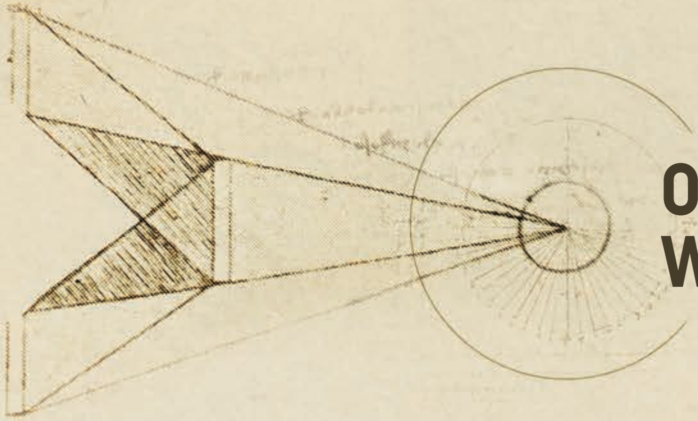


ON FUTURE WAR

APRIL 2024

Eroding Trust in Government

What Games, Surveys, and Scenarios Reveal about Alternative Cyber Futures

By Yasir Atalan, Jose M. Macias, and Benjamin Jensen

In the Future . . .

- **Societies will be held hostage through cyberspace by states and non-state actors seeking to target the most vulnerable as part of larger political warfare campaigns waged online.** In place of costly offensive cyber campaigns, malign actors will seek to undermine trust and confidence in government through disrupting basic needs and services such as food aid and medical assistance, creating an insidious new form of countervalue targeting.
- **Gender dynamics will increasingly play a significant role in shaping perceptions of cyber threats, especially in the context of misinformation campaigns.** The manipulation of gender-based differences through deepfakes and computational propaganda will exacerbate fault lines adversaries can use to further polarize society and undermine trust and confidence in governing institutions.
- **Distrust in government will be further compounded as citizens struggle to understand cybersecurity strategy and the funding levels required to protect critical infrastructure.** Governments will continue to face challenges in educating the public about evolving cyber threats and balancing the ways and means required to protect the ability to provide public goods online.

Introduction

What is the future of cyber war? Over the last 20 years, most accounts stress large-scale operations waged by states targeting rival military networks and power grids through a mix of espionage and offensive information campaigns. In these scenarios, planes fall out of the sky and entire cities go dark. Yet this vision discounts the prospects of a more indirect and insidious approach: holding a society hostage through targeting its ability to credibly share information and deliver public goods and services online.

This edition of the *On Future War* series combines tabletop exercises, a public survey, and scenarios created with generative artificial intelligence to analyze how cyber threats are evolving. The best prediction of an uncertain future is based on combining expert opinion and public attitudes to visualize and describe cyber operations almost certain to change the character of war.

This installment of *On Future War* uses a novel mix of expert forecasts, public surveys, and future threat scenarios generated by artificial intelligence (AI) to analyze the changing character of cyber campaigns targeting the U.S. federal government. Based on data gathered from six tabletop exercises (TTXs) with over 50 leading cyber experts and foreign policy practitioners, as well as a public survey of over 1,000 participants from across the United States, experts and the public see a cyber future marked by attacks on government services, critical infrastructure, and trust in society itself. The findings highlight a preference among potential adversaries for undermining the United States through cyberattacks that cause widespread disruption in essential services and small businesses coupled with espionage campaigns designed to steal patents and support long-term technological competition. Furthermore, the findings indicate a trend toward using cyber operations to destabilize social order and undermine public trust, particularly in the context of significant political events such as elections and foreign policy crises. This finding points to a future where cyber warfare is not only a tool for direct socioeconomic disruption but also a means to sow discord and manipulate public opinion.

The public survey, modeled on the project's TTX framework, revealed a general lack of clarity and awareness about the U.S. government's cybersecurity funding. It also unveiled a striking gender gap in perceptions: men were considerably more inclined to deem the current cybersecurity funding as sufficient compared to women. Similarly, women exhibited greater concern over the consequences of deepfake technologies compared to men. Furthermore, integrating U.S. Census Bureau and Massachusetts Institute of Technology (MIT) Election Data and Science Lab data with survey results revealed that the political preferences of participants' congressional districts had minimal influence on individual player perceptions and strategies.[1] The research team also controlled and tested environmental socioeconomic variables at the district level—including majority–minority districts by population, household median income, educational achievement, healthcare coverage, and social net benefits—but did not find them significantly impactful on individual player perceptions. In other words, the U.S. public shares a common concern about the future of cyber war that transcends political and regional differences assumed to divide the nation. These ideas echo in Future Lab's recent study on defending the .gov ecosystem.[2]

To address the evolving cyber threat landscape, a multifaceted approach is recommended. First, a comprehensive cybersecurity strategy is essential to protect social services such as the Supplemental Nutrition Assistance Program (SNAP) and Medicaid, particularly during critical events such as elections. The United States cannot risk malign actors holding the most vulnerable U.S. citizens hostage during a major crisis or political transition. Second, enhancing

public awareness and transparency in cybersecurity funding is vital, necessitating extensive educational campaigns and the establishment of an organization for collecting and analyzing cyber statistics. The U.S. government must engage the public with data about threats and trends. An informed polis is more resilient, but currently the U.S. government lacks a coherent, data-driven collection of cyber statistics to inform the private sector and general public.

The U.S. government is unlikely to mobilize sufficient attention and resources if it does not invest in public-facing data, a lesson learned long ago with respect to economic statistics. Additionally, fostering real-time information sharing among federal agencies and the private sector is key to a cohesive cyber defense strategy and maintaining public trust. With a pool of data, the government can make forecasts about future threats and better align federal resources, including money, labor, and technology.

The Changing Character of Cyber Warfare

While scholars and practitioners once perceived cyber operations as decisive battlefield instruments that heralded a new way of war, the reality has proved to be different.[3] States are increasingly crafting multifaceted cyber strategies that incorporate coercion and a blend of mis-, dis-, and malinformation campaigns. In place of traditional military operations, more espionage and information operations are taking place.[4] As cyber strategies evolve beyond conventional military tactics and traditional espionage, there appears to be a marked shift in focus toward critical civilian infrastructure, reflecting a strategy aimed at exploiting the interconnectedness and vulnerabilities of modern societies.[5]

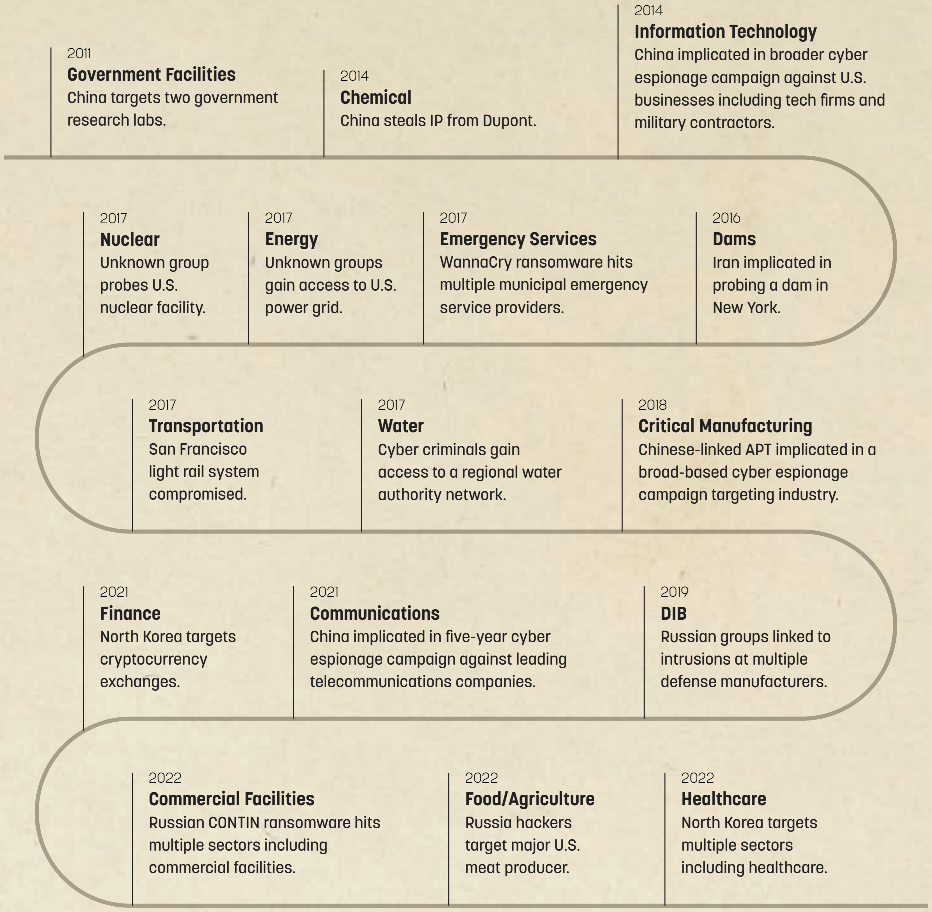
Critical Infrastructure

The traditional focus on military and intelligence targets in cyber operations has expanded to encompass a broader spectrum of targets, including civilian critical infrastructure. This shift represents a strategic move toward countervalue targeting, where the aim is to undermine governments by digitally taking citizens hostage, thereby changing the character of the threat environment.[6] For instance, the Volt Typhoon espionage campaign by the Chinese Communist Party in 2023 targeted critical infrastructure networks through a service provider, demonstrating the strategic value placed on these targets.[7] Similarly, on December 23, 2015, Ukrainian energy firms suffered unexpected blackouts affecting vast customer areas, alongside reports of malicious software in various essential service sectors. Technical investigations revealed the presence of BlackEnergy malware on their systems, though its exact contribution to the incidents remains under scrutiny.[8]

Countervalue targeting inverts decades of military strategy and introduces a new form of cyber warfare that threatens the very foundations of civilian life. The focal point is the critical infrastructure of modern states, which is integral to the welfare of its citizens. These sectors have emerged as key battlefields in cyberspace. In fact, according to the Dyadic Cyber Incident and Campaign Dataset, states are 4.5 times more likely to see a rival target the non-security agencies of their government and the private sector than their military and intelligence agencies.[9] This type of cyber operation is especially alarming because it threatens to severely disrupt everyday civilian services.

The increasing frequency of indiscriminate ransomware attacks across critical infrastructure sectors underscores countervalue targeting and vulnerabilities to civilian services.[10] For example, the 2017 WannaCry ransomware attack, which rapidly disseminated across the United Kingdom's National Health Service, had a highly specific and targeted nature and impacted multiple municipal emergency service providers. The convergence of digital and critical infrastructure networks opens new vulnerabilities, transforming these sectors into attractive targets for adversaries aiming to inflict economic and societal damage.[11]

Figure 1: Cyber Critical Infrastructure Targeting



2011
Government Facilities
China targets two government research labs.

2014
Chemical
China steals IP from Dupont.

2014
Information Technology
China implicated in broader cyber espionage campaign against U.S. businesses including tech firms and military contractors.

2016
Dams
Iran implicated in probing a dam in New York.

2017
Emergency Services
WannaCry ransomware hits multiple municipal emergency service providers.

2017
Energy
Unknown groups gain access to U.S. power grid.

2017
Nuclear
Unknown group probes U.S. nuclear facility.

2017
Transportation
San Francisco light rail system compromised.

2017
Water
Cyber criminals gain access to a regional water authority network.

2018
Critical Manufacturing
Chinese-linked APT implicated in a broad-based cyber espionage campaign targeting industry.

2019
DIB
Russian groups linked to intrusions at multiple defense manufacturers.

2021
Communications
China implicated in five-year cyber espionage campaign against leading telecommunications companies.

2021
Finance
North Korea targets cryptocurrency exchanges.

2022
Commercial Facilities
Russian CONTIN ransomware hits multiple sectors including commercial facilities.

2022
Food/Agriculture
Russia hackers target major U.S. meat producer.

2022
Healthcare
North Korea targets multiple sectors including healthcare.

Source: CSIS Futures Lab. Originally published in Jensen et al., *CISA's Evolving .gov Mission: Defending the United States' Federal Executive Agency Networks* (Washington, DC: CSIS, October 2023), https://www.csis.org/analysis/cisas-evolving-gov-mission-defending-united-states-federal-executive-agency-networks.

Political Warfare

Political and cognitive warfare have emerged as recent themes in the literature on modern conflict, reflecting the strategic evolution of cyber operations.[12] Research has examined how the manipulation of digital information ecosystems, particularly through "fake news," disinformation, and online manipulation, poses significant threats to trust in democratic institutions and processes.[13] This manipulation is not merely an act of disinformation, but a strategic component of political warfare designed to influence and control public perception.

Political warfare has evolved with the digital age, becoming a tool for states to achieve objectives without open conflict. Cyber operations against critical infrastructure are now part of this strategy. These actions undermine trust in democratic processes and can sway public opinion through "fake news," disinformation, and online manipulation. Cyberattacks on infrastructure serve a dual purpose: they cause immediate disruption and exert long-term psychological impact, aligning with political warfare aims. Cognitive warfare specifically targets the way people think, influencing their actions during sensitive times such as elections.[14] This form of warfare uses the global reach of digital technology to manipulate collective intelligence. By changing perceptions, adversaries can weaken the credibility of governments and destabilize societies from within.

Cyber operations have thus become a critical component of political and cognitive warfare. By disrupting essential services, attackers can magnify societal divisions and erode trust in public institutions, potentially manipulating the political landscape to their advantage. This is exemplified by Russia's cyber activities, where such operations are viewed not only as a breach of digital security but as an active measure in a broader campaign of political warfare.[15] The targeting of critical infrastructure through cyber operations becomes a tool to exacerbate existing societal divisions, weaken trust in public institutions, and ultimately alter the political landscape to favor the attacking state's objectives.

From Trends to Games, Scenarios, and Surveys

Understanding how these trends shape the future of cyber operations and deterrence requires pivoting from policy analysis by case study to more diverse, multi-method assessments of twenty-first-century strategic competition. Methods such as games and public surveys provide a way to compare expert assessments and attitudes among the general population. These approaches provide valuable insights into the strategic logic behind various types of cyberattacks, their impact on government services, and the necessary measures required to strengthen cybersecurity. Furthermore, public surveys can help shed light on the general awareness and perceptions of cybersecurity threats, highlighting gaps in public education and government communication.

Using generative AI to build scenarios offers a novel mechanism for synthesizing findings and supporting policy analysis. AI-generated scenarios—especially when fine-tuned and calibrated—offer a method for turning preliminary research findings into narrative, slice-of-time scenarios. This combination of human insight and machine synthesis is a key component of the ongoing research relationship between the CSIS Futures Lab and ScaleAI.[16] The ongoing research explores the human-machine interaction and its effect on scenario building.

Would You Like to Play a Game?

To analyze how experts in cybersecurity assess emerging threats and approach cyber strategy, the researchers in the CSIS Futures Lab designed a TTX entitled Shadow Table. Shadow Table had these experts assess the optimal targets for holding the United States hostage during the upcoming 2024 U.S. presidential election, including recommendations for hypothetical state and non-state actors. Unbeknownst to the participants, they were randomly assigned to different groups based on how the U.S. government would seek to counter their selected strategy. As a result, the design captured adversary feedback loops while increasing the ability of the researchers to collect data on the underlying strategic logic, target preferences, and resource allocations of would-be attackers (i.e., the ends, ways, and means of cyber strategy).

The CSIS Futures Lab ran Shadow Table virtually with six separate groups totaling 55 participants. In each session, participants included experts in cybersecurity and cyber strategy, ranging from public and private sector chief information security officers (CISOs) to academics and national security experts. During each session, the participants played two scenarios covering major threat vectors: (1) advise a major nation-state and (2) advise a non-state actor network. In each scenario, participants could select the malign actor they wanted to advise, with states including

China, Russia, Iran, and North Korea and non-state actors including right-wing extremists, left-wing extremists, and criminal groups. As a result, researchers in the CSIS Futures Lab could compare and contrast different state and non-state approaches while controlling for actor type and assess motivations through a mix of data capture and moderated discussions. Put simply, the games were built to capture strategic preferences and examine how experts anticipate malign cyber actors might target the United States during the upcoming 2024 U.S. presidential election.

During the state and non-state scenarios, players gave recommendations on how best to undermine U.S. elections by targeting public services administered by the federal government. These services span a broad range, encompassing essential basic needs such as food and medical assistance to economic programs such as farm loans and critical research conducted by universities and national research institutes. Specifically, players first selected how much time and effort they recommended allocating toward building malware targeting federal programs and services in three areas: (1) the provision of basic needs, (2) small and medium-sized businesses, and (3) science and technology. Second, players recommended their preferred attack method for each, recommending how to allocate a finite set of resources among four methods: (1) low-cost deepfakes, (2) low-cost disruption, (3) espionage, or (4) higher-cost, more complex degradation. Of note, these attack methods are linked to commonly accepted categories used in academic studies on cyber strategy.[17] By forcing players to allocate scarce resources against different attack targets and methods, the game captured how experts approach cyber strategies designed to disrupt core government services during a key political transition.

Cyberattack Methods

Deepfakes: The creation of fake images, text, and videos designed to skew public perception.

Disruption: Low-cost, temporary operations that deface websites or lead to temporary denial of service.

Espionage: Stealing sensitive information and creating access for future cyberattacks.

Degradation: More complex attacks that shut down core functions, destroy data, or take networks offline for a longer period of time.

Based on this design, Shadow Table served as a forum to both discuss strategy and capture statistical data on preferences. The use of TTXs as a quantitative approach to inform decisionmaking processes is an established line of practice dating back to the nineteenth century.[18] The game design used in Shadow Table reflects emerging trends in analytical wargaming that adapt simulations to capture data in a manner that supports evidence-based policy recommendations.[19] It expands the application of these methods from international to domestic crises, blending traditional elements such as comparing expert-vs.-public outcomes and statistical analysis with new dimensions such as electoral periods and socioeconomic factors.[20] The methodology allows for creative self-selection by participants, focusing on their perception of roles and objectives as a mechanism for identifying different strategic approaches.[21] This approach facilitates a quantitative analysis of political and cognitive warfare by these actors, drawing on political psychology in international relations.[22]

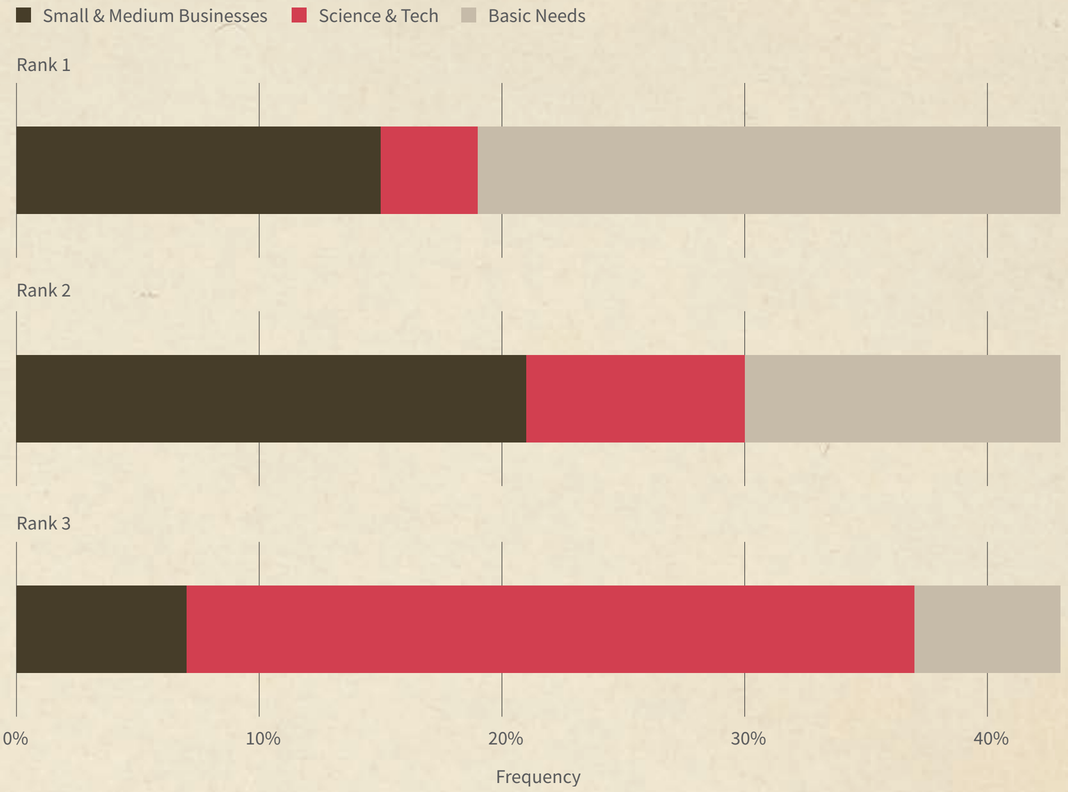
Shadow Table Findings

Overall, experts selected the option to disrupt basic needs more than other targets, and the preference was statistically significant in both the state and non-state threat scenarios.[23] Figures 2.1 and 2.2 illustrate expert targeting preferences most likely to disrupt trust and confidence in the U.S. federal government during a key political transition such as an election or during a foreign policy crisis. The majority of experts prioritized attacks on the provision of basic needs, reflecting a strategy to disrupt the lives of civilians and potentially cause unrest during elections. This preference for targeting basic needs was consistent regardless of whether participants were playing as state or non-state actors, underscoring the perceived effectiveness of such attacks in destabilizing the U.S. federal government and its executive agencies. Furthermore, the choice of target indicates that attackers prefer to sow chaos or tap into the deep personal fears of civilians that rely on such basic needs. For example, SNAP food assistance alone serves as a lifeline for over 40 million socioeconomically disadvantaged U.S. citizens.[24] Disrupting food access during an election could catalyze further polarization and even unrest.

During discussions, participants detailed their strategic logic and the utility of targeting basic needs. Experts saw this attack vector as the best placed to create chaos and increase public mistrust in institutions. Furthermore, groups discussed how these attacks—if effective—could lead to protests, unrest, and a loss of trust in the U.S. government's ability to protect basic needs. In addition, experts saw the resulting economic distress and fear amplify public discontent and raise questions about the competence and reliability of government institutions. Expert discussions revealed a prevailing assessment that compromising people's basic needs could also make the population at large more susceptible to dis- and misinformation campaigns, thereby opening up additional vectors for foreign manipulation and radicalization.

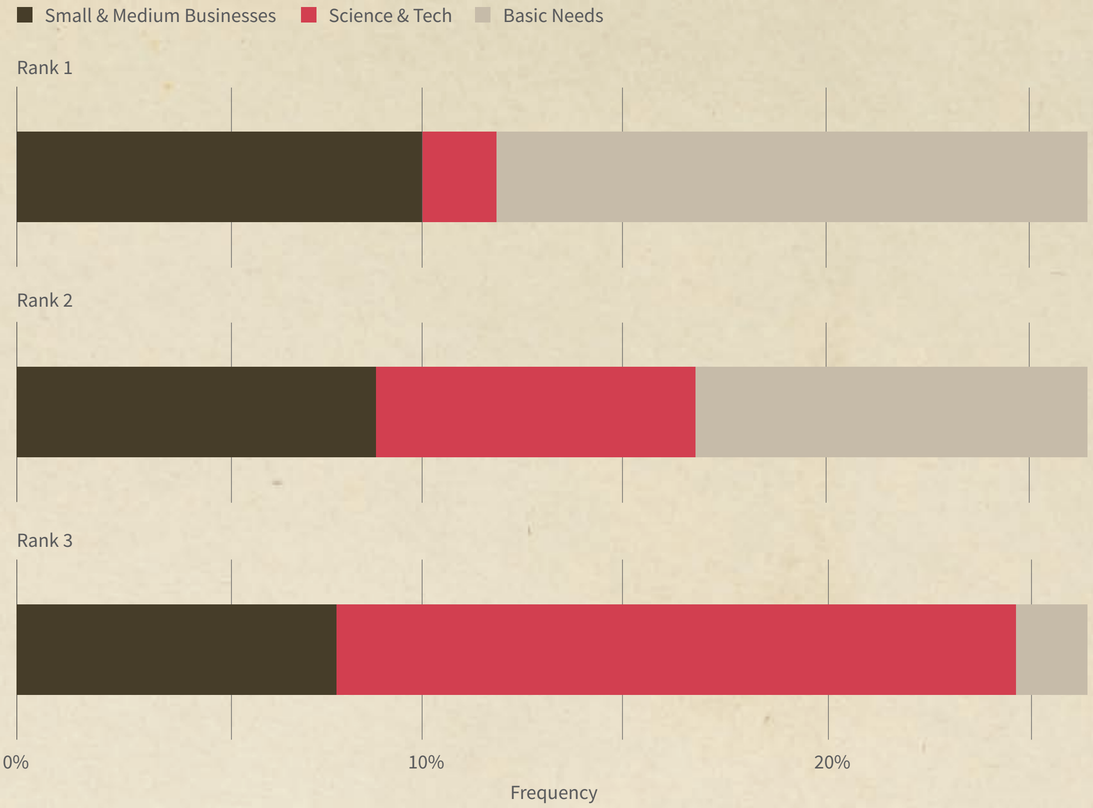
In other words, experts saw targeting vulnerable groups as the best way to undermine the U.S. government.

Figure 2.1: Non-state Actor Targeting Preferences



Source: CSIS Futures Lab. Originally published in Jensen et al., *CISA's Evolving .gov Mission: Defending the United States' Federal Executive Agency Networks.*

Figure 2.2: State Actor Targeting Preferences



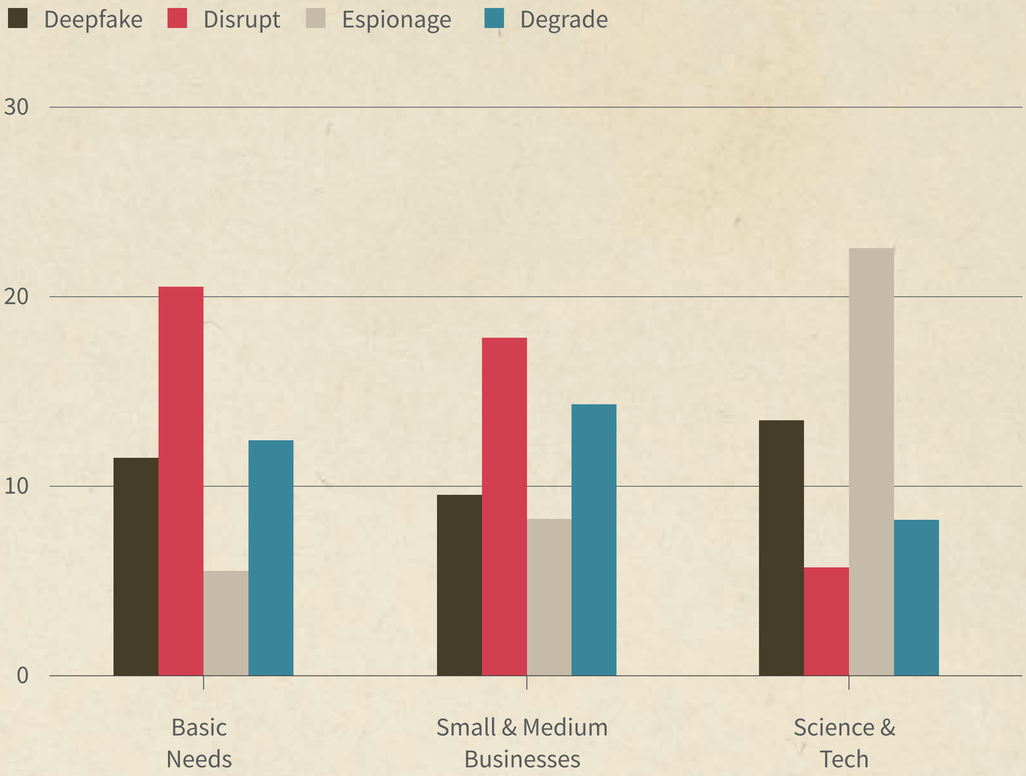
Source: CSIS Futures Lab.

In addition, experts noted opportunities for sowing chaos by targeting federal agencies supporting small and medium-sized businesses. For example, targeting federal grants administrated through agencies such as the Small Business Administration could produce a cascading economic effect. In 2023, the agency delivered over $50 billion in assistance, with much of it focused on underserved communities that experts perceived as likely to amplify political discord.[25] Even more disturbing, cyberattacks that manipulated economic data produced by the U.S. Departments of Labor and Commerce could easily cause disruption to financial markets that rely on credible government statistics.[26] Experts saw federal agencies that support economic activity as being most susceptible to cascading effects, with even small intrusions creating fear and panic likely to undermine trust and confidence in the federal government. The participants shared a perception that such attacks would not only cause direct harm but also create a domino effect, impacting the economy and increasing public discontent.

In addition to target preferences, researchers in the CSIS Futures Lab analyzed how experts allocated resources to different attack types across the two scenarios. To capture this data, the TTX forced players to allocate notional resource points across four potential cyberattack methods: (1) the use of deepfakes to alter public perception, (2) low-cost disruptions (e.g., website defacement and limited denial-of-service attacks), (3) espionage campaigns designed to steal data and gain access for future attacks, and (4) more complex degradation attacks capable of shutting down entire networks or services.

As seen in Figure 3.1, when analyzing non-state attack vectors, experts had a fairly balanced approach outside of deepfakes and had preferences for conducting espionage against agencies involved in science and technology. During the discussions, participants assessed that unlike traditional state-based cyber operations, their espionage preference with respect to non-state actors was more about extracting information for follow-on mis-, dis-, and malinformation campaigns linked to the use of deepfakes. By compromising scientific data or spreading misinformation, adversaries could increase doubt in government policies and actions, leading to public confusion and weakened trust in the current presidential administration. Participants acknowledged the role of science and technology in responding to national emergencies and health crises, such as the Covid-19 pandemic. They saw the potential to undermine public trust in government responses by targeting and distorting scientific data related to vaccination efficacy, treatment protocols, or disease spread. Participants noted that adversaries could amplify existing controversies, such as those surrounding climate change or vaccinations, to intensify polarization and create a society where truth is obscured.

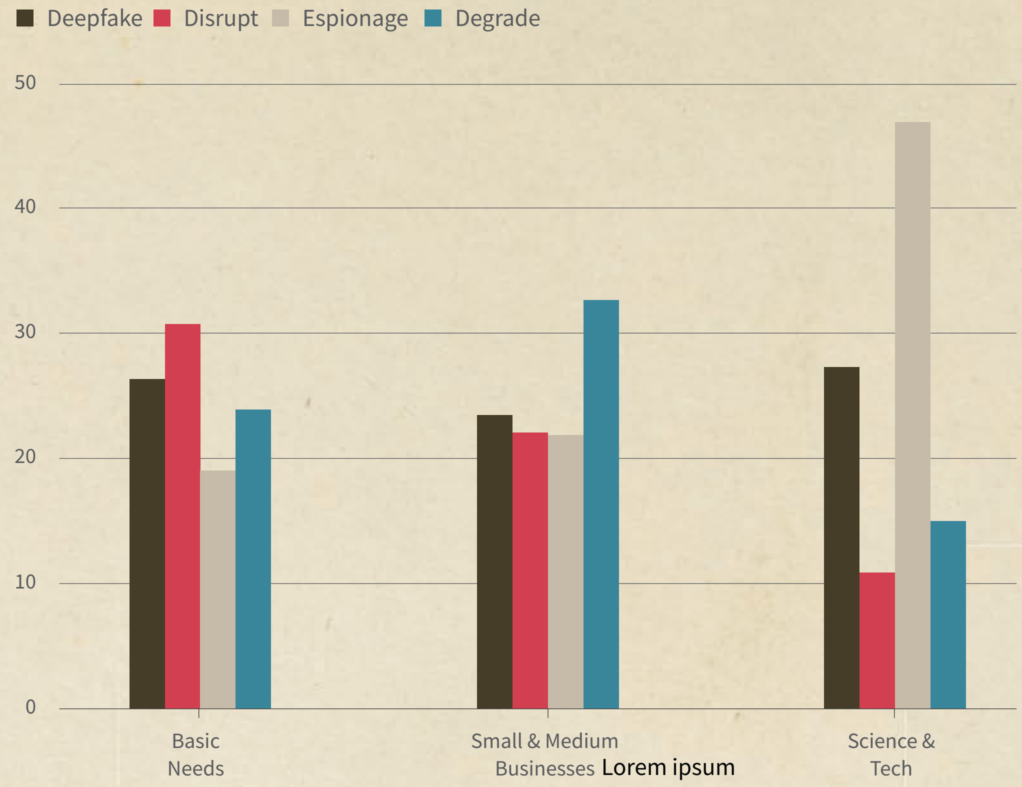
Figure 3.1: Non-state Actor Cyberattack Type Preferences



Source: CSIS Futures Lab. Originally published in Jensen et al., *CISA's Evolving .gov Mission: Defending the United States' Federal Executive Agency Networks.*

As seen in Figure 3.2, when participants analyzed optimal targets for state actors, they adopted a similar set of preferences. Experts see espionage as a tool to win long-term technology competition with authoritarian states eager to steal intellectual property (IP), a finding that parallels previous CSIS research efforts.[27] Second, while disruption was the preferred attack method for basic services and agencies supporting small and medium-sized businesses, experts assumed that states such as China, Russia, Iran, and North Korea would invest more effort in disrupting basic services. This was consistent across the state and non-state actor scenarios.

Figure 3.2: State Actor Cyberattack Type Preferences



Source. CSIS Futures Lab. Originally published in Jensen et al., *CISA's Evolving.gov Mission: Defending the United States' Federal Executive Agency Networks.*

Looking across the games, it is clear that experts see vulnerabilities in the federal agencies. These experts see viable attack options for authoritarian states seeking to create chaos during an election by disrupting the delivery of food and medical care to vulnerable populations and distorting economic data and assistance to U.S. businesses. They see non-state actors as eager to launch similar campaigns but leverage mis-, dis-, and malinformation to further polarize the country by distorting public health research. This attack logic speaks to the importance of federal services and associated critical infrastructure and how these critical requirements for modern society are also critical vulnerabilities if left unprotected.

From Games to Public Surveys

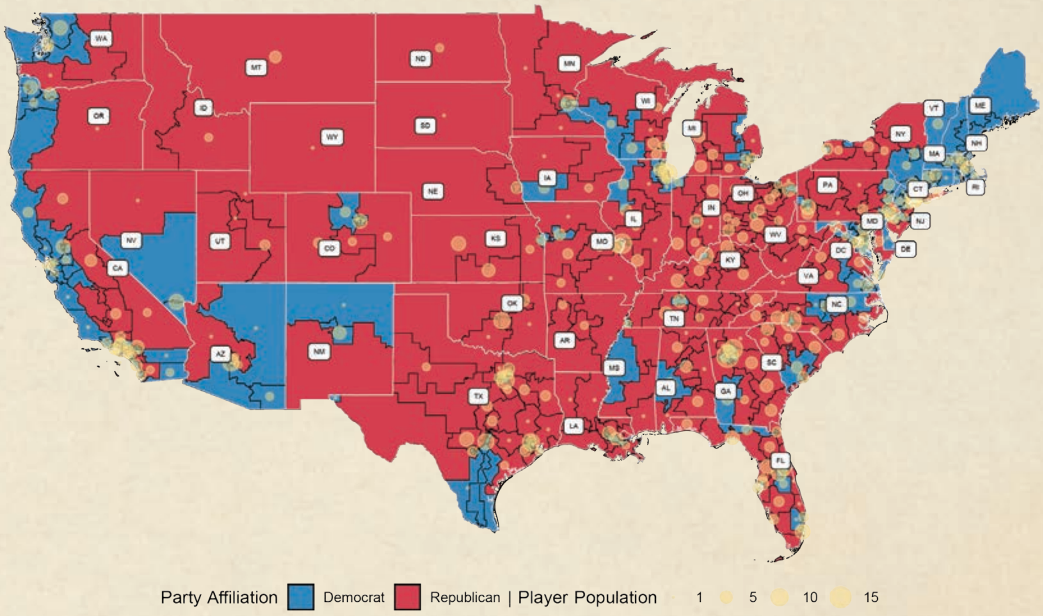
To compare observations from experts gathered during the TTX with the general public, researchers at the CSIS Futures Lab converted the game into a public survey using the online platform Prolific. The researchers ensured that the participants were from sufficiently diverse backgrounds and geographic locations to reflect the demographic makeup of the United States.[28] In adapting Shadow Table, the research team also built in attention checks and only recorded responses where the respondents passed these checks.[29]

Like the original TTX, participants were randomly assigned into either a state or non-state malign actor group and asked to make recommendations about their preferred target (i.e., basic needs, small and medium-sized businesses, or science and technology) and method (i.e., deepfakes, disruptions, espionage, or degradation). Unlike the expert TTX, the researchers did not have the general public weight assign resource values to their attack methods, given that the general public was likely to be less familiar with cybersecurity and foreign policy issues. Thus, when juxtaposing the outcomes from both expert and public samples, the research team focused on their initial choices. These choices reflect how different groups image cyber strategy preferences of malign actors.

Participants were presented with descriptions of two types of cyberattacks. The first was a conventional distributed denial-of-service (DDoS) attack, while the second involved the use of deepfakes and disinformation to tamper with health records. When asked which type of attack was more worrisome, respondents indicated that the attack involving deepfakes was of greater concern than the traditional DDoS cyberattack. Deepfakes are emerging as a significant concern in cyber warfare tactics. This was supported by the TTX, which highlighted that deepfakes are increasingly used to spread hostility and disrupt societal harmony for political gains. These digitally manipulated videos or images can convincingly depict individuals saying or doing things they never did, thereby posing unique challenges in ensuring information authenticity and maintaining trust.

To deepen the understanding of participant preferences, the research integrated U.S. Census Bureau data from the 2021 American Community Survey five-year estimate, providing socioeconomic and geometric details at the congressional district level.[30] In addition, the researchers integrated data from the MIT Election Data and Science Lab, focusing on congressional elections.[31] As seen in Figure 4, the player sample is distributed across the continental United States. The player population can be observed through its density, whereby increments increase the size of each circle. In addition, this map is colored by party affiliation for each district as of the 116th Congress (2019–20). The color schemes follow blue for Democratic districts and red for Republican districts. As the map shows, the sample is geographically and politically representative of the U.S. population.

Figure 4: Public Survey Player Population by 116th Congress Districts



Source: CSIS Futures Lab analysis based on "American Community Survey 5-Year Data (2009-2022)," U.S. Census Bureau, December 7, 2023, https://www.census.gov/data/developers/data-sets/acs-5year.html; and "Data," MIT Election Lab + Science Lab, https://electionlab.mit.edu/data.

The final dataset included players' congressional district information; socioeconomic variables on race, income, healthcare coverage, social net benefits, and poverty; and MIT election data, confirming that the survey was geographically representative of the U.S. population. At a granular level, zip code analysis was also conducted, but results did not deviate from the orginal analysis at the congressional district level. The detailed statistical results are available in the accompanying methodology annex.

Findings

Overall, the public thinks that the most likely states to target U.S. federal agencies and critical infrastructure are Russia and China. Similar to the experts, they see these states as focused on disrupting how the U.S. federal government and executive agencies distribute basic services such as food and medical assistance and as likely to use deepfakes to undermine trust in institutions.

As seen in Table 1, both experts and the public view Russia and China as the predominant authoritarian states interested in undermining U.S. public institutions. Similar to the TTX, the public survey started with adopting an adversary role (either state or non-state). Participants were tasked with selecting the entities in both categories. Experts that engaged in the virtual TTX leaned more toward Russia (57 percent), while the public favored China (47 percent). Apart from this divergence, results show that experts and the public converge on similar preferences.

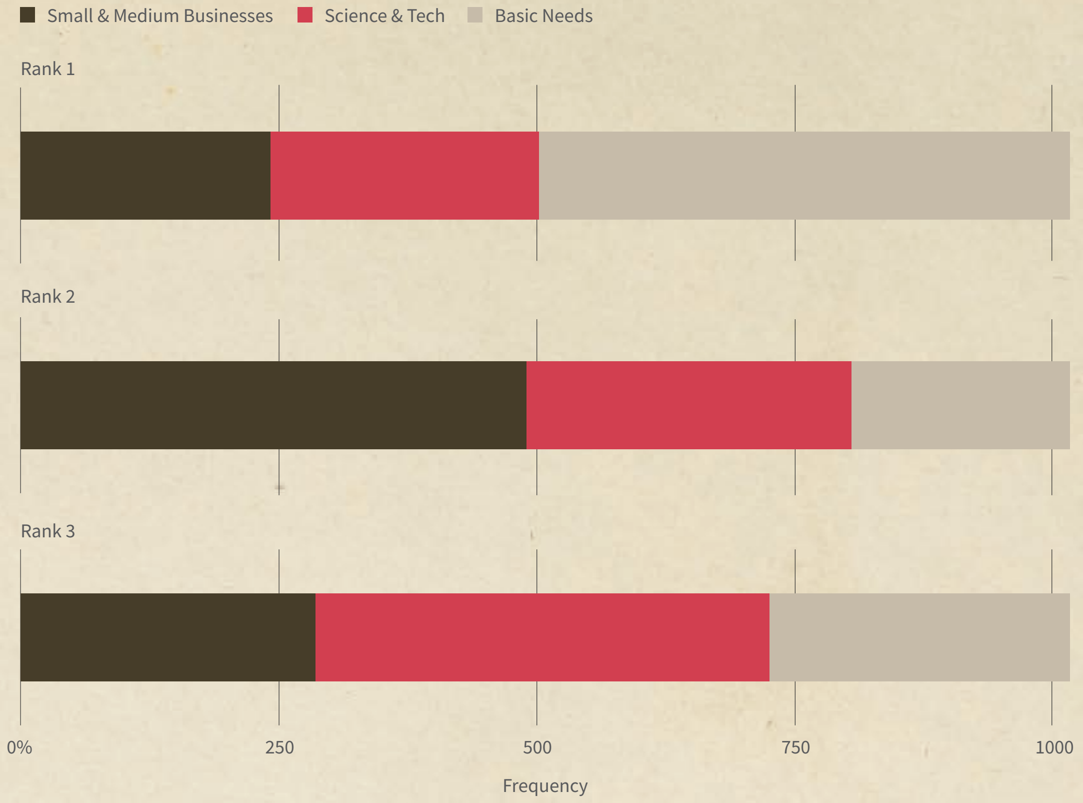
Table 1: Comparing Attacker Choices

Grouping	Entity	Experts	Public
State	China	37%	47%
	North Korea	0%	10%
	Russia	57%	41%
	Iran	6%	2%
Non-state	Right-Wing Group	42%	38%
	Left-Wing Group	10%	9%
	Financially Motivated	46%	43%
	Lone Wolf	2%	10%

Source: CSIS Futures Lab. Originally published in Jensen et al. *CISA's Evolving .gov Mission: Defending the United States' Federal Executive Agency Networks.*

The general public is worried about Russia and China and sees these states as most likely to target federal executive services and critical infrastructure linked to basic needs. As seen in Figure 5, 49 percent of participants selected basic needs as their first choice overall. These findings are consistent with the expert TTX observations in which players identified disrupting basic services as the optimal mechanism for causing chaos sufficient to undermine trust and confidence in the U.S. government during an election and, by extension, future foreign policy crises. In other words, the traditional defensive advantages provided by the United States' geography, including separation from adversaries across oceans, is fading fast as malign actors seek ways of launching attacks through cyberspace against core government functions and critical infrastructure.

Figure 5: Public Federal Service Targeting Preferences

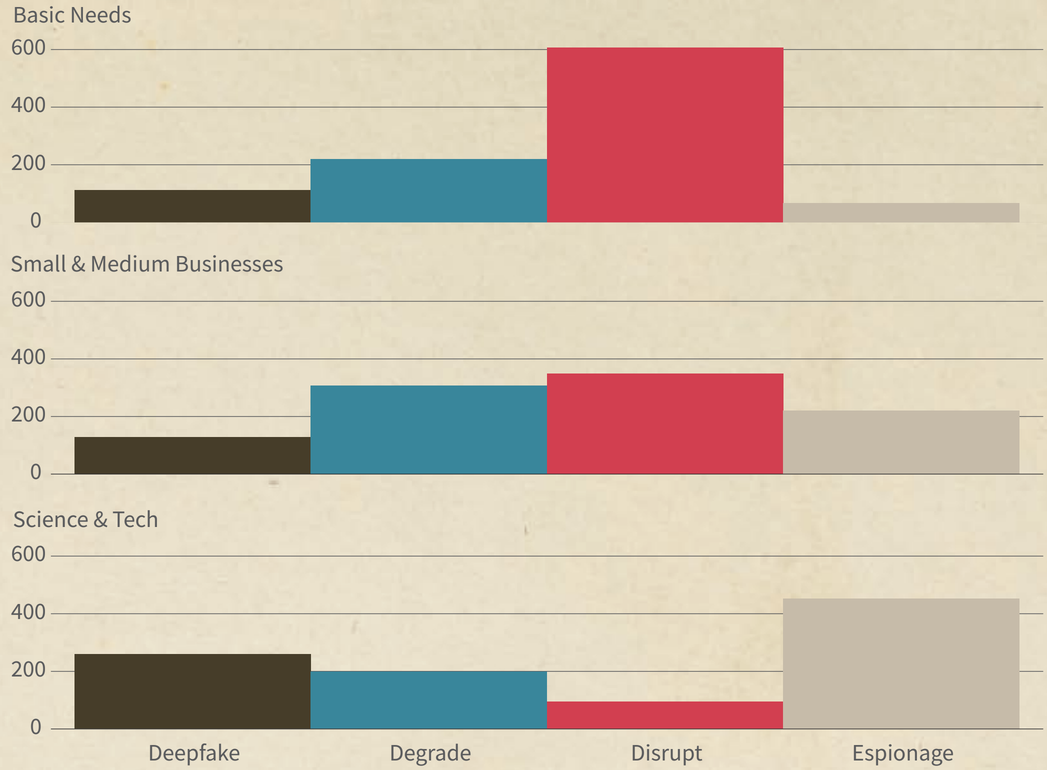


Source: CSIS Futures Lab.

Strategy—the alignment of ends, ways, and means—proved consistent between expert TTXs and the survey of the general public. Both groups prioritized low-cost cyber disruptions against federal agencies and critical infrastructure linked to basic needs and deepfakes linked to science and technology. Figure 6 shows that 60 percent of participants chose to disrupt when targeting basic needs, and 28 percent chose deepfakes when targeting services related to science and technology. The shared preference for using deepfakes to target science and technology is consistent with documented disinformation campaigns during the pandemic that had polarizing effects.[32] In other words, it is not just basic services and critical infrastructure that are vulnerable and at risk during political transitions and crises. Malign actors at home and abroad will target the very foundations of scientific truth.

Based on the public survey, there are clear differences in how different genders and demographic cohorts' approach cyber strategy. Men are less concerned about deepfakes and believe the government is allocating enough money to cybersecurity. For example, men were 48 percent more likely than women to believe that current spending is sufficient. These concerns are not affected by median household income or party preferences. In other words, gender differences can predict cyber strategy preferences. One possible explanation is that women have disproportionately been victimized by social media and deepfakes, including revenge porn and fabricated images, which likely shapes how they view the future of federal cybersecurity. This dark truth translates into the rational calculation for women to be both more concerned about the risks of deepfakes and more likely to want increased U.S. government funding for cybersecurity. Notably, this does not appear to be a partisan issue.

Figure 6: Public Cyberattack Preferences across Targets



Source: CSIS Futures Lab. Originally published in Jensen et al. *CISA's Evolving .gov Mission: Defending the United States' Federal Executive Agency Networks.*

Cybersecurity and Gender

The odds that a man is concerned about deepfakes as a form of political warfare are 27 percent lower than surveyed women. Men are also 48 percent more likely to believe the federal government is allocating sufficient funds for cybersecurity.

Second, age matters. There are clear demographic cohort effects that shape how U.S. citizens see future cyber campaigns designed to hold the .gov ecosystem at risk. Older cohorts (i.e., aged 55 to 64 or over 65) tend to recommend espionage and targeting science and technology more than basic needs and federal services that assist small and medium-sized businesses. The most likely explanation for this divergence is rational. Older Americans, especially those over 65, are more likely to draw on federal programs associated with basic needs, including Medicare and Social Security.[33] Similar to the findings associated with gender, even when survey respondents imagine future cyber campaigns, they tend to avoid targets that would bring them harm in their daily lives. An alternative explanation is that older Americans came of age in an era more defined by public sector basic research and major programs—such as during the Space Race—that they associate with national power and pride. However, both of these explanations are best guesses as to why there are age cohort effects associated with how Americans imagine future malign campaigns designed to hold the nation hostage in cyberspace.

The research team used zip code-level data to conduct robustness checks. The analysis confirmed that gender and age are associated with how groups think malign actors will target the U.S. federal government in cyberspace. Specifically, older cohorts (i.e., aged 55 to 64 and over 65) remain

less likely to target basic services and government programs associated with supporting small and medium-sized businesses. These cohorts are more likely to recommend cyber campaigns targeting science and technology. Factors such as political party affiliation, income levels, and majority-minority districts are not statistically significant. This contrast implies that gender and demographic cohorts play a larger role than political ideology, income, or race and ethnicity in shaping how Americans imagine the risks from cyber operations.

Unlike the district-level analysis, party linkage emerges as possible factors shaping malign cyber strategy preferences in the zip code-level robustness check. In Democratic and mixed political zip codes, participants were less likely to target small and medium-sized businesses. This finding further demonstrates rational preferences by the U.S. public with respect to cyber strategy.

Lastly, political ideology did not appear to alter which rival foreign state participants perceived as likely to hold the U.S. government hostage during the upcoming 2024 presidential election. Where participants live (i.e., Democratic- or Republican-leaning zip codes) did not have an impact on the state actor they selected (i.e., Russia, China, Iran, or North Korea). This finding extends to non-state actors. While one might assume Republican-leaning districts would be more likely to select left-wing groups as the malign actor, and Democrats the opposite, this was not the case. The only difference appeared with respect to non-state actor motivation, with Democrat-leaning zip codes being more associated with "lone wolf" cyber actors as opposed to financially motivated cyberattacks (i.e., cybercrime). This difference may suggest that political ideology shapes how people view opposing group motivations, with Democrat-leaning areas more inclined to see malign activity in cyberspace by non-state actors associated with isolated political radicals.

From Surveys to Scenarios

To visualize and describe the findings from experts and general public TTXs, the research team employed a novel approach to constructing scenarios that drew on generative AI. Specifically, the CSIS Futures Lab loaded the text transcripts from the TTXs, comments from the public surveys, and a corpus of over 300 documents on cyber operations and modern strategy to fine-tune a model using Scale AI's Donovan platform and a retrieval assisted generation (RAG) large language model (LLM).[34]

RAG works to optimize how the base model classifies text (i.e., fine-tuning) and predicts the next logical sequence. By using a select corpus trained on cyber and great power competition, the expectation is that text generated in response to queries is more accurate and aligns with key concepts. This fine-tuning is further enhanced by training the model with the prompts that are based on the emerging themes of TTX discussions. To facilitate this process of refinement and structure prompts given to the LLM, the CSIS Futures Lab defined a series of trends based on analyzing the TTX results. In other words, the model used thousands of pages of texts and transcripts to answer prompts about how discrete trends could comingle to produce alternative futures.[35] The result is a series of "slices-of-time"

A Recipe for AI-Generated Scenarios

- ✓ **Select a base LLM (e.g., ChatGPT, Bard, or Llama).**
- ✓ **Add a corpus of authoritative texts on strategy and critical factors the model can reference.**
- ✓ **Mix in structured observations about ends, ways, means, and feedback loops (e.g., TTX transcripts).**
- ✓ **Garnish with tailored prompts (e.g., using trends and themes to refine questions about alternative futures).**

that provide portraits of alternative futures in which malign actors seek to hold the United States hostage by launching cyber campaigns targeting federal executive agencies and critical infrastructure during political transitions and foreign policy crises.

The use of LLMs in this context is a time-efficient method that enhances understanding but requires skilled handling to avoid biases. In military planning, the effective use of LLMs depends on translating critical thinking and research into structured queries for the AI model.[36] These models complement, rather than replace, human expertise, and military professionals must adeptly convert their knowledge and concepts into AI-interrogable formats. Generative AI, increasingly used in social science, offers significant opportunities and challenges when integrated into wargaming, red teaming, and scenario construction. It can subtly influence crucial leadership decisions and is subject to the "black box" challenge, where the reasoning behind AI-generated outcomes is not always clear.[37] This necessitates ethical governance, transparent methods, and accountability to responsibly manage AI's role in wargaming, a key factor in determining future conflict outcomes.

Societies Held Hostage

The first major trend that emerged from the TTX discussions concerned how interdependence creates new forms of vulnerability. A connected society requires a mix of online government services and critical infrastructure to function. As a result, the disruption of basic needs and polarizing deepfakes (i.e., disinformation) can amplify underlying fault lines in society during political transitions and foreign policy crises.

Differences in State Actors' Strategies

TTX participants pointed out that there are significant differences in the strategies of different state actors. During the TTXs, Russia, for instance, was more engaged in disruptive cyber activities, while China was more focused on strategic and espionage-oriented approaches. This assumption is consistent with academic literature on different state strategies in cyberspace.[38] As a result, cyber defense strategies—in both the public and private sectors—need to adapt to different threat characteristics. This process of adaptation will require access to public data on different threat vectors, including statistics on how new attacks compare to past efforts (i.e., cyber statistics).

Chaos and Instability

An overarching theme was the creation of chaos and instability, especially with the upcoming 2024 election in mind. By targeting critical services and undermining public confidence, state actors could weaken the U.S. federal government's legitimacy and provoke divisive reactions among the population. This focus on windows of political vulnerability highlights a need to ensure there are sufficient resources as well as collaboration with the private sector to deny adversaries the ability to hold the United States hostage during its political transitions or foreign policy crises.

Priority on Disruption and Immediate Impact

The immediate disruption of services and the ensuing chaos was identified as a key strategy that attackers may prioritize. These tactics aim to impact public perception in the short term leading up to the 2024 election. By causing immediate and visible disruptions, the attackers could potentially cause widespread panic and a loss of confidence among the public in the government's capabilities. This emphasizes the need for robust disaster recovery plans and the ability to quickly restore services after an attack.

Cross-Domain Attacks

Another emerging pattern was the idea of cross-domain attacks that not only involve cyberattacks but also physical disruptions. For instance, cyber-physical attacks on critical infrastructure could amplify the overall impact of the attacks, increasing their effectiveness in sowing discord and undermining public confidence. This highlights the need for defenses that extend beyond purely digital assets and can also protect against physical disruptions resulting from cyberattacks.

Based on these dynamics, the CSIS Futures Lab generated the following scenario using Donovan:

Fracturing Trust

In the run-up to the 2024 U.S. presidential election, two distinct trends of cyber activity involving Russian and Chinese actors emerge. Leveraging cyber strategies that have been evident in previous conflicts, Russian state operatives appear intent on fanning the flames of political discord within the U.S. electorate. Concurrently, Chinese state-sponsored black-hat hackers are continuously launching large-scale operations aimed at pilfering unprotected IP databases within the United States.

Russian cyber activities cast a long shadow of a Cold War-style influence operation that deploys strategically crafted disinformation and propaganda campaigns. These campaigns, which are designed to fracture public resolutions and incite social chaos, allude to the tactics used to interfere in the 2016 U.S. presidential election. There appears to be an orchestrated effort to manipulate political perceptions and beliefs in an attempt to shift the electoral landscape in a direction favorable to Russian strategic interests.

China's cyber activities, in stark contrast, possess apparent economic drivers. The IP of the United States, held in the form of patents, methodologies, and blueprints, are the primary focus of these cyber breaches. By syphoning off such data, China could potentially undercut U.S. economic competitiveness on a global platform.

Inevitably, these trends converge, resulting in a dire situation for the United States. The effects of these cyber operations are not restricted to abstract sociopolitical and economic dimensions. Both Russian and Chinese operations have displayed a propensity to target U.S. critical infrastructure, specifically the federal systems that deliver basic assistance programs. Such activities could severely undermine the trust and confidence of U.S. citizens in the government's ability to ensure their welfare.

This scenario is a good example of how these developments could take place in the near future given the vulnerabilities identified during the TTXs and public survey. Of note, the scenario is also the most logical extrapolation from recent trends in cyber operations and great power competition.[39] According to the scenario, the focus of Russian operatives on disseminating disinformation and propaganda to influence public perception and create social chaos is consistent with the document's findings on political and cognitive warfare. Similarly, in line with findings from the TTXs, espionage, particularly in the science and technology domain, has a strategic emphasis on cyber threats. This resonates with the activities of Chinese hackers, which center on IP theft to undercut U.S. economic competitiveness.[40] This scenario shows the need for robust measures

against potential disinformation campaigns using deepfakes and espionage activities against research and development. If the U.S. government cannot find a way to address deepfakes and protect its science and technology enterprise, the country will be increasingly vulnerable and subject to coercion in the twenty-first century.

Gender Dynamics Will Continue to Shape How the Public Views Cybersecurity

The second major trend observed concerns the rise of mis-, dis-, and malinformation. During the TTXs, participants focused on rising threats related to deepfakes and AI. The public survey confirmed these concerns but highlighted a clear divide between how self-identified men and women view the threat of deepfakes. As a result, future campaigns to hold the United States hostage during a political transition or foreign policy crisis are likely to see disinformation campaigns tailored to different segments.

Disinformation and Manipulation of Stolen Data

During the TTXs, there was a debate regarding the effectiveness of deepfakes and disinformation campaigns in swaying public opinion. Some participants argued that these tactics might sow discord rather than significantly change people's minds. This discussion pointed toward the potential for dis- and misinformation campaigns to amplify existing social cleavages. Even small groups with hardened worldviews can amplify disinformation and spread it outside their networks.

The Gender Gap and Utilization of Deepfakes and Disinformation

During the TTXs, participants highlighted how malign actors could use deepfakes to make the government appear incompetent or even outright malicious in delivering essential needs. Combining real information leaks with deepfakes could further erode trust in the government's crisis management capabilities. Additionally, the public survey highlighted how gender and age cohort differences shape how the U.S. public views cybersecurity. This disparity in sensitivity offers adversaries an opportunity to tailor attacks that exacerbate confusion, complicating the development of effective strategies to counter these threats.

Based on these dynamics, the CSIS Futures Lab generated the following scenario using Donovan:

The Gender Divide in Cyber Warfare

Heading into the contentious 2024 U.S. presidential election, extensive studies revealed that women voters expressed far greater concern about potential deepfake videos and manipulated information than men. This gender disparity offered a prime opportunity for exploitation by foreign adversaries keen on disrupting U.S. democracy.

In the months before the election, Russian state-sponsored disinformation campaigns specifically targeted women voters across social media. Fake news stories and doctored videos portrayed female political candidates as corrupt, unqualified, and even mentally unstable. Some deepfake footage depicted female candidates making inflammatory racist and misogynistic remarks. Other manipulated videos showed women lawmakers struggling to respond coherently to basic policy questions. Many appeared designed to prey on gender biases that question women's competency for high office. The goal was to suppress support for female candidates among women voters.

Meanwhile, Chinese cyber operatives stole massive datasets from women's health organizations and services. They threatened to leak sensitive medical records of female patients from Planned Parenthood and OBGYN practices unless demands were met. This sparked fears that hacked personal health information could be used for blackmail or extortion. Patients worried that intimate details about reproductive health, pregnancies, and sexual health could be made public in an attempt to ruin reputations and lives.

In the wake of the election, Russian disinformation tactics continued preying on female voter anxieties. Deepfake videos portrayed female members of the cabinet as inept crisis managers unable to deliver basic government assistance to struggling Americans. Doctored footage showed relief supplies rotting in warehouses due to incompetence as Americans suffered.

Unlike the first scenario, the above vignette shows how generative AI can help visualize alternative futures based on critical outcomes. AI is not magic. It is math. And the integration of datasets on strategy, net assessment, and cyber operations, alongside transcripts from the games, alters how the underlying model weights different text combinations to write the story. This story is best characterized as a "what if" scenario and a demonstration of how a particular outcome—regardless of party—intersects with observed patterns and trends in cyber operations as they relate to disinformation. Here the model assumes that a woman—regardless of party—wins the 2024 presidential election, a prospect current polling suggests as unlikely but not impossible. Rather than interpret the results as forecasts about elections, the better perspective is to use the fictional future scenario as a foundation for discussing how authoritarian states are and will likely continue to target gender fault lines in the United States.[41] This focus of discontent could create new preferences for how malign actors will seek to target federal executive agencies and critical infrastructure, with a particular focus on health and human services as well as medical providers highlighted in the scenario.

Distrust in Government Will Continue

The third major trend observed across the TTXs and public survey responses concerns the declining trust in government across democratic societies and the United States, in particular. There was an underlying assumption across different groups that free people currently experience a trust deficit. According to a recent Pew Research, the U.S. trust in the federal government decline from 73 percent in 1958 to 16 percent in 2023.[42] A second major trend observed concerns the rise of mis-, dis-, and malinformation. During the TTXs, participants focused on rising threats related to deepfakes and AI. The public survey confirmed these concerns but highlighted a clear divide between how self-identified men and women view the threat of deepfakes. As a result, the future campaigns to hold the United States hostage during a political transition or foreign policy crisis are likely to see such campaigns tailored to different segments.

Disrupting State and Local Elections

Participants in the TTX underscored the value of targeting state and local election systems, perceiving them to be more vulnerable to cyberattacks. Such attacks could disrupt the electoral process and weaken faith in the democratic system. More important, this reflected a desire to sow discontent by making it appear that every local disruption was a function of systemic issues at the federal level.

Espionage and Long-Term Goals

Across the TTX and public surveys, participants saw espionage as more than just a means to steal information and technology. They also saw it as a way to undermine trust in government, as Americans perceived each new breach as a sign of a breakdown of sovereignty and the ability of the federal government to safeguard U.S. innovation and the personal information its citizens. This desire to steal IP and undermine trust was seen by participants as a long-term goal beyond any one political transition or foreign policy crisis.

Propaganda by Deed

A nineteenth- and twentieth-century tactic of using protests, terrorist attacks, and other subversive deeds to catalyze further unrest and even open revolt. The idea is closely linked to revolutionary theory and the concept of a "foco" used by Che Guerva. The concept has been used by modern terrorist organizations and is increasingly associated with far right-wing and Islamic extremists.[53]

Importance of Insider Threats[43]

The threat posed by insiders, whether intentional or accidental, was a key point in the TTX discussions. Participants noted that insiders, whether in the United States or other countries, could potentially compromise federal networks. This highlights the need for a holistic approach to cybersecurity that goes beyond protecting against external threats and also addresses the potential risks posed by insiders. It also shows how the breakdown in trust creates new threat vectors as disenfranchised citizens look for new forms of protest and "propaganda by deed."[44] This threat parallels the broader phenomenon also on display in the rise of activities such as swatting involving federal or local elected officials, which involves falsely calling in SWAT teams to a' residence.[45]

Strategic Timing

The TTX discussions also pointed to the importance of timing in launching cyber operations designed to undermine trust and confidence in the U.S. government. The participants noted that attackers are likely to time their attacks to coincide with critical events, such as elections or other moments of national significance, to maximize their impact and influence public sentiment. This underlines the need for heightened vigilance during such periods and the importance of having contingency plans in place. It also suggests that cyber operations have become a form of propaganda by deed in networked societies.

Based on these dynamics, the CSIS Futures Lab generated the following scenario using Donovan:

Chaos at the Ballot Box

The 2024 U.S. presidential election highlights intensifying cyber threats seeking to undermine democracy and national security. Russian hackers disrupt local election systems and infrastructure, timing attacks for maximum impact. Chinese operatives focus on espionage targeting confidential data to advance long-term strategic interests. Meanwhile, insider threats pose increasing risks of unauthorized disclosures and system compromises.

> Prior to the election, a disgruntled federal contractor with access to classified systems leaks troves of confidential documents revealing the government's cyber capabilities and gaps. Adversaries gain insight, enabling more successful future attacks on exploited weaknesses.
>
> Weeks before the 2024 election, ransomware strikes voter registration databases in six key battleground states right before registration deadlines. Chaos ensues at local election offices as critical voter rolls are locked down. Tens of thousands lose the ability to update their registration status, request absentee ballots, or fix errors ahead of election day.
>
> On election day, reporting systems crash in counties across swing states, delaying results. Claims of voter suppression and fraud spread. Protests form amid the uncertainty calling the election's integrity into question.
>
> Throughout the election, Chinese hackers steal datasets from both political parties and all levels of government. In the long term, this facilitates future blackmail and enormous economic advantage from pilfered trade secrets, IP, and proprietary research.

Like the second scenario (The Gender Divide in Cyber Warfare), the above vignette shows how generative AI can help visualize alternative futures based on the convergence of key trends. Here the prompts based on trends observed during the TTXs change how the model weights words and their sequence to write a dystopian story.[46] Like wargames, these scenarios are not predictive as much they are illustrative, a helpful mechanism for catalyzing policy debates and security assessments.[47] As a result, the story is a gateway to a larger set of stress tests and red-teaming efforts required to identify vulnerabilities that a mix of foreign states and insiders could use to attack federal agencies and critical infrastructure.

Policy Implications

A connected society is as vulnerable as it prosperous. Each connection creates possibilities for exchanging goods and ideas but opens a vector for spreading malware and holding the entire system hostage. As a result, modern resilience starts with cybersecurity and ensuring that the federal government and critical infrastructure are sufficiently protected from both foreign and domestic threats. Seen in this light, the following policy recommendations warrant further debate and considerations based on the findings from the TTXs, public survey, and generative AI scenarios.

Charting a Path toward Comprehensive Cybersecurity for Essential Services

A major finding across all the games, surveys, and scenarios was that future cyber threats will increasingly target the basic needs provided by the federal government as a way of holding the United States hostage during political transitions and foreign policy crises. Traditionally, cyber defense focused on sensitive military and intelligence infrastructure, but this observation changes the logic. Increasingly both federal CISOs and actors such as the Cybersecurity and Infrastructure Security Agency (CISA) will need to prioritize protecting services such as providing food and healthcare to large segments of the U.S. public. These ideas echo the larger recent study on defending the .gov ecosystem.[48] Furthermore, this new focus on public needs will likely require expanding core programs such as threat hunting to include more active red teaming and dynamic consequence management exercises that include stress testing how best to engage the public during a cyber crisis.

Addressing Gender and Age Dynamics in Cyber Threat Perception

The fact that gender and age are playing a significant role in shaping perceptions of cyber threats—particularly in the context of misinformation campaigns—means the federal government has to change how it assesses threats and communicates with the U.S. public. Women's heightened concern about deepfakes and misinformation calls for targeted strategies to address and counter these threats that will likely involve working with private sector social media companies.[49] More generally, CISOs across the federal government, and CISA in particular, will need to incorporate gendered perspectives into cybersecurity policies and awareness campaigns. This could involve conducting gender-specific studies to understand varying threat perceptions and developing tailored public awareness initiatives that address these concerns. By acknowledging and addressing gender-based and age-based differences in cyber threat perception, public communication strategy can become more effective in countering misinformation campaigns and preventing societal divisions.

Enhancing Public Awareness and Transparency in Cybersecurity Funding

The apparent lack of public awareness about government funding and efforts in cybersecurity underscores the need for transparent and persistent communication strategies. The federal government must actively engage with the public to explain the complexities of the cyber threat landscape and the importance of resilience building. This recommendation involves not only investing in robust cybersecurity measures but also in extensive public education and information campaigns.[50] By improving public understanding and involvement in cybersecurity matters, governments can strengthen societal resilience against cyber threats and ensure a more informed and cooperative approach to national cyber defense.

Funding an Entity to Collect, Analyze, and Share Cyber Statistics

There were expert debates and disagreement across demographic cohorts about whether or not the U.S. government sufficiently resources cybersecurity. This divergence likely speaks to a larger issue: the public does not understand the full extent of the threat and experts are often lost in debating different aspects. There is no, single credible source of information about cyberattacks in the same way that there are public databases on everything from weather patterns to crime statistics to economic data. It should come as no surprise that large segments of the U.S. population see a threat but struggle to understand what the right balance of ways and means is to reach the goal of secure online services and critical infrastructure. Therefore, the U.S. government—whether in the Office of the Cyber Director or CISA—needs to establish an outlet for publishing cyber statistics. This effort should build on new public and private sector data pooling initiatives and ensure cyber dashboards are as accessible to a woman in rural Kansas as they are to a federal CISO in Washington. With a pool of data, the government can make forecasts about future threats and better align federal resources, including money, labor, and technology. This will allow the government to better inform the private sector and general public about the cyber threats and cybersecurity measures.

Conclusion

The shape of the threat is clear. As science fiction writer William Gibson puts it, "The future is already here, it is just not evenly distributed." The United States has already seen massive data breaches, IP theft, and efforts to plant malware on its critical infrastructure.[51] Foreign actors increasingly look like they are employing cyberattack vectors targeting the federal government and critical infrastructure to "wreak havoc."[52] The open question is what the United States will do

about it. The games, surveys, and generative AI scenarios in this paper represent an effort by the CSIS Futures Lab to employ novel research methods to understand modern policy challenges.

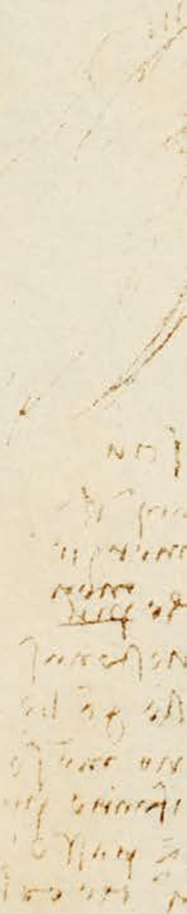
Addressing these threats requires open, honest debate that embraces not just opinion but also large datasets, facts, and even creative scenarios. Diversity of thought and perspective will lead to deeper insights. Too often security questions are treated as sensitive and closed policy discussions, limiting the ability of an educated public to debate the best course of action. Democracy requires these debates and a vibrant marketplace of ideas. Securing the connectivity the U.S. citizens rely on is too important to be left to unaccountable experts debating a handful of marquee case studies and opaque security programs. The public has a stake in understanding the threat and debating how best to confront it. That debate will be messy, but then again so is democracy. ■

Yasir Atalan *is an associate data fellow in the Futures Lab at the Center for Strategic and International Studies (CSIS) in Washington, D.C., and a graduate fellow in the Center for Data Science at American University.* ***Jose Macias*** *is a research associate in the Futures Lab at CSIS and a Pearson fellow at the Pearson Institute for the Study and Resolution of Global Conflicts at the University of Chicago.* ***Benjamin Jensen*** *is a senior fellow in the Futures Lab at CSIS and a professor in the Marine Corps University, School of Advanced Warfighting. The views expressed herein are those of the authors and do not represent the policies of the U.S. government, Department of Defense, Department of the Navy, or the U.S. Marine Corps.*

This report was made possible by support provided by Gray Space Strategies—as part of a larger research project they are conducting for Booz Allen Hamilton—and the Carnegie Corporation of New York.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

Leonardo da Vinci Sketches: wowinside/AdobeStock



ENDNOTES

1 The political preference of the congressional district is a spatial variable and was not collected from our initial survey. Rather, we repurposed players' geodata to join with spatial U.S. Census Bureau and MIT election data to extract the political preference of the player's environment (116th congressional district); this does not represent the individual player party choice nor their individual beliefs.

2 Benjamin Jensen et al., *CISA's Evolving .Gov Mission: Defending the United States' Federal Executive Agency Networks* (Washington, DC: CSIS, October 2023) https://www.csis.org/analysis/cisas-evolving-gov-mission-defending-united-states-federal-executive-agency-networks.

3 Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use" in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010), 77–97, https://nap.nationalacademies.org/read/12997/chapter/8.

4 Benjamin Jensen, Brandon Valeriano, and Ryan Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford, UK: Oxford University Press, 2018); Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* 24, no. 1 (2017): 159–72, https://www.jstor.org/stable/27119085; Robert Chesney and Max Smeets, eds., *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest* (Washington, DC: Georgetown University Press, May 2023); Jon R. Lindsay and Erik Gartzke, "Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains," *Journal of Strategic Studies*, 45, no. 5 (June 2020): 743–76, doi:10.1080/01402390.2020.1768372; and Grace B. Mueller et al., "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures," CSIS, July 13, 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

5 Jensen et al., *CISA's Evolving .Gov Mission*.

6 Ibid., Recommendation 3.1.

7 Raphael Satter, Zeba Siddiqui, and James Pearson, "U.S. Warns China Could Hack Infrastructure, including Pipelines, Rail Systems," Reuters, May 26, 2023, https://www.reuters.com/world/china/china-rejects-claim-it-is-spying-western-critical-infrastructure-2023-05-25/.

8 "Cyber-Attack against Ukrainian Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, March 4, 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.

9 Of the 429 campaigns publicly attributed between rival states between 2000 and 2020, 77 targeted government military agencies; 177 targeted government, nonmilitary agencies; and 175 targeted the private sector. See Ryan C. Maness et al., "Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID): Cyber Conflict from 2000 to 2020," *Cyber Defense Review* 8, no. 2 (July 2023), https://www.jstor.org/stable/48743091.

10 Ibid.

11 Mueller et al., "Cyber Operations during the Russo-Ukrainian War"; Dustin Volz and Jim Finkle, "U.S. Indicts Iranians for Hacking Dozens of Banks, New York Dam," Reuters, March 24, 2016, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF; Andy Greenberg, "Hackers Gain Direct Access to US Power Grid Controls," *Wired*, September 6, 2017, https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/; "Agriculture Industry on Alert after String of Cyber Attacks," GovTech, June 14, 2022, https://www.dnj.com/story/news/crime/2017/07/05/murfreesboro-police-fire-computers-infected-virus/453774001/; Andrew Liptak, "Hackers

Are Holding San Francisco's Muni Light-Rail System for Ransom," CNBC, November 28, 2016, https://www.cnbc.com/2016/11/28/hackers-are-holding-san-franciscos-muni-light-rail-system-for-ransom.html; Tom Polansek and Nandita Bose, "JBS Meat Plants Reopen as White House Blames Russia-Linked Group over Hack," Reuters, June 3, 2021, https://www.reuters.com/world/us/russia-linked-hacking-group-is-behind-cyberattack-against-jbs-bloomberg-news-2021-06-02/; and Cluster25 Threat Intel, "Cybersecurity Risks and Challenges in the Chemical Industry," DuskRise, April 12, 2023, https://blog.cluster25.duskrise.com/2023/04/12/cybersecurity-in-chemical-industry.

[12] Jensen, "The Cyber Character of Political Warfare."

[13] Susan Morgan, "Fake News, Disinformation, Manipulation and Online Tactics to Undermine Democracy," *Journal of Cyber Policy* 3, no. 1 (May 2018): 39–43, doi:10.1080/23738871.2018.1462395; and Samuel C. Woolley and Philip N. Howard, eds., *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York: Oxford University Press, 2018).

[14] Kimberly Underwood, "Cognitive Warfare Will Be Deciding Factor in Battle," SIGNAL Magazine, August 15, 2017, https://www.afcea.org/content/cognitive-warfare-will-be-deciding-factor-battle; Hansen F. Splidsboel, Russian Hybrid Warfare: A Study of Disinformation (Copenhagen: Danish Institute for International Studies, 2017), https://www.econstor.eu/bitstream/10419/197644/1/896622703.pdf; and Benjamin Jensen and Divya Ramjee, "Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs," CSIS, *Commentary,* December 20, 2023, https://www.csis.org/analysis/beyond-bullets-and-bombs-rising-tide-information-war-international-affairs.

[15] Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies* 42, no. 2 (January 2019): 212–34, doi:10.1080/01402390.2018.1559152; and Oliver Backes and Andrew Swab, *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States* (Cambridge, MA: Belfer Center for Science and International Affairs, November 2019), https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf.

[16] "CSIS Futures Lab Announces Partnership with Scale AI," CSIS, November 15, 2023, https://www.csis.org/blogs/csis-futures-lab-announces-partnership-scale-ai.

[17] Jensen, Valeriano, and Maness, *Cyber Strategy;* and Maness et al., "Expanding the Dyadic Cyber Incident and Campaign Dataset."

[18] Matthew B. Caffrey, Jr., *On Wargaming: How Wargames Have Shaped History and How They May Shape the Future* (Newport, RI: Naval War College Press, 2019), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1043&context=newport-papers.

[19] Benjamin Jensen and David Banks, *Cyber Operations in Conflict: Lessons from Analytic Wargames* (Berkeley, CA: UC Berkeley Center for Long-Term Cybersecurity, April 2018), https://cltc.berkeley.edu/cyber-operations/; David E. Bank and Benjamin M. Jensen, "Wargaming International and Domestic Crises: Island Intercept and Netwar" in Cyber *Wargaming: Research and Education for Security in a Dangerous Digital World*, eds., Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schechter (Washington, DC: Georgetown University Press, 2023).

[20] See Benjamin Schechter, Jacquelyn Schneider, and Rachael Shaffer, "Wargaming as a Methodology: The International Crisis Wargame and Experimental Wargaming," *Simulation & Gaming* 52, no. 4 (2021), doi:10.1177/1046878120987581.

[21] Jensen and Banks, *Cyber Operations in Conflict*.

[22] Joshua D. Kertzer and Dustin Tingley, "Political Psychology in International Relations: Beyond the Paradigms,"*Annual Review of Political Science* 21, no. 1 (2018): 319–39, doi:10.1146/annurev-polisci-041916-020042.

[23] For detailed statistics, reference the methodology annex at https://www.csis.org/analysis/eroding-trust-government-what-games-surveys-and-scenarios-reveal-about-alternative-cyber.

[24] Drew DeSilver “What the Data Says about Food Stamps in the U.S.,” Pew Research Center, July 19, 2023, https://www.pewresearch.org/short-reads/2023/07/19/what-the-data-says-about-food-stamps-in-the-u-s/.

[25] Small Business Administration, “SBA Announces Biden-Harris Administration’s Progress in Small Business Lending with End-of-Year Capital Program Numbers,” Press release, November 21, 2023, https://www.sba.gov/article/2023/11/21/sba-announces-biden-harris-administrations-progress-small-business-lending-end-year-capital-program.

[26] Ellen Hughes-Cromwick and Julia Coronado, “The Value of US Government Data to US Business Decisions,” *Journal of Economic Perspectives* 33, no. 1 (Winter 2019): 131–46, doi:10.1257/jep.33.1.131.

[27] Benjamin Jensen, “How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy,” Statement before the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet, September 20, 2023, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/jensen-testimony_0.pdf.

[28] “Representative Samples,” Prolific, February 6, 2024, https://researcher-help.prolific.com/hc/en-gb/articles/360019236753-Representative-samples.

[29] Franki Y.H. Kung, Navio Kwok, and Douglas J. Brown, “Are Attention Check Questions a Threat to Scale Validity?,” *Applied Psychology* 67, no. 2 (2017): 264–83, doi:10.1111/apps.12108.

[30] “2021 American Community Survey (ACS) 5-Year Estimates,” U.S. Census Bureau, August 16, 2023, https://www.census.gov/programs-surveys/acs/data.html.

[31] “U.S. House 1976–2022,” MIT Election Data and Science Lab, Harvard Dataverse, July 7, 2023, https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi%3A10.7910%2FDVN%2FIG0UN2. These observations allowed for the inclusion of political party information in a comprehensive spatial dataset. A spatial join was executed by converting the participant data into a spatial object and merging it with the updated census spatial dataframe. This process aligned the two datasets based on geographical overlap within congressional districts.

[32] J. Scott Brennen et al., “Types, Sources, and Claims of COVID-19 Misinformation,” University of Oxford, Reuters Institute, April 7, 2020, https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation.

[33] While there were also statistically significant correlations between living in Democrat-leaning and majority-minority districts and preferences for targeting small and medium-sized businesses and science and technology, these were limited. The only consistent finding across the district-level data and robustness checks was the age-cohort distribution and targeting preferences.

[34] “Scale AI Announces Partnership with Center for Strategic and International Studies,” Scale AI, November 14, 2023, https://scale.com/blog/scale-csis-partnership-announcement; “CSIS Futures Lab Announces Partnership with Scale AI,” CSIS; and Benjamin Jensen and Dan Tadross, “How Large-Language Models Can Revolutionize Military Planning,” War on the Rocks, April 12, 2023, https://warontherocks.com/2023/04/how-large-language-models-can-revolutionize-military-planning/.

[35] The methodology annex lists sample text sources and prompts used to construct the scenarios

but maintains player anonymity by not publishing the text from the TTX transcripts, consistent with the Chatham House rule and best research practices.

36 Jensen and Tadross, “How Large-Language Models Can Revolutionize Military Planning.”

37 Ivanka Barzashka, “Wargames and AI: A Dangerous Mix That Needs Ethical Oversight,” Bulletin of the Atomic Scientists, December 4, 2023, https://thebulletin.org/2023/12/wargames-and-ai-a-dangerous-mix-that-needs-ethical-oversight/.

38 Jensen, Valeriano, and Maness, *Cyber Strategy*.

39 Ibid.; Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press,2018); and Mark Galeotti, *Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CA: Yale University Press, 2022).

40 Jensen, “How the Chinese Communist Party Uses Cyber Espionage to Undermine the American Economy.”

41 For an overview of why authoritarian states are particularly concerned about gender, see Kathleen J. McInnis, Benjamin Jensen, and Jaron Wharton, “Why Dictators Are Afraid of Girls: Rethinking Gender and National Security,” War on the Rocks, November 7, 2022, https://warontherocks.com/2022/11/why-dictators-are-afraid-of-girls-rethinking-gender-and-national-security/.

42 “Public Trust in Government: 1958-2023,” Pew Research Center, September 19, 2023, https://www.pewresearch.org/politics/2023/09/19/public-trust-in-government-1958-2023.

43 Caroline Cahm, *The Rise of Revolutionary Anarchism*, 1872-1886 (Cambridge, UK: Cambridge University Press, 2002); and Diana Rieger, Lena Frischlich, and Gary Bente, Propaganda *2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos* (Köln, Germany: Wolters Kluwer, 2013)

44 Neville Bolt, David Betz, and Jaz Azari, *Propaganda of the Deed 2008: Understanding the Phenomenon* (London: Royal United Services Institute, 2008), https://static.rusi.org/200809_whr_propaganda_of_the_deed_0.pdf.

45 Carl Smith, “The Terrifying New Tactic Used to Harass Public Officials,” Governing, January 29, 2024, https://www.governing.com/management-and-administration/the-terrifying-new-tactic-used-to-harass-public-officials.

46 Andreas Stöffelbauer, “How Large Language Models Work: From Zero to ChatGPT,” Medium, October 24, 2023, https://medium.com/data-science-at-microsoft/how-large-language-models-work-91c362f5b78f.

47 Jacquelyn Schneider, “What War Games Really Reveal: Outcomes Matter Less Than Who Pays and Who Plays,” *Foreign Affairs,* December 26, 2023, https://www.foreignaffairs.com/united-states/what-war-games-really-reveal.

48 Jensen et al., *CISA’s Evolving .Gov Mission*, Recommendation 3.8.

49 Melissa Heikkiläarchive, “Three Ways We Can Fight Deepfake porn,” *MIT Technology Review*, January 29, 2024, https://www.technologyreview.com/2024/01/29/1087325/three-ways-we-can-fight-deepfake-porn-taylors-version/?truid=*%7CLINKID%7C*.

50 See Jensen et al., *CISA’s Evolving .Gov Mission*, Recommendation 3.1.

51 Brandon Valeriano and Benjamin Jensen, “Building a National Cyber Strategy: The Process and Implications of the Cyberspace Solarium Commission Report,” *2021 13th International*

Conference on Cyber Conflict (CyCon), Tallinn, Estonia, May 25–28, 2021, doi:10.23919/CyCon51939.2021.9467806.

52 Ken Dilanian, Summer Concepcion, and Kyla Guilfoil, “FBI Director Warns Chinese Hackers Aim to ‘Wreak Havoc’ on U.S. Critical Infrastructure,” NBC News, January 31, 2024, https://www.nbcnews.com/politics/national-security/fbi-director-warn-chinese-hackers-aim-wreak-havoc-us-critical-infrastr-rcna136524.

53 Source: Caroline Cahm, *Kropotkin: And the Rise of Revolutionary Anarchism, 1872-1886* (Cambridge: Cambridge Univrsity Press, 2002); and Diana Rieger, Lena Frischlich, and Gary Bente, *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos* (Cologne, Germany: Wolters Kluwer Deutschland GmbH, 2013), https://eucpn.org/sites/default/files/document/files/39._propaganda_2.0_-_psychological_effects_of_right-wing_and_islamistic_extremist_internet_videos.pdf.