of Democracy (V-Dem) Digital Society Project (DSP) dataset (2000~2018) released in 2019, and socio-economic variables of 137 countries from different data sources to test hypotheses of domestic conditions facilitating the spread of Internet disinformation.

Empirical results have confirmed the “informational autocracy promotion” hypothesis: the autocracies adopting Internet censorship and spreading disinformation online to domestic population are more probable to apply Internet disinformation to attack their neighboring democracies than neighboring autocracies for their geopolitical interest. Moreover, the more domestic government-sponsored Internet disinformation and lower educated level of domestic population would increase the hazard suffering from foreign disinformation online. The spread pattern of foreign disinformation online in some democracies such as Taiwan, Latvia, Hungry, and Georgia around the autocratic powers such as China and Russia match the autocracy promotion hypothesis in cyberspace. Our study contributes to the field by considering both international and domestic determinants of Internet disinformation from aboard.

A Framework of Global Disinformation Campaign

After the Cold War, scholars of democratic theory advocated a gentle strategy to accommodate autocracies in the Post-Cold War era. Incorporating autocracies into an international economic and political order successfully led to the third wave democratization in the 1990s and color revolution in the 2000s. In recent years, the global trend of authoritarian resurgence appeared when China, Russia, and other leading autocracies not only survived their rule but also exported their virtue over the globe (Gat 2007; Walker 2015). Academic interest turns to autocratic powers’ influences aboard and stimulates an increasing body of theorizing on the internationalization of authoritarianism, such as autocracy diffusion (Ambrosio 2010), autocracy promotion (Bader 2010), and autocratic sharp power (Walker and Ludwig 2017). However, literature suggests that the empirical evidence is vague and regionally limited, and difficult to trace domestic and foreign sources of Internet attacks and disinformation campaigns (Brownlee 2017; Tolstrup 2015; Way 2015; 2016). Based on studies of regime diffusion and promotion, we illustrate a new theoretical framework of international spread of disinformation campaigns. Four types of literature are categorized according to initiators and receptors of disinformation attacks (Table 1).

Table 1. Literature of Internet Disinformation Campaign between Different Regimes

International Internet disinformation		Receptor	
		Democracy	Autocracy
Initiator	Autocracy	Autocracy promotion	Autocracy support
	Democracy	Internet populism	Democracy promotion

In the first category of literature, the “autocracy promotion theory,” originally refers to a variation of international strategies that autocracies intendedly applied to undermine democracies. As Tansey (2015) argued, those who accuse autocracy promotion need to consider the agency, target, motives, and effects of the suspected international affairs of autocracies. Lankina et al. (2016) found that in contrast to democratic diffusion of European Union, which is more likely to invest in civil society organizations, autocracy promotion is more likely done by establishing political and economic networks. The concept of autocracy promotion could also be defined by exclusively and inclusively ways. While the exclusive way illustrates all international forces that predisposed the regime toward authoritarian rules, the inclusive way “embraces all initiatives,” which means actions creating a friendly environment for autocracy survival could also count as political strategies of autocracy promotion (Burnell 2010).

Otherwise, Yakouchyk (2019) suggested the concept, “autocracy support”, which refers to the strategies that one autocracy adopts to stabilize another autocracy (von Soest 2015). For example, Bader (2015) analyzed different forms of Chinese bilateral engagement, including state visits, arms trading, aid projects, economic cooperation, and trade dependence. The result showed that only export dependence on China might increase the likelihood of survival for autocracies while doing little to their democratic counterparts. Studies of “autocracy promotion” and “autocracy support”, nevertheless, mostly applied the cross-national time-series data of conventional diplomatic affairs and neglected Internet disinformation so far (except Lutscher et al. 2020).Overall, the two concepts share the same implication, namely an “autocratic initiator” hypothesis, whether regime type of the receptor is.

The third category is the disinformation attacks among democracies. As recent studies of populism argued, the peering and polarization of netizens could be the dynamic of radical politicians or partisans as the insiders of democracy. Therefore, the disinformation online could easily flow internationally among democracies and be applied by politicians and parties to reshape the domestic political landscape. Cumulative evidence of disinformation attacks on social media emerged, as the 2016 presidential election campaign of the United States and Brexit campaign (Faris et al. 2017). Following the public concern of rising populism online in democracies, we named the category of disinformation literature as the “Internet populism”.

The last category refers to the attacks from democracies to autocracies, namely the strategy of “democracy promotion.” Studies of democratization argued, in contrast to conspiracy, the international and domestic determinants of democracy diffusion or autocracy diffusion might be structural, unintended, and contingent in history (Capoccia and Ziblatt 2010; Gunitsky 2018). Criticism against democracy promotion consider it as a fallacy of Western international organizations managing humanization aids (Carothers, 2002). Although the effect of democracy promotion has been wildly doubted, autocracies such as Russia and China of criticized the conspiracy of democracy promotion and consequently blocked the Western Internet business giants out. It shall be noticed that, the last two concepts, Internet populism and democracy promotion, share a "democratic initiator" hypothesis, whether regime type of the receptor is.

In the field of international affairs, democratic peace theory underlines how two countries interact with each other based on their essence of regime type. It claimed that international conflicts are less likely to happen among similar regimes, especially in midst democracies (Gleditsch 1992; Bennett 2006). Therefore, unlike the suggestion of the populist hypothesis, democracies would less likely fall into the disinformation campaign against each other. In addition, the strategy of democracy promotion online has been limited by the strengthening Internet censorship of autocracies in the recent decade (Chang and Lin 2020). Therefore, among four categories, we expect that the global disinformation campaign data would match the autocratic initiator hypothesis; that is, in contrast to democratic powers, autocratic powers are more likely to attack or support others via disinformation campaign. However, we suggest that regime type of initiator cannot be the only factor sufficient to delineate the international pattern of disinformation campaigns. Initiators' incentive and capacity spreading disinformation and receptors' "susceptibility" should be underlined to complement the argument of informational autocracy promotion.

Initiator's Geopolitical Incentive and Internet Capacity

The initiator's geopolitical incentive to launch disinformation attacks could be measured by its geographic proximity and involvement of armed conflicts. We assume that even if information strike can reach countries regardless of their geographic positions, autocratic initiators prefer to launch their Internet disinformation attacks toward neighboring regimes. International armed conflicts usually happen among neighboring countries due to contested territories. Considering the cost of involving the armed conflict and the risk to lose it, autocratic initiators tend to apply disinformation attacks to the neighboring regimes in contract to armed conflicts. Moreover, geographical proximity increases the possibility of information infiltration and manipulation because of sharing similar historical backgrounds and massive experiences of interaction. Given cross-border acquaintance with similar language and culture, autocracies are capable of producing fact-alike information to reshape public perception and conduct autocratic-friendly foreign policies of nearby regimes (Ambrosio 2010 Weyland 2017; Brownlee 2017; Guriev and Treisman 2019). Therefore, we assume that geographical proximity is a facilitating factor for autocratic initiator to preserve benefits, and to apply Internet disinformation attack as a new form of international conflict strategy.

Hypothesis 1 (H1): neighboring autocratic initiator (NAI): a receptor country is more likely attacked by Internet disinformation from neighboring autocracies than from neighboring democracies.

As the informational autocrat theory argued, applying Internet censorship and disinformation could be a cheaper instrument than violent repression for authoritarian political control (Guriev and Treisman 2020). The same political logic could be extended to the international conflicts of the autocrat. In the international conflicts, in contract to democracies, autocracies encounter less political constraints to apply disinformation to the domestic population and foreign enemies. Therefore, the neighboring autocracy that has engaged in some armed conflicts has stronger incentive to launch disinformation campaigns aboard to the receptor.

Hypothesis 2 (H2): neighboring autocratic war-maker: a receptor country is more likely attacked by Internet disinformation from neighboring autocracies involving armed conflicts.

The risk of receptor suffering from foreign disinformation campaign also depends on the initiators' internet capacity. In this study, the domestic internet capacity refers to the state capacity of spreading disinformation and censoring information to the domestic population. The informational autocrats have adopted various new informational technologies to mitigate threats and bolster political legitimacy (Guriev and Treisman 2020). Domestic disinformation, spread by cyber troops served for governments or parties, leads to political polarization and discontents, aiming to exploit public opinion or even overturn election (Bradshaw and Howard 2018a; 2018b; 2019). There are consequences of domestic disinformation attacks, nevertheless. Study showed that the more domestic disinformation attacks from the state, the more vulnerable the societies are to foreign disinformation attacks (Faris et al. 2017).

We argue that states effectively conducting domestic disinformation and censorship would more capable to demonstrate online influence on interrupting politics of foreign countries. As studies on "authoritarian sharp power" (Walker and Ludwig 2017) suggested, for the autocratic powers, it is reasonable to apply the domestic Internet capacity, which might not primarily for international conflict by design, to support their friends and repress their enemies aboard. As Bradshaw and Howard (2018b, 29) found, with the tool of disinformation campaigns, only handful autocracies are capable of misguiding foreign audiences. Therefore, the association between the initiator's domestic internet capacity and foreign internet disinformation attacks on the receptor, whether it is democracy or not, are applied to our hypothesis:

Hypothesis 3 (H3): Internet capacity: the higher the autocratic initiator's capacity of domestic Internet disinformation and Internet censorship, the greater the foreign Internet disinformation on the receptor.

The Susceptibility of Receptor: Democracy and Socio-demographic Factors

National interests of geographic proximity are sparking points to trigger cyberattack, especially for neighboring countries with different regime types (Ambrosio 2010; Babayan 2015; Libman and Obydenkova 2018; Vanderhill 2013; Von 2015). On basis of political survive theory (Bueno de Mesquita et al. 2003), Bader et al. (2010) argued that, from interacting with similar political regimes in the neighborhood, autocrats could obtain private substance for domestic winning coalition. When disinformation attack triggers public distrust in authoritative information of contiguous democracies, intimate relationship between societal and political actors is disrupted and legitimacy of democracy is undermined (Bennett and Livingston 2018). In addition, building regional alliances and regional regime identity does not only benefit autocracies' national interests but also protect autocracies from democracy diffusion (Kneuer and Demmelhuber 2016, 784). At last, neighboring autocracies of the initiator could prevent from disinformation attacks by their own censorship. Therefore, the autocratic initiator is more likely to spread disinformation to the democratic receptors, that is, the autocracy promotion hypothesis.

Hypothesis 4 (H4): autocracy promotion: in contrast to autocracies, democracies are more likely attacked by Internet disinformation from neighboring autocracies.

Although internet censorship is usually not conducted by democratic governments, disinformation could be spread by political elites or citizens in the society. For example, Guess et al. (2019) argued that while dissemination is much less effective than people think, it is usually done by aging, lower educated, and conservative population. In studies of democracies, critical media literacy is viewed as an essential factor to deepen the democratic institution (Kellner and Share 2007; Mihailidis and Thevenin 2013), which is no doubt a strategy that aims to eliminate the threat the media could cause and improve its beneficial role in democracy. Therefore, we underline two domestic factors of the receptor, namely socio-demographic susceptibility, that may worsen effects of disinformation: education and age.

Tremendous studies worked on how people with different educational levels react to disinformation, but a consensus has yet to achieve. Reuter et al. (2019) also discovered that educated individuals are more sensitive to the perception of fake news in Germany. Furthermore, Bedard and Schoenthaler (2010) showed that high school graduate has significantly better ability to identify satire or fake news. Horne and Adali (2017) argued that compared to real news, fake news has a more comprehensible content and shorter length, whcih people with lower education levels could easily follow .

On the contrary, some studies show that education level did not make any difference of resisting disinformation. Some suggested that higher levels of education did not reduce the degree of confirmation bias, that is, people seek information that confirms their existing opinion, despite incorrect. Confirmation bias leads to poor decision making and lacking awareness of disinformation (Gatlin et al. 2019). There is also study showing that education level plays no role in affecting credibility, quality, and fake news perception (Gosselt 2019). Despite the inconsistent results on the micro-level studies, we assume that on the aggregative level, a better educated civil society shall show a better awareness and resistance of disinformation.

Some previous studies reported the relationship between age and deceived by disinformation. Hasher and Zacks (1988) suggested that the abilities to prevent false information declined in the elderly as their cognitive ability decay though time (see also Peters et al., 2007). In a recent study, Guess, Nagler, and Tucker (2019) found aged people above 65 shares nearly seven times more fake articles than the younger group, even after ideology and partisanship were controlled. He et.al (2019) Chinese elders on Wechat are more likely to spread rumors as well as escalate rumor anxiety. However, the effect of an aging society could be very different from an aged group because the aging society with longer life expectancy usually caused by wealthier, higher educated, and heather population. We attempt to test these findings to a macro-level scale.

Hypothesis 5 (H5): socio-demographic susceptibility: the lower educated level, and younger population of recipient country could be more susceptible under foreign Internet disinformation.

Data and Methods

The balanced panel dataset was created by combining various resources. It includes data from 160 countries in 2001-2017. Base on the 215 countries or territories of the World Development Indicator from the World Bank, we merged data from various origins, and some countries are then omitted. The number of countries declined to 137 because we have to conduct a matrix of initiator and receptor of disinformation, and drop not only the origin country but also the destination country if their missing variable could difficultly be imputed. Variables are explained respectively in the following paragraphs (please see Appendix Table 1 as data sources, Appendix Table 2 as data descriptions, and supplementary files for the details).

Dependent variable

The dependent variable is foreign government dissemination of false information (abbreviated as foreign disinformation below). It is from the Digital Society Project (DSP) dataset (2000–2018) released together with V-dem project, version 9 in 2019. The variable derived from the question: "How routinely do foreign governments and their agents use social media to disseminate misleading viewpoints or false information to influence domestic politics in this country?" The respondent could answer in a 0-4 ordinal scale. It was then converted to an interval scale of 0%-99% by the Bayesian item response theory measurement model. Formerly in the DSP database, the lower the variable value is, the more serious the phenomenon is in the country. However, for the comprehensibility of the statistic result, we reversed the variable value order and transformed it into a value from 1 to 100 based on the maximum and the minimum variables. Therefore, in our dataset, a higher value implies a more severe foreign disinformation attack.

Control variables

We controlled the following variables: economic development and Internet coverage. Economic development is a fundamental factor correlating the dynamic of internet activities, which is a crevasse for false information dissemination (Wunnava and Leiter 2009). The level of economic development as measured by the natural logarithm of GDP per capita (GDP per capita, current US$) from the World Bank' World Development Indicator (WDI) database. The data of Internet coverage is also from the WDI database, indicating the percentage of the population that is using the internet. The variable Foreign Disinformation bases on the disinformation disseminated via social media; therefore, the availability of the Internet should be a premise to bring out. Furthermore, the diffusion of the Internet, which we consider as internet coverage, inevitably affect the effectiveness of spreading information and disinformation.

Explanatory variables

We applied eight explanatory variables, categorizing in domestic determinants, geopolitical determinants, and one interaction term. Domestic determinants are for illustrating the conditions of the receptor; geopolitical determinants are for describing the initiators; and the interaction term is for testing the hypothesis of autocracy promotion.

Domestic variables

To illustrate the conditions of the receptor of foreign disinformation, we applied five variables: Domestic Internet censorship (shown as Internet censorship in the following), Domestic disinformation, Regime type, Secondary school enrollment and life expectancy. The indicator of Internet censorship is derived from the V-dem project, measuring the governments' efforts to censor the Internet. To clarify, the DSP only concerns with Internet filtering (blocking access to certain websites or browsers), denial-of-service attacks, and partial or total Internet shutdowns. It does not deal with the censored content unless the censorship is used as a pretext for suppressing political information or opinions. The ordinal indicator was converted to an interval scale, a lower value implies a more restricted Internet. In our dataset, we reversed the variable value order and transformed it into 0% ~99% according to the maximum and minimum value, as for now, a higher value means a more serious attempt of Internet censorship.

Domestic disinformation originates from the DSP database as well. It measures "how often do the government and its agents use social media to disseminate misleading viewpoints or false information to influence its population". Compared to our dependent variable, foreign disinformation, both regarding the false information with political attempts circulating on social media, despite that the source is different. Formerly in the V-dem project, a lower value implies the tendency of domestic governments to spread disinformation on social media. We also reversed the variable value order and transformed it into 0%~99% according to the maximum and minimum value.

Regime type is a critical variable to test our hypothesis of disinformation dissemination between states. As Broadshaw and Philip (2018) mentioned, political actor across all regime types and geographical borders would manipulate the information accessed by the foreign or domestic audience to support their interests. Moreover, to what we concern, the autocrats actively adopted the technology with an attempt to erode democracy. We applied Polity IV to categorize regime types. Polity IV is a database covering 164 countries from 1800-2017. It scores from -10 to +10, with -10 the most autocratic and 10 the most democratic. In our study, we implement the variable classified in two categories: autocracies (scored -10 to 5) and democracies (scored 6-10). The baseline group will be autocracies in out statistics.

Finally, secondary school enrollment and life expectancy derived from the WDI database. The former is for capturing the education level of a state, while the latter representing the level of aging population, which could be the reversed indicator of lower educated and younger susceptible population of foreign disinformation attacks.

Geopolitical variables

To illustrate the conditions of the for the initiators, we applied four variables of any neighboring country: regime type, armed conflict, domestic Internet censorship and domestic disinformation of the most autocratic neighboring regime (abbreviated as NAI in the following). This study aims to analyze the issue from a geopolitical perspective, therefore, the initiators in this study are neighboring countries initiating foreign disinformation attack. We identify the neighbors of 215 countries listed in the WDI database via they are neighboring regimes based on contiguous and maritime boundary (Grafton 2012). However, the neighbors of overseas territory are excluded (ex: neighborhoods of Puerto Rico won't count as the US neighbors). And given that South Sudan gained independence from Sudan in 2011, Sudan is not the neighbor of Kenya, Republic of Congo, Uganda since then.

This process generates multiple neighbors for each country. Subsequently, we selected the most autocratic state in the neighbors (according to the Polity IV database). If there is an autocracy (Polity < 6) presented as the neighboring country, we apply a dummy variable to identify the suspect initiator. The receptor could be surrounded by democracies, and the suspect initiator could change during the two decades if one autocracy replaced another as the minimum scored neighbor. The data of Internet censorship and domestic disinformation of these selected countries as the most autocratic neighbor of the receptor were processed to generate the other interactive explanatory variables.

Interaction term

Lastly, an interaction term was incorporated to test our hypothesis: regime type of the neighboring countries, autocratic initiator (NAI=1 if any) times its armed conflict, its Internet censorship, and its domestic disinformation. Moreover, we assume that the interaction term of the receptors' regime type and the initiators' capacity of domestic disinformation shall change the receptors' degree of being attack by foreign disinformation. According to the autocracy promotion hypothesis, in contrast to autocracies with a neighboring autocracy, democracies with a neighboring autocracy have significantly higher risk to be attacked (autocratic initiators' domestic disinformation*democracy (=1) of receptor).

Global Trends of Key Variables

Where are the victims of foreign disinformation? Figure 1 shows the time-dependent pattern of the ten countries most attacked by foreign disinformation, plus the global trend. The trajectory of global trend of foreign disinformation increases over the years. It could be taken as a solid evidence that states widely adopt disinformation as an international conflict strategy. Observing the listed top countries, Taiwan triumphed as the most attacked by the neighboring autocracy, China. The information environment is extremely vulnerable in Taiwan under the cyber invasion of China, which takes the advantage of similar language used on social media and meddles in the Taiwan's democratic institution for China's interest. Taiwan is a typical victim in our concern, severely suffered by China's disinformation attack under the tension as a frontier of autocracy promotion (Dickey 2019).

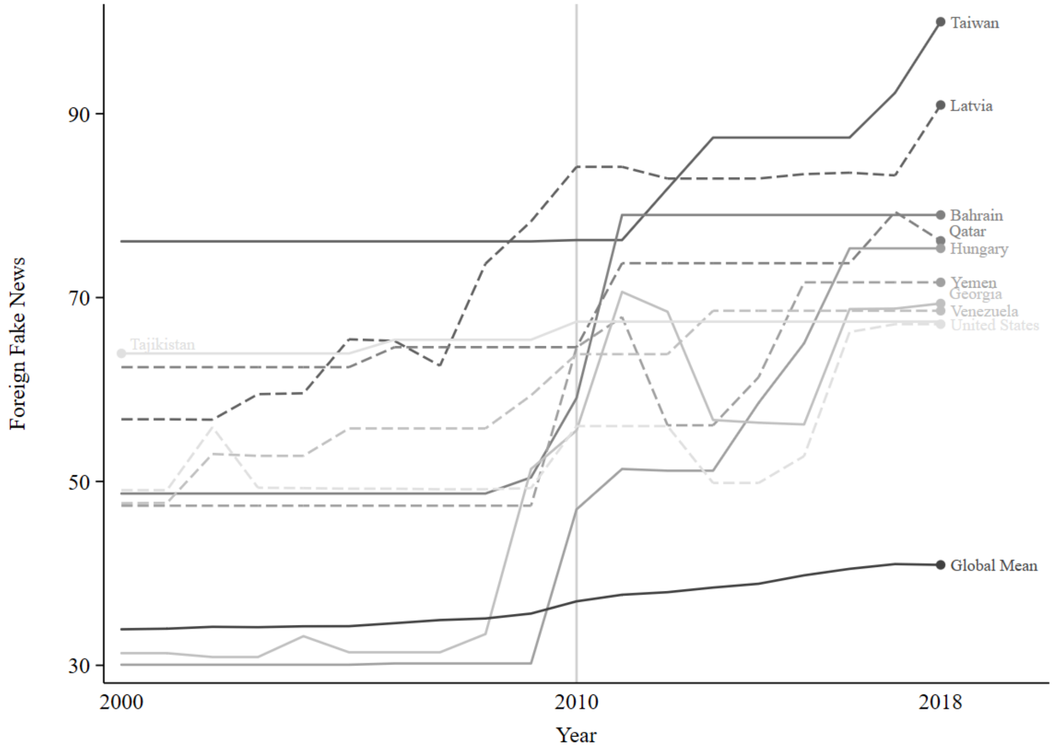

Figure 1. Global trend and trajectories of the top ten countries under foreign fake news attacks

The democracies neighboring Russia also suffer from foreign disinformation seriously. Latvia, Hungary, and Georgia are countries with geographical proximity and intensive diplomatic relations with Russia. The former Soviet Union member had shared institutional legacies, vital resources, common culture, and language that were inherited by new-born independent countries later. However, the shared legacy has turned out to be tensions nowadays due to Russia's pursuit of identity as the dominant power in the region (Nygren 2007). Baltic countries near board Russia, are seen as a buffer zone against Western intrusion, in which Russia aggressively influence the internal policies (Ciziunas 2008). Latvia, as one of the Baltic countries, has a sizeable Russian-speaking population that is exploited by the Kremlin in its disinformation campaign, leading to a relatively large presence of Russian Media. In Latvia, the political trust in Russia increased with the rising of Russian Media (Berzina 2018).

Fierce disinformation warfare was famously noted in the 2008 brief conflict between Russia and Georgia, in which two countries were competing to control the information flowing to the global community. Even though Georgia seemed to win the information war in the end, the disinformation strategies of Russia in 2008 were later adjusted to apply to Ukraine conflict in 2014. That is to say, Georgia act as an R&D lab of the Russian disinformation campaign as Taiwan does under the interference of China (Writer 2018).

Arabic countries got caught between Saudi Arabia and Iran, such as Qatar, Bahrain and Yemen, suffered the most from the attack of foreign disinformation. Yemen had suffered from a bloody civil war led by two major fractions, the Abdrabbuh Mansur Hadi led Yemeni government and the Houthi armed movement, since 2015. The civil war had recently settled in November 2019. During the complicated conflict, Saudi Arabia had intervened in the country. Yemen was a place under chaos, on which regional and global powers leverage at the time. Qatar, neighboring Saudi Arabia on its south, is another target of cybercrime due to its high internet penetration, intensive engagement in global politics, and economic interests from sufficient oil. Cybercrime occurred in various forms, such as hack attacks, influencing their media and Internet infrastructure. For example, SEA (Syrian Electronic Army) had exploited the high coverage of smartphone in Qatar to disseminate disinformation undermining the reputation of the Qatar government (Tabassum 2018).

Iran has already been aggressive on implying cyber tools on the neighboring countries, such as Yemen and the West, influencing the target countries' public opinion. The country is well known for its censorship and the restriction of civil rights, fighting against internal dissents via cyber tools. Inheriting an authoritarian political characteristic, Iran has ruthlessly developed trained cyber troop, recruited domestic talents to devote to the security of the nation. (Farwell and Arakelian, 2013).

It is clear that the most attacked countries were influenced by the neighboring autocracies that attempt to expand their geopolitical power over the region, such as China, Russia or Iran. The intensive interactions may also lead to a higher risk of the iWar. The trend gives us a first glance at the geopolitics of foreign disinformation dissemination. In our precedent analysis, we assume that the regime type of neighboring states is a key factor that influences the countries' extent of foreign disinformation dissemination.

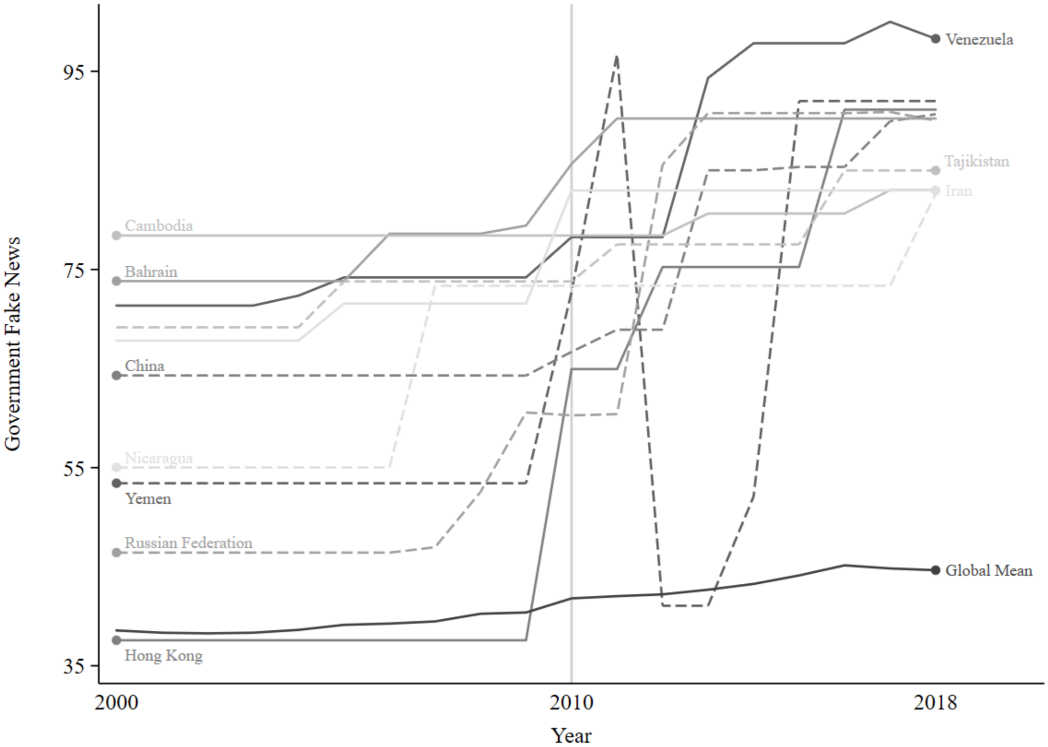

Figure 2. Global trend and trajectories of the top ten countries suffered from government fake news

We assume the origins of foreign disinformation are neighboring autocracies with strong domestic Internet capacity. The capacity of computational propaganda, Internet censorship, and disinformation could not only apply to domestic opinion manipulation but also to geopolitical conflicts. Figure 2 shows the ten countries in which the governments spread the most disinformation domestically . As Bradshaw and Howard portraited in the report (2019), most countries listed in Figure 2 have active cyber forces, such as Cambodia, Venezuela, Tajikistan, Bahrain, Russia, Iran and China.

The three authoritarian powers, Russia, Iran, and China, which are mentioned above to be the source of attack are shown in Figure 2. These three countries invest tremendously in the iWar. Bahrain, Venezuela, Yemen, and Tajikistan are both listed in Figure 1 and Figure 2. Their society is the most attacked, both by its own government and foreign powers, echoing our assumption that the more domestic disinformation attacks from the state itself, the more vulnerable the society is to the foreign disinformation attacks.

Models

We applied a standardized high dimensional fixed-effect (HDFE) model containing autoregressive terms of a few lagged variables: Internet user, the natural logarithm of GDP per capita, and determinants regarding the ability to manipulate the internet. The HDFE regression model that comprised the following autoregressive terms: lagged dependent variables, year and country dummies, and lagged independent variables. The advantage of this HDFE regression model is its exclusion of the effects of unobserved timeinvariant variables (e.g., geographic region and national religion). The autoregressive term was used to control for the continuity of lagged dependent variables, implying that these variables violated the parallel trend assumption of difference-in-difference regression models. The results please refer to Table 1.

Analysis

Firstly, we dealt with our minor concentration in Model 1. As Table 1 shows, effects of life expectancy and the second school enrollment are significant (H5). Both features reduce foreign disinformation dissemination in states. The result confirms that education level tempers the influence of the disinformation attack abroad, but also rejects the previous claims that elder societies are more susceptible to the foreign attack.

Table 1 High Dimensional Fixed-effect Regression on Foreign Disinformation (Standardized)

	Foreign Disinformation					
	(1)	(2)	(3)	(4)	(5)	(6)
Democracy (t-1)	-0.079**	-0.023	-0.025	-0.025	-0.024	-0.031
	(0.026)	(0.026)	(0.026)	(0.026)	(0.026)	(0.026)
Internet Censorship (t-1)		-0.011	-0.005	-0.002	-0.007	-0.007
		(0.018)	(0.018)	(0.018)	(0.018)	(0.018)
Domestic Disinformation (t-1)		0.229***	0.223***	0.221***	0.214***	0.219***
		(0.020)	(0.020)	(0.020)	(0.020)	(0.020)
Neighboring Autocracy (NAI = 1) (t-1)			0.245***	0.236***	0.211***	0.211***
			(0.031)	(0.032)	(0.033)	(0.033)
Armed Conflict of NAI (t-1)				0.025*	0.028*	0.025*
				(0.011)	(0.011)	(0.011)
Internet Censorship of NAI (t-1)					0.060***	0.059***
					(0.015)	(0.015)
Domestic Disinformation of NAI (t-1)					-0.007	-0.074***
					(0.013)	(0.022)
Domestic Disinformation of NAI × Democracy (t-1)						0.085***
						(0.023)
Internet Coverage (t-1)	0.087***	0.071***	0.067***	0.063***	0.062**	0.064***
	(0.019)	(0.019)	(0.019)	(0.019)	(0.019)	(0.019)
ln(GDP pc) (t-1)	0.150**	0.175***	0.162**	0.170***	0.140**	0.153**
	(0.052)	(0.051)	(0.050)	(0.050)	(0.051)	(0.051)
Life Expectancy (t-1)	-0.186***	-0.157***	-0.139***	-0.143***	-0.138***	-0.113**
	(0.041)	(0.040)	(0.040)	(0.040)	(0.040)	(0.040)
Secondary School Enrollment (t-1)	-0.086***	-0.100***	-0.084***	-0.077**	-0.075**	-0.074**
	(0.025)	(0.025)	(0.024)	(0.025)	(0.025)	(0.025)
Constant	0.060***	0.026	-0.148***	-0.148***	-0.132***	-0.117***
	(0.017)	(0.017)	(0.028)	(0.028)	(0.029)	(0.029)
Country Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
Year Fixed Effect	Yes	Yes	Yes	Yes	Yes	Yes
R^2	0.938	0.942	0.943	0.943	0.944	0.944
Adjusted R^2	0.934	0.938	0.939	0.940	0.940	0.940

Note: N = 2,466. Coefficient of linear regression absorbing multiple levels of fixed effects model, standard errors in parentheses, * *p* < .05, ** *p* < .01, *** *p* < .001, two-tailed test

As for the control variables, GDP per capita is significant, indicating that the foreign attack abroad occurred along with better economic condition. The percentage of internet user also shows significance, which is intuitive since social media disinformation attack happened only if the public have access to the Internet. The regime type indicates that democratic regimes are less susceptible to disinformation globally. However, we see that the effect of regime type expunges as other variables add on, indicating that the democracy itself, usually be surrounded by other democracies such as those countries in North America, Southern Pacific, and European Union, may not be the main target of the attack.

We then examine the states' capacity to manipulate the Internet in Model 2. The indicator of receptor's internet censorship is not significant. The indicator of receptor's domestic disinformation dissemination is significant, escalating the extent of the attack. In this model, the variable of democracy does not show appreciable effect on foreign disinformation.

The result suggests that the more the governments disseminate fake news domestically, the more foreign severe attack could be (Faris et al. 2017). Otherwise, life expectancy and the second school enrollment reduce the extent of foreign disinformation, while GDP per capita and the percentage of internet have positive correlation with the disinformation attack from abroad.

In Model 3, we added the NAI, if any appeared neighboring the receptor, into the model with controls in the Model 2. As the NAI hypothesis (H1) expected, it significantly increased the degree of receptor's foreign disinformation. In Model 4, we added if the selected NAI of Model 3 engaged in any armed conflicts (t-1). The armed conflict variable of the NAI last year is also significantly increased the degree of receptor's foreign disinformation. As the autocratic war-maker hypothesis (H2) expected, autocracies tend to apply disinformation in conflicts. The results of the two models show the effects of NAIs' geopolitical incentive on sponsoring disinformation campaign to the receptor, whether the regime type of the later so far.

In Model 5, the NAI's Internet capacity, both the indicator of its Internet censorship and government-sponsored domestic disinformation, was add on. The indicator of the NAI' internet censorship presents significant with a positive correlation to foreign disinformation attacks, while domestic disinformation dissemination of NAI does not show its significant effect, on the receptor. The autocracies' Internet capacity nearby can extrapolate to the attack in the receptor (H3). To be precise, autocracies project their domestic Internet capacity and extrapolating them as tools to intervene in public attitudes in neighboring regimes.

Model 6 further includes the interaction term between democracy and NAIs' domestic disinformation dissemination. The interaction term (if the receptor is democratic) is significant with a positive coefficient, while the NAI' domestic disinformation dissemination shows a negative effect (if the receptor is not democratic). Here, we have the evidence to argue that autocracies that dedicate to disseminating false information may utilize their ability to attack neighboring democracies rather than other regime types. The manipulation strategies showed here echoes the autocracy promotion hypothesis (H4).

The regime type variable representing democracies is significant only in Model 1 and 6. That is to say, the democratic regime may have some resilience. However, after considering the neighbors' targeted attempt, regime type acts a minor role in confronting foreign disinformation attacks. In other words, the NAIs' attempt are the more critical. .

To reconfirm our argument, the result of Model 6 is applied to predict the relationship between receptors' foreign disinformation and the NAIs' domestic disinformation, divided by two groups of receptors' regime types, autocracies and democracies, in Figure 3. The more significant slope of "democracies" indicates that as the manipulation abilities of NAI increase, the attack to democratic receptors mounts up more rapidly than that is in autocracies. We thus argue that autocracies with high Internet capacity would utilize their strength to attack their neighbors, and democracies suffer the most. However, it is also worth noticing that democracies receive less foreign disinformation than autocracies as a whole due to their geographical clustering.

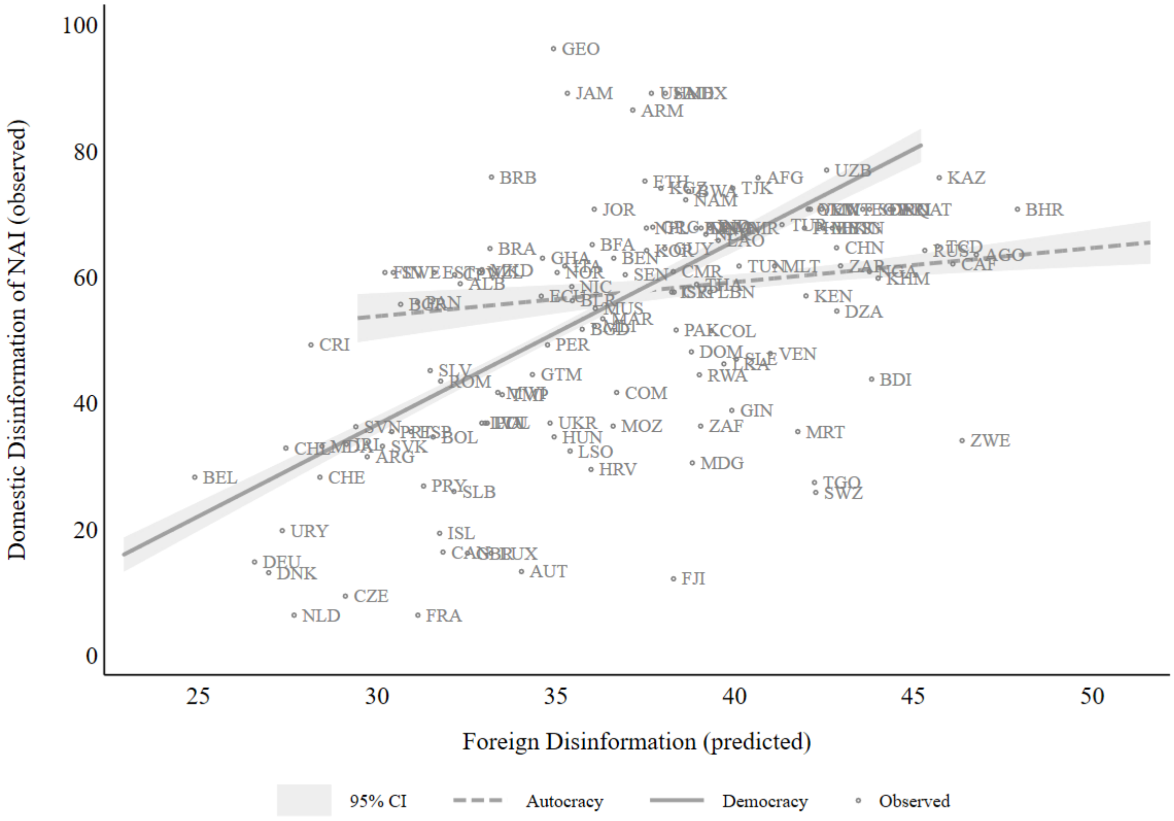

Figure 3. Government Fake News of NAI and Foreign Fake News.

In sum, empirical result pictures a unique pattern, showing that autocracies target their disinformation strategies on democracies. Our study illustrated that disseminating false information is a novel strategy for autocracy promotion applied in geopolitics. Moreover, previous studies demonstrated that autocratic regimes pose economic or political influence on their neighborhoods to develop the geostrategic interest for persisting their survival (Babayan 2015; Libman and Obydenkova 2018; Vanderhill 2013; Von 2015). In our case regarding the disinformation attack, we find that geographical proximity "does in fact matter, it likely does not matter on its own" (Ambrosio, 2010).

Conclusion

The study explores the determinant of foreign disinformation dissemination in states all over the world. The findings give insights in understanding novel trends of autocracy promotion and empirical basis to foreign disinformation prevention strategies. Our findings may contribute to the literature in several aspects.

First, on the issue of international security, the pattern of autocracy promotion by disinformation campaigns echoes the mounting literature on autocracies' "sharp power." We argue that the pattern of autocracy promotion is confined to neighborhood regions where powerful autocracies claim interests. The interest-driven model should be distinguished from ideology-driven model. In other words, iWar is a new strategy for autocracies to grip its regional profits, not to fight for the global battle of ideology, at least before the pandemic.

Second, factors of real politics such as the state and geographical space should be addressed in Internet politics. Cyber-utopianism delineates the Internet sphere as borderless and a realm where no actor can control information flow (Katz & Rice, 2002; May, 2002). However, we find that autocracies have adopted information weapons to infiltrate politics of nearby democracies, and geographical proximity is a factor of amplification (Bennett and Livingston 2018). Political actors and geographic space of real politics have shaped the online livelihood.

Third, the study reveals education level strikes a significant influence on reducing foreign disinformation attacks. This suggests that media literacy and the cognitive ability to recognize disinformation is of importance; and states and civil societies, especially in democracies, suffering from foreign disinformation attacks could enhance the education level and digital literacy to temper the damage. In addition, there is a negative relation between aging and foreign attacks. More study should be conducted on the topic since aging is an inevitable global trend.

Last, the finding sheds light on how manipulating information domestically matters. Since domestic political actors are utilizing computational propaganda on democratic procedures, preventing them from being their own worst enemy should be on the agenda. Disinformation undermine the credibility of democratic institutions. Political actors implementing the propaganda should keep this in mind and take responsibility for the preservation of democracy.

Overall, disinformation circulating on internet has raised awareness in global politics. Our study reconfirms that the toxic information are no longer piece of words or videos randomly generated by innocent individuals, instead, it is a battle between democracies and autocracies, especially on geopolitical advantages and conflicts. To fight against that, a comprehensive research agenda of the arts of iWars should be further arranged.

Bibliography

Aday, S., Farrell, H., Lynch, M., Sides, J., & Freelon, D. (2012). New media and conflict after the Arab Spring. *United States Institute of Peace*, *80*, 1-24.

Ambrosio, T. (2010). Constructing a framework of authoritarian diffusion: Concepts, dynamics, and future research. *International studies perspectives*, *11*(4), 375-392.

Ambrosio, T. (2012). The rise of the “China Mode” and “Beijing Consensus”: Evidence of authoritarian diffusion? *Contemporary Politics*, *18*(4), 381-399.

Babayan, N. (2015). The return of the empire? Russia's counteraction to transatlantic democracy promotion in its near abroad. *Democratization*, *22*(3), 438-458.

Bader, J. (2015). China, autocratic patron? An empirical investigation of China as a factor in autocratic survival. *International Studies Quarterly*, *59*(1), 23-33.

Bader, J., Grävingholt, J., & Kästner, A. (2010). Would autocracies promote autocracy? A political economy perspective on regime-type export in regional neighbourhoods. *Contemporary Politics*, *16*(1), 81-100.

Bedard, M., & Schoenthaler, C. (2018). Satire or fake news: Social media consumers' socio-demographics decide. In *Companion Proceedings of the The Web Conference 2018* (pp. 613-619).

Benková, L. (2018). *The Rise of Russian Disinformation in Europe.*

Bennett, S. D. (2006). Toward a continuous specification of the democracy-autocracy connection. *International Studies Quarterly 50(2)*, 313-338.

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European journal of communication*, *33*(2), 122-139.

Berzina, I. (2018). Political trust and Russian media in Latvia. *Journal on Baltic Security*, *1*(ahead-of-print).

Bradshaw, S., & Howard, P. N. (2018a). *Challenging truth and trust: A global inventory of organized social media manipulation.* Project on Computational Propaganda.

Bradshaw, S., & Howard, P. N. (2018b). The global organization of social media disinformation campaigns. *Journal of International Affairs, 71(1.5)*, 23-32.

Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*. Project on Computational Propaganda.

Brownlee, J. (2017). The limited reach of authoritarian powers. *Democratization*, *24*(7), 1326-1344.

Bueno de Mesquita, B., Smith, A., Siverson, R.M., and Morrow, J.D., (2003). *The logic of political survival*. Cambridge, MA: MIT Press.

Burnell, P. (2010). Is there a new autocracy promotion? Working paper, FRIDE. March 2010.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The guardian*, *17*, 22.

Capoccia, G., & Ziblatt, D. (2010). The historical turn in democratization studies: A new research agenda for Europe and beyond. *Comparative Political Studies, 43(8–9)*, 931–968.

Carothers, T. (2002). The end of the transition paradigm. *Journal of democracy, 13(1)*, 5-21.

Chang, C. C. and Lin, T. H. (2018). “Blocking the Spring Out: Internet Coverage, Internet Censorship and Civil Society in 156 Countries during 1995-2017”, paper presented at World Congress of International Political Science Association, Brisbane, Australia: International Political Science Association, 2018-07-21 ~ 2018-07-25.

Chow, K. P., Yau, K., & Li, F. (2015). Cyber attacks and political events: The case of the occupy central campaign. In *International Conference on Critical Infrastructure Protection* (pp. 17-27). Springer, Cham.

Ciziunas, P. (2008). Russia and the Baltic states: Is Russian imperialism dead? *Comparative Strategy*, *27*(3), 287-307.

Davis, S. (2018). Russian Meddling in Elections and Referenda in the Alliance. General Report of Science and Technology Committee, NATO Parliamentary Assembly, 18 November.

Deibert, R. J. (2019). The Road to Digital Unfreedom: Three Painful Truths About Social Media. *Journal of Democracy*, *30*(1), 25-39.

Dickey, L. (2019). Confronting the challenge of online disinformation in Taiwan. In Y. Tatsumi, P. Kennedy, & J. Li (eds.), *Disinformation, cybersecurity, and energy challenges* (pp. 11-22). Washington, DC: Stimson Center.

Douglas, K. M., Sutton, R. M., Callan, M. J., Dawtry, R. J., & Harvey, A. J. (2016). Someone is pulling the strings: Hypersensitive agency detection and belief in conspiracy theories. *Thinking & Reasoning*, *22*(1), 57-77.

Fallis, D. (2015). What is disinformation? *Library Trends*, *63*(3), 401-426.

Faris, R., Roberts, H., Etling, B., Bourassa, N., Zuckerman, E., & Benkler, Y. (2017). Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election. *Berkman Klein Center Research Publication*, *6*.

Farwell, J. P., & Arakelian, D. (2013). What does Iran's cyber capability mean for future conflict? *Seton Hall Journal of Diplomacy and International Relations*, *14*(1), 49.

Gat, A. (2007). The return of authoritarian great powers. *Foreign Affairs*, *86*, 59.

Gatlin, K. P., Cooley, L. G., & Elam, A. G. (2019). Confirmation bias: Does it vary by culture or education level? *International Journal of Business Marketing and Management*, 4 (2), 40-43.

Gleditsch, N. P. (1992). Democracy and peace. *Journal of Peace Research*, *29(4),* 369-376.

Gosselt, J. F. (2019). *“Fake it till you make it” An experiment of fake news perception by use of experts and support* (Unpublished master's thesis). University of Twente.

Grafton, R. Q. (2012). United Nations Convention on the Law of the Sea (UNCLOS). In *A Dictionary of Climate Change and the Environment*. Edward Elgar Publishing Limited.

Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science advances*, *5*(1), eaau4586.

Gunitsky, S. (2018). Democratic waves in historical perspective. *Perspectives on Politics 16 (3),* 634-651.

Guriev, Sergei, and Daniel Treisman, “Informational Autocrats,” *Journal of Economic Perspectives* 33, no. 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3208523.

Hasher, L., & Zacks, R. T. (1988). Working memory, comprehension, and aging: A review and a new view. *The psychology of learning and motivation*, *22*, 193-225.

He, L., Yang, H., Xiong, X., & Lai, K. (2019). Online rumor transmission among younger and older adults. SAGE Open. https://doi.org/10.1177/2158244019876273

Ho, M. (2019). Challenging Beijing’s mandate of heaven: Taiwan’s Sunflower Movement and Hong Kong’s Umbrella Movement. Philadelphia: Temple University Press.

Horne, B. D., & Adali, S. (2017, May). This just in: fake news packs a lot in title, uses simpler, repetitive content in text body, more similar to satire than real news. In *Eleventh International AAAI Conference on Web and Social Media*.

Huang, P. (2019). Chinese cyber-operatives boosted Taiwan’s insurgent candidate. *Foreign Policy, 26*.

Katz, J. E., & Rice, R. E. (Eds.). (2002). *Social consequences of internet use: Access, involvement and expression*. Cambridge, Mass.: MIT Press.

Kellner, D., & Share, J. (2007). Critical media literacy, democracy, and the reconstruction of education. *Media literacy: A reader*, 3-23.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, 107 (2), 1-18.

King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument. *American Political Science Review*, 111 (3), 484-501.

Kneuer, M. and Demmelhuber, T. (2016). Gravity centres of authoritarian rule: a conceptual approach. *Democratization*, *23*(5), 775-796.

Lankina, T., Libman, A. & Obydenkova, A. (2016). Authoritarian and democratic diffusion in Post-communist regions. *Comparative Political Studies*, *49* (12): 1599-1629.

Li, L. (2018). Transparency, Propaganda and Disinformation: 'Managing' Anticorruption Information in China. *Journal of Comparative Law*.

Libman, A., & Obydenkova, A. V. (2018). Regional international organizations as a strategy of autocracy: the Eurasian Economic Union and Russian foreign policy. *International Affairs*, *94*(5), 1037-1058.

Lutscher, P. M., Weidmann, N. B., Roberts, M. E., Jonker, M., King, A., & Dainotti, A. (2020). At home and abroad: The use of denial-of-service attacks during elections in nondemocratic regimes. *Journal of Conflict Resolution*, *64*(2–3), 373-401.

May, C. (2002). *The information society: A sceptical view*. Cambridge, Mass.: Polity Press.

Mihailidis, P., & Thevenin, B. (2013). Media literacy as a core competency for engaged citizenship in participatory democracy. *American Behavioral Scientist, 57*(11), 1611-1622.

Milo, D., & Klingová, K. (2017). *The vulnerability index: Subversive Russian influence in Central Europe*. Globsec Policy Institute.

Ngok, M. (2011). Value changes and legitimacy crisis in post-industrial Hong Kong. *Asian Survey*, *51*(4), 683-712.

Nygren, B. (2007). *The rebuilding of Greater Russia: Putin's foreign policy towards the CIS countries*. Routledge.

Pacepa, I. M., & Rychlak, R. J. (2013). *Disinformation: Former Spy Chief Reveals Secret Strategy for Undermining Freedom, Attacking Religion, and Promoting Terrorism*. WND Books.

Peters, E., Hess, T. M., Västfjäll, D., & Auman, C. (2007). Adult age differences in dual information processes: Implications for the role of affective and deliberative processes in older adults' decision making. *Perspectives on Psychological Science*, *2*(1), 1-23.

Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy*, *30*(1), 53-67.

Reuter, C., Hartwig, K., Kirchner, J., & Schlegel, N. (2019). Fake News Perception in Germany: A Representative Study of People's Attitudes and Approaches to Counteract Disinformation.

Ryan, J. (winter,2007). iWar: A new threat, its convenience and our increasing vulnerability. Retrieved January 25, 2020, from North Atlantic Treaty Organization website: https://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

Tabassum, A., Mustafa, M. S., & Al Maadeed, S. A. (2018). The need for a global response against cybercrime: Qatar as a case study. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-6). IEEE.

Tansey, O. (2015). Questioning 'autocracy promotion'. *Comparative Democratization (APSA Section Newsletter)*, *13*(1), 1.

Taubman, G. (1998). A not-so World Wide Web: The Internet, China, and the challenges to nondemocratic rule. *Political Communication*, *15*(2), 255-272.

Tolstrup, J. (2015). Black knights and elections in authoritarian regimes: Why and how Russia supports authoritarian incumbents in post-Soviet states. *European Journal of Political Research*, *54*(4), 673-690.

Valeriano, B., and Maness, C M. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347-360.

Van Prooijen, J. W., Krouwel, A. P., & Pollet, T. V. (2015). Political extremism predicts belief in conspiracy theories. *Social Psychological and Personality Science*, *6*(5), 570-578.

Vanderhill, R. (2013). *Promoting authoritarianism abroad*. Boulder, CO: Lynne Rienner Publishers.

Vargo, C. J, Guo L., and Amazeen M. A. (2018). The agenda-setting power of fake news: A big data analysis of the online media landscape from 2014 to 2016. *New Media & Society*, *20*(5), 2028-2049.

Von Soest, C. (2015). Democracy prevention: The international collaboration of authoritarian regimes. *European Journal of Political Research*, *54*(4), 623-638.

Walker, C., & Ludwig, J. (2017). The meaning of sharp power: How authoritarian states project influence. *Foreign Affairs*, *16*.

Way, L. A. (2015). The limits of autocracy promotion: The case of Russia in the 'near abroad'. *European Journal of Political Research*, *54*(4), 691-706.

Way, L. A. (2016). Weaknesses of Autocracy Promotion. *Journal of Democracy*, *27*(1), 64-75.

Weiss, J. C. (2013). Authoritarian Signaling, Mass Audiences, and Nationalist Protest in China. *International Organization*, *67* (1), 1-35.

Weyland, Kurt. (2017). Autocratic diffusion and cooperation: The impact of interests vs. ideology. *Democratization*, 24(7), 1235-1252.

Writer, S. (2018, December 26). China uses Taiwan as R&D lab to disrupt democracies. Retrieved January 25, 2020, from https://asia.nikkei.com/Politics/International-relations/China-uses-Taiwan-as-R-D-lab-to-disrupt-democracies

Wunnava, P. V., & Leiter, D. B. (2009). Determinants of intercountry Internet diffusion rates. *American Journal of Economics and Sociology*, *68*(2), 413-426.

Yakouchyk, K. (2019). Beyond autocracy promotion: A review. *Political Studies Review*, *17*(2), 147-160.

Zarrabi-Kashani, H. (2014). Iran and the Arab Spring: Then and now.

Ziblatt, D. and Capoccia, G. (2010). The Historical Turn in Democratization Studies. *Comparative Political Studies 43(8-9),* 931-968.

Appendix Table A1 Data Sources

Variables	Measurement	Data Source	N before Imputation
Foreign disinformation (of the receptor)	Foreign governments dissemination of false information. Question: How routinely do foreign governments and their agents use social media to disseminate misleading viewpoints or false information to influence domestic politics in this country? Responses: 0: Extremely often. Foreign governments disseminate false information on all key political issues. 1: Often. Foreign governments disseminate false information on many key political issues. 2: About half the time. Foreign governments disseminate false information on some key political issues, but not others. 3: Rarely. Foreign governments disseminate false information on only a few key political issues. 4: Never, or almost never. Foreign governments never disseminate false information on key political issues.	Varieties of Democracy (V-Dem) ver. 9	No imputation
Domestic disinformation (of the receptor)	Government dissemination of false information to domestic population. Question: How often do the government and its agents use social media to disseminate misleading viewpoints or false information to influence its own population? Responses: 0: Extremely often. The government disseminates false information on all key political issues. 1: Often. The government disseminates false information on many key political issues. 2: About half the time. The government disseminates false information on some key political issues, but not others. 3: Rarely. The government disseminates false information on only a few key political issues. 4: Never, or almost never. The government never disseminates false information on key political issues.	V-Dem ver. 9	2,460/2,466

Variables	Measurement	Data Source	N before Imputation
Internet censorship of the receptor	Internet censorship attempts include Internet filtering (blocking access to certain websites or browsers), denial-of-service attacks, and partial or total Internet shutdowns. Censorship of topics such as child pornography, highly classified information such as military or intelligence secrets, statements offensive to a particular religion, or defamatory speech is not concerned unless this sort of censorship is used as a pretext for censoring political information or opinions. We are also not concerned with the extent of internet access, unless there is absolutely no access at all (in which case the coding should be 0). The ordinary scale follows: 1: The government successfully blocks Internet access except to sites that are pro-government or devoid of political content. 2: The government attempts to block Internet access except to sites that are pro-government or devoid of political content, but many users are able to circumvent such controls. 3: The government allows Internet access, including to some sites that are critical of the government, but blocks selected sites that deal with especially politically sensitive issues. 4: The government allows Internet access that is unrestricted, with the exceptions mentioned above.	V-Dem ver. 9	No imputation
Neighboring Autocracy (NAI = 1)	Neighboring regime's Polity Score, 1 = at least one non-democracy appeared from the country with minimum Polity Score. The country ID will be applied to identify the following NAI.	Polity IV	No imputation
Armed Conflict of NAI	The frequency of Armed Conflict occurred of the selected NAI.	UCDP/PRIO Armed Conflict Dataset ver. 19.1	No imputation
Democracy (of the receptor)	Receptor's Polity Score, 1 = democracies; 0 = non-democracies.	Polity IV	No imputation
Domestic disinformation of NAI	The disinformation score of the selected NAI.	V-Dem ver. 9	No imputation
Internet censorship of NAI	The Internet censorship score of the selected NAI.	V-Dem ver. 9	No imputation
Internet coverage	Individuals using the Internet (% of population) of the receptor	World Development Indicators (WDI)	2,439/2,466
ln(GDP pc)	GDP per capita, PPP (constant 2011 international $) of the receptor.	WDI	2,455/2,466

Variables	Measurement	Data Source	N before Imputation
Life expectancy	Life expectancy at birth, total (years) of the receptor.	WDI	No imputation
Secondary school enrollment	School enrollment, secondary (% gross) of the receptor.	WDI	2,054/2,466

Table A2 Description of Variables for 137 Countries during 2000 - 2018

Variables	Mean	SD	Min	Max
Foreign Disinformation	36.848	18.108	0.000	100.000
Democracy	0.638	0.481	0	1
Internet Censorship	31.471	20.568	0.000	100.000
Domestic Disinformation	40.927	21.536	0.000	100.000
Neighboring Autocracy (NAI = 1)	0.718	0.450	0	1
Armed Conflict of NAI	0.265	0.716	0	7
Internet Censorship of NAI	44.133	24.923	0.000	100.000
Domestic Disinformation of NAI	52.580	22.144	0.000	100.000
Internet Coverage	30.551	29.187	0.000	98.260
ln(GDP pc)	9.087	1.230	6.302	11.770
Life Expectancy	69.780	9.342	38.702	84.680
Secondary School Enrollment	76.469	30.178	6.112	163.931

Note: N = 2,466. The year range of Foreign Disinformation is 2001-2018 and that of the other variables 2000-2017.

Table A3 Correlation Matrix of Selected Variables

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
(1) Foreign Disinformation	1										
(2) Democracy	-0.291*	1									
(3) Internet Censorship	0.318*	-0.690*	1								
(4) Domestic Disinformation	0.414*	-0.596*	0.673*	1							
(5) Neighboring Autocracy (NAI = 1)	0.276*	-0.350*	0.320*	0.301*	1						
(6) Armed Conflict of NAI	0.032	-0.020	0.045*	0.055*	-0.024	1					
(7) Internet Censorship of NAI	0.369*	-0.398*	0.482*	0.425*	0.633*	0.055*	1				
(8) Domestic Disinformation of NAI	0.303*	-0.238*	0.310*	0.341*	0.562*	0.093*	0.666*	1			
(9) Internet Coverage	-0.044*	0.341*	-0.390*	-0.397*	-0.275*	0.031	-0.260*	-0.125*	1		
(10)ln(GDP pc)	-0.072*	0.364*	-0.363*	-0.415*	-0.331*	-0.025	-0.219*	-0.145*	0.773*	1	
(11)Life Expectancy	-0.048*	0.397*	-0.356*	-0.363*	-0.349*	0.056*	-0.214*	-0.088*	0.724*	0.830*	1
(12)Secondary School Enrollment	-0.090*	0.411*	-0.381*	-0.415*	-0.334*	-0.019	-0.260*	-0.134*	0.733*	0.851*	0.829*

Note: * *p* < .05, two-tailed test.