A Qualitative Analysis of the Relationship Between Cyberthreats and Democratic Backsliding

Amy I. Browning
William & Mary

A Qualitative Analysis of the Relationship Between Cyberthreats and Democratic Backsliding

Amy Browning

Coastal Virginia Commonwealth Cyber Initiative

Cybersecurity Undergraduate Research Program

Dr. Michael Lapke

April 14, 2023

TABLE OF CONTENTS

Introduction

Cyberthreat Case Studies

Conclusion

The recent Russian invasion of Ukraine in late February 2022 stunned the world as the most devastating conflict in the West since the second World War. Aside from the horrific human cost and the increased geopolitical tensions the war has produced, the conflict is serving as an important test of modern warfare strategy and technological capabilities. Because of the pressure on - and self-interest of - NATO states to refrain from joining in conventional warfare tactics to assist Ukraine, the focus has been on providing weapons, supplies, and military training to fuel an internal defensive and counteroffensive response. Yet, a more covert approach with the capability to both physically harm and gain crucial information from adversaries exists - the utilization of cyberwarfare.

When done successfully, cyberattacks can cripple key infrastructure necessary for carrying out military operations and maintaining crucial lines of communication between field infantry and leadership officers. Russia is already a prominent threat in cyberspace, and has a history of carrying out cyberattacks in Eastern Europe prior to the February 2022 Ukraine invasion (Buresh, 2021). More recently in the Russia-Ukraine war, cyberattacks on civilian services have expanded, likely due in part from the failure of conventional warfare necessitating alternative tactics for Russia (Miller, 2023). With the cyber sector being critical to the Russian offensive it's only natural to place equal, if not greater, importance on the capability and willingness of Ukraine and NATO allies to conduct counter cyberattacks. If state propensity towards conducting cyberattacks and responding/preparing for cyberthreats is increasingly relevant in modern conflicts, what can current research tell us about the relationship between a state's political institutions and their respective proficiency in the cyber realm?

Background

The political saliency of regime type relating to frequency and degree of foreign conflict cannot be understated. Democratic peace theory- which can be traced back to the work of 18th-century German philosopher Immanuel Kant as well as American *Common Sense* author Thomas Paine - has long been popular in the study of International Relations, and although the driving factors behind the theory continue to be contested, evidence from historical and current conflicts largely support the concept. The theory postulates that democracies are reluctant to go to war with other democracies, favoring peaceful solutions over armed conflict. Scholars generally attribute this behavior to the influence of shared institutions, norms, or both;

democratic institutions require significant time, public support, and preparation before engaging in conflict, while shared norms between democracies encourage compromise-centered thinking and mutual respect for agreements (Farnham, 2003).

Recent research extends democratic peace theory to be equally applicable in cyberspace, with democracies being found to have a “pacifying effect on the initiation of state-sponsored cyberattacks” (Albert et al., 2022, para. 1). Since democratic institutions seemingly indicate less proclivity for offensive cyberattacks, one must inquire about the degree to which regime type and instigation or reception of cyberthreats are intertwined, if at all. Russia itself has experienced significant democratic backsliding under Vladimir Putin’s efforts to shift the state towards a personalist autocracy (Shevtsova, 2008; McFaul, 2018; Fish, 2018) - could this be relevant when discussing the state’s cyberattacks? Does the loss of democratic institutions encourage the usage of cyberattacks to obtain state objectives? Alternatively, does the usage of cyberthreats and expansion of technological capabilities as a means to collect inter-state and intra-state information by top areas of government lead to democratic backsliding and the erosion of democratic ideals? The inherent tie between democratic backsliding and cyberthreats must be explored further, especially in a time where cyberwarfare and more independent state-sponsored cyberattacks are increasingly common and worrisome to international security.

Concepts Defined

The importance of regime classification and transition in states around the globe is central to many academic disciplines - particularly the realm of international security - whether the focus is on physical, economic, civil, or cyber elements. Over the last century, periods of democratization and autocratization have shaped global affairs and provided information on the conditions likely to force or encourage regime change, which allows states to better anticipate the climate of future diplomatic relations. The latest wave of autocratization originated in the post-cold war 1990s and has accelerated in the past decade; characterized by a more gradual erosion of democratic values, scholars are eager to theorize the driving factors behind the movement. Instead of military coups, “democratically elected incumbents have been responsible for more than two-thirds of all episodes of contemporary autocratization” through employing restrictions on civil society, limiting media usage, and undermining democratic institutions (Aydin-Duzgit et al,, 2019, para. 5). It must be noted that this latest wave of autocratization includes a country becoming less democratic or shifting into autocratic classification, as both changes are due to the same process, with one simply at a higher caliber. Autocratization is a multifaceted process, but it is often spurred on by increased control given to the executive - such as through emergency decrees and special powers (Lührmann and Rooney, 2021).

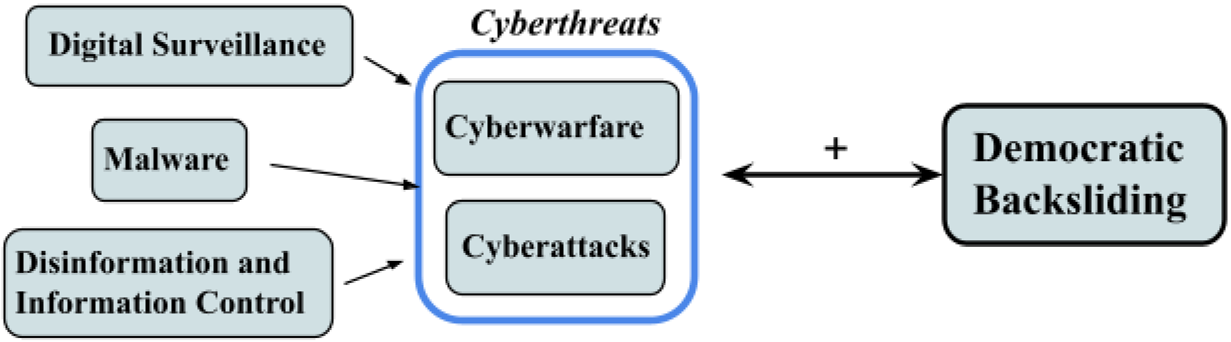
Nearly adjacent to the concept of autocratization is the process of democratic backsliding. Both terms refer to the same regime change trend, but democratic backsliding is usually used to describe the fluidity of the process and applicability to all state classifications. Democratic backsliding can occur in what would normally be viewed as healthy democracies, or in fresh, barely recognized democratic regimes. The term implies a loss of democratic quality - a change *within* the system, not *of* the system (Gerschewski, 2018). Naturally, democratic backsliding is quite concerning for global democracies; if the quality of one state's democracy can slip by without much pushback, what's to say it can't happen elsewhere? What factors were at play in the cases of, say, Russia, Venezuela, and Belarus, that can also be observed occurring in states like Tunisia, Poland, and even the United States? These questions are routinely studied to diagnose domestic problems and prepare for foreign policy adjustments. One key - perhaps under researched - component of democratic backsliding is the relevancy of activity in cyberspace. The ability for personalist leaders to shape public opinion through social media, utilize crowd/personal surveillance technology, and access user data to inform institutional malpractices or political steps, could all be aided by the accessibility and prevalence of increasingly advanced cyber systems. Due to expansive growth in the cyber-field in recent decades, the question of whether such a rise has contributed (and may continue to contribute) to democratic backsliding must be studied. Alternatively, democratic backsliding itself could lead to both domestic and international cyberthreats, as democratic institutions which traditionally serve as a protector of public privacy and a check for cyberattacks are weakened. International security experts must incorporate this linkage into conflict deterrence frameworks, and politicians and diplomats alike working in/from democracies have an interest in mitigating such a relationship. This paper seeks to answer this causal order question between democratic backsliding and cyberthreats, and provide insight on whether the latest wave of autocratization is due in part to developments in the cyberfield.

The construct of a cyberthreat has not been specifically defined in scholarly literature, as by its very nature it is a category filled with whatever the user wishes to focus on or believe most pertinent to the applicable state, system, group, or individual experiencing the “threat” from cyberspace. From a national security perspective, “cyberthreat” would include the following sub constructs: internal or external hostile intelligence agents, spreading disinformation, malicious code/malware (Whitman and Mattord 2012), ransomware (Stallings and Brown 2015), and digital surveillance. These terms are often employed en-masse or in a time of conflict or tension between states, in which case they are usually referred to as being a cyberattack or an act of cyberwarfare. Essentially, a cyberthreat seeks to utilize a targeted action to obtain information, damage digital or physical systems, or disrupt operations central to a particular cause. This paper employs the usage of the term “cyberthreats” to indicate a collection of defined topics, as limiting the term would be dismissing possible past activities or future capabilities done with malicious or exploitative intent in cyberspace. Cyberattacks and cyberwarfare fall under the classification of cyberthreat, as their anticipation fuels defensive measures. For the US Government, a cyberattack is generally viewed as any “malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself” (NIST CSRC). To other scholars, a cyberattack is an action aimed to “undermine the functions of a computer network for a political or national security purpose” (Hathaway et al., 2012, p. 821). Throughout this paper many sources will refer to cyberthreats as cyberattacks, as reports of incidents are written after, not in anticipation of, cyberthreats.

Research Methodology

This paper will explore the relationship between cyberthreats and democratic backsliding. As recent research has indicated that democracies are less likely to carry out cyberattacks (Albert et al., 2022), one may be inclined to assume that as democratic institutions are eroded in a state, that state is more likely to carry out (and perhaps receive in return) cyberthreats. However, the desire for weaker states to compete with global powers for intelligence, resources, and other assets may encourage partially democratic or authoritarian regimes to use cyberthreats to even the playing field. After all, competing with powerful armies like the United States and South Korea is easily a lost cause, but increased capacity to conduct cyberattacks can heighten a state’s power advantage without needing to invest in conventional warfare/security, which is much more competitive. As states are perceived as greater threats or have more bargaining weight, the regime may wish to cling to power to maintain the success they are experiencing. Cyberthreats to the public of a state can also stem from leaders wishing to control their perception in the population; such cyberthreats then naturally weaken democratic institutions and usually involve disinformation, digital surveillance, and electoral fraud. This desire to utilize cyberthreats to advance state or personal interests may inadvertently contribute to the trend of global autocratization seen in recent years. To understand the degree to which democratic backsliding may contribute to an increase in cyber threats, or vice versa, a qualitative analysis of key states will be conducted. These case studies will be broken into sections according to the categorization of cyberthreat: disinformation/information control through data breaches, malware attacks, and digital surveillance, so comparisons between states may be more easily made. The thorough examination of the cyberspace actions of Russia, the United States, China, and Iran, in regards to both democratic backsliding and cyberthreat assessment, will serve to fill the lack of information on the linkage between the two terms.

Conceptual Framework:



Disinformation and Information Control

Disinformation and information control are vital to examine when attributing a purposeful usage of a cyberattack to influence domestic public opinion on a leader or state policy, or to sway international view of an issue. Disinformation, the "deliberate provision of false information to mislead", or information control (i.e, the ability to release sensitive or secure material to the public) are more likely to be used by authoritarian governments or employed to discredit or disturb democracies (Matthews, 2019, para. 1). The most notable instance of a campaign based information manipulation by a foreign power in recent years is the actions of the Russian Federation in the 2016 U.S. presidential election. Multiple state-sponsored hacking groups - mainly APT 28 and The Dukes - released sensitive emails and communications from the U.S. Democratic National Committee, disrupting the information flow into civil society and the security of information in electoral institutions. According to a U.S. declassified intelligence report, Russia hoped to sway the presidential election to favor Donald Trump instead of Hillary Clinton by leaking the information (Sanger, 2017). As the American public learned of both the security compromise of the DNC, and the unflattering information that was exposed, public confidence in the U.S. electoral system naturally wavered, making democratic strength the additional victim of the cyberattack.

The spread of disinformation as a cyberthreat is often accomplished through the exploitation of social media platforms. With these platforms experiencing a massive boom in both quantity of users and daily engagement over the past decade, with over 4 hours per day in some nations (Buchholtz, 2022), using social media to popularize a narrative or boost engagement on a topic of state interest is relatively easy. Russian disinformation networks have repeatedly used fake accounts to target U.S. users, spreading fabricated news in an effort to influence U.S. elections (Frenkel & Barnes, 2020). These disinformation attacks frequently permeate every major social media platform to lend credibility to the given false information, a technique originally found in digital marketing (BBC, 2018). Iran has also used similar tactics on Twitter to "disrupt the public conversation" around elections (Sardarizadeh, 2020) and influence American democracy in the safety of cyberspace. Using disinformation to undermine democratic institutions is a popular method for states, as it yields near-immediate results that are difficult to reverse - lies spread on average six times faster than the truth (Aral et al., 2018) - and has comparatively low implementation costs. From a financial standpoint, such disinformation cyberthreats are an attractive option for state strategic interests, as directing hundreds of online bots is but a fraction of other defense spending or espionage options.

Such a decline in faith of democratic processes is a key contributor to democratic backsliding. As political institutions are targeted by a state-sponsored cyberattack, whether the state's interest is in manipulating the result of an election or simply sowing uncertainty in the election itself, the quality of foreign democracies are put in jeopardy. The meddling in democracies such as France, the United Kingdom, Sweden, the Netherlands, and Germany expose the Russian pattern of utilizing cyberthreats as a covert method of global influence to break down democratic institutions (Brattberg & Maurer, 2018). This strategy is not isolated to Russia: other nations including China (Singleton, 2022) and Iran (U.S. Dept. of State, 2022) have repeatedly used the same strategy without much consequence. Regardless of the original desired outcome of the instigator, these cyberattacks result in increased apprehension of election legitimacy and lend support to narratives of fraud or a broken democratic system. The methodical usage of campaigns intended to undermine public faith in democratic processes and delegitimize electoral systems can therefore accelerate a state's democratic backsliding - suggesting that recent cyberattacks and future cyberthreats pose a serious concern for democracies all over the world.

In tandem with targeted attacks on democracies, Russian internal democratic backsliding is exacerbated by the careful crafting of online media to act as an echochamber for pro-Russian and pro-Putin sentiment; such sentiment is then used to justify cyberattacks on other nations - e.g. Estonia, Georgia, and Ukraine. In Estonia, the 2007 distributed denial-of-service attacks (likely carried out by Russian youth groups and national sympathizers) exemplified the weight private cyberspace users carried in mobilizing narratives perpetuated online into the physical world (Russell, 2014). The instigators of the attack originating from a state with restricted information access leads to the probable linkage between circular reasoning/justification amongst civil society groups in cyberspace, and attacks carried out to protect the interests of the state. For this reason, the ability to limit a traditionally open cyberspace leads to "ideology as paramount in [cyber]conflict" through the propensity for the growth of shared values that challenge authoritarian rule (Flynn, 2019).

Disinformation cyber threats are not only relevant in election periods or with propaganda: states can also raise geopolitical tensions by creating fake news stories, starting rumors, or manufacturing support for a state interest. In 2020, Poland and Lithuania were victims of a (likely) Russian cyber disinformation attack aimed at "undermining relations between the two NATO allies" (Associated Press, 2020), as part of a larger effort to undermine eastern european democracy and connection to the rest of the west. Russian disinformation attacks targeting Lithuania - a formerly authoritarian state serving as a reminder of how states can "transform themselves into thriving, free, and democratic nations" - have also increased since the 2022 Russian invasion of Ukraine, to bolster pro-Russian parts of civil society and reprimand Lithuania for its close relationship with the EU, NATO, and democracy as a whole (McCarthy 2015).

The simmering conflict between China and Taiwan is also being fought in cyberspace, with China launching a "cyberwarfare and disinformation campaign meant to disrupt Taiwan's democracy" and its people's way of life (Rogin 2022). This disinformation campaign has created narratives of the Taiwanese government being controlled by the CIA, spread information to undermine the government's response to the COVID-19 pandemic, and has promoted pro-Beijing candidates in elections, all tactics which erode Taiwan's democracy and weaken the state to be more susceptible to Chinese influence or possible future physical attack. These disinformation campaigns are also used to indirectly address the U.S.'s involvement in the delicate relationship between Taiwan - and its international recognition as a state - and China, and dissuade further U.S. support of Taiwan. When U.S. House of Representatives Speaker Nancy Pelosi visited the island in August 2022, abrasive messages on hacked public signage targeted the politician, calling her a "'warmonger'" and directing her to "'get out of Taiwan'" - attacks adding to the "'fake news on social media… pav[ing] the way for [a Chinese] eventual operation'" through hijacking public opinion and demoralizing the public (Mccandless Farmer, 2022). In this case it is clear how cyberthreats - specifically the spread of disinformation - are used to promote public scrutiny of democracy and thus contribute to democratic backsliding.

Russian disinformation and information control also aids in preventing the spread of democratic ideals or growth or western sympathy, fueling the continued autocratization of the state. Although not uniformly successful (Meredith 2013), Russia asserts dominance in cyberspace over their own populace by "restricting internet access out of fear [users] can threaten the legitimacy of [the] centralized government" (Flynn 2019, p. 194). Despite not propagating outright false information, the control of the information allowed to be viewed on public servers still reaches the desired effect of disinformation: influence over the diffusion of beliefs, facts, events, or ideologies deemed threatening or necessitating subversion by the state. Noting the role of digital organization and connection through cyberspace in the democratization efforts in other nations, most recently with the Arab Spring (King, 2014; AlSayyad & Guvenc, 2015), Russia has carefully amputated avenues for public dissent and reapplied such tools to a global agenda advancing their strategic interests - to aid in the establishment of administrations and policies favorable to the Kremlin.

Iranian information control exhibits how a theocracy or autocratic regime uses disinformation to maintain anti-democratic values and do damage control on global reputation. Even in an age with widespread internet access for approximately 56 million Iranians, information control through censorship and state intimidation is commonplace; through cyber disinformation operations, Iran is able to "exaggerate [their] moral authority while minimizing [their] repression" of the public, and has done so even more heavily after the 2009 Green Movement - a nonviolent protest movement aimed at democratizing the state - which caused the government to "see social media activism as enabling an existential threat" (Brooking & Kianpour, 2020, para. 5 & 3). The spike in usage of social media sock puppets and propaganda networks following the Green Movement - an explicit threat to the regime with their slogan "Where is my vote?" - consists of an active ongoing strategy to subvert civil society. This strategy is incredibly salient when determining the effects of cyberthreats on democratic backsliding, because if a state is using cyberattacks to prevent the emergence of democracy, the same can be said for encouraging the erosion of democracy.

Malware Attacks

Malware attacks are cyberthreats that may seem inconsequential to the quality of a democracy at first glance. However, the ability to and choice of a state to carry out such an attack - that is, if the cyber operation is considered legal/state-sponsored or not - can indicate if democratic values are sound and protected. Similar to disinformation campaigns, malware attacks can also be used to target democratic institutions and undermine elections or public confidence in political systems. Instead of targeting potential voters with disinformation to influence their personal decision of which candidate to vote for, malware can simply alter votes and fabricate results, without needing to go through the trouble of reaching members of the public individually. Such tactics can be implemented domestically, to lengthen or solidify a leader's place in power, creating a more definite autocracy, or internationally, to generate uncertainty over results and frustration or disenfranchisement amongst voters, leading the victim state towards a path of democratic backsliding.

The democratic backsliding of Ukraine prior to the 2022 invasion from Russia was largely fueled by Russian malware attacks during election periods, or the threat of such events leading to public apprehension. The 2014 Ukrainian presidential election, which occurred after former President Viktor Yanukoych - widely regarded as an ally of the Kremlin - was removed from office during the Ukrainian Revolution, held great geopolitical ramifications for Russia, which sought to prevent the neighboring state from forming closer EU and NATO ties. To accomplish this objective, state-sponsored hackers infiltrated the Ukrainian Central Election Commission (CEC). The CEC later "uncovered malware …that incorrectly declared the far-right leader Dmytro Yarosh the winner", which compounded with a Russian news outlet reporting the fabricated results to confuse the public and raise concerns over democratic legitimacy (Kozloff, 2018, para. 12). The timing of this attack, which occured directly after the Russian sympathizer President was ousted from his post, and Ukrainians were demanding western partnership and ideals, exemplifies how cyberthreats can become a tool to instigate a decline in democratic quality at the direction of foreign adversarial interest.

Malware attacks targeting critical infrastructure can also contribute to democratic backsliding. If civil society is uncertain of a democracy's ability to secure the public from harm or foreign interference, the democracy may be seen as failing to deliver the basic civic protections its citizens demand. Unlike disinformation or other forms of malware attacks, it is difficult to directly trace denial of service or ransomware attacks to democratic backsliding, as they are usually isolated events affecting a comparatively smaller percentage of the state population. However, cyberattacks in Georgia (Roguski, 2020), Poland (Kozlowski, 2023), Lithuania (Kagubare, 2022), and Ukraine (Zinets, 2016), amongst others, show the wide scope of damage that can be done. As the victims of these malware attacks reel from their consequences, especially if the target was critical infrastructure like hospitals or oil pipelines, the public within those states are likely to feel inadequately protected and thus wary of their government's power. In this sense, not all cyberthreats contribute directly to democratic backsliding - they may just serve to sow the seed of doubt.

An analysis of malware attacks would be incomplete without delving into Stuxnet - largely regarded as the first known act of cyberwarfare. Developed by U.S. and Israeli intelligence, the Stuxnet worm is a form of malware originally designed to strategically target and damage components of the Iranian nuclear program. The worm was able to physically cripple nuclear infrastructure by destroying centrifuges - an extremely sophisticated design for the 2010 attack. Due to initial uncertainty over the instigators of the attack, the lack of ability to politically signal in cyberspace and respond appropriately was exposed (Lachow, 2011). Stuxnet also introduced new technology that could be reverse-engineered, prompting concerns over increased cyberterrorism threats to the United States (Chen, 2014). Yet, the legality or justification behind Stuxnet itself does not receive the same scrutiny as cyberattacks carried out by authoritarian regimes, despite its dangerous nature.

The implicit justification of Stuxnet can be attributed to the western view of Iran as a dangerous, unpredictable nuclear power necessitating mitigation in a controlled, indirect manner - so as to stay under the threshold of direct conflict while still lessening the bargaining power of the state. However, the decision of two democracies - the United States and Israel - to conduct what is widely viewed as an act of cyberwarfare, can lend critical information to how domestic democratic backsliding can fuel cyberthreats, starting the cycle from the state rather than the cyberattack. Scholars generally agree that the Stuxnet malware attack was an act of illegal force, due to the known physical damage it caused (Akhtar-Khavari & Haataja, 2018; Waterman, 2023). This distinction matters because democracies are by virtue held to standards by their population (or representatives of their population) on when to use physical force with adversaries. Although it may seem menial to some as it is generally viewed as in the state and public interest of both Israel and the U.S. to hinder the growth of the Iranian nuclear program, the decision of both states to launch Stuxnet may be indicative of a dismissal of democratic institutions in favor of greater centralized executive power.

One other important type of malware is spyware - malicious software meant to compromise a computer network to obtain information desired by another entity. The usage of this technology in authoritarian regimes is relatively straightforward as there are limited/no expected privacy protections for citizens, but the implementation of such software in democracies is both controversial and potentially threatening to democratic institutions themselves. When spyware from a democratic state against its own citizens is uncovered, direct evidence of cyber tactic usage increases as a result democratic backsliding emerges, as the right to individual privacy and freedom from government interference and control is generally a pillar of democratic norms (Nelson, 2004; Asrani-Dann, 2005). When democracies monitor citizens without due process, especially those whose profession encourages them to be skeptical or critical of government policies, such as journalists (Koukakis, 2022), concerns over the illegal weaponization of such data for business or political interests arise.

Spyware such as Pegasus - a technology designed by an Israeli firm providing real-time surveillance and access to photos, texts, and any other communications from the infected device - has been purchased by numerous democracies under the pretense of fighting national security threats; however, the technology can easily be used nefariously by democracies to target domestic dissenters - as seen with the Spanish use of the spyware against Catalonians working towards independence (Farrow, 2022). In a more overt linkage between the spyware and decline of democratic quality, Pegasus has been found to "exacerbate authoritarianism across Africa" (Allen & La Lime, 2021), and is a frequent tool of authoritarian governments wishing to intimidate and control threat to their regimes - as seen with the murder of Jamal Khashoggi by the Saudi government following months of Pegasus monitoring (Kirchgaessner, 2021). The continued purchasing of this spyware by democracies - who consider or actively use the cyberthreat, "undermine[s] the cause of human rights" and democratic institutions (Feldstein, 2021, para. 5). The hypocrisy of technology which is produced by a democracy being able to be sold to autocratic regimes to then be used to enforce authoritarian principles and further subvert political democracy is striking. As spyware is deployed in democracies such as Greece, Hungary, Poland, Mexico, and Spain - many of which are already being confronted with charges of democratic backsliding by scholars, the ability for these cyber threats to "erode many of the institutions, processes, and values" of the global democratic institutional foundation must be taken seriously (Deibert, 2023, para. 7). When democracies choose to spy and conduct cyberattacks on citizens, they are borrowing tactics originally only thought to be used in authoritarian regimes, crumbling the foundation of those very democracies.

Digital Surveillance

The umbrella term of digital surveillance encompases a variety of cyberthreats, mainly: spyware, network security, and physical surveillance technology - including facial recognition, biometric scanning, and crowd monitoring. Digital surveillance is intrinsically a violation of a person's privacy, making it an infringement on civil liberties in democracies. Because of this, digital surveillance is most commonly thought of as a tool of authoritarian regimes to control populations and anticipate dissent. The degree and methods of digital surveillance are important to examine under the context of democratic backsliding; some may assume that authoritarian regimes precede digital surveillance, as that political institution would allow for the implementation of such a threat. However, it may be the case that digital surveillance allows a government to degrade down the democratic backsliding scale. Empowered by data on the interests, approval, and whereabouts of civil society enabled through digital surveillance, state leaders may be able make strategic decisions that allow them to stay and grow in power. Additionally, once a regime is classified as an authoritarian, there is a necessity to ease what political scientists call the "dictator's dilemma". Essentially, an authoritarian leader will never know how much public support they actually hold, as there is no voting or public expression of opinion, causing the state or leader to possibly over or under shoot their desired expenditure on co-optation or repression - leading to inefficiencies. If leaders are able to ease the dictator's dilemma their power can be more stable and far-reaching, creating an incentive to collect as much information as possible on civil society, usually through digital surveillance.

The People's Republic of China is the primary example of a state with an extensive digital surveillance network. Phone tracking devices, facial recognition, voice prints, and some of the "largest DNA databases in the world", are all part of an extensive system set up by the state to collect as much information on its citizens as possible, in order to "ultimately help the government maintain its authoritarian rule" (Cardia et al., 2022, para. 3). Although not a cyberthreat in the traditional single-use targeted approach sense, this surveillance network compromises the privacy of millions of people to inform government choices and achieve state interests - the same objectives desired by other forms of cyberthreats. Additionally, China's innovative digital surveillance technology is also being sold to other nations in the Global South for usage in regimes either experiencing democratic backsliding or further autocratization (Jili, 2022), raising concerns that regimes may be able to cling to power faster and more effectively than ever before. It is also worth noting that the threat from digital surveillance extends well beyond democratic backsliding, as China has used the tactic to aid in its persecution (and arguable genocide) of the Uygher ethnic minority, which are classified as "focus personnel" and specially monitored in addition to the blanket virtual identity network applied to all residents

(Petersen, 2021). Yet, the Chinese government doesn't use its vast surveillance network only for the physical repression of individuals - online censorship and filtration is equally important.

The Chinese Communist Party is careful of its collection of personal data and surveillance - acknowledging that blanket censorship could lead to public unrest, the government ensures the long-term survival of its authoritarian regime by providing a controlled outlet for public dissent. By pursuing "networked authoritarianism", the state permits conversations regarding the nation's problems in online public forums so citizens have a way to air grievances; the state is then able to both track said grievances to monitor dissent, and respond via social media and websites to these concerns, leading to authoritarian legitimation through addressing public needs (Feldstein, 2021). This sophisticated system of digital surveillance feeding an authoritarian feedback loop suggests the data retrieved from these cyber operations could be used to fuel China's shift into a personalist authoritarian regime under Xi Jinping (Shirk, 2018; So, 2019). The argument for backsliding originating in a democracy is not applicable in this situation as China is clearly authoritarian, but a personalist regime can be viewed as a "tighter ship" and farther removed from democratic ideals by having just one figurehead controlling most of the state - thus creating "diminished prospects for democratisation" (Frantz & Kendall-Taylor 2017, para. 6).

Recent shifts in other authoritarian states away from democratic hope towards personalist structure (Taussig, 2017) is in part enabled by digital surveillance cyber operations. The digital surveillance network China has pioneered has been actively marketed and employed in Global South states (Jili, 2022) contributing to the rise in authoritarian governments through public control and monitoring. Nations like Ecuador (Chan et al., 2019), Venezuela (Young, 2022), and Turkey (Alemdarglu & Tepe, 2020) have all borrowed and bought their surveillance systems from China, showing how the cyberthreat can easily diffuse to states vulnerable to personalist rule, and expedite such processes. Success of the Chinese model in subverting civil society is in part due to its independence from global tech giants such as Facebook and Twitter; Chinese-owned and censored platforms such as WeChat and Weibo (Peskoe-Yang, 2018) fit into China's Golden Shield Project to bypass the digital freedom enabled by foreign social media platforms. The technology that China uses to run these digital surveillance networks is then being exported abroad to expand "digital authoritarianism" (Burgers & Robinson, 2016) - with the state "host[ing] media officials from dozens of countries for two- and three-week seminars on its sprawling system of censorship and surveillance" to increase power and weaken democracy abroad (Shahbaz, 2018, para. 5). Digital surveillance cyberthreat usage may be used in China and its state customers as a blanket suppression and information collection tool, but such cyber operations can also be used in response to threatened uprisings to shift regimes towards democracy, as seen with Iran in the Green Movement.

Beginning in 2009, the Green Movement was a period of mass protests and major unrest in the Islamic Republic of Iran, born out of public outcry over the 2009 presidential election in which voters noted electoral fraud from the state (Haghighatjoo, 2016). During the Green Movement, the Islamic Republic utilized malware attacks as well as network surveillance to gain control over the population and quell cries for democracy, with such cyber operations also serving to prime the state for future offensive cyberspace capabilities and harsher crackdown on democratic deals (Anderson & Sadjadpour, 2018). The Stuxnet computer worm attack on the Iran nuclear program, as previously discussed, also prompted the regime to improve its ability to conduct cyber attacks and maintain a surveillance network on the Iranian public to ensure state longevity and security from foreign entities. Yet, the leaders of Iran primarily fear their own citizens' power, and the "risk that the internet will unleash something like the Arab spring", making domestic efforts the central focus of the Supreme Leader's cyber strategy (Lewis, 2019, para. 2). By honing in on internal digital surveillance and spyware to establish databases with extremely detailed personal information (Starks & Schaffer, 2023), Iran demonstrates how state-sponsored cyberthreats against domestic populations are often in a position to cause more democratic backsliding or prevention of democratic germination than foreign interference (as explored prior in this paper).

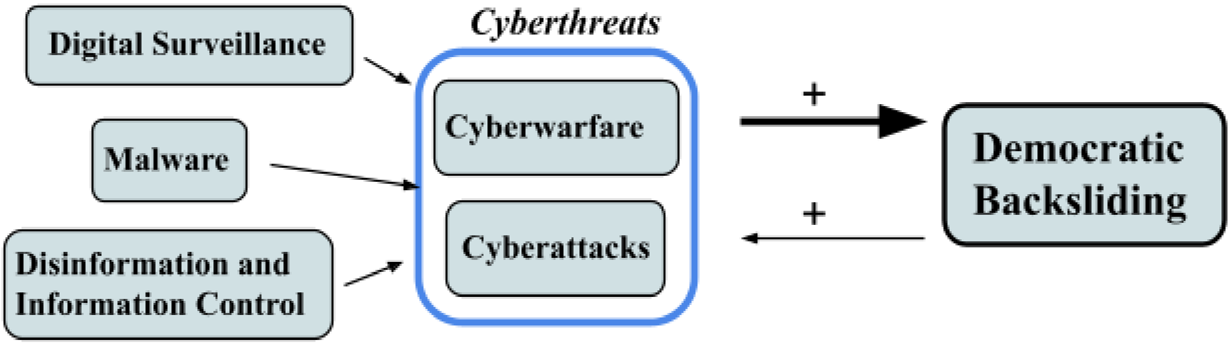
In contrast to digital surveillance done by authoritarian regimes to maintain their regime type, the presence of digital surveillance through cyber operations conducted by democracies is an indicator of democratic backsliding, as the government is exerting more power and control onto its population without their knowledge. State secret surveillance by democracies is naturally meant to be hidden, meaning surveillance techniques are likely not compatible with the rule of law or democracy (Koonthamattam, 2022). State secrets are revealed with whistleblowers, however, with Edward Snowden being the most famous example. In 2013, Snowden, a National

Security Agency employee, leaked classified intelligence to reporters, exposing how the U.S. government used a surveillance program called PRISM to collect phone records and spy on network users domestically and abroad - breaking U.S. privacy laws along the way (BBC, 2014). The existence of a state-sponsored surveillance program illegal by its own state's laws, in arguably the most powerful democracy in the world, exemplifies how no nation is free from the influence of cyber developments. Although recent U.S. democratic backsliding (Berger, 2021) cannot be definitively linked back to the PRISM program unveiled by Snowden, public concern over privacy invasion and oversteps of power fuel the claim that the American democratic system may not work how its people demand it to, and civil rights have the potential to be infringed upon further.

Linking Democratic Backsliding and Cyberthreats

As discussed in the background, there is a lack of research on the linkage between cyberthreats and democratic backsliding, i.e., how cyberthreats increase democratic backsliding or how democratic backsliding increases cyberthreat usage. Scholarly literature has no consensus in the form of conventional wisdom or ongoing debate over the two sides of the causal order, as cyber threat research in relation to regime type has mainly focused on the result of cyberattacks, not the political institutions which enable them or make up their targets. What scholars have focused on is the relative capability of various regime types to respond to cyberthreats or conduct cyberwarfare, as well as under what conditions they are likely to do so. However, it is important to understand how the process of an eroding democracy can influence cyber activity, or how cyberthreats themselves erode democracy. This research paper has filled some of the gap in this knowledge by dissecting examples of state-sponsored cyberattacks and their relationship with democracy and democratic backsliding. At the beginning of this paper a conceptual framework was introduced to show the process tracing between the two main variables: democratic backsliding and cyberthreats (usage) - separated by a double-sided arrow to signify the potential for the relationship to go both ways or serve as a feedback loop. After conducting the series of case studies, the conceptual model can be altered as follows:

Adjusted Conceptual Framework:



The model has been changed to reflect the relative weight of cyberthreats increasing democratic backsliding (heavier) versus democratic backsliding increasing cyberthreat usage (comparatively smaller). This is due to the ability of cyberthreats as an isolated phenomenon to threaten democratic ideals innately - when a foreign adversary uses a cyberattack against a democracy it is most often to compromise its political institutions, as seen with Russian election interferences or Iranian disinformation bots undermining public confidence in the democratic electoral system. Restriction of state media and internet access also increases democratic backsliding due to regimes' ability to control public sentiment and discourse around the government and repress democratic values. Digital surveillance systems invading the privacy of individuals to serve state interests creates a blatant overreach of power/control and thus democratic backsliding.

Authoritarian states like Russia and China, or democratic states like the U.S. or Israel, being able to conduct more cyberattacks *because* of degenerating democracy is comparatively difficult to prove through direct process tracing. In other words, we are uncertain if these cyberattacks occur because a state is already experiencing the backsliding and less oversight, or if the cyberattack usage is more independent of the process and simply worsens backsliding on its own. This uncertainty is primarily attributed to the secrecy of cyberattack operations within states - the motivations and legality of such actions can easily become difficult to discern. This research has strong evidence for both causal orders between democratic backsliding and cyberthreat usage: the reason why the relationship of cyberthreat usage leading to democratic backsliding is stronger than the reverse is because the latter is more difficult to find direct causal evidence for, without the risk of confounding variables. Democratic backsliding likely leads to increased cyberthreat usage, as shown in the model and discussed in this paper with the legality of Stuxnet and usage/ownership of the spyware PRISM and Pegasus, despite their murky relation to democratic norms. However, there is greater definition concerning how cyberthreats lead to democratic backsliding, as shown in Iran's crackdown with digital surveillance after the Green Movement, Russia's erosion of democratic hope over the past few decades with increased cyberspace control, and states like China and Russia being able to meddle in foreign democratic processes or sovereign states to initiate or spur on backsliding.

It is important to acknowledge that this conclusion could be in part due to the structuring of this research by cyberthreat construct and not democratic backsliding construct - leading to a greater focus on cyberthreats as the primary driver behind the causal order between the two variables. However, when conducting this research there was a noticeable lack of analysis on how cyber tactics change as regimes change over time within the same state - for example, how Chinese cyberthreat capability existed prior to Xi Jinping versus after, or how as Putin's Russia peeled back democracy, cyberthreat usage changed due to increased state-control or emphasis. Additional research should therefore be completed in this area.

Closing Thoughts

It is well established that as global tensions continue to rise, potential cyberconflict and the results of cyberattacks are core concerns for actors with stakes in international security and cooperation. For example, China may deem a possible invasion of Taiwan as having greater risks than reward, but the state will still attempt to subvert Taiwanese democracy using cyberthreats as a next-best alternative. This strategy allows China to enforce foreign policy objectives without starting a physical conflict and disrupting international order or triggering an allied response. Additionally, using cyberthreats as a means to encourage democratic backsliding can be a precursor to conventional forms of conflict, as seen with the Russian invasion of Ukraine.

In order to address the policy gap that occurs due to this cyberthreat approach - that is, the ability for foreign state to linger under the threshold for a global response while still achieving domestic goals, like the Russian meddling in the 2016 U.S. presidential election -

deterrence efforts (e.g. NATO directives, individual state deterrence strategies like the U.S. Department of Defence concept of 'Integrated Deterrence') must incorporate the cyber realm into their frameworks. Investment in cybersecurity infrastructure is also crucial for independent states as well as alliances, and constant monitoring for democratic backsliding or targeting due to cyberthreats must be conducted to address foreign interference that may otherwise go unnoticed. Essentially, large scale cyber attacks are easy to identify and conduct appropriate responses, but the strategic slow erosion of democracy must also be given attention and addressed.

Bibliography

Albert, C., Garrett, E., Hunter, L., & Rutland, J. (2022). Democracy and cyberconflict: How regime type affects state-sponsored cyberattacks. *Journal of Cyber Policy*, *7*(1), 72–94. https://doi.org/10.1080/23738871.2022.2041060

Alemdaroglu, A., & Tepe, S. (2020, September 16). Erdogan is turning Turkey into a Chinese client state. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2020/09/16/erdogan-is-turning-turkey-into-a-chinese-client-state/

Allen, N., & La Lime, M. (2021, November 19). How digital espionage tools exacerbate authoritarianism across Africa. *Brookings*. Retrieved from https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/

AlSayyad, N., & Guvenc, M. (2015). Virtual Uprisings: On the Interaction of New Social Media, Traditional Media Coverage and Urban Space during the "Arab Spring." *Urban Studies*, *52*(11), 2018–2034. https://www.jstor.org/stable/26146115

Anderson, C., & Sadjadpour, K. (2018). Iran: Target and Perpetrator. In *Iran's Cyber Threat: Espionage, Sabotage, And Revenge* (pp. 9–16). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep26913.8

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

Asrani-Dann, S. (2005). The Right to Privacy in the Era of Smart Governance: Concerns Raised by the Introduction of Biometric-Enabled National ID Cards in India. *Journal of the Indian Law Institute*, *47*(1), 53–94. http://www.jstor.org/stable/43951951

Associated Press. (2020, December 15). Poland, Lithuania are targets of Cyber Disinformation attack. *AP NEWS.* Retrieved from https://apnews.com/article/technology-poland-lithuania-russia-hacking-4eaae5334dd2403e37e8560e4de71219

Atrews, R. (2020). Cyberwarfare: Threats, Security, Attacks, and Impact. *Journal of Information Warfare*, *19*(4), 17–28. https://www.jstor.org/stable/27033642

Aydin-Duzgit, S., Gerald Daly, T., Godfrey, K., Lindberg, S. I., Lührmann, A., Petrova, T., & Youngs, R. (2019, June 27). Post–Cold War Democratic Declines: The Third Wave of Autocratization. *Carnegie Europe*. Retrieved from https://carnegieeurope.eu/2019/06/27/post-cold-war-democratic-declines-third-wave-of-autocratization-pub-79378

Babb, C. E. (2022). Digital Dictators: How Different Types of Authoritarian Regimes use Cyber Attacks to Legitimize Their Rule. PhD Dissertation, *Carleton University*. https://doi.org/10.22215/etd/2022-15146

BBC. (2014, January 17). Edward Snowden: Leaks that exposed US spy programme. *BBC News*. Retrieved from https://www.bbc.com/news/world-us-canada-23123964

BBC. (2018, December 17). Russia 'meddled in all big social media' around US election. *BBC News*. Retrieved from https://www.bbc.com/news/technology-46590890

Barnes, J. E., & Frenkel, S. (2020, September 1). Russians Again Targeting Americans with Disinformation, Facebook and Twitter Say. *The New York Times*. Retrieved from https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html

Berger, M. (2021, November 22). U.S. listed as a 'backsliding' democracy for first time in report by European think tank. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/2021/11/22/united-states-backsliding-democracies-list-first-time/

Brattberg, E., & Maurer, T. (2018). Five European Experiences With Russian Election Interference. In *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks* (pp. 5–28). Carnegie Endowment for International Peace. http://www.jstor.org/stable/resrep21009.6

Bricker, B. J. & Justice, J. W. (2019). Hacked: Defining the 2016 Presidential Election in the Liberal Media. *Rhetoric and Public Affairs*, *22*(3), 389–420. https://doi.org/10.14321/rhetpublaffa.22.3.0389

Brooking, E. T., & Kianpour, S. (2020, February 11). Iranian digital influence efforts: Guerrilla Broadcasting for the twenty-first century. *Atlantic Council*. Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/

Brown, L. & Stallings, W. (2015). Computer Security Principles and Practice (3rd ed.). *Pearson*.

Buchholz, K. (2022, April 29). Which countries spend the most time on social media? *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2022/04/social-media-internet-connectivity/

Buresh, D. L. (2021). Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects. *Journal of Advanced Forensic Sciences*, *1*(2), 15–26. https://doi.org/10.14302/issn.2692-5915.jafs-21-3930

Burgers, T., & Robinson, D. R. S. (2016). Networked Authoritarianism Is on the Rise. *Sicherheit Und Frieden (S+F) / Security and Peace*, *34*(4), 248–252. http://www.jstor.org/stable/26429018

Cardia, A., Mozur, P., Qian, I., & Xiao, M. (2022, June 21). Four Takeaways From a Times Investigation Into China's Expanding Surveillance State. *The New York Times*. Retrieved from https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html

Chan, M., Kessel, J. M., & Mozur, P. (2019, April 24). Made in China, Exported to the World: The Surveillance State. *The New York Times.* Retrieved from https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html

Chen, T. M. (2014). Cyberterrorism After Stuxnet. *Strategic Studies Institute, US Army War College*. http://www.jstor.org/stable/resrep11324

Chim, W. (2018). Russia’s Digital Awakening. *Connections*, *17*(2), 5–18. https://www.jstor.org/stable/26936535

Deibert, R. J. (2022, December 12). The Autocrat in Your iPhone. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert

Dever, J., & Dever, J. (2013). Cyberwarfare: Attribution, Preemption, and National Self Defense. *Journal of Law & Cyber Warfare*, *2*(1), 25–63. http://www.jstor.org/stable/26441240

Ee, S., & Galante, L. (2018). Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. *Atlantic Council*. http://www.jstor.org/stable/resrep20718

Farrow, R. (2022, April 18). How democracies spy on their citizens. *The New Yorker*. Retrieved from https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

Farnham, B. (2003). The Theory of Democratic Peace and Threat Perception. *International Studies Quarterly*, *47*(3), 395–415. http://www.jstor.org/stable/3693592

Feldstein, S. (2021, July 21). Governments Are Using Spyware on Citizens. Can They Be Stopped? *Carnegie Endowment for International Peace.* Retrieved from https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019

Feldstein, S. (2021, May 11). How the dictator's Digital Dilemma Constrains Leaders' choices. *Council on Foreign Relations*. Retrieved April 13, 2023, from https://www.cfr.org/blog/how-dictators-digital-dilemma-constrains-leaders-choices

Fish, M. S. (2018). What Has Russia Become? *Comparative Politics*, *50*(3), 327–346. https://www.jstor.org/stable/26532689

Flynn, M. J. (2019). Strategic Cyber: Responding to Russian Online Information Warfare. *The Cyber Defense Review*, 193–208. https://www.jstor.org/stable/26846128

Frantz, E. A., & Kendall-Taylor, A. (2017, October 30). The move to one-man rule in China and beyond. *The Interpreter*. Retrieved from https://www.lowyinstitute.org/the-interpreter/move-one-man-rule-china-beyond

Gerschewski, J. (2019, January 1). “Autocratization And Democratic Backsliding: Taking Stock Of A Recent Debate.” In *Democracy Promotion In Times Of Uncertainty: Trends And Challenges* (pp. 5–9). Peace Research Institute Frankfurt. http://www.jstor.org/stable/resrep20032.5

Haataja, S., & Akhtar-Khavari, A. (2018). Stuxnet and international law on the use of force: An informational approach. *Cambridge International Law Journal*, *7*(1), 99–121. https://doi.org/10.4337/cilj.2018.01.05

Haghighatjoo, F. (2016). The Green Movement and Political Change in Iran. In D. Brumberg & F. Farhi (Eds.), *Power and Change in Iran: Politics of Contention and Conciliation* (pp. 224–250). Indiana University Press. https://doi.org/10.2307/j.ctt1bmzp38.12

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, *100*(4), 817–885. http://www.jstor.org/stable/23249823

Jili, B. (2022, October 17). China's surveillance ecosystem and the global spread of its tools. *Atlantic Council*. Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/

Kagubare, I. (2022, June 27). Russian-backed hackers target Lithuanian websites. *The Hill*. Retrieved from https://thehill.com/policy/cybersecurity/3538629-russian-backed-hackers-target-lithuanian-websites/

King, S. J. (2014). Social media and civil society in the Tunisian revolution: implications for democracy and peacebuilding. In S. B. Maphosa, L. DeLuca, & A. Keasley (Eds.), *Building Peace from Within* (pp. 268–279). Africa Institute of South Africa. https://doi.org/10.2307/j.ctvh8r4g3.22

Kirchgaessner, S. (2021, July 18). Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests. *The Guardian*. Retrieved from https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus

Koonthamattam, L. (2022, May 2). Digital Surveillance in democracies: 'Who will guard the guardians?'. *Geneva Solutions*. Retrieved from https://genevasolutions.news/science-tech/digital-surveillance-in-democracies-who-will-guard-the-guardians

Koukakis, T. (2022, April 27). Why Every Democracy Should Fear Israeli Spyware. *Haaretz*. Retrieved from https://www.haaretz.com/israel-news/2022-04-27/ty-article-opinion/.premium/why-every-democracy-should-fear-israeli-spyware/00000180-7ee8-d9ba-a3f7-ffebd68c0000

Kozloff, N. (2018, December 7). Ukraine's 2019 elections: Preparing for more Russian cyberattacks. *Wilson Center*. Retrieved from https://www.wilsoncenter.org/blog-post/ukraines-2019-elections-preparing-for-more-russian-cyberattacks

Kozlowski, A. (2023, January 18). Polish Cyber Defenses and the Russia-Ukraine War. *Council on Foreign Relations.* Retrieved from https://www.cfr.org/blog/polish-cyber-defenses-and-russia-ukraine-war

Lachow, I. (2011). The Stuxnet Enigma: Implications for the Future of Cybersecurity. *Georgetown Journal of International Affairs*, 118–126. http://www.jstor.org/stable/43133820

Lewis, J. A. (2019, June 25). Iran and Cyber Power. *Center for Strategic & International Studies*. Retrieved from https://www.csis.org/analysis/iran-and-cyber-power

Lührmann, A., & Rooney, B. (2021). Autocratization by Decree: States of Emergency and Democratic Decline. *Comparative Politics*, *53*(4), 617–635, 1–14. https://www.jstor.org/stable/27090047

Martin, D. A., Shapiro, J. N., & Nedashkovskaya, M. (2019). Recent Trends in Online Foreign Influence Efforts. *Journal of Information Warfare*, *18*(3), 15–48. https://www.jstor.org/stable/26894680

Matthews, J. P. (2019). Defending Liberal Democracies Against Disinformation. *American Intelligence Journal*, *36*(2), 86–94. https://www.jstor.org/stable/27066376

Mccandless Farmer, B. (2022, October 9). China's cyber assault on Taiwan. *CBS News*. Retrieved from https://www.cbsnews.com/news/china-cyber-assault-taiwan-60-minutes-2022-10-09/

McCarthy, D. A. (2015). Defending the Tower in the Age of Twitter: Lithuanian Lessons on Russian Disinformation. *Council of American Ambassadors.* Retrieved from https://www.americanambassadors.org/publications/ambassadors-review/spring-2015/defending-the-tower-in-the-age-of-twitter-lithuanian-lessons-on-russian-disinformation

McFaul, M. (2018). Choosing Autocracy: Actors, Institutions, and Revolution in the Erosion of Russian Democracy. *Comparative Politics*, *50*(3), 305–325. https://www.jstor.org/stable/26532688

Meredith, K. (2013). Social Media and Cyber Utopianism: Civil Society versus the Russian State during the “White Revolution,” 2011-2012. *St Antony's International Review*, *8*(2), 89–105. http://www.jstor.org/stable/26228740

Miller, M. (2023, January 11). Russia's cyberattacks aim to 'terrorize' Ukrainians. *POLITICO*. Retrieved from https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561

Nelson, L. (2004). Privacy and Technology: Reconsidering a Crucial Public Policy Debate in the Post-September 11 Era. *Public Administration Review*, *64*(3), 259–269. http://www.jstor.org/stable/3542591

NIST CSRC. (n.d.). Cyber Attack - Glossary: CSRC. *National Institute of Standards and Technology.* Retrieved from https://csrc.nist.gov/glossary/term/cyber_attack#:~:text=Definition(s)%3A,resources%20or%20the%20information%20itself

Office of the Spokesperson. (2022, February 1). Rewards for Justice – Reward Offer for Information on Iranian Cyber Actors' Interference with 2020 U.S. Presidential Election. *U.S. Department of State.* Retrieved from https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-iranian-cyber-actors-interference-with-2020-u-s-presidential-election/

Peskoe-Yang, L. (2018, November 20). How China's State-Sponsored Social Networks Control Misinformation - and Dissent. *IEEE Spectrum*. Retrieved from https://spectrum.ieee.org/how-chinas-statesponsored-social-networks-control-misinformationand-dissent

Peterson, D. (2021, September 23). How China Harnesses data fusion to make sense of surveillance data. *Brookings*. Retrieved from https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/

Potter, R. (2016, October 16). Cyberattacks and the Authoritarian Context. *The Diplomat*. Retrieved from https://thediplomat.com/2016/10/cyberattacks-and-the-authoritarian-context/

Rogin, J. (2022, November 8). Opinion | Taiwan is on the Frontlines of China's Worldwide Cyberwar. *The Washington Post.* Retrieved from https://www.washingtonpost.com/opinions/2022/11/08/taiwan-internet-resilience-china-cyberattacks-disinformation/

Roguski, P. (2020, March 6). Russian Cyber Attacks Against Georgia, Public Attributions and sovereignty in Cyberspace. *Just Security*. Retrieved from https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

Rotondo, A., & Salvati, P. (2019). Fake News, (Dis)information, and the Principle of Nonintervention: Scope, limits, and possible responses to cyber election interference in times of competition. *The Cyber Defense Review*, 209–224. https://www.jstor.org/stable/26846129

Russell, A. L. (2014). Cyber Attacks on Estonia. In *Cyber Blockades* (pp. 69–95). Georgetown University Press. http://www.jstor.org/stable/j.ctt9qdsfj.9

Sanger, D. E. (2017, January 6). Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says. *The New York Times*. Retrieved from https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html

Sardarizadeh, S. (2020, October 1). US election 2020: Twitter removes Iranian accounts disrupting debate. *BBC News*. Retrieved from https://www.bbc.com/news/election-us-2020-54373314

Sardini, N. H., Suwana, F., & Wijayanto. (2022). Cyber Terror, the Academic Anti-corruption Movement and Indonesian Democratic Regression. *Contemporary Southeast Asia*, *44*(1), 31–55. https://www.jstor.org/stable/27130807

Shahbaz, A. (2018). The Rise of Digital Authoritarianism. *Freedom House*. Retrieved from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Shevtsova, L. (2008). Vladimir Putin. *Foreign Policy*, *164*, 34–40. http://www.jstor.org/stable/25462247

Shirk, S. (2018). China in Xi's "New Era": The Return to Personalistic Rule. *Journal of Democracy*, *29*(2), 22-36.

Singleton, C. (2022, November 4). Chinese Election Meddling Hits the Midterms. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2022/11/04/china-us-midterm-election-interference-meddling-social-media-cybersecurity-disinformation/

So, A. Y. (2019). The Rise Of Authoritarianism In China In The Early 21st Century. *International Review of Modern Sociology*, *45*(1), 49–70. https://www.jstor.org/stable/48636762

Starks, T., & Schaffer, A. (2023, January 17). Iran sought a surveillance project with 'unprecedented' reach. *The Washington Post.* Retrieved from https://www.washingtonpost.com/politics/2023/01/17/iran-sought-surveillance-project-with-unprecedented-reach/

Taussig, T. (2022, March 9). The Rise of Personalist Rule. *Brookings*. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2017/03/23/the-rise-of-personalist-rule/

Waterman, S. (2013, March 24). U.S.-Israeli cyberattack on Iran was 'act of force,' NATO study found. *The Washington Times.* Retrieved from https://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?utm_source=RSS_Feed&utm_medium=RSS

Whitman, M. E., & Mattord, H. J. (2012). Principles of Information Security (4th ed.). Course Technology, *Cengage Learning*.

Young, B. R. (2022, June 27). Venezuela is Becoming a Chinese and Russian Cyber Hub on America's Doorstep. *The National Interest*. Retrieved April n.d., from https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/venezuela-becoming-chinese-and

Zinets, N. (2016, December 29). Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'. *Reuters*. Retrieved from https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC