The 2024 Elections, Disinformation, Cyberattacks and the Possibility of Insurgency in the US

https://www.e-ir.info/2024/09/26/the-2024-elections-disinformation-cyberattacks-and-the-possibility-of-insurgency-in-the-us/

MICHAEL W. MOSSER AND DAN G. COX, SEP 26 2024

Consider the following scenario: Candidate Donald Trump loses the 2024 election by a narrow Electoral College margin. In fact, he gains more popular votes than Kamala Harris, but as in the 2000 and 2016 elections, idiosyncrasies in the American Electoral College were enough to push the election to Harris. Major news outlets called the race soon after the close of polling on Election Day, but many right-wing pundits and social media information sources encouraged their subscribers and followers to refuse to abide by the "mainstream" results. Trump refuses to concede, and spends the month of November holding rallies around the United States where he claims the election was "stolen" in a far more egregious manner than the 2020 election. Far-right commentators in both traditional and social media outlets lament that the American electoral system is corrupt and untrustworthy. Stoking the fires, Russian and Russian-affiliated disinformation agents flood conservative social media echoing the same sentiment.

By early December 2024, Trump supporters begin to hold large-scale protests, some turning violent, in several major cities in the Midwest and South. Soon, protests expand beyond Trump-friendly venues and into major cities where counter-protesters began to push back. In the midst of the growing chaos, Russia, China, and Iran decide to strike, putting Operation Cold Winter into effect. To begin, Russia enlists freelance journalists to cover bogus rumors and spread disinformation on the results of the election, going so far as to create plausible-sounding media outlets such as the "Chicago Chronicle" or the "New York News Daily."[1] When a disinformation story is picked up by a major American news source, bots and trolls are enlisted to cite the story and propagate it through social media in order to further the disinformation campaign. Shortly after the Christmas and New Year holidays, well-organized protests are launched in major cities around America. The protestors demand the election results be overturned and Donald Trump instated as the President. Russian disinformation agents began to amplify this discourse. They propagate a story carried by CNN and Fox News that invited election monitors from the Organization for Security and Cooperation in Europe (OSCE) had declared the election "not free and fair."[2] Both news organizations retract the story later, but the damage had been done.

Russia takes the next two weeks to intensify the narratives it had sown earlier. First, its agents began reporting that the Harris Administration would seek vengeance against Trump supporters, using much more specific "microtargeting" tactics.[3] Russian trolls, RT, Russian-backed false news outlets and other manipulated reporters begin to propagate and reinforce the narrative that Harris officials will interrupt electricity and essential services to Trump supporters. Simultaneously, Russian operatives introduce a new narrative on left-leaning social media sites claiming that Trump supporters were planning to overthrow the US government and install a Trump dictatorship. Microtargeting deepfake campaigns on both sides of the political spectrum are launched on social media, showing "Donald Trump" and "Kamala Harris" making statements that demonize the other and calling for supporters to rise up.[4] Protests become larger, and low-level violence between opposition groups is now a common occurrence.

Iran begins its phase of the operation on January 27, 2025. As in the past, Iranian cyberattacks again targeted water supply systems. However, instead of limiting the attack to Pennsylvania, they targeted twelve eastern states, including Washington D. C. during the height of the protest. The disruption of fresh water to citizens was followed by an online campaign that promoted stories reading that the Biden Administration was punishing conservatives or the

government had lost control of the water supply, depending on the target. Russian trolls used large language model (LLM) AI to help discern appropriate targets.[5] Panic began to foment in a small percentage of the US population in these twelve northeastern states. Next, Chinese "Net Warriors" activate malware buried in the US electrical grid and turn off as much of the power in as many states as possible. Local and national news begin reporting on the danger of power outages in many midwestern and eastern states with subfreezing temperatures. Russian cybergang DarkSide, working with operatives from the Main Intelligence Directory of the General Staff (GRU), emerge from hiding in Colonial Pipeline's IT systems and lock 40 percent of the transfer valves on the pipeline's physical structure. The pipeline goes down for months, further exacerbating the energy problems in the eastern and southeastern United States.

Later in the week, Russia and China open up a barrage of cyberattacks through formal military and intelligence channels attempting to disrupt banking services, beef and poultry processing plants, other energy providers and even a nuclear power plant. Energy stocks decline dramatically, and the larger stock market enters "correction" territory. In a novel cyberattack, PLA and PLA-affiliated hackers infiltrate Amazon and placed millions of fake orders. This results in 70 percent of the warehouse inventory being shipped to citizens who did not order the goods and would not pay for them. In the chaos that ensued, Amazon had no way to recapture much of the lost goods, and its share price fell more than 50 percent, bringing the stock market down another seven percent. President Harris closes Wall Street, and retreats to Camp David to plan a recovery, but her popularity ratings fall below 15%. The GOP-controlled House of Representatives begins to draft articles of impeachment, and prominent politicians across the political spectrum begin to call for her resignation. Along with its economy, the US democracy is crippled.

Though the above scenario is fiction, threats both real and imagined abound to American democracy, its economy and its open society. During the Cold War, films such as *The Manchurian Candidate* or *Three Days of the Condor* forced Americans to confront the specter of high-level conspiracies to destroy the country, with threats coming both from without and within.[6] More recently, no threat looms larger in the contemporary popular imagination than the actual hijacking of an American presidential election by an adversary such as Russia or China, and the attendant political violence that would no doubt ensue.

Policymakers and pundits endlessly debate in the press which candidate Russian President Vladimir Putin prefers to win the 2024 American election, and what actions he will authorize to affect his preferred outcome. Now that Vice President Harris has supplanted President Joe Biden as the Democratic candidate for president, the speculation on whether or how Russia involved itself in the election is even more rife. We consider this debate, while fascinating, to be ultimately beside the point; the Russian state has neither the capability to precisely enough manipulate the myriad sub-national elections that comprise the 2024 election nor the overt desire to do so. Indeed, such an aim does not even fulfill Putin's strategic objectives very well. Even if Russia has a preferred candidate, is able to somehow engineer the federalized electoral system to get that candidate elected, and is then able to somehow "control" that newly-elected President, it is unclear whether the risks of such direct meddling would be worth the benefits.

Despite popular conceptualizations of the president of the United States as all-powerful, the executive branch is still subject to constitutional checks and balances. Elected officials in both the legislative and executive branches are (still) accountable to the public that elects them, and constitutional provisions exist to impeach of the executive for conducting high crimes and misdemeanors, of which the ceding of American foreign policy to an adversary surely would be an example. These constitutional guardrails make an overt strategy of seeking to control American foreign policy through a preferred candidate tenuous at best. Further, given that a May 2023 Pew survey conducted on the issue of American attitudes toward Russia found that more than six in ten Americans have very unfavorable views of the country,[7] most candidates are unlikely to overtly support Putin's foreign policy objectives of restoring the greatness of the former Russian Empire, degrading or destroying NATO, and diminishing American power and leadership in the world.[8]

For its part, China is also likely not in the business of overtly attempting to influence election winners and losers. While contemporary Chinese foreign policy is driven by the same decision calculus as every other state in the international system, China has a long history of strategic thinking that gives it a deep well from which to draw. In many ways, ancient military writers influence contemporary Chinese strategy. Both former US Ambassador to China

Michael Pillsbury and China scholar Alastair Johnston argue that Chinese strategy leans heavily on their warring states' history, *c.* 475-221 BCE.[9] Because of this reliance on the warring states period and the seven military strategists of the time, like Sun Tzu, China often orients its strategy on the Thirty-Six Stratagems, first elucidated in the distant past. In these stratagems, there is a great emphasis on deception and degrading enemies indirectly, which would indicate that attempting to choose the correct candidate and ensure his or her election really is not in keeping with tenets of Chinese strategic thought. Instead, one of the stratagems (Stratagem Five), known colloquially as "loot a burning house" sheds far more light on China's possible intentions than does a discussion of which candidate China prefers. The meaning behind the stratagem is simple: when your enemy is in disarray, vulnerable, or weak, that is the time to add energy to the system to push the enemy system into chaos, and possibly self-destruction.

For these reasons, among others, it is far more likely that Russia and China are more interested in eroding confidence in the American election system, with consequences ranging from the relatively benign (e.g., voter apathy depressing turnout) to the increasingly destructive (e.g., the normalization of political violence within society), to the existential (e.g., the normalization of political violence by the state), potentially leading to an insurgency or civil war. Individually, these efforts are dangerous to American democracy. Combined, they may be catastrophic. When one views Russian and Chinese disinformation campaigns and cyberattacks sponsored or condoned by the Russian government in this new light, disinformation and cyberattacks no longer seem uncoordinated, ham-fisted, or unconnected events. For much of the early 21st century, China appeared to be focused on cyberattacks that steal American intellectual property.[10] Recently, however, the FBI has warned that Chinese government-affiliated hackers are preparing to attack American infrastructure and cause "real-world harm."[11] This new trend has elevated China to the prime cyber threat against the United States.

Chinese cyber-attacks against American companies and infrastructure, though dangerous, are known quantities and can be defended against. But another disturbing angle has emerged: that of China utilizing American weaknesses in its own information space against it. China is likely aware of Russian disinformation operations against the American population, even if not engaged in outright coordination and information sharing.[12] Looking at the system holistically, a frightening picture emerges that could be building toward a future integrated operation which would accelerate instability in the American political system. The first phase would be a coordinated effort to foment discontent, disinformation, and paranoia among differing sides of the political spectrum. The second phase would entail a coordinated series of cyberattacks across multiple economic, energy, transportation, and media domains to ensure that discontent turns into violence and, perhaps, insurgency. The next section of this paper examines the connection between disinformation and the American population, specifically the American electorate, and lays the groundwork for a scenario whereby Chinese and Russian coordinated disinformation campaigns serve to systematically weaken the country from the inside out.

Disinformation and the American Electorate

Disinformation in the American electorate is a topic that provokes reactions ranging from hyperbolic to yawns.[13] Research into whether disinformation is a clear and present danger is hampered by the fact that a sizeable proportion of the American public does not believe it exists, much less that it is harmful. Despite this existential challenge to the American electoral system, few voters consider disinformation to be the threat that disinformation researchers do. And even among cybersecurity professionals, election-oriented disinformation is not regarded in the same way as America's physical and cyber election infrastructure, which upon the creation of the Cybersecurity and Infrastructure Security Agency (CISA) in 2017 was elevated to a "critical infrastructure" subsector (under the "government facilities" sector).[14] Such a designation means that "the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country."[15]

CISA was created out of the Department of Homeland Security's (DHS's) National Protection and Programs Directorate in large part as a direct reaction against Russian hackers targeting US election infrastructure in the run-up to the 2016 presidential election.[16] It has as its mission to "lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure."[17] Since its inception, CISA has been more in the public eye

than many federal security agencies.[18] It became best known immediately after the 2020 election, when then-Director Chris Krebs was fired by President Trump for noting that the 2020 election was "the most secure in American history" and debunking rumors that the election had been stolen using CISA's "Rumor Control" website, as well as his personal social media account.[19]

Recently, and belatedly, CISA and others have now begun to consider the risks posed by generative AI and other tools of malicious threat actors in cyberspace.[20] In collaboration with international partners such as the UK's National Cyber Security Centre (UK-NCSC), the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ), as well as the U.S. National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Cyber Command Cyber National Mission Force (CNMF), CISA in late 2023 released a joint Cybersecurity Advisory (CSA) raising awareness of a Russia-based threat actor group known as "Star Blizzard."[21]

Integrating Cyberattacks into a Campaign to Create Chaos

We have already established that Russian threat actors engage in disinformation campaigns online through social media, the use of proxies in the media, and the establishment of false media outlets, like Russia Today (RT), to provoke and stoke extremists across the political spectrum. But the ability of threat actors to do so effectively relies at least as much on the open-society nature of their target. Few societies are as open, relatively speaking, as the United States.[22] The celebrated freedoms of the American population, and the expectations of that population for the continuation of those freedoms, paradoxically makes defending them from threats from abroad extraordinarily challenging.[23]

The United States is almost perfectly positioned for exploitation by outside influences.[24] The U.S. is, as two scholars noted, "perniciously polarized" with increasingly serious consequences for institutional and behavioral norms.[25] Both sides of the increasingly polarized political spectrum distrust each other and the media, with only 40% of Americans surveyed expressing trust in the government itself.[26] And recent global events, far from uniting the parties as they have in the past, have reinforced what is a burgeoning isolationist sentiment, at least among Trump-affiliated Republicans.[27] Many voters in the United States, it seems, are turning inward, distrustful of the outside world and becoming increasingly disenchanted not merely with the rules-based international order, but perhaps with the rules and institutions of democracy itself.[28]

There is a long and uncertain path from dissatisfaction with the government of the day, to dissatisfaction with democracy, to participating in violent acts against a democratically elected government. But recent trends In the United States are worrying: more than three-quarters of Americans believe the country is going in the wrong direction, with over 90% of Republicans in a recent survey responding in the affirmative.[29] The same survey found that nearly one-fourth of Americans agree with the statement that "because things have gotten so far off track, true American patriots may have to resort to violence in order to save our country." A breakdown of responses to that question finds that 33% of Republicans feel that statement to be true, versus 22% of independents and 13% of Democrats. Support for the statement rises to 46% of those who feel the 2020 election was stolen from President Trump.[30]

Given the supercharged partisan divide in the US, and the inability of many Republican voters to even admit the 2020 election was not stolen, forecasting the potential for violence after the 2024 election is fairly uncontroversial. In the most infamous case, after an incendiary rally where they were exhorted to "fight like hell" to take the country back, Trump supporters stormed and seized the US Capitol on 6 January 2021. That "Fight!" language was repeated after the assassination attempt on President Trump in July 2024, though so far violence has not erupted between opposing camp supporters based on this incident.

In the years since the 2020 election, and especially since the 6 January 2021 attack on the US Capitol, American democracy has essentially been in stasis. Internal threats to the Republic appear to be quiescent, or at least diminished. As the 2024 election campaign moves into full swing, however, the political temperature seems to be rising. Though one of President Trump's four criminal cases has concluded with 34 felony convictions now on his

record, the others slowly wind through the courts.[31] Moreover, with the surprise withdrawal of President Biden from the race, and the rapid elevation of Vice President Harris to be the Democratic Party standard-bearer, partisan rhetoric in support of the two general election candidates has begun to ramp up.

In recent months, however, there was a chance for a significant injection of fuel to the partisan fire. Prior to clinching of the nominations by former President Trump and President Biden (and before President Biden withdrew from the race), a pair of 2023 court cases created an atmosphere that could have been used by either former President Trump's or President Biden's most ardent supporters to resort to political violence should their preferred candidate fail to win the 2024 election. In late 2023, the Colorado Supreme Court and the Maine Secretary of State both barred the former president from remaining on the ballot in their states' presidential election primaries; each determined that Donald Trump had violated the Insurrection Act of the 14th Amendment to the US Constitution.[32] On 4 March 2024, the US Supreme Court reversed the Colorado Supreme Court, ruling unanimously that President Trump should be permitted to remain on the ballot.[33] The Justices found that the Colorado plaintiffs failed to make their case and that "the Constitution makes Congress, rather than the States, responsible for enforcing Section 3 against federal officeholders and candidates."[34] Before the ruling, speculation abounded as to reactions from the left and the right should the decision go against their preferred outcome. some overheated rhetoric even held that a split decision by the conservative majority of the Supreme Court allowing President Trump to remain on the ballot might encourage Democratic activists to pursue extra-legal options, similar to how the loose collective known as "antifa" was held to be engaging in similar violent tactics against political opponents during the Trump administration.[35] In the event, the Court's unanimous ruling and Democratic lawmakers' resigned reactions to it foreclosed the possibility of violence from the left.[36]

Thus, in mid-2024, American dissatisfaction with the political system remains only at a low boil. It is easy to foresee an alternative scenario playing out, however, supercharged not just by misinformation among the American public but also by state-sponsored disinformation in conjunction with a coordinated non-state actor cyberattack campaign to accelerate dissatisfaction with the US election system and escalate this dissatisfaction to the level of violence.

Unfortunately, experts and military cybersecurity experts examining cyberattacks tend to view these as one-off events occurring in isolation. There are many reasons to view cyberattacks in this way. First, Russia, China, Iran, and North Korea attempt to conceal the origin of their attacks, especially attacks conducted by intelligence or military personnel.[37] Second, many cyberattacks result in criminal monetary gain for the cyberattacking group, so even if Russia state actors were probing a US critical infrastructure vulnerability, it is difficult to discern through the criminal enterprise noise. Therefore, it is challenging to ascertain which attacks were solely motivated by individuals and civilian groups for criminal gain and which were sponsored, influenced, enticed, and even conducted by the Russian government. However, instead of focusing on attribution and actors to find potentially probing or linked cyberattacks, we have decided to focus on targets and extrapolate how a coordinated effort against specific targets can help us understand what a future operation might look like. In exploring this future scenario, each fictional attack has already actually occurred in some form in isolation in the past in the United States.

While cyberattacks have been occurring for decades in the West, recent developments seem to indicate that Russia is probing the US system for weakness. While both Russia and China likely believe that the United States' house is burning, China seems content to let Russia take the lead in developing a possible operational approach through a coordinated cyberattack that would foment violence and economic chaos in the United States. As we will explain below, Iran has recently joined in overtly, perhaps indicating wider coordination between Russia, China, and Iran.

The year 2021 was a watershed year for cyberattacks. However, because two attacks, the Solar Winds and Colonial Pipeline attacks, were so surprising that analysts missed the wider implications when one grouped these two attacks with several other notable attacks that year. The current phase of cyberattacks has been called the era of ransomware[38] but this myopic view of cyberattacks obscures the growing operational aspects. There are also so many cyberattacks per year and attribution is difficult. This further obscures seeing a holistic picture of probes and operational schema from Russia, China, and Iran. In 2021, targets became more diverse, and several attacks indicated that Russia was attempting to obtain information from the American economic, transportation, and critical infrastructure systems that could be used in a future coordinated attack. Many of these attacks occurred in temporal

proximity to one another further indicating a desire to see what was possible if cyberattacks were used in a military campaign.

The first attack occurred in January of 2021. Russian cybercrime gang REvil attacked a technology component supplier, Quanta. REvil demanded millions in ransom, or it would release schematics for highly sensitive components. Quanta did not respond and REvil released some of the stolen data on public servers. Unfortunately for REvil, the released data did not appear to be as significant as they had hoped it would be.[39] Quanta did not publicly respond to REvil, nor did they initially release the scope of the attack. Shifting tactics, REvil realized Quanta supplied Apple so they shifted to threatening to publish schematics to the newest version of the iMac and iPad online.[40] The released schematics also did not seem damaging to Apple, so this ransomware attack largely failed. The damage could have been much worse, though, as Quanta also supplies Alienware computers, Lenovo, Cisco, and Microsoft.[41] Also in January 2021, Firewall vendor Accellion released a bad patch to address known vulnerabilities. Unfortunately, the patch created even greater problems as it exposed Acellion's File Transfer Process, which routed sensitive files through a single, dedicated computer. This created a chokepoint for sensitive data which ransomware group Clop exploited. The main problem was that so many major companies used this firewall and were at risk from the attack.[42] One of the victims, Kroger, agreed to pay $5 million to pharmacy customers who lost their information to Clop from the Accellion breach.[43]

Shortly after these attacks in the spring and early summer months, a rapid succession of seemingly unrelated attacks occurred. The first attack was discovered in March of 2021. A Chicago-based insurer suffered a sophisticated ransomware and service disruption attack. On 21 March, an unknown ransomware gang infiltrated and absconded with sensitive personal information for over 75,000 clients. The cybergang was also able to shut down corporate email and CNA's website and portal.[44] CNA eventually paid $40 million to restore their system's operability. This was one of the largest ransoms ever paid to cybercriminals.[45] The most (in)famous ransomware disruption of 2021 was the May attack on Colonial Pipeline, which supplies gasoline to much of the US East Coast. On May 7, 2021, Colonial Pipeline suffered an infiltration of its IT infrastructure due to an inability to properly implement multifactor authentication (MFA). An old account which had fairly wide access but only single factor authentication had laid dormant on the system. DarkSide, a Russian-based cybergang, gained access to the system through a former employee's account simply by hacking a password.[46]

DarkSide exfiltrated sensitive operating systems and data and threatened to disrupt the entire pipeline. The CEO, Joseph Blount, Jr., ordered the pipeline shut down to minimize the potential damage hackers could have done. Eventually, the company paid $5 million as a ransom to DarkSide.[47] However, before the ransom was paid and the flow of oil was restored, multiple states suffered serious energy disruptions for five days.[48] This created fuel shortages in seventeen eastern states stretching from New York to Georgia.[49] This story had observable ramifications, with fuel shortages affecting millions of people on the Eastern Seaboard while the economy was still struggling with the effects of the COVID pandemic. The Colonial Pipeline hack and its aftermath dominated the media in 2021 as the most important and damaging cyberattack of modern times.

Colonial Pipeline was not the only cyber attack of late spring 2021, however. Shortly afterwards, in June of 2021, a large meat processing plant, JBS, was attacked. The hack notably resulted in the shutdown of multiple plants not just in the United States but also in Canada and as far away as Australia. In order to restore meat packing services, JBS paid $11 million in Bitcoin to an undisclosed hacking group. The US government later claimed to have evidence that the hacking group was Russian in nature. No data was found to have been stolen in the cyberattack, but the reputational effects were severe.[50]

The notable cyberattacks in 2021 were all ransomware attacks and not direct attacks on American national security infrastructure; it is therefore understandable that links between these attacks were not made. Due to its massive effects on a major portion of the American population, the Colonial Pipeline attack was the most sensational attack and garnered the lion's share of press coverage. The attacks also seemed to be predominantly carried out by Russian cybergangs supported or at least tolerated by the Russian government. Even if some of these attacks were not a concerted effort by Russia to probe the American system for weaknesses, the observable results of the attacks are the same. Not only Russia, but other adversaries such as China and Iran could observe the results of these

attacks and discern there was a critical vulnerability in American cyberspace.

Clearer evidence for the operationalization of cyberspace by America's enemy materialized recently. A new series of tightly clustered events indicate that Russia, China, and Iran are interested in potentially disrupting the US economy and stable governance. An odd ransomware attack occurred in November of 2023. A widespread cyber disruption diverted multiple ambulances from several hospitals in the northeast United States. The hackers infiltrated the dispatching systems and put out false notices to ambulances that the emergency rooms were at capacity and no longer accepting patients.[51]

In early December of 2023, an Iranian cybergang known as "CyberAv3ngers" attacked several water supply and sewage systems.[52] The CyberAv3ngers claimed that the water distribution systems used Ultronics Vision Series programmable logic controllers and that these controllers were made by an Israeli company. Therefore, due to the Israeli war against Hamas, Iran had decided to punish as many Israeli companies as possible while also sending a warning to the United States in hopes that the US government would pull its support from Israel. The attack was localized to the state of Pennsylvania but still caused disruption to the citizens there. The group made no demand for money making this one of the first significant political cyberattacks. First American financial company was also disrupted in December of 2023. First American funds First American Trust and other third-party banks and was unable to perform this service for several days when its system was infiltrated by cyberhackers. Interestingly, First American has not stated this was a ransomware attack. First American was able to restore services through a temporary website within a few days.[53]

Finally, in late December of 2023, the US Congress reported that a massive Chinese infiltration into US critical infrastructure and services was discovered. US cybersecurity experts disrupted a sweeping cybersecurity infiltration. Officials felt that China was staging in cyberspace to potentially mount espionage campaigns, discredit officials in the military and government, engage in intellectual property theft and cyberattacks against infrastructure in an effort to undermine the United States.[54] US security officials emphasized that China was infiltrating with the intent of attacking at some future date. Further, they noted that the operation looked to be aimed at causing societal chaos through economic disruptions and increasing distrust of public officials.[55]

The more recent operations indicate a similar theme of adversaries planning, testing, or actually attempting to disrupt the US economy, critical infrastructure, energy, and society. The difference that two years made was notable. Currently, we can observe more than Russian-backed cybergangs engaging in ransomware attacks. Iran attacked the United States politically. China was positioned and planning to potentially mount an operation to disrupt American society by sowing confusion and discord. Collusion might also be present between China, Russia, and Iran but it does not have to be. Coincidental timing between these three adversaries could be enough to degrade or destroy American society.

The Line Between Rhetoric and Reality is Blurring

While many scenarios predicting election violence have so far been the stuff of Hollywood thrillers like "Leave the World Behind" and "Civil War," the possibility of election violence is realistic, or at least plausible.[56] America is becoming increasingly polarized, and is becoming polarized more rapidly than other OECD countries.[57] While not directly linked to affective polarization, political violence appears to be more accepted among certain segments of the American population.[58] Though incidents of political violence in the United States—directed at the government and fostered by a toxic information environment that enabled or empowered conspiracy theories—have been present in the country for generations, in the 1970s right-wing political violence began to be directed specifically at people like federal agents.[59] Nevertheless, "what is occurring today does not resemble this recent past."[60] On January 6, 2021 the first violent insurgent act occurred when a mob angry with an election outcome stormed the US capitol by force and occupied it for hours. Several of the occupiers were killed as police and military personal tried to provide safety to Congressional representatives. The polarization and distrust between the two political sides has only increased since that incident.

Russia and China are fomenting chaos online, while much of the US government is preoccupied with either

questioning or preserving the integrity of electronic voting machines. Rather than focus on the mechanics of elections, the US government should work to preserve the integrity of political discourse. This is no easy task in a country that prides itself on protecting free speech. However, foreign infiltrators to our social media space must be rooted out and removed. The Western press also has a responsibility not to fall victim to false or misleading reporting from Russian and Chinese-sponsored sites and freelance journalists who have been duped into reporting falsehoods. This, too, will be very difficult.

All of the cyberattacks depicted in the scenario outlined earlier in this article have already occurred in the past. The difference in the scenario is one of scale, timing, and coordination.[61] If Russia, China, and Iran can coordinate information and cyberattacks into a coherent operation at a time when distrust, suspicion and acceptance of violence is already building in the United States, this is a likely outcome. The upcoming election in November of 2024 might one such exploitable event. There is not a great deal of time to prepare for and counter this possibility. Russia, China, and Iran believe the American house is burning. There is plenty of evidence to suggest that they might loot it as it burns.

References

23-719 Trump v. Anderson (03/04/2024). “23-719 Trump v. Anderson (03/04/2024).” Accessed March 16, 2024. https://d3i6fh83elv35t.cloudfront.net/static/2024/03/23-719_19m2.pdf.

“About CISA | CISA.” Accessed March 17, 2024. https://www.cisa.gov/about.

Albertson, Bethany, and Kimberly Guiler. “Conspiracy Theories, Election Rigging, and Support for Democratic Norms.” *Research & Politics* 7, no. 3 (July 2020): 205316802095985. https://doi.org/10.1177/2053168020959859.

Baev, Pavel. “The Limits of Authoritarian Compatibility: Xi’s China and Putin’s Russia.” Brookings, June 2020. https://www.brookings.edu/articles/the-limits-of-authoritarian-compatibility-xis-china-and-putins-russia/.

Bandurski, David. “China and Russia Are Joining Forces to Spread Disinformation,” March 11, 2022. https://policycommons.net/artifacts/4141779/china-and-russia-are-joining-forces-to-spread-disinformation/4950451/.

Bloomberg.com. “Apple Targeted in $50 Million Ransomware Hack of Supplier Quanta.” April 21, 2021. https://www.bloomberg.com/news/articles/2021-04-21/apple-targeted-in-50-million-ransomware-hack-of-supplier-quanta.

Bloomberg.com. “Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom.” May 13, 2021. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom.

Bloomberg.com. “Hackers Breached Colonial Pipeline Using Compromised Password.” June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Boxell, Levi, Matthew Gentzkow, and Jesse M. Shapiro. “Cross-Country Trends in Affective Polarization.” Working Paper. Working Paper Series. National Bureau of Economic Research, January 2020. https://doi.org/10.3386/w26669.

Chicago Tribune. “CNA Cyberattack in March Exposed Personal Information of More than 75,000 People, Filings Reveal,” November 2, 2021. https://www.chicagotribune.com/2021/11/02/cna-cyberattack-in-march-exposed-personal-information-of-more-than-75000-people-filings-reveal/.

“CISA and International Partners Release Advisory on Russia-Based Threat Actor Group, Star Blizzard | CISA,” December 7, 2023. https://www.cisa.gov/news-events/alerts/2023/12/07/cisa-and-international-partners-release-advisory-russia-based-threat-actor-group-star-blizzard.

“CISA Offers Guidance to Election Officials on Mitigating Generative AI Risk.” Accessed March 17, 2024. https://adv

ance-lexis-com.ezproxy.lib.utexas.edu/document?crid=e72ac1ce-2854-4547-aaca-1815a4e58c1f&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A6B5S-92H1-JBHM-S01H-00000-00&pdsourcegroupingtype=&pdcontentcomponentid=412529&pdmfid=1516831&pdisurlapi=true.

Civil War. Action. A24, DNA Films, IPR.VC, 2024.

Clark, Mitchell. “One of the US’s Largest Insurance Companies Reportedly Paid $40 Million to Ransomware Hackers.” The Verge, May 20, 2021. https://www.theverge.com/2021/5/20/22446388/cna-insurance-ransomware-attack-40-million-dollar-ransom.

“Consolidated_Risk_in_Focus_Gen_AI_Elections_508c.Pdf.” Accessed March 17, 2024. https://www.cisa.gov/sites/default/files/2024-01/Consolidated_Risk_in_Focus_Gen_AI_Elections_508c.pdf.

Council on Foreign Relations. “Indicting Russia’s Most Destructive Cyberwar Unit: The Implications of Public Attribution.” Accessed March 17, 2024. https://www.cfr.org/blog/indicting-russias-most-destructive-cyberwar-unit-implications-public-attribution.

Dina Smeltz, Craig Kafura. “Majority of Trump Republicans Prefer the United States Stay out of World Affairs.” Research. The Chicago Council on Global Affairs, February 16, 2024. https://globalaffairs.org/research/public-opinion-survey/majority-trump-republicans-prefer-united-states-stay-out-world.

Dobber, Tom, Nadia Metoui, Damian Trilling, Natali Helberger, and Claes de Vreese. “Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?” *The International Journal of Press/Politics* 26, no. 1 (January 1, 2021): 69–91. https://doi.org/10.1177/1940161220944364.

“Election Security | Cybersecurity and Infrastructure Security Agency CISA.” Accessed March 17, 2024. https://www.cisa.gov/topics/election-security.

“Elections in the United States of America.” Accessed March 17, 2024. https://www.osce.org/odihr/elections/usa.

“First American Assures Security of Funds Following Recent Cyberattack.” Accessed March 17, 2024. https://www.insurancebusinessmag.com/us/news/cyber/first-american-assures-security-of-funds-following-recent-cyberattack-471400.aspx.

“Five Possible Hacks to Worry About Before Election Day.” Accessed March 17, 2024. https://advance-lexis-com.ezproxy.lib.utexas.edu/document?crid=47d61183-9858-4d11-b7c2-49b51fa94166&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5PHW-W351-DXY4-X3MD-00000-00&pdsourcegroupingtype=&pdcontentcomponentid=6742&pdmfid=1516831&pdisurlapi=true.

Forbes. “404.” Accessed March 17, 2024. https://www.forbes.com/404-home/.

“Foreign Influence in the United States.” Text file., February 6, 2024. https://congressional-proquest-com.ezproxy.lib.utexas.edu/congressional/result/congressional/congdocumentview?accountid=7118&groupid=114746&parmId=18DD6DA392F#0.

Hariprasad, Vishaal. “Council Post: The New Era Of Ransomware—And What It Means For Businesses.” Forbes. Accessed March 17, 2024. https://www.forbes.com/sites/forbesbusinesscouncil/2023/11/30/the-new-era-of-ransomware-and-what-it-means-for-businesses/.

Helmore, Edward. “US Supreme Court under Pressure to Rule Swiftly on States’ Trump Ballot Bans.” *The Guardian*, December 29, 2023, sec. US news. https://www.theguardian.com/us-news/2023/dec/29/maine-trump-ballot-us-supreme-court.

Humprecht, Edda. “The Role of Trust and Attitudes toward Democracy in the Dissemination of Disinformation—a Comparative Analysis of Six Democracies.” *Digital Journalism* 0, no. 0 (2023): 1–18. https://doi.org/10.1080/21670811.2023.2200196.

Johnston, Alastair Iain. *Cultural Realism Strategic Culture and Grand Strategy in Chinese History* . Princeton Studies in International History and Politics. Princeton, NJ: Princeton Univ. Press, 1998. https://doi.org/10.1515/9780691213149.

Kleinfeld, Rachel. “The Rise of Political Violence in the United States.” *Journal of Democracy* 32, no. 4 (2021): 160–76.

Lambie, John. “History of Open and Closed Societies.” In*How to Be Critically Open-Minded — A Psychological and Historical Analysis*, edited by John Lambie, 131–60. London: Palgrave Macmillan UK, 2014. https://doi.org/10.1057/9781137301055_9.

Leave the World Behind. Drama, Mystery, Thriller. Esmail Corp., Higher Ground Productions, Netflix Studios, 2023.

Lindsay, Greg, Jason C Brown, Brian David Johnson, Christopher Owens, Andrew Hall, and J H Carrott. “Microtargeting Unmasked: Safeguarding Law Enforcement, the Military, and the Nation in the Era of Personalized Threats,” n.d.

Lozada, Carlos. “Review | How to Read Vladimir Putin.” *Washington Post*, March 16, 2022. https://www.washingtonpost.com/outlook/2022/03/03/putin-essays/.

Lyngaas, Sean. “Cyberattack on US Hospital Owner Diverts Ambulances from Emergency Rooms in Multiple States | CNN Politics.” CNN, November 27, 2023. https://www.cnn.com/2023/11/27/politics/cyberattack-hospital-diverts-ambulances/index.html.

Martina, Michael, Patricia Zengerle, Andrew Goudsward, and Patricia Zengerle. “US Officials Deliver Warning That Chinese Hackers Are Targeting Infrastructure.” *Reuters*, January 31, 2024, sec. Cybersecurity. https://www.reuters.com/technology/cybersecurity/chinese-hackers-are-targeting-us-infrastructure-fbi-chief-testify-2024-01-31/.

“Meat Giant JBS Pays $11m in Ransom to Resolve Cyber-Attack.” June 10, 2021. https://www.bbc.com/news/business-57423008.

Merken, Sara, and Sara Merken. “Kroger Agrees to Pay $5 Million over Accellion Data Breach.” *Reuters*, July 1, 2021, sec. Litigation. https://www.reuters.com/legal/litigation/kroger-agrees-pay-5-million-over-accellion-data-breach-2021-07-01/.

Mitchell, Amy, and Mason Walker. “More Americans Now Say Government Should Take Steps to Restrict False Information Online than in 2018.” *Pew Research Center* (blog). Accessed March 17, 2024. https://www.pewresearch.org/short-reads/2021/08/18/more-americans-now-say-government-should-take-steps-to-restrict-false-information-online-than-in-2018/.

Mongrain, Philippe. “Suspicious Minds: Unexpected Election Outcomes, Perceived Electoral Integrity and Satisfaction With Democracy in American Presidential Elections.” *Political Research Quarterly* 76, no. 4 (December 2023): 1589–1603. https://doi.org/10.1177/10659129231166679.

Myers, Steven Lee. “Spate of Mock News Sites With Russian Ties Pop Up in U.S.” *The New York Times*, March 7, 2024, sec. Business. https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html.

Network Contagion Research Institute. “9/14/20 – Network-Enabled Anarchy: How Militant Anarcho-Socialist Networks Use Social Media to Instigate Widespread Violence Against Political Opponents and Law Enforcement.”

Accessed March 17, 2024. https://networkcontagion.us/reports/network-enabled-anarchy/.

Newman, Lily Hay. “The Accellion Breach Keeps Getting Worse—and More Expensive.” *Wired*. Accessed March 17, 2024. https://www.wired.com/story/accellion-breach-victims-extortion/.

Perlroth, Nicole. “How China Transformed Into a Prime Cyber Threat to the U.S.” *The New York Times*, July 19, 2021, sec. Technology. https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html.

———. *This Is How They Tell Me the World Ends the Cyber Weapons Arms Race* . New York: Bloomsbury Publishing, 2021.

Pew Research Center. “Americans’ Dismal Views of the Nation’s Politics.” *Pew Research Center – U.S. Politics & Policy* (blog), September 19, 2023. https://www.pewresearch.org/politics/2023/09/19/americans-dismal-views-of-the-nations-politics/.

Pillsbury, Michael. *The Hundred-Year Marathon: China’s Secret Strategy to Replace America as the Global Superpower / Michael Pillsbury.* First Edition. New York: Henry Holt and Co., 2015.

Press, Jennifer McCoy, Benjamin. “What Happens When Democracies Become Perniciously Polarized?” Carnegie Endowment for International Peace. Accessed March 16, 2024. https://carnegieendowment.org/2022/01/18/what-happens-when-democracies-become-perniciously-polarized-pub-86190.

PRRI | At the intersection of religion, values, and public life. “Threats to American Democracy Ahead of an Unprecedented Presidential Election | PRRI,” October 25, 2023. https://www.prri.org/research/threats-to-american-democracy-ahead-of-an-unprecedented-presidential-election/.

“Risk in Focus: Generative A.I. and the 2024 Election Cycle | CISA.” Accessed March 16, 2024. https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle.

Rutenberg, Jim, and Steven Lee Myers. “How Trump’s Allies Are Winning the War Over Disinformation.” *The New York Times*, March 17, 2024, sec. U.S. https://www.nytimes.com/2024/03/17/us/politics/trump-disinformation-2024-social-media.html.

Sanger, David E., and Nicole Perlroth. “Trump Fires Christopher Krebs, Official Who Disputed Election Fraud Claims.” *The New York Times*, November 18, 2020, sec. U.S. https://www.nytimes.com/2020/11/17/us/politics/trump-fires-christopher-krebs.html.

Satter, Raphael, and Raphael Satter. “US Warns Hackers Are Carrying out Attacks on Water Systems.” *Reuters*, March 20, 2024, sec. Cybersecurity. https://www.reuters.com/technology/cybersecurity/us-warns-that-hackers-are-carrying-out-disruptive-attacks-water-systems-2024-03-20/.

Silver, Laura, Sneha Gubbala, and Jordan Lippert. “Americans See Both Russia and China in a Negative Light – but More Call Russia an Enemy.” *Pew Research Center* (blog). Accessed March 17, 2024. https://www.pewresearch.org/short-reads/2023/05/10/americans-see-both-russia-and-china-in-a-negative-light-but-more-call-russia-an-enemy/.

Sims, David. “The 13 Best Movies About Why You Shouldn’t Trust the Government.” *The Atlantic* (blog), June 5, 2020. https://www.theatlantic.com/culture/archive/2020/06/13-best-movies-about-government-mistrust/612712/.

Spracher, William C. “Homeland Security and Intelligence: Can Oil Mix with Water in an Open Society?” *Low Intensity Conflict & Law Enforcement* 11, no. 1 (2002): 29–54. https://doi.org/10.1080/09662840420002682 92.

Statista. “Trust in Government Worldwide by Country 2023.” Accessed March 17, 2024. https://www.statista.com/statistics/1362804/trust-government-world/.

The Daily Wire. “Recent Chinese Cyberattacks Aim To Cause ‘Societal Chaos’ In U.S.: Report,” December 11, 2023. https://www.dailywire.com/news/recent-chinese-cyberattacks-aim-to-cause-societal-chaos-in-u-s-report.

Thomson-DeVeaux, Amelia. “Why Many Americans Might Be Increasingly Accepting Of Political Violence.” *FiveThirtyEight* (blog), January 6, 2022. https://fivethirtyeight.com/features/why-many-americans-might-be-increasingly-accepting-of-political-violence/.

“Tracking the Criminal and Civil Cases against Donald Trump.” Accessed March 17, 2024. https://projects.apnews.com/features/2023/trump-investigations-civil-criminal-tracker/index.html.

“Under the Din of the Race Lies a Once and Future Threat: Cyberwarfare.” Accessed March 17, 2024. https://advance-lexis-com.ezproxy.lib.utexas.edu/document?crid=0982aca9-568a-4f1c-80a5-3de235e47958&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5M41-YGX1-DXY4-X4W2-00000-00&pdsourcegroupingtype=&pdcontentcomponentid=6742&pdmfid=1516831&pdisurlapi=true.

“W26669.Pdf.” Accessed March 17, 2024. https://www.nber.org/system/files/working_papers/w26669/w26669.pdf.

Warren, Tom. “Microsoft and OpenAI Say Hackers Are Using ChatGPT to Improve Cyberattacks.” The Verge, February 14, 2024. https://www.theverge.com/2024/2/14/24072706/microsoft-openai-cyberattack-tools-ai-chatgpt.

Washington Post. “Analysis | What Will Happen to America If Trump Wins Again? Experts Helped Us Game It Out.,” October 10, 2022. https://www.washingtonpost.com/magazine/2022/10/10/country-after-second-trump-term/.

Wilkie, Christina. “Colonial Pipeline Paid $5 Million Ransom One Day after Cyberattack, CEO Tells Senate.” CNBC, June 8, 2021. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

Winder, Davey. “Ransomware Gang Demands $50 Million For Apple Watch And MacBook Pro Blueprints.” Forbes. Accessed March 17, 2024. https://www.forbes.com/sites/daveywinder/2021/04/23/ransomware-gang-demands-50-million-for-apple-watch-and-macbook-pro-blueprints/.

Zoellner, Danielle. “Seventeen States Declare Emergency over Hack as US Energy Secretary Tells Americans Not to ‘Hoard’ Fuel.” *The Independent*, May 11, 2021, sec. News. https://www.independent.co.uk/news/world/americas/us-politics/colonial-pipeline-hack-hoard-fuel-b1845855.html.

Notes

[1] Myers, “Spate of Mock News Sites With Russian Ties Pop Up in U.S.,” New York Times, 7 March 2024. https://www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html (last accessed 15 March 2024).

[2] The US is a founding participating state of the OSCE, and election monitoring is a key facet of the organization’s mission. Many prior US elections have had OSCE observers present, including the general election of November 2020. See https://www.osce.org/odihr/elections/usa (last accessed 14 March 2024).

[3] Lindsay et al., “Microtargeting Unmasked: Safeguarding Law Enforcement, the Military, and the Nation in the Era of Personalized Threats.”

[4] Dobber et al., “Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?”

[5] *The Verge*. “Microsoft and OpenAI Say Hackers are Using ChatGPT to Improve Cyberattacks.” February 14, 2024. https://www.theverge.com/2024/2/14/24072706/microsoft-openai-cyberattack-tools-ai-chatgpt.

[6] David Sims, “The 13 Best Movies About Why You Shouldn’t Trust the Government,” *The Atlantic*, 5 June 2020.

Available at https://www.theatlantic.com/culture/archive/2020/06/13-best-movies-about-government-mistrust/612712/

[7] "Americans see both Russia and China in a negative light – but more call Russia an enemy," Pew Research Center, 10 May 2023; https://www.pewresearch.org/short-reads/2023/05/10/americans-see-both-russia-and-china-in-a-negative-light-but-more-call-russia-an-enemy/

[8] Carlos Lozada. "How to Read Vladimir Putin." *The Washington Post*. March 3, 2022. https://www.washingtonpost.com/outlook/2022/03/03/putin-essays/.

[9] Michael Pillsbury. *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower*. (New York, NY: St. Martin's Griffin, 2016), and Alastair Ian Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*. (Princeton, NJ: Princeton University Press, 1995).

[10]"How China Transformed Into a Prime Cyber Threat to the U.S." *New York Times*, 19 July 2021,https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html

[11]"US officials deliver warning that Chinese hackers are targeting infrastructure," Reuters.com, https://www.reuters.com/technology/cybersecurity/chinese-hackers-are-targeting-us-infrastructure-fbi-chief-testify-2024-01-31/ (last accessed 15 March 2024).

[12] See Bandurski, D., 2022. *China and Russia are joining forces to spread disinformation* , Brookings Institution. United States of America. Retrieved from https://policycommons.net/artifacts/4141779/china-and-russia-are-joining-forces-to-spread-disinformation/4950451/ on 04 Mar 2024. CID: 20.500.12592/cmfj66. For an alternative perspective, see Baev, Pavel. "The limits of authoritarian compatibility: Xi's China and Putin's Russia." *Global China* (2020).

[13] Pew Research Center, "More Americans now say government should take steps to restrict false information online than in 2018," 18 August 2021, available at https://www.pewresearch.org/short-reads/2021/08/18/more-americans-now-say-government-should-take-steps-to-restrict-false-information-online-than-in-2018/ (last accessed 16 February 2024). See also Humprecht, "The Role of Trust and Attitudes toward Democracy in the Dissemination of Disinformation—a Comparative Analysis of Six Democracies"; Albertson and Guiler, "Conspiracy Theories, Election Rigging, and Support for Democratic Norms."

[14] "Election Security," CISA.gov, https://www.cisa.gov/topics/election-security (last accessed 18 February 2024).

[15] Ibid.

[16] David Sanger, "Five Possible Hacks to Worry About Before Election Day". *The New York Times .* November 3, 2016 Thursday. https://advance-lexis-com.ezproxy.lib.utexas.edu/api/document?collection=news&id=urn:contentItem:5PHW-W351-DXY4-X3MD-00000-00&context=1516831; By DAVID E. SANGER. "Under the Din of the Race Lies a Once and Future Threat: Cyberwarfare". *The New York Times.* November 7, 2016 Monday. https://advance-lexis-com.ezproxy.lib.utexas.edu/api/document?collection=news&id=urn:contentItem:5M41-YGX1-DXY4-X4W2-00000-00&context=1516831.

[17] CISA, "Mission," found at https://www.cisa.gov/about (last accessed 18 February 2024)

[18] NexisUni searches with the keywords "CISA" and "cybersecurity" and confined to US newspapers between 2017 and 2024 return over 10,000 results, with almost 4,000 results coming from the New York Times alone: (https://advance-lexis-com.ezproxy.lib.utexas.edu/api/permalink/874d8dd9-4e23-4977-97be-b04f7bf2a90c/?context=1516831).

[19] Sanger and Perlroth, 17 November 2020. "Trump Fires Christopher Krebs, Official Who Disputed Election Fraud

Claims," https://www.nytimes.com/2020/11/17/us/politics/trump-fires-christopher-krebs.html?smid=url-share (last accessed 15 March 2024).

[20] CISA, "Risk in Focus: Generative A.I. and the 2024 Election Cycle," 18 January 2024. https://www.cisa.gov/sites/default/files/2024-01/Consolidated_Risk_in_Focus_Gen_AI_Elections_508c.pdf
See also "CISA offers guidance to election officials on mitigating generative AI risk". Inside Cybersecurity, January 23, 2024. https://advance-lexis-com.ezproxy.lib.utexas.edu/api/document?collection=news&id=urn:contentItem:6B5S-92H1-JBHM-S01H-00000-00&context=1516831. Accessed February 18, 2024.

[21] "CISA and International Partners Release Advisory on Russia-based Threat Actor Group, Star Blizzard," 7 December 2023. https://www.cisa.gov/news-events/alerts/2023/12/07/cisa-and-international-partners-release-advisory-russia-based-threat-actor-group-star-blizzard

[22] Lambie, J. (2014). History of Open and Closed Societies. In: How to be Critically Open-Minded — A Psychological and Historical Analysis. Palgrave Macmillan, London. https://doi.org/10.1057/9781137301055_9

[23] Spracher, William C. "Homeland Security and Intelligence: Can Oil Mix with Water in an Open Society?"*Low intensity conflict & law enforcement* 11, no. 1 (2002): 29–54.

[24] *Foreign Influence in the United States*, U.S. Congress. Senate Committee on Homeland Security and Governmental Affairs, 2024. https://search.lib.utexas.edu/permalink/01UTAU_INST/1jebi5l/cdi_proquest_congressional_hearing_s48_20240206_24904

[25] McCoy, Jennifer and Benjamin Press, "What Happens When Democracies Become Perniciously Polarized?" Carnegie Endowment for International Peace, 18 January 2022. https://carnegieendowment.org/2022/01/18/what-happens-when-democracies-become-perniciously-polarized-pub-86190 (last accessed 15 March 2024).

[26] "Share of population who trust their government worldwide 2023, by country," https://www.statista.com/statistics/1362804/trust-government-world/ (last accessed 18 February 2024).

[27] Chicago Council on Global Affairs, "Majority of Trump Republicans Prefer the United States Stay out of World Affairs." 16 February 2024, available at https://globalaffairs.org/research/public-opinion-survey/majority-trump-republicans-prefer-united-states-stay-out-world?utm_source=media&utm_campaign=ccs&utm_medium=atlantic (last accessed 18 February 2024).

[28] Pew Research Center, "Americans' Dismal Views of the Nation's Politics," 19 September 2023, available at https://www.pewresearch.org/politics/2023/09/19/americans-dismal-views-of-the-nations-politics/ (last accessed 18 February 2024).

[29] PRRI, "Threats to American Democracy Ahead of an Unprecedented Presidential Election," 25 October 2024, available at https://www.prri.org/research/threats-to-american-democracy-ahead-of-an-unprecedented-presidential-election/ (last accessed 18 February 2024).

[30] Ibid.

[31] "Trump Investigations: Tracking the Cases," Associated Press https://projects.apnews.com/features/2023/trump-investigations-civil-criminal-tracker/index.html (last accessed 14 March 2024).

[32] Edward Helmore. "US Supreme Court Under Pressure to Rule Swiftly on States' Trump Ballot Bans." December 29, 2023. https://www.theguardian.com/us-news/2023/dec/29/maine-trump-ballot-us-supreme-court.

[33] Supreme Court of the United States, "23-719 Trump v. Anderson (03/04/2024)" https://d3i6fh83elv35t.cloudfront.net/static/2024/03/23-719_19m2.pdf (last accessed 15 March 2024)

[34] *Ibid.*

[35] "9/14/20 – Network-Enabled Anarchy: How Militant Anarcho-Socialist Networks Use Social Media to Instigate Widespread Violence Against Political Opponents and Law Enforcement," Network Contagion Research Institute (NCRI).

https://networkcontagion.us/reports/network-enabled-anarchy/ (last accessed 14 March 2024).

[36] While possible, this scenario is generally considered less plausible than its counterpart among Republican voters, as incidences of political violence in support of Al Gore in the contested 2000 election were sporadic and very low-level. See Mongrain, Philippe. "Suspicious Minds: Unexpected Election Outcomes, Perceived Electoral Integrity and Satisfaction With Democracy in American Presidential Elections." *Political research quarterly* vol. 76,4 (2023): 1589-1603. doi:10.1177/10659129231166679

[37] *Council on Foreign Relations*. "Indicting Russia's Most Destructive Cyberwar Unit: The Implications of Public Attribution." November 23, 2020. https://www.cfr.org/blog/indicting-russias-most-destructive-cyberwar-unit-implications-public-attribution.

[38] Vishaal Hariprasad. "The New Era of Ransomware—And What it Means for Businesses." *Forbes*. November 30, 2023. https://forbes.com/forbesbuisinesscouncil/2023/11/30/the-new-era-of-ransomeware-and-what-it-means-for-businesses/?sh=d3f7986d855 and Nicole Perlroth. *This is How They Tell Me the World Ends*. (New York: Bloomsbury Publishing, 2021).

[39] Davey Winder. "Ransomware Gang Demands $50 Million for Apple Watch and Macbook Pro Blueprints." (April 23,2021).*Forbes*.https://www.forbes.com/sites/daveywinder/2021/04/23/ransomware-gang-demands-50-million-for-apple-watch-and-macbook-pro-blueprints/?sh=7f47e4a65839.

[40] Kartikay Mehorta. "Apple Targeted in $50 Million Ransomware Hack of Supplier Quanta." *Bloomberg*. April 21, 2021. https://www.bloomberg.com/news/articles/2021-04-21/apple-targeted-in-50-million-ransomware-hack-of-supplier-quanta.

[41] Davey Winder. "Ransomware Gang Demands $50 Million for Apple Watch and Macbook Pro Blueprints." (April 23, 2021).

[42] Lily Hay Newman. "The Accellion Breach Keeps Getting Worse—and More Expensive." *Wired.* (8 March 2021). https://www.wired.com/story/accellion-breach-victims-extortion/.

[43] Sara Merken. "Kroger Agrees to Pay $5 Million Over Accellion Data Breach." *Reuters*. (July 1, 2021). https://www.reuters.com/legal/litigation/kroger-agrees-pay-5-million-over-accellion-data-breach-2021-07-01/.

[44] Robert Channick. "CNA Cyberattack in March Exposed Personal Information of More Than 75,000 People, Filings Reveal." *Chicago Tribune*. (November 2, 2021). https://www.chicagotribune.com/2021/11/02/cna-cyberattack-in-march-exposed-personal-information-of-more-than-75000-people-filings-reveal/.

[45] Mitchell Clark. "One of the US's Largest Insurance Companies Reportedly Paid $40 Million to Ransomware Hackers." *The Verge*. (May 20, 2021). https://www.theverge.com/2021/5/20/22446388/cna-insurance-ransomware-attack-40-million-dollar-ransom.

[46] Willaim Turton and Kartikay Mehorta. "Hackers Breached Colonial Pipeline Using Compromised Password." *Bloomberg.* June 4, 2021. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

[47] "Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom," 13 May 2021, Bloomberg.com

https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom (last accessed 14 March 2024).

[48] Christina Wilkie. “Colonial Pipeline Paid $5 Million Ransom One Day After Cyberattack, CEO Tells Congress.” June 8, 2021. *CNBC*. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

[49] Danielle Zoellner. “Colonial pipeline: 17 states declare emergency over hack as energy secretary tells people not to ‘hoard’ fuel.” 11 May 2021. *The Independent*. https://www.independent.co.uk/news/world/americas/us-politics/colonial-pipeline-hack-hoard-fuel-b1845855.html.

[50] *BBC.* “Meat Giant JBS Pays $11m in Ransom to Resolve Cyber-Attack.” June 10, 2021. https://www.bbc.com/news/business-57423008.

[51] Sean Lyngaas. “Cyberattack on US Hospital Owner Diverts Ambulances from Emergency Rooms in Multiple States.” *CNN*. November 27, 2023. https://cnn.com/2023/11/27/politics/cyberattack-hospital-diverts-ambulances/index.html.

[52] Satter and Satter, “US Warns Hackers Are Carrying out Attacks on Water Systems.”

[53] Abigail Adriatico. “First American Assures Security of Funds Following Recent Cyberattack.” *Insurance Business*. December 21, 2023. https://www.insurancebusinessmag.com/us/news/cyber/first-american-assures-security-of-funds-following-recent-cyberattack-471400.aspx.

[54] Michael Martina, Patricia Zengerle and Andrew Goudsward. “US Officials Deliver Warning that Chinese Hackers are Targeting Infrastructure.” Reuters. January 31, 2024. https://www.reuters.com/technology/cybersecurity/chinese-hackers-are-targeting-us-infrastructure-fbi-chief-testify-2024-01-31/.

[55] Tim Pearce. “Recent Chinese Cyberattacks Aim to Cause ‘Societal Chaos’ in U.S.” *Daily Wire*. December 11, 2023. https://www.dailywire.com/news/recent-chinese-cyberattacks-aim-to-cause-societal-chaos-in-u-s-report.

[56] *Leave the World Behind*; *Civil War*.

[57] Boxell, Levi, Matthew Gentzkow and Jesse M. Shapiro, “Cross-Country Trends in Affective Polarization,” National Bureau of Economic Research (NBER) working paper, November 2021 https://www.nber.org/system/files/working_papers/w26669/w26669.pdf, last accessed 16 March 2024.

[58] Thomson-DeVeaux, “Why Many Americans Might Be Increasingly Accepting Of Political Violence.” FiveThirtyEight.com, 6 January 2022. https://fivethirtyeight.com/features/why-many-americans-might-be-increasingly-accepting-of-political-violence/ (last accessed 15 March 2024).

[59] Kleinfeld, “The Rise of Political Violence in the United States.”

[60] Ibid., p. 162

[61] Note that ransom played no role in the scenario; the goal was chaos, rather than extortion

Dan G. Cox wishes it to be known that this work represents the view of the author only, and does not reflect the views of the School of Advanced Military Studies, the Command and General Staff College, the US Army, or the Department of Defense. Michael Mosser has no competing interests to declare.

About the author:

Michael W. Mosser is the Director of the Center for European Studies (CES) and Associate Professor of Instruction at the University of Texas at Austin with appointments in the Department of Government and the International Relations and Global Studies (IRG) program. From 2022 to August 2024, he was the Executive Director of the Global Disinformation Lab (GDIL), as well as a Distinguished Scholar in the Robert S. Strauss Center for International Security and Law.

Dan G Cox is a professor of political science at the US Army School of Advanced Military Studies. He has written broadly on the future of war. He served in the NATO partnership for Peace on a mission to Armenia. All opinions expressed here are his and do not represent the US Army, School of Advanced Military Studies, or any DoD or US governmental agency.