



RISKGAMING

02

DeepFaked and DeepSixed:
AI Election Security and the
Future of Democracy

DANNY CRICHTON

DeepFaked and DeepSixed:

**AI Election Security and
the Future of Democracy**

CREATED BY
Danny Crichton

PUBLISHED BY
Lux Capital

Contents

Overview	17
What is Riskgaming?	21
Gameplay & Rules	25
Roles & Clues	31
Intelligence Community Roles	34
Department of Justice & Law Enforcement Roles	40
Department of Homeland Security Roles	48
Department of Defense Roles	54
State Department Roles	58
Election Agency and Organization Roles	66
Civil Society Roles	72
Technology Company Roles	78
Traditional Media Roles	84
Social Media Roles	92
Telecom Roles	98
White House Roles	104
Threats	117
Scene 1: Before Election	118
Scene 2: During and After Election	126
Players with Unused Clues	137
Contact	139

About Lux Capital

Lux Capital is a New York- and Silicon Valley-based venture capital firm investing in companies on the edge of scientific and technological breakthroughs. Over the past two decades, Lux has expanded from our New York City roots to Silicon Valley, and built a firm with over \$5 billion AUM and more than 30 full-time professionals, with a wide spectrum of technical backgrounds and the versatility to invest at any stage, from \$100,000 to \$100 million.

About Riskgaming

Riskgaming is a strategic simulation game that immerses players in complex scenarios reflecting real-world challenges and dynamics.

CHARACTER-DRIVEN STRATEGY

Players take on the role of richly-detailed characters who can strategically build or break trust with each other throughout the game.

EMERGENT BEHAVIOR

Players make strategic decisions influenced by personal and external incentives, allowing for spontaneity and surprise.

AUTONOMOUS DECISION-MAKING

All players select their actions independently of each other during a scenario, reflecting the autonomy of real-world decision-makers.

PROFOUND EXPERIENCES

Each scenario faithfully models the real world, allowing players to experience an alternative reality that informs our own.

About the Creator

Danny Crichton analyzes technology, growth and power as Editor-in-Chief of Riskgaming and Head of Editorial at Lux Capital. In addition, he's a Fellow with the Manhattan Institute. He's published research on semiconductors, technology and economic development with Manhattan Institute's City Journal, the Foreign Policy Research Institute, and the National Review.

Prior to Lux, he was managing editor at TechCrunch as well as previously a foreign correspondent based in Seoul, South Korea. While there, he wrote more than 1,000 news stories and longform analyses chronicling U.S.-Asia technology relations, semiconductors, data infrastructure, fintech, disaster and climate tech, venture finance, product development, and a wide number of other complex subjects with technical and policy intersections.

In addition to his reporting and analysis at TechCrunch, he co-hosted its leading podcast Equity; co-programmed stages at its flagship Disrupt SF and Berlin conferences as well as its Sessions and Early Stage events; launched the premium news service Extra Crunch and grew it to seven figures of revenue; co-managed a multi-million dollar freelance budget; developed the TC-1 series of deep startup profiles and The TechCrunch List; and contributed broadly to the organization's news, operational, and talent development strategy.

Formerly, he was an early-stage venture capitalist with General Catalyst in Palo Alto and Charles River Ventures in Boston and New York.

He was awarded a Fulbright research scholarship to South Korea, where he studied the development of Korea's startup ecosystem. He's an honors graduate of Stanford University, where he studied mathematical and computational sciences and wrote a thesis on the development of computer science as an academic discipline, which won the school's Firestone Medal for Excellence in Undergraduate Research.

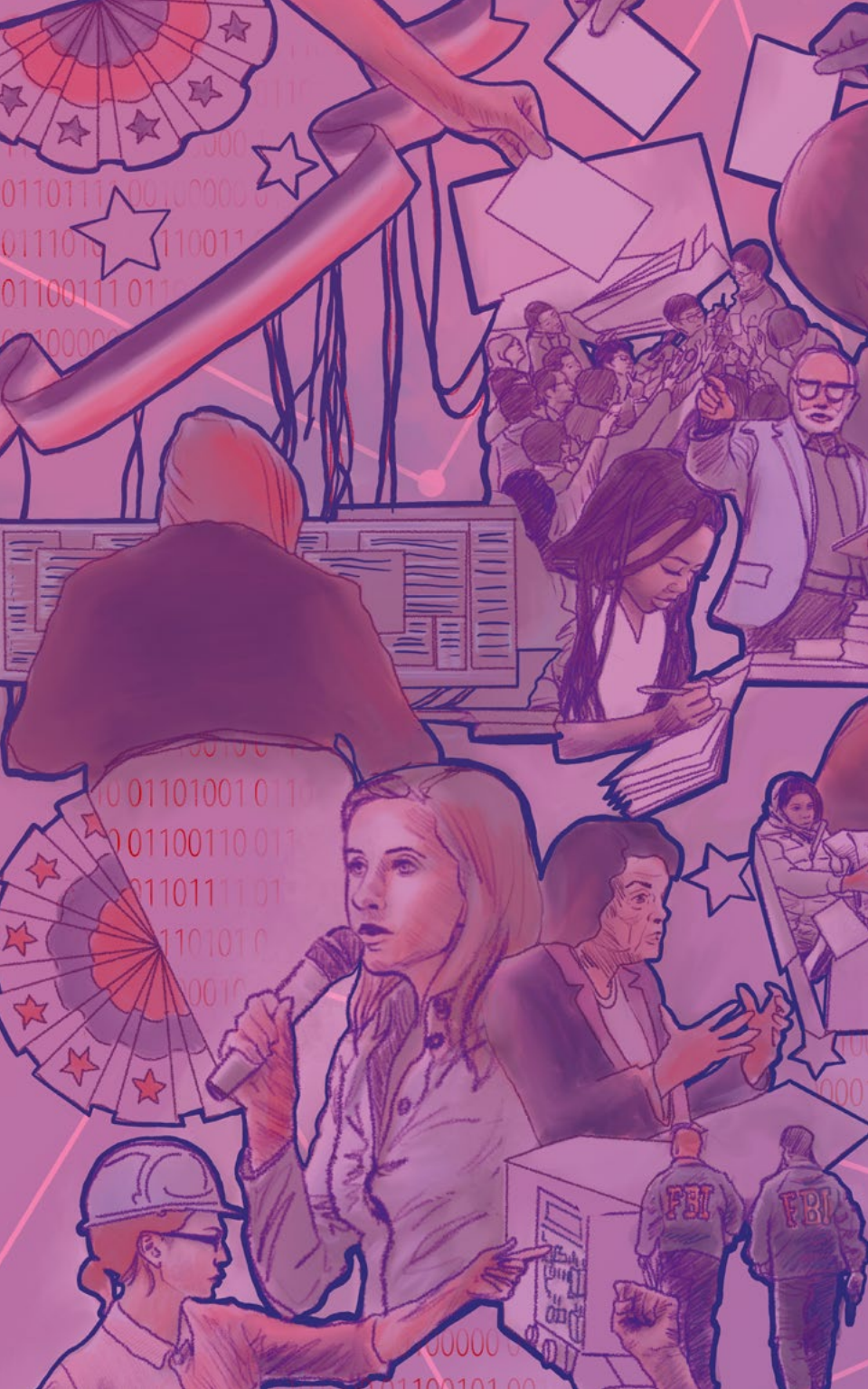
Danny is based in Brooklyn, New York.

Acknowledgements

This game was triggered by a conversation with Miles Taylor and Evan Burfield in late 2023 and was formally conducted in January 2024 with a distinguished group of 54 citizens concerned about the future of America's election integrity. I want to thank everyone who participated as well as our hosts at TheFuture.us and Galaxy Interactive for their engagement and support.

Credits

Game Designer and Editor-in-Chief, Danny Crichton
Director of Programming, Laurence Pevsner
Front Cover Illustration, Tiya Tiyasirichokchai
Production Designer, Justin Barber
Website Designer, James Clements



HOW TO DOWNLOAD THE GAME

All materials for the game, including the spreadsheet that drives it, design notes and player handouts, are available on the Lux Capital website.

To download the game materials, please head to luxcapital.com/riskgaming or use this QR code.





Overview

OVERVIEW

Once a staid procedural motion at the heart of democracy, election systems have increasingly become the locus for a battle of power not just between domestic factions, but also by foreign actors seeking to transform their adversaries' policies in the cheapest and most effective way possible. The sudden rise of generative artificial intelligence technologies has exacerbated this conflict, creating new threats before, during and after elections that can harm their integrity and the legitimacy of their results in the eyes of citizens.

While much attention has been paid to politically responding to these threats as well as speculation on how different candidates might react to events that benefit and hurt their chances at the polls, this is the first scenario to look at the complexity of securing elections when critical information is held by dozens of different actors, from intelligence agents and diplomats to private-sector officials in technology, cybersecurity and telecom as well as civil society leaders. Each of these actors knows clues to potential threats, but can they work together and connect the dots in time?

In DeepFaked and DeepSixed: AI Election Security and the Future of Democracy, up to 54 players take on diverse public- and private-sector roles who have been called to the White House Situation Room. The President has ordered the erection of an election security fusion cell to combine disparate information sources together to identify threats to the integrity of the upcoming election.

The game consists of two independent scenes: the first is set one week before the U.S. presidential election, and the other is set on Election Day and its immediate aftermath.

Players are offered a clue to use in each scene. The clue is likely accurate and may match other players' information, or it could be misleading or outright wrong. As a group, all players in the Situation Room are attempting to offer their information, connect it with other relevant evidence, identify the most likely threats to American democracy, and rank the severity of those threats for a response from government.

DeepFaked and DeepSixed simulates both the wide-range of actors and knowledge that makes securing elections difficult, as well as the frantic and chaotic process to find signal in a complex and ever-evolving threat environment where new technologies like AI, deepfakes, synthetic media, cryptocurrency and more are upending traditional notions of security.

This game was officially conducted in January 2024 in partnership with TheFuture.us and Galaxy Interactive with a group of current and former government officials, political candidates, journalists, think tank experts, tech executives and venture capitalists. A feature piece on the scenario and its conclusions was written by Dan De Luce and Kevin Collier for NBC News.



What is Riskgaming?

Mike Tyson said that “everyone has a plan until they get punched in the face,” but people often leave out the rest of that sentence, in which Tyson continues and says “Then, like a rat, they stop in fear and freeze.”

No one wants to be a rat, certainly not in the rat capital of the world that is New York City. So how do we punch ourselves in the face and get ready for the challenges ahead of us?

That's where Riskgaming comes in. Riskgaming has two goals. The first is understanding the complex connections between technology, science and policy that make issues like AI election security so challenging. The second goal is more abstract: understanding the motivations, capabilities and limitations of each actor participating in the game in order to build up an empathy for why people — even those we radically disagree with — make the decisions they do.

Policymaking is chaotic and inchoate, with operational decisions made in stressful situations with limited to no information at all. Our goal with Riskgaming is to simulate that chaos as best as we can and prepare us to be punched in the face, as it were.



Gameplay & Rules

Unlike many of our Riskgaming scenarios, DeepFaked and DeepSixed is a simple game with minimal rules designed for a massive group of participants.

At the start of the experience, the Game Leader offers each player a random or pre-selected role that comes with two clues to be used separately in each of the game's two scenes. Players are encouraged to stand in a reasonably large room (the Situation Room), particularly if all 54 roles are played.

Critically, everyone is who they say they are, and every player is trying to do the best they can given the information they have available to them. This means that there are no "rogue" characters who are attempting to undermine the game from inside, and no player should play their character to undermine the election security fusion cell. While some characters may hold misinformation, they believe any and all information in their possession.

During each scene, there are an unknown number of threats to be identified by the players based on the clues they are offered. Each threat is unique, and evidence of each threat is written subtly into the clues of all the players.

The Game Leader will introduce the game and the first scene, which covers a period right before the upcoming election. The scene will last for about 20 minutes (or at the Game Leader's discretion), during which players will talk to one another, trying to find threat patterns in the clues that each of them holds. If any player or group of players thinks they have identified a threat, then they should report this potential threat to the Game Leader, who will write it down on a sheet of paper or a white board for public display.

After the scene is complete, the Game Leader will read out the threats that have been identified by the group. Over about 10 minutes (or at the Game Leader's discretion), players can debate

which threats offer the most promising leads and attempt to rank them from most pressing to least. Depending on the size of the group, the Game Leader can moderate this discussion in any way they deem fit.

After the discussion has concluded, the Game Leader will identify threats that are real, with each identified threat offering 1 victory point for the group. If a “Primary” threat (as identified in the Threats list) is among the top three threats identified by the group, then it’s awarded 2 points instead of one. Any threat that is unidentified during the scene or any threat that is imagined by the group is counted as -1 victory points. The Game Leader can debrief the threats and describe how specific clue information might have helped to identify a specific threat.

The whole group then begins scene two, which covers a period during and after the election. Once again, the same process applies, but this time players should exclusively use their second clues. Information from the first scene’s clues are not applicable to the second scene.

After debriefing the threats from the second scene, the Game Leader should end the game and offer a final score based on the total points awarded across scenes one and two. Groups with positive scores have done very well!

Finally, the Game Leader should moderate a discussion among players about the clues, roles, and election threats that were experienced during the game. This discussion can be as lengthy and profound as is appropriate for the players who participated.

In all, we recommend allotting about two hours for DeepFaked and DeepSixed: roughly 45 minutes per scene plus the final debriefing. Longer games are not better, as time pressure is a crucial aspect for reconstructing the chaos of a typical intelligence fusion cell.

HOW TO HANDLE SMALLER GROUPS?

DeepFaked and DeepSixed was designed for a group of 54 people with an even balance of clues across the different threats in each scene. In the event that a group is smaller than 54 people, a few options are possible.

First, if the group is just shy of 54, randomize the roles and simply drop certain characters out of the game. Just as in real life, individuals with critical information may miss their flight connections, lose internet access or simply miss a meeting where they could have offered their information to others. Randomly losing pieces of a puzzle is a regular part of intelligence analysis and a faithful reproduction of reality.

However, if the group is significantly smaller, it's also acceptable to offer multiple roles to the same player. Ultimately, each role has one piece of critical information per scene, and so a player can simply parlay two or more pieces of critical information rather than just one.

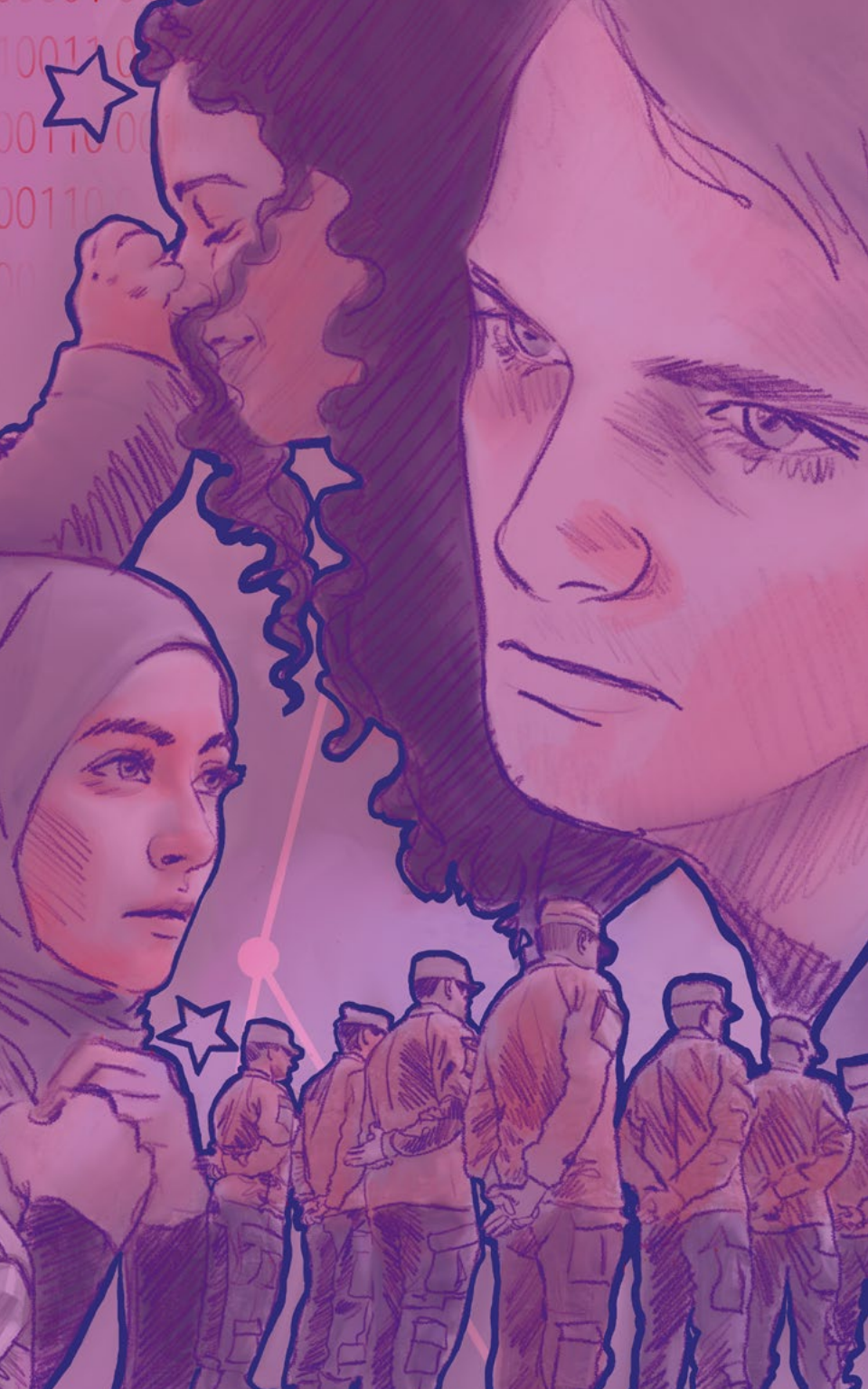
We do not recommend running the game with fewer than 12 people. The challenge of the game is building connections between information held by many different characters. As the number of players shrink, that design becomes overly simplistic and ultimately uninteresting.

HOW TO HANDLE LARGER GROUPS?

If there are a handful of more players than characters available, then the Game Leader should offer the additional players the role of “intelligence analyst” whose job is to help connect the information in the Situation Room together.

While these players have no original information themselves, they can quickly work the room and see if there are overlapping pieces of information that may identify a threat.

For much larger groups, we recommend splitting the group in half and running two groups independently. This can be particularly interesting given that the two groups will likely identify and rank very different sets of threats — deepening everyone’s understanding of the main thesis of the game.



Roles & Clues

Following are two clues for each of 54 roles playable in *DeepFaked and DeepSixed*.

The first clue used in scene one generally offers a bit of background about the role in addition to information pertinent to threats before the election.

The second clue for scene two is generally a bit shorter and covers Election Day and the week after.

All roles are considered equal within the context of the fusion cell at the White House Situation Room. Roles are drawn from the intelligence community, Department of Justice, Department of Homeland Security, Department of Defense, State Department, election agencies and organizations, civil society, technology companies, traditional media, social media, telecoms and the White House. The names of non-government organizations have been invented, and all story details of the game are assumed to be fictional without relation to any real organization.

Intelligence Community Roles



SCENE 1

As the nerve center of the Intelligence Community, it's your job to connect dots and ultimately advise the President on the order of the day (or chaos, as it were). Some of the dots that are attracting your attention these days are movements in a special unit of Iran's Islamic Revolutionary Guard Corps that emphasizes cyber warfare. Iran seems to be undertaking a massive hack of the U.S. election, with probes of election systems and infrastructure increasingly arriving from a building compound in a suburb of Tehran or through VPNs that can be traced back there. On top of that, signals intelligence seems to indicate more comms chatter between Iran and some of its intermediaries — even more than Russia these days.

SCENE 2

One of the new and unusual threads that has materialized during the election season is that India seems to be surreptitiously influencing certain U.S. states through overseas action. Maybe it's a response to U.S. messaging during Prime Minister Narendra Modi's own election a few months ago? Either way, you have to wonder how involved Indian intelligence is in multiple threats currently underway against U.S. democracy right now.

SCENE 1

SIGINT is the gleaming light of the Intelligence Community. While HUMINT is getting expensive and impossible thanks to digital, everyone loves an eavesdrop — and satellites and communications hacking makes that increasingly easy. The U.S. election has led to a surge in every signal imaginable — everyone and their grandmother (and even their grandmothers' cats) seems hell-bent on influencing the outcome of the American election. It's all the usual culprits, but there does seem to be an increase in chatter coming from Iran that you have notified the Director of National Intelligence on. Iran has not traditionally played the largest role in U.S. electoral interference, but there's a start for every nefarious plot.

SCENE 2

CIA has been convinced for years that the Senator is in the pocket of Iran, but there has been little to no signals intelligence that corroborates their account. Recently, a video has circulated showing that the Senator's campaign staff was accepting Bitcoin from Iranian agents, but several top deepfake researchers have proven that the video is a forgery. Once again, you've shown that the paranoids over at Langley might be overdoing it just a little.

SCENE 1

After 25 years in CIA's Directorate of Analysis, you finally got what you had been asking for in the employee resource groups for years — a gym. In 2022, after a decade of construction, the new CIA HQ gym finally opened, and its ribbon-cutting ceremony happened to coincide with your first week as CIA Director. A PR victory! While working out on a "secure Peloton" (an agency joke — it's an Amazon Basics stationary bike because god forbid), an aide comes in to tell you that the mayor of Fairfax, VA has called. She's a friend and happens to own the home next to yours, and she says that there are videos of her circulating on the internet calling on voters to stay home on Election Day. She has no idea how they were made, but says, "you seem like the kind of person who knows how to spoof these things — was it you?" You intend to mow into her yard just a little bit more next year when it thaws.

SCENE 2

You've known the Senator for a long time given his involvement in U.S. foreign policy. You also know that he has accepted millions of dollars in bribes from the regime in Tehran for years, a fact that can't be proven without revealing critical HUMINT clandestine tools that keep the Agency in the loop on the rogue state's nuclear program. Now, apparently, the video of his campaign manager accepting cryptocurrency from the regime is a fake. That's hard to reconcile.

SCENE 1

The unexamined life is not worth living, and since you examine every living thing on Planet Earth 24/7, I suppose that makes you more reflective than Socrates. The level of signals intelligence is off the charts this election. Every country is pushing and prodding American voters using their cyber tools, but one pattern has caught your jaded and increasingly myopic eye: an increase in cryptocurrency flows to Macau. With China's crackdown on crypto the past few years, that figure has significantly decreased over the years — only for it to surge recently, and in what appears to be consistent transactions of roughly 0.00050 BTC. Is that a special number?

SCENE 2

There have been SWATings called in all across the country naming polling sites as places where there are active shooter sites. The source of the calls are a mystery, with most being called in from local payphones. While SWATings are a well-worn playbook often used by internet trolls against their victims, the tactics seem eerily similar to one another. Could they be coordinated by some larger power? The videos showing the polling sites streaming across the feeds in the Center are frightening, to say the least.

Department of Justice & Law Enforcement Roles



SCENE 1

The Attorney General advocates for justice, and justice is often gained in the public's imagination one spotlight trial at a time. So when the FBI recently apprehended six members of a voter fraud ring in Florida, you finally found that picture-perfect case to make a splashy statement. Unfortunately, that ring is a group of high schoolers who were conspiring to create fake voter registrations — and even under the best of circumstances, it's complicated to prosecute kids. It's even harder when your last state campaign's tagline was "Putting Kids First." But these teenagers ingenuously documented their plans on an online forum for gamers, and this could be just the tip of the spear against American democracy that the DoJ must be prepared to stop.

SCENE 2

After delays in postal processing prevented some completed mail-in ballots from reaching poll sites in time for counting, there have been a number of instances where a group dubbing itself the "Citizen Election Security Brigade" have broken into postal processing centers demanding to find more misplaced ballots. You've ordered an immediate prosecutorial response against any person who has joined or been a part of this or affiliated groups, but your reaction has also put the Department of Justice under fire for drawing attention away from the mishandling of ballots.

SCENE 1

You've spent your life trying to protect America against foreign threats, but those foreign threats are multiplying, and they never seem to stop. Recently, you've picked up a series of intelligence findings connecting a network of influential social media accounts to the propagation of footage of a major presidential candidate's staff apparently offering citizenship to undocumented workers. Stopping or even tamping down that distribution is a complicated legal action under even the best circumstances, but these videos seem directed and amplified by some hostile power. What's to be done?

SCENE 2

Your brother reports that some of his friends have received text messages about Election Day from a +375 number, which traces to Belarus. The text messages ask the receiver to fill out a pre-registration form to verify a voter's identity. You thank your brother, apologize again for missing his birthday last week, and send his comments to the FBI for investigation.

SCENE 1

Aside from judges, the FBI Director has one of the longest terms in office at 10 years. Maybe they should call it a sentence instead of a term, since that's what this job feels like most days. Election years cause professional anxiety across the J. Edgar Hoover building, and they also tend to intensify the homegrown threats from all types of extremism. You assigned a well-resourced group of agents to track election interference and meddling, and they recently put together an adamant case: a group of teenagers in Florida looking to invent fictional identities in order to stuff the ballot boxes in a crucial swing state. Their online forum had hundreds of passive followers, but tracking down all of these IP addresses (many of them masked) is painstaking work, and prosecutors probably just want the main group put on trial anyway.

SCENE 2

Law enforcement was on edge right before the election, but now they are absolutely overwhelmed with the sheer number of threats being called in from jurisdictions all over the country. There are active shooter threats underway in dozens of locations, and given that many poll sites are set up at schools and churches, whole districts are shutting down for the day to stop terrified parents from worrying about their children. Every child loves a vacation day, but no one loves it when democracy takes a vacation itself.

SCENE 1

A lifelong veteran of the prism (prison?) of bureaucracy known as the FBI, you've moved up the ranks into that number two position that means you do all the work and take all the blame. Recently, your mother was talking about how delighted she was that the The Columbus Citizen-Press resurrected after a nearly four decade hiatus in Ohio's capital, apparently due to the largess of a recently crowned multimillionaire in the area. She says her crochet club has been loving the articles posted on Facebook, and that its voter guide has been "very informative about the true state of America and whether your vote even really matters."

SCENE 2

The Bureau has been focused on this "Citizen Election Security Brigade" for many years now, but it's been a relatively quiet group without much of a strategy — just one of hundreds of extremist groups that the FBI checks in on every once in a while. Now, after breaking into several postal processing centers, the group has become an absolute partisan Rorschach test, and the FBI's investigation has to explore both their violent attack on federal facilities, but also whether postal workers may have deliberately sabotaged the vote as well.

Deputy Commissioner of the Counterterrorism Bureau, NYPD

SCENE 1

JFK is one of the greatest smuggling airports in the world, a hive of scum and villainy and even an on-time plane taking off once in a while. To counter drug and arms trafficking, you launched the Guardian Initiative, a fusion center at the NYPD Counterterrorism Bureau that brings together public social media posts, drug smuggling data, and arms sales across the United States to look for actionable correlates for the Bureau. Recently, the Initiative's team lead noticed that arms sales rose in a range of districts across New York that are completely uncorrelated with traditional norms seen over the past few years. There's also been an uptick in gun seizures from holders without a gun license — a worrying sign.

SCENE 2

A series of intercepted communications indicates that Russia is coordinating a violent threat campaign in a variety of voter precincts across the country, using targeted SMS messages and AI-based interactive calls to convince voters that their physical safety is not assured if they vote. Strangely however, New Yorkers have received no such messages so far on Election Day and you've seen zero evidence that this campaign exists.

Department of Homeland Security Roles



SCENE 1

The homeland gets harder to secure year after year, and not just on the physical terrain of what most people think of as the homeland, but on the digital plane as well. It's a growing challenge for the Department, still reeling from the insanity of its sudden birth two decades ago. The number of threats is overwhelming, but two have caught your eye. First, there is a growing wave of anti-5G fanatics shooting down cell towers who seem to be also attempting to stop the electronic uploading of voter data from precincts via cellular communications. Their origins are unknown, but any attack on core U.S. infrastructure is, of course, a major priority. Second, there seems to be growing activity from China attempting to sway a series of state legislative races in key states with deeper economic ties to the Middle Kingdom.

SCENE 2

The FBI director told you about SWATings taking place all across the country at voting sites, and now it is all over the news media that a group of vigilantes are working to shut down the American election. The media is encouraging voters to stay home, and so you have been dispatched to the podium to reassure Americans that their vote is safe.

SCENE 1

Every day is a day driving 100 MPH in a car without airbags — and probably without brakes or an auto body either. Such is the life of protecting the cyber infrastructure of the federal government, 50 state governments, and thousands of local municipalities across the country. Recently, you got an intelligence briefing from a star analyst that noted how hackers are increasingly foregoing exfiltrating information out of government systems, but rather infiltrating information in. You consider the risk of benefits fraud at the Social Security Administration, then realize they are still mostly processing paper and breathe a sigh of relief.

SCENE 2

You were warned by the Director of National Intelligence about the involvement of India in influencing American elections. That prompted you to investigate some of the government's IT procurement contracts, only to find out that many of the U.S.-listed companies are mere shells for overseas vendors, mostly from Bangalore, India's IT hub. You suddenly have a revelation that perhaps this is the route India is taking to influence the election, and send out a bulletin to election officers across the country.

SCENE 1

Investigating social media has become politically toxic, and yet, so much of American life remains confined to a handful of walled digital realms. That's where the investigations should take place! Recently, there's been an uptick in complaints filed about a collection of Facebook pages that seem to impersonate the names of local newspapers that have long since gone bankrupt (which, sadly, are not hard to find in news deserts all across America). It's not illegal to sound a bit similar to another business, nor is it illegal to open and operate a Facebook page. There's honestly not much to do other than filing away the reports into the doom file.

SCENE 2

The Department has been tasked with determining to what extent the ballots touched by the "Citizen Election Security Brigade" in its recent attacks on postal processing facilities were manipulated. Unfortunately, security cameras in the facilities are not generally in good working order (many, ironically, having been lost in the mail), and many rooms with envelopes of ballots are completely unaccounted for by security systems. You will have to report that it is impossible to know whether ballots were spoiled, thrown away, manipulated, or untouched.

SCENE 1

Within the crazy bureaucratic bedfellows of American governance, among the strangest is the Secret Service's dual mission of protecting the country's most important leaders and also investigating threats to the country's financial infrastructure. On the former, it's not always easy protecting the world's most targeted humans, but there are downtimes every once in a while. Recently, while having lunch at the White House Mess, you were scrolling through Facebook videos on the unclassified web when you suddenly stumbled across a video in your feed of what looks like one of the presidential candidates handing out citizenship to a random person. It seemed ridiculous, so you asked your deputy where it took place and apparently it never happened. The internet's a weird place, as is this rhubarb quiche. I guess that's why they call the cafeteria a "mess."

SCENE 2

Threats to major political figures including the presidential candidates haven't crescendoed as much as you expected given the election's polarization, and that is giving you some bandwidth to consider some of the financial threats to the U.S. election. Agents in your investigatory division have found evidence that criminals are breaking into popular but relatively insecure peer-to-peer cash apps to acquire identity information in order to vote illegally in the U.S. election, presumably through mail-in ballots. Voting in the names of others is illegal, but what matters to the Secret Service's jurisdiction is the attack on financial infrastructure. You follow up with the key companies involved to secure the right data to begin prosecuting cases.

Department of Defense Roles



SCENE 1

Americans may have one of the most heterogeneous systems for voting anywhere in the world, and that's just as true when it comes to the U.S. military, where servicemen and servicewomen have to register to vote in tens of thousands of local jurisdictions. Thankfully, the Federal Post Card Application has made this process quite a bit easier over the years, but hurdles remain — and cyberattacks are still a regular challenge. Recently, active-duty military soldiers have complained that the Application has been regularly offline, complaints that have aggregated enough to reach the SecDef's office. It's time to get Cyber Command and the rest of government to investigate — these downtimes are likely strategic denial-of-service attacks designed to influence America's upcoming election.

SCENE 2

Weird as it is, Election Day is typically quiet around most of the world, almost as if global leaders collectively inhale while waiting for the judgment of the American people. One pattern has caught your eye though: Turkey, a key NATO ally, seems to have funneled its cheap Sarsılmaz guns to a number of Americans. It's not a popular brand, but a recent Defense Intelligence Agency report seems to indicate that Ankara is attempting to increase exports to the West to match the financial success of its Bayraktar TB2 drone in Ukraine and counter the country's recent heavy inflation.

SCENE 1

Fort Meade has far less tasty beer than its name might otherwise suggest. That hasn't changed your impression of U.S. Cyber Command — well, it has a little. But as the Commander around here, you manage the U.S.'s offensive and defensive cyberwars — the ones that mostly don't hit the papers and the minds of the public. One big challenge the past week: there's been a widely disseminated hacking tool called Postmark that has allowed hackers to break into the majority of MacroHard's Relationship email servers and read as well as edit the text of already-sent emails. What intelligence could America's foreign enemies have learned?

SCENE 2

Attempted hacks of digital U.S. government assets have crescendoed to a new record on Election Day, keeping the entire Command overwhelmingly busy. Among the most pressing threats: a Brazilian gang that is attempting to break into several defense contractors; a Maltese hacker that broke into a military personnel database; and a Filipino group that seems to have secured base diagrams for U.S. installations all over the world. None of these seem relevant to Election Day, but the timing is suspicious.

State Department Roles



SCENE 1

U.S. elections are nightmares for the country's diplomatic service. Given the overwhelming power of the United States, any change in the politics here is going to reverberate globally, and so naturally, every country in the world has a stake in the outcome of the U.S. election. Recently, you received one of those sterling cables from a time when people could still write from your ambassador in Albania, who says that a local group of software engineers has built out a social media marketing engine that's making a financial killing by trolling U.S. voters. Given the intense scrutiny on foreign interference in U.S. elections, you order a follow up and begin to disseminate the information across the federal government.

SCENE 2

There seems to be wide-scale international manipulation of a video from Miami-Dade County showing ballots being disposed of in a dumpster. Multiple countries seem involved including perhaps Russia, Iran and India, matching an earlier analysis from State's Bureau of Intelligence and Research that America's adversaries would take advantage of these moments to unleash division in the U.S. populace.

SCENE 1

Back in freshman undergrad when you had your first taste of vodka at a dorm party and spit it out, you should have canceled your Russian Studies class, switched to any other subject, and never looked back. But switch you did not, because the 1990s were heady, Gorby was popular, shock therapy was smart and Russia was where the money was. Now, you're marooned in the dark nights of Moscow, drinking that vile elixir at quantities that even the Russians can't tolerate. At a rare (and exceedingly low-key) dinner function at Café Pushkin recently, a Putin-adjacent plutocrat joked offhandedly that Russia was prepping "chaos" of a whole new order and that November 2024 would be "offering Americans the shock therapy that you so enjoyed offering Russia." Was it the vodka talking or was this a backchannel message?

SCENE 2

Moscow's weather is turning worse, if that was even possible. A source entwined with the Russian security services mentions that the "chaos" has begun, and noted with pleasure that it seems like the United States knows how to count ballots "à la russe." You head back to the U.S. embassy across from the Russian White House, prepare a cable for Washington, and then prepare for another night of vodka tastings "à la russe."

SCENE 1

This job used to be better in a pre-Xi world, or so you have been told. With the lockdowns during Covid and pervasive digital and physical surveillance from the Ministry of State Security, it's become ever harder just to walk outside the U.S. embassy compound and meet with sources, or even get a bite of jianbing. But recently, you were talking with an industrial association leader (who is almost certainly part of China's United Front efforts) about their efforts to sway the elections of state and local elections in the United States in favor of more pro-China candidates. You asked about federal elections and the leader demurred, saying China realizes that "both candidates are the same" for the presidency and neither would change the course of U.S.-China relations.

SCENE 2

It's freezing cold in Beijing already, and the baijiu even at 120 proof is just not doing the job anymore. You've done your best sourcing all across the capital under the ever-present eyes of Papa Xi's minions, but you haven't heard of any initiative to influence the election in the United States. Maybe you obviously missed something given how clamped down the capital is these days, or maybe there just isn't much anything going on over here? Should you report a nothing-burger?

SCENE 1

It's always a bit awkward to be an envoy to another country that your home country doesn't recognize exists. But as special envoy, it is your job to ensure that Iranian issues still get their hearings on the seventh floor of Foggy Bottom, and that generally means meeting with dyspeptic democracy dissidents in DC. Recently, a number of these dissidents have been speculating — presumably via contacts at home — that Iran wants to do more to disrupt the upcoming U.S. election as payback for what the regime seems to believe is U.S. interference in its own 2021 presidential election (plus the last couple of decades of tit-for-tat). You intend to raise the right alarms throughout the federal government.

SCENE 2

The Senator is known for his deep connections with the broader expat Persian community, and regularly hosts fundraisers with Iran regime-adjacent figures. For someone so close to the foreign policy workings of the United States, you've always been surprised by the bonhomie exhibited to one of the axes of evil, but one doesn't always comprehend the intricate mechanics of campaign finance. However, the recent video of his campaign staff taking a direct bribe from Iran has been declared a fake, and that seems premature from your vantage point.

SCENE 1

North Korean defectors have shrunk from a reasonably consistent flood down to a trickle. With the rise of North Korea's border wall on the Chinese frontier during the Covid-19 pandemic, the Hermit Kingdom has managed to almost completely stem the flow of information to the South and to the rest of the world. However, it just so happens that one defector managed to get away from an elite bureau of the Korean People's Army, an extremely rare insight into the closed regime. He describes how North Korea is attempting to increase its foreign exchange revenue by impersonating worldwide government agencies and securing cash through everything from taxes to parking fines. Can you spell IRS as K-I-M?

SCENE 2

While there haven't been any more key defectors from the North, you think you have found another one of the Korean People's Army tricks through a synthesis of intelligence that you were recently handed: a series of websites that allow you to pay to watch your ballot being recounted. These sites only take credit cards, but seem perfectly in line with what you know of the DPRK's modus operandi.

SCENE 1

There is a world outside the DC Beltway, and it's known as Virginia. There's also the rest of America, too, I suppose. Deep in the horizon somewhere before China is Eastern Oregon, where your brother Brad moved about a decade ago to pursue a "career" as a ski bum. A good-natured soul if still profitless from his bachelor's degree, he's recently become concerned about a group of neighbors who have been coordinating on Facebook about what they are dubbing "The Second Observation," which brings the Second Amendment's right to bear arms to observing elections in the United States. He keeps saying, "Yo man, it's bad," but he doesn't have much else to report.

SCENE 2

Your sources within the broad Russian disinformation world have informed you that Russia's new agency is using up-to-date AI techniques to wreck havoc on the U.S. elections. You don't really know how, but apparently, it has to do with interactive calls with voters.

Election Agency and Organization Roles



SCENE 1

The Help America Vote Act of 2002 instantiated this agency to improve the quality of America's elections in the aftermath of the Great Floridian Hanging Chad Debate of 2000. It's traditionally an anodyne Commission, but with elections coming under more partisan pressure, the Commission's work is increasingly facing tough scrutiny from all sides. One job of the Commission is to ensure that voter registration is fair and professional, and an analyst recently found that a number of jurisdictions are now using convenience fees for processing online voter registration forms. You control some of the purse strings for election assistance, and it's time to push back against these hidden taxes that are really just extractions from America's democracy and most vulnerable citizens.

SCENE 2

You just watched the video showing a group of poll workers dumping ballots behind a polling site in Florida's Miami-Dade County. But that can't be right — you recently helped transition that county to an all electronic model with a paper trail, so disposing ballots like this wouldn't do anything to the election. Why is the media so obsessed with this story?

SCENE 1

The hardest part of your job a couple of years ago was explaining that there were 50 more Secretaries of State than just the one that habituated Foggy Bottom. As the representative of the chief administrative officers of the various states, it's your nonpartisan job to protect the wherewithal of these key officers of American democracy. Recently, a Freedom of Information Request filed by a local reporter exposed that the secretary of state of a key battleground had emailed around a plan entitled "Confidential: Election Suppression Plan." How do you even begin to defend that? This job was supposed to be an easy 11-3 with a long lunch, and now it's turning into a 9-1-1 emergency.

SCENE 2

You've received reports from Minnesota and Michigan that their election portals accidentally posted fake election data that might have triggered the news media to declare the winner for the presidency too early. You check in with other secretaries of state to see if they have noticed anything similar.

SCENE 1

You expanded your cybersecurity and threat intelligence teams at Kingdom this year given that the paper cuts of the ballots of yore have been replaced by far more sinister threats. A researcher on your cybersecurity team discovered a series of posts on a dark-web forum of the GPS coordinates for all of the poll sites using Kingdom Voting Systems, an apparent leak of your company's customer database. Given that most voting equipment sales are in the public domain though, it doesn't seem particularly useful. You ask the researcher if they have seen anything else, and they report that Fentanyl has gotten cheaper: "Want me to get you some?" You briefly consider a euphoric high before shaking your head and walking away.

SCENE 2

The news media is rapidly disseminating the results of critical swing states like Minnesota, where your Kingdom machines are widely used. Yet, according to your data analytics team, none of the Kingdom voting machines have started uploading their voting data yet in the state. Were the election results pre-rigged?

SCENE 1

As the second-largest voting systems company in the United States, elections are actually relatively quiet affairs. Counties tend to purchase and test systems well in advance of the big day, which means that sales are quiet and the focus is on preventing the unthinkable: a hack or crisis that degrades the reputation of Intelligematic's hardware. Despite dozens of security threats being probed by your cybersecurity team and regular communications from the federal government, no one seems to have identified any serious threat to the election. All the threats seem a bit too much like a media narrative over empirical science.

SCENE 2

Your cybersecurity analytics team had time to analyze a video purporting to be from Miami-Dade County showing a group of poll workers throwing away piles of ballots. But a close-up analysis of the ballot papers shows that they don't match the format printed by the Intelligematic machines that were recently installed in the county. Something doesn't match.

Civil Society Roles



SCENE 1

You've been PAVE-ing the way for better ballot access for a decade or two or three — it's getting too long to be worth counting (unlike those ballots!). Recently, a number of PAVE network affiliates have reported that counties are accepting voter registration over the internet — but only for a convenience fee. Otherwise, constituents must print out the form and mail in their paperwork to be registered. The whole thing reeks of a neoliberal tech startup cashing in on an illegal poll tax, undermining the equity that you strive for in elections every day.

SCENE 2

You've been inundated with complaints from senior citizens in Maricopa County, Arizona that they are receiving threatening text messages and calls telling them not to vote on Election Day due to gun violence at their polling site. Some of the submitters said that they fell into conversations with the callers, who seemed "very weird" and "unfriendly" and seemed to run out of things to say after a few rounds of questions and responses. The callers never identify themselves, but did use the name of the person they were talking to.

SCENE 1

The Alliance for Ballot Integrity (ABI — no one could find a better acronym) stands for preventing the theft of American elections. Thou shalt not steal, and thou shall not steal an American election, for sure. Recently at church this past Sunday, a group of fellow parishioners reported their concerns about a new video on WeTube that showed the church pastor calling on voters to come out in droves to the polls, even though the church generally stays away from politics. The likeness was striking, and no one knows where the video came from. When asked, the pastor says that he did not record or post the video and confirmed that the church stays away from partisan politics out of deference to its IRS non-profit status.

SCENE 2

Multiple states are reporting early election results well in advance of when they would normally report data. With a surge of mail-in and absentee ballots, it seems impossible that the results of a majority of precincts could be reported within minutes of the polls closing. You smell something extraordinarily fishy, and it's not the fish tacos that are now cold sitting on your desk from earlier.

SCENE 1

One of the strangest aspects of being part of the UN system is recognizing the hypocrisy of Western nations when it comes to election integrity. Sure, there are the colossal global frauds that no one will defend, but there are also plenty of problems with the West's implementation of elections that shouldn't be papered over. Legacy systems are often far behind the quality of new systems with updated processes and procedures — and yet, no one seems to recognize that nascent democracies can do it better at times. And so when you discovered recently that a number of counties in the Midwest are mandating a \$20 convenience fee for processing online voter registration, you are hardly shocked. Now it's time to just write another angry report into the UN maw and return to Geneva.

SCENE 2

You've observed elections in dozens of countries, and so when the Postal Service suddenly had a slowdown right as the election took place preventing the processing of hundreds of thousands of mail-in ballots, you saw all the tell-tale signs of malfeasance typical of countries that generally have much less self-regard for themselves than the United States. This is election corruption of the first order, and winter storm or no winter storm, no government can pretend to slow so many ballots and not make it political.

Technology Company Roles



SCENE 1

OverAI's top product, RamblePTG, has been a massive success the past two years, garnering huge media attention and tens of millions of active users. The research team has been analyzing users' queries and the responding answers, hoping to upgrade PTG-4 into the next-generation PTG-5 model. Recently, there's been a massive uptick in usage from Belarus asking queries along the lines of "Using passages from the Bible, convince a Lutheran to not vote for a presidential candidate in America." A researcher sent an email over to OverAI's public policy team cc'd to you with some charts emphasizing the sudden increase and their concerns about electoral interference. It's one of a dozen priorities, and definitely not the top one.

SCENE 2

Your team has notified you on Election Day of a sudden surge of requests on RamblePTG asking for variations of the text, "There's an active shooter currently on the loose near your precinct voting location. Please stay home until an all clear has been issued by Maricopa County authorities." That sort of request violates OverAI's policies, but the requests are coming from hundreds of spam accounts that aren't paying subscribers. You direct the team to throttle these requests as best as they can.

SCENE 1

Bluemond, Washington has been such a hospitable home after many years suffering the travails of DC winters (not that Seattle and its Pacific Northwest environs are really all that much better). One of the more challenging jobs for any company is announcing failure, and recently, MacroHard had to deliver serious and market-moving negative news: it left its Relationship email server software unpatched for several months with a zero-day bug, which allowed any hacker to access a number of public agency email accounts. Logs might have been corrupted as well, making any changes made by the hackers almost impossible to track. That will be fun to explain to technophobic politicians.

SCENE 2

You instituted multiple protocols around core Generative AI algorithms that accompany most of MacroHard's products these days. Even so, several groups have been able to create deepfakes of leading political candidates on Election Day, and particularly after the election. You have submitted the deepfakes to the FBI, hoping to help them verify which videos might be forgeries and which ones you know nothing about and could be authentic. But the onslaught is overwhelming, and the FBI lacks the resources to do a rapid triage of so many different videos.

SCENE 1

Amazing Web Services has dominated the cloud infrastructure race the past decade, and global video streaming and delivery is one of the categories it leads the market. Recently, your cloud operations team noticed that there's been a surge of deliveries on a series of videos showing some political candidates — and notably a presidential candidate — offering citizenship to anyone who comes asking for it, presumably to goose up their election returns. In one case, the livestream broke, since the surge in traffic to the video was so sudden and so great that the traffic routers weren't prepared. What's going on with these videos, and should the company still be hosting them?

SCENE 2

Earlier this morning, it was brought to the Chief Information Security Officer's attention that there was a bug in a critical credential service that operates the identity and access layer for some secondary government websites. While none of the sites are likely mission critical, the bug would have allowed a user to break in and edit the sites. As part of responsible disclosure, it's time to notify those affected, although with Election Day and its aftermath in full swing, you're concerned (and maybe a little thrilled) that no one will pay attention.

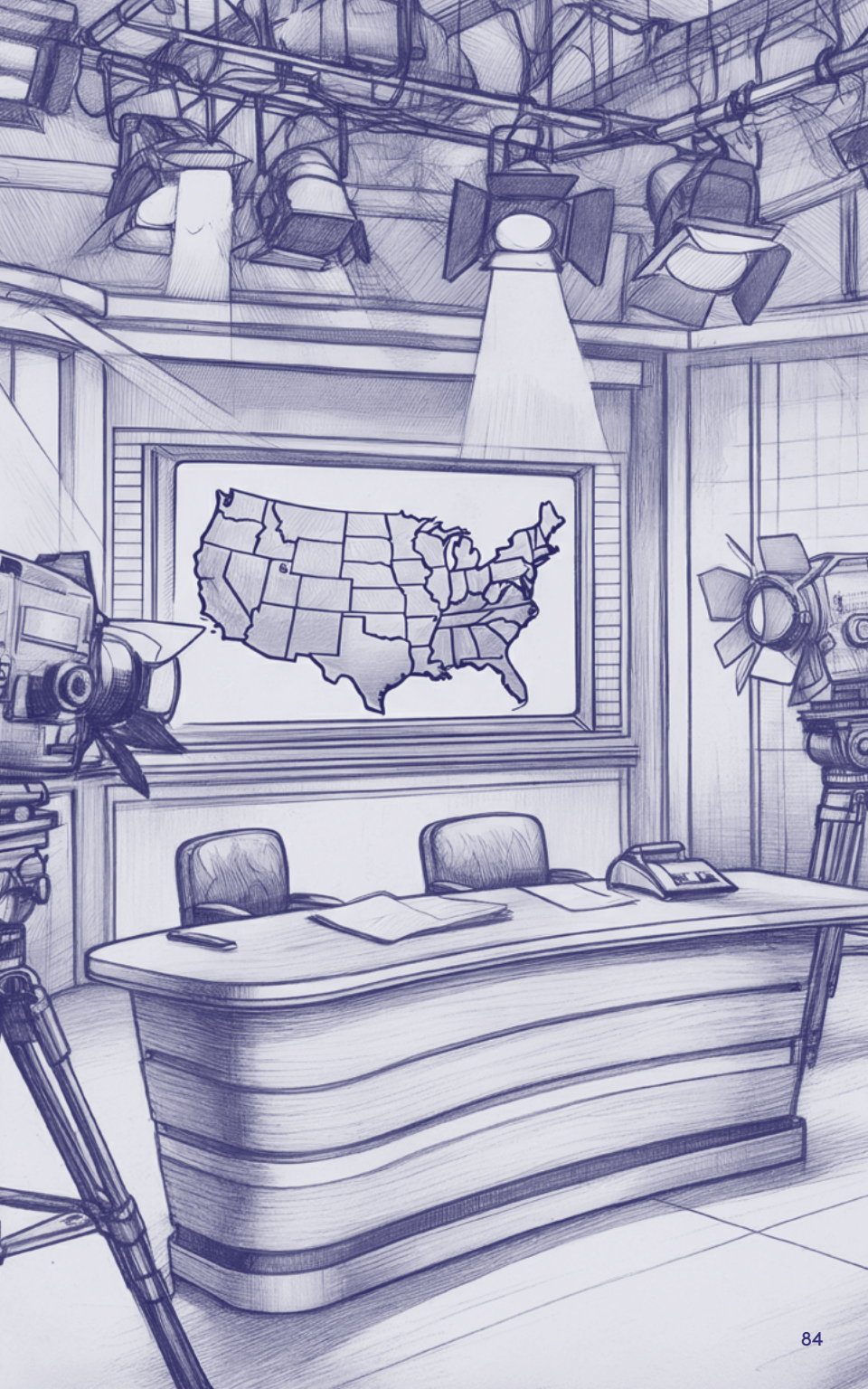
SCENE 1

As one of the most important services for software developers looking to send SMS messages to their end users, Whirlio happens to sit at the nexus of America's communications, even if many messages are simply six digit codes for two-factor authorization. One major use case that the company has marketed is its SMS reminders business, which recur and help to drive revenue. This year, SMS election reminders have been a big business for many political campaigns, one of those playbooks that everyone suddenly seems to follow. An analyst on your data science team, however, noticed that some of the election reminders being sent out have the wrong date on them. You knew politicians were dumb, but you didn't realize they were this dumb.

SCENE 2

In the days after the election, there has been a surge of SMS messages threatening that times are "going to get rough" as several states go through a recount process. In a typical example, an SMS message says that riots are inevitable and that one should "bring protection in case it gets ugly." You raise notes with your contacts in the national security and law enforcement communities, but they are overwhelmed with threats and aren't all that responsive to your data.

Traditional Media Roles



SCENE 1

Broadcast is the medium of choice for most humans on the planet. Sure, there are the elites that, like, read, or something. But for the vast mass of humanity, a well-crafted video on some sort of tube or a soothing radio program is always going to enthrall and capture their attention better. As the nationwide rep for local radio and TV broadcasters all across America for NCB (which always, always gets confused with NBC), you are always alert to any exception to this cardinal rule. And recently, there's been a number of local broadcast stations that have raised concerns that their social media traffic has waned in lieu of a new crop of online news publications that have captured the public's attention with decent local reporting, a comprehensive set of articles, and voter guides for the upcoming election. Who is funding such an extensive and deeply-reported network of sites? Does this spell the end for "if it bleeds, it leads?"

SCENE 2

Multiple radio stations who are organization members have written in and said that their call-in shows are slammed with voters frustrated by the level of gun violence at their polling places. While it's hectic on Election Day and in its aftermath, so far the media hasn't reported any deaths anywhere in the country though — why the discrepancy?

President, Digital News Association in Radio and Television (DNART)

SCENE 1

Traditional and online news media — which forms the backbone of your non-profit organization — has been on its back heels for years now, riven by partisanship and crushed under the weight of unprofitable business models after years of pivoting to video, pivoting away from video, pivoting to subscription and finally, pivoting to annihilation. Yet, the work that journalists do everyday to watchdog the U.S. government is more critical than ever. Recently, there have been claims that there are fake news websites popping up all across the U.S., but there have already been several who have joined your organization, and so far, they all seem to have good origin stories. You sense a conspiracy to malign the good work of the next-generation of local reporters — not a rarity in this hyper-partisan era.

SCENE 2

News directors across America are pursuing stories about a “day of action” in which a citizen militia threatens to invade ballot recount centers across several critical swing states. They are also saying that many citizens are getting ominous texts and voicemail messages warning them to stay away from such centers, since they might soon become locations of violence. It’s a story, but also feels like some sort of crime is underway.

SCENE 1

The election year is tight, but the only thing tighter is the ratings. With established candidates repeating the same campaign anthems of yesteryear, ratings are tough — and the election cycle is the most important year out of four for driving those profit numbers up on a mostly-news channel. Recently, one of the associate producers on daytime discovered a video of a major presidential candidate's staff offering some sort of document to non-U.S. citizens and encouraging them to vote. She warned that it would take some time to verify, but this is exactly the kind of thing that you do process journalism on — report every bit of the story publicly including the verification process. You order straight for broadcast and think about that bonus check after the election.

SCENE 2

For a lousy year of ratings, you finally got a last-minute fillip of good news (well, bad news, but that depends on your profit model!) After serious bad weather, the Postal Service fell behind on mail delivery throughout the country, just as the election was getting underway, delaying the delivery of mail-in ballots. If that wasn't enough, now members of a shadowy "Citizen Election Security Brigade" are breaking into postal processing centers and attempting to prove that the postal service lied about the delay. This has got all the drama for primetime and daytime TV, and is just the story of electoral malfeasance you were looking for.

SCENE 1

Michigan is the battleground state that could flip all of American politics, and that means you're inundated with visits by candidates and their surrogates. Covering this all for the leading political journal in the state is taxing, not least because the takeout salads just aren't what they used to be given inflation. While nibbling on a Caesar salad that you'd like to "Et tu, Brute?", your old friend Julie from your high school days starts texting you about her fears for the integrity of the upcoming presidential vote after years of no communication. She says that she is considering heading to tomorrow's Lansing Gun Show and purchasing a new rifle for "the riots on Day One, or even just to stop the riots in their tracks on Day Zero." She follows up with a fire emoji and a meme that doesn't make any sense to you, and you hope, anyone else.

SCENE 2

You've been covering Michigan politics for a very long time, and you have never seen an election that is coming down so close to the wire called so early in the Wolverine State. You don't recall the state updating its election procedures to make the ballot count easier — so how could so much information be ready so soon?

SCENE 1

Blogger. It's one of those job titles that feels legitimate today, even though you know it's a neologism that barely registers in the grand expanse of humanity's existence. But it's better than your previous life as a journalist, where constant layoffs and the forever threat of a hedge fund takeover loomed over the horizon. You've taken the American Electoral Project to new heights, covering the intricacies of election security the past few cycles. But recently, you were offered a job at a new news startup in your hometown, a site that didn't exist two years ago but is now conquering social media and the reading diets of the local citizenry. They're offering you the best of both worlds: don't quit the blog, but write for us as well. Oh, and a pretty penny to boot. Why not take the offer?

SCENE 2

The active shooter threats have been coming in all morning of Election Day. You notice that there is a correlation between their locations and the work you have been doing on a political extremist group that is hellbent on overthrowing American democracy and replacing it with a cult-like leader known only as "The One." The news media seems completely unable to connect the dots between the different events though, so you sit down and get writing on a new blog post that you hope might get picked up by the Times.

Social Media Roles



SCENE 1

Chirper, rebranded “Y” these days (but no one calls it that because it asks an existential question no one can answer), has been your home for the past few years. Quite literally, as you sleep six days a week on a couch that your billionaire patron brought into the office from one of his châteaux. In your position, your job is to try to do ... something, for the country or at least for your sanity and theoretically for the company as well. Recently, there’s been a surge of activity related to a series of videos showing a major presidential candidate’s team offering some sort of citizenship certificate to un-qualified voters. Real or fake? Should we take it down — or stoke the traffic that’s been multiplying rapidly?

SCENE 2

Traffic is roaring over a video from Miami-Dade County showing election workers manipulating the vote there. A huge number of prominent and well-verified accounts have cross-examined the video and proven its authenticity. Plenty of people have reasons for hiding the mistakes in the U.S. election system, but that’s why free speech and the First Amendment is so important: to allow citizens to correct their government’s overreach. Chirper’s algorithm is tilted to amplify the controversy and drive increasing traffic, and you hope, also spread truth in America as the Founding Fathers intended.

SCENE 1

WhutsUpp? It was a Budweiser tagline, and now it's the world's most popular chatting app. As the leader of the cyber policy team, it's never a dull moment trying to track what a billion-plus users are doing everyday, a challenge that's only become more opaque with end-to-end encryption the past few years. Recently, there's been a surge of takedown requests filed through the app by users pointing to many WhutsUpp channels which are attempting to impersonate well-known local media franchises. The cases are challenging since the names don't match any existing media publications — this is definitely one for the legal team to flesh out, and you send off a note to the general counsel for guidance.

SCENE 2

WhutsUpp has been a critical hub for election conversations, but one of the biggest challenges around cyber policy has been a series of pseudonymous accounts that have stoked election fears, particularly in local mayoral elections on issues like homelessness and crime. Data scientists show that many of the commentaries aren't originating with U.S. phone numbers, which are mostly required for use in the app. You send notes to the government about what may be a foreign influence campaign in U.S. elections.

SCENE 1

Despite being an ostensibly ephemeral photo sharing app, the reality is that the digital history of all FlashChat users is anything but ephemeral. Most public policy issues at the company these days involve various forms of catfishing and the illegal outreach to children by potential predators, but the election and FlashChat's widespread success among youth has suddenly made domestic politics a huge priority for the policy team, which falls under your purview. You've repeatedly asked your data science counterparts for information about the virality of certain types of menacing posts about the election, but so far, they have been unable to find any patterns in the data. Maybe it's mostly ephemeral after all?

SCENE 2

Images and messages are circulating all over FlashChat about how a group dubbed the "Citizen Election Security Brigade" is planning on hosting massive violent operations at polling sites all across the country, potentially using guns. The messages are centered in a handful of swing states, and younger users are particularly terrified of voting due to regular coverage of school shootings in the national media.

SCENE 1

It's never a dull moment at WeTube, which brought a collective spirit to video sharing that the hostile "You" branding just couldn't accomplish. You took over as VP of Content in 2021, right after the last big U.S. election, and you are raring for action during the 2024 contest. There's been the usual pabulum, with illegal videos shared and then taken down following the company's long-standing disinformation policy. But recently, a smart data scientist on the elections policy team unearthed a disturbing new trend: a number of videos purporting to be from religious leaders pushing their believers either to vote or not vote, often on channels with few to no followers. The page views on these videos are significantly higher than normal for such new channels without algorithmic amplification, raising the question of how people are finding these videos.

SCENE 2

A fake video of a Senator's campaign manager accepting money from Iran through Bitcoin has been spreading rapidly across WeTube. The Senator's staff has asked for it to be taken down for libel, and you have complied after a group of well-known computer scientists declared that the audio and video in the clip is a deepfake.

Telecom Roles



SCENE 1

BT&T has been through the wringer over the decades since Mama Chime was broken up in antitrust action decades ago, only for the industry to assiduously re-consolidate down again to three main players. For the past few years, the focus was on expanding network quality through 5G technology as well as expanding access to differentiated content. Recently though, 5G expansion has hit a major snag: armed vigilantes who are randomly knocking out cell antennas fearing cancer. With so many more systems to be installed, it's slowing progress on BT&T's wireless network expansion plans. You've recently explained to government officials the importance of cellular quality to elections — the only thing people seem to be watching these days, since they certainly aren't watching those media assets the company purchased.

SCENE 2

With illegal active shooter threats being called in all over the country, you have taken the unprecedented step of using your company's first responder network asset and texting a message to all domestic police and firefighting personnel that there has been a surge of fake threats being called in across the country, and to be sure to verify any claims of violence with actual evidence. That decision erupts in controversy both across the media and among first responders, who find the use of a critical communications channel for political uses "disgusting."

SCENE 1

Unbeknownst to most Americans but knownst to most national security officials, VastHorizon has an extensive keyword-based analytics infrastructure that evaluates billions of unencrypted SMS text messages each day for phrases that might indicate criminal or terroristic intent. In the past few weeks, there has been an astonishing increase in discussions indicating violent intent with weapons and especially a type of custom-modified AR-15 assault rifle popular with 3D printing hobbyists. The phrase “Battle of Balaclava” is also trending in the analytics dashboard.

SCENE 2

You have been recently notified by a network infrastructure equipment provider that there was a major flaw in the security and authentication layer of the product that may have allowed some text messages to be rerouted without knowledge of VastHorizon. Because of the nature of the flaw, there are no good logs on exactly what took place, but you suspect that the timing of the flaw and the election is no coincidence.

SCENE 1

CosmicCast walks a fine line on electoral politics, given the importance of friendly local officials in offering profitable franchise agreements for cable services. That takes up the bulk of the government relations work at the company, but this year, the intense U.S. election is also drawing more than its normal share of attention. You've heard increasing concerns from some of the leaders of the telecommunication workers union about threats to cable infrastructure as a means of shutting down the vote. They are asking what the company is doing to protect workers in the event that they become the target for some of this radical ire. You promised to raise those concerns with local, state and federal officials.

SCENE 2

There has been a surge in advertising dollars for a set of television commercials claiming that a "day of action" is near, and that every citizen may have to rise up to protect democracy from those who would shut it down. The boost in ad revenue is a godsend in a tough economic year for the media industry, but given the content, you did inquire with the ad sales teams to check the source of the funds. So far, all of them appear completely legitimate.

White House Roles



SCENE 1

Cybersecurity is overwhelmingly important, which is why decades after the first computer virus swept through university computer clusters, there's finally a National Cyber Director advising the president directly on these issues (better late than never, one could say). One concern of yours recently has been around North Korea's global pillage of financial systems in pursuit of currency reserves. After the theft of tens of millions of dollars from the central bank in Bangladesh in 2016, the federal government has found hints that North Korea is extracting money out of America on a regular basis. But from where?

SCENE 2

One of the most important security considerations for the government is wireless, and you were recently informed by a major equipment vendor that there was a bug in its security software that allowed SMS messages to be re-routed without the knowledge of the network operator. That might explain why millions of Americans have been getting violent text messages the past few days during and after the election. You rush to disseminate the news across the government.

SCENE 1

Like many White House functions, the CTO's job is to coordinate an impossibly diverse alphabet soup of agencies and departments around IT policy. Such a corporate job would be difficult even with the board and CEO's blessing, but the cacophony and turf wars of official Washington makes the job all but impossible. One of the most important initiatives you have been working on has been accelerating the deployment of software patches across government software. Fed IT policies generally require significant testing before patches can be released, but with the number of zero-day hacks increasing, the government needs to patch faster lest it leave critical information systems open to any hacker in the world. You've emphasized this at the federal level, but even more work needs to be done at the state and local levels.

SCENE 2

One of your more lurid fascinations on the web is following hackers live-streaming their exploits on sites like OnlyHacks. It's amazing watching some of the best white-hat and sometimes black-hat hackers as they work, and it gives you an insight into the minds of the people that often fight back against the government. Will a channel showcase some sort of election tampering or hacking? You don't want to watch American democracy end at the touch of a keystroke, but it is amazing to watch it nonetheless in the comfort of a warm bed.

SCENE 1

Artificial intelligence went from academic research labs to the center of the national security discussion in just a few years, and that means you are now managing one of the most rapidly-changing and yet little-understood aspects of the modern threat environment. You've been skeptical about the potential for some of these technologies like deepfakes — there's a calibration required between speculative fiction, science fiction and science fact — and it's critical to get that right. Recently, you had conversations with a group of human rights leaders, who said that they all have had deepfaked videos of themselves posted on WeTube and other video sharing platforms. Some of the videos are innocuous and seem like harmless fun, but others attempt to undermine the case for global human rights law or push voters to protest elections by staying away from the polls. It seems like a domestic source is producing these — but who?

SCENE 2

Over the past few months, you've attempted to put together the rudiments of a deepfake verification group, a network of organizations that attempt to ascertain whether a piece of content is fake or real. So far, they've identified thousands of AI-generated images related to the election, and that's helped to tamp down a lot of problems. But one group in particular, which goes by the name of "StudioGhAlbli", has been more successful than others in impersonating candidates, particularly governors. You are trying to bring more attention to the issue of state executives, since the media seems only to care about the presidential race.

SCENE 1

It's your job to shore up America's information infrastructure, a task that is Sisyphean in its travails. One of your top priorities in recent weeks has been attempting to secure more iPhones in the government by using Apple's new Lockdown Mode feature that prevents the auto-loading of content and that should prevent some foreign intelligence gathering through zero-day hacks. You just read a new report indicating that dozens of key personnel around the upcoming election have had battery issues with their iPhones — likely indicating some sort of uplink that's transmitting information and draining their batteries faster than usual. A cursory search on the web doesn't show that the battery issue is widespread.

SCENE 2

Your daughter, who is studying computer science at MIT, says that there is a new hack circulating around the dark web that can break into both of the major ballot machine systems and adjust voter counts as they are uploaded to the internet through wireless cellular communications. Since most states won't do recounts, the changes could have vast repercussions for the election that just took place. You thank her, hang up, and then just realized that she mentioned that she's crawling around the dark web. What are they teaching up there in Cambridge?

SCENE 1

The thrill of the pace of the White House Comms operation continues to flutter in your heart even as critics remain relentless in their fusillade of critiques against you. At the mid-morning press gaggle that you hosted for the press corps outside the Brady Briefing Room, several reporters from regional papers asked about rumors that there is some sort of shadowy cabal that intends to bomb or kill people as they walk to the polls, and whether you had heard anything about that? You said, completely off the record, that you had no information on such a network, but would check in with national security leaders and get back to the assembled group. You urged the press not to report on such weak and fear-mongering rumors without justification and deeper investigation.

SCENE 2

Watching poll workers throw away ballots in Miami, you are shocked but not surprised. Some analysts have analyzed the video and declared it fake, while other legitimate analysts have declared it real. The president demands the highest focus be placed on election integrity, which means communicating that the federal government will immediately investigate these poll workers and whether their actions should be prosecuted.

SCENE 1

Empirical economic research is the lifeblood of the Council, and it's your job to corral that work and make it useful to the President and the broader White House. Recently, a working paper has been circulating on social media demanding more oversight of certain voter precincts for fraud. The author, who wrote under a pseudonym, uses a geospatial discontinuity statistical design to prove that a number of precincts are at far higher likelihood for fraud than others. This individual demands that the Federal Government increase oversight of those locations, which happen to correlate with key demographic groups in the election. The Council rejects the methodology used in the paper (the results seem to be the artifact of bad statistical code), but it is getting serious attention across social media if not the mainstream press.

SCENE 2

After claims that the Senator accepted money from Iran went viral all over social media, you asked a professor who is extremely proficient in cryptocurrency transactions to look into the case. Despite some level of obfuscation and mixing to hide the digital currency trail, it does indeed appear that there is a trail from Iranian-held accounts to the Senator's campaign fund. Why no one is focused on the evidence remains a mystery.

SCENE 1

As a long-time economics professor on the business of media, your academic research has touched on everything from antitrust theory and industrial organization to the economics of information, public goods and the value of open-source software development. It was that wide range of research that brought you into the White House. Recently, your hometown newspaper converted its paper copies into an online edition covered in ads and mostly distributed through social media. The company kept about 2-3 of the original 6 reporters, and it's been great to get the news back home without the need for paper delivery. The one curious fact though is that they changed from the "Times" to the "Tribune" — maybe there is a future academic theory paper about names, brands and online distribution?

SCENE 2

For years, your mother has been an election judge in your hometown. She's reporting that there have been numerous threats to the ballot recount center where she has been assigned, and she told you that she refuses to go in despite it being "my civic duty." She says that many other recount judges are making a similar decision as well, fearing for their safety after a list of recount sites was posted on the internet with veiled threats against them.

SCENE 1

Paranoia abounds everywhere in your work. The truth is getting tougher to understand, and the raw sewage of noise has completely overwhelmed the signal available to everyone in the national security world. Recently, you saw a clip of the president's campaign staff offering citizenship certificates to newly-arrived immigrants, a clip that was easily debunked but is now spreading throughout social media and the mainstream press. You've attempted to track down its source, but have found nothing. You also attempted to call the policy leaders at companies that are amplifying the story, but that tactic was fruitless. Does anyone care about the truth anymore?

SCENE 2

Before the election, you had brought together a fusion cell to evaluate high-profile videos and other media that might be deepfaked or edited to try to get ahead of major news stories planted in the media by foreign adversaries like China. But the fusion has become diffuse, after the group split 50/50 over the recent video from Miami showing poll workers throwing away ballots. It seems ridiculous to imagine that any manipulation to an election could be so crude, but then again, is it really so hard to imagine?

SCENE 1

One of the sundry tasks of your job is ensuring that cybersecurity threat intelligence and information is properly collected and disseminated across the White House and throughout the federal bureaucracy. Recently, there's been an uptick in foreign governments using specialized device intrusion software to break into iPhones using hacked iMessages that can lead to exfiltration of critical user data. You've teamed up with the White House deputy CTO to try to encourage more government employees to protect their devices, while advising the president about the risk of further foreign leaks.

SCENE 2

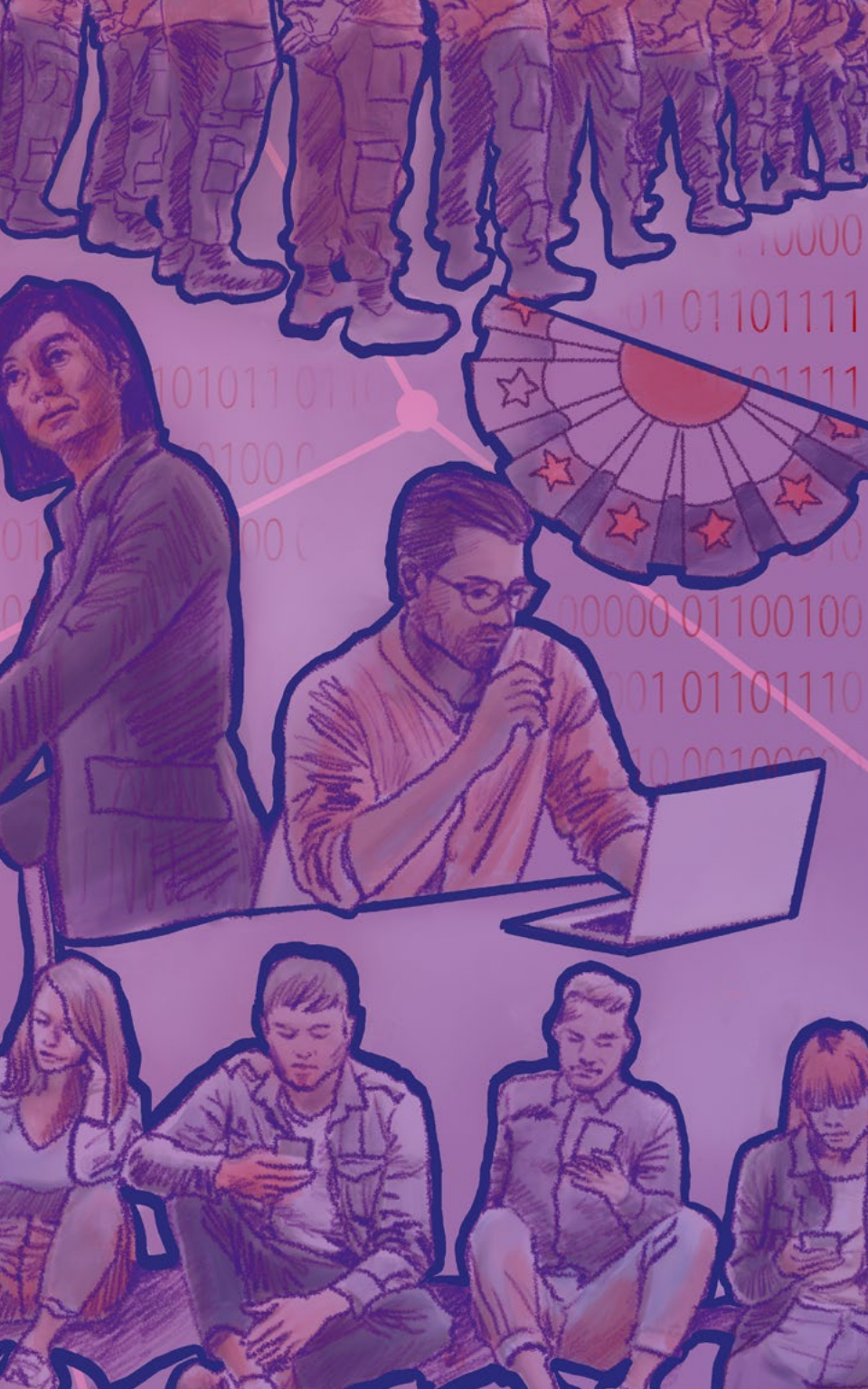
Protecting the count of the vote is crucial for a fair election, but the government was much more prepared for Election Day than for the inevitable aftermath. Now, there are threat intelligence reports lighting up all across the country that could undermine recounts underway in multiple swing states. You inform White House staffers, but they are in a bind: if they intervene, then it might appear that they're attempting to influence the vote, and thus, the outcome for their boss. Even so, you demand much more immediate action.

SCENE 1

One of the jobs that has rolled up to you in the labyrinthine design of U.S. IT policy is software supply chain security, and ensuring that all code running on U.S. devices is signed by friendly nations (or at minimum, isn't running code from unfriendly nations). Recently, the CTO office has learned that many laptops are running a time-zone calculation tool that originates from China, and that regularly connects to overseas servers. Cybersecurity reviews haven't found any important data in these uploads, but the uploads have increased as the election has gotten closer.

SCENE 2

After the video of the Senator's staff went viral, you asked a group of top deepfake experts who you convened to help with the U.S. election to observe the video. Using the most up-to-date algorithms, they determined with a high degree of certainty that the video was a forgery, likely designed to undermine the Senator's flagship issues on foreign policy. It's a great example of how academic-government relations can help bring truth into the light.



Threats

Scene 1: Before Election



VOTER REGISTRATION

RETURN ENVELOPE

1

Charge of the Ballot Brigade (Primary)

A decentralized network of political cells as part of the "Citizen Election Security Brigade" movement is making phone calls and texts to each other coordinating a loose plan to send armed citizens to major polling sites and ensure that the election is not rigged.

PLAYERS INVOLVED:

9, 21, 24, 36, 43, 49

KEY LESSON:

Bottoms-up, decentralized groups can be hard to find, and likely will fall under broad constitutional protections for free speech and free association.

Russia's government activates a new Internet Research Agency-like group for increasing the vote of certain demographic groups and reducing it for others. Downloading videos online of prominent speakers — including pastors, mayors, and other civil society leaders — the agency creates deepfake audio clips with targeted messages and voicemails them to key voters.

PLAYERS INVOLVED:

3, 17, 27, 29, 41, 47

KEY LESSON:

The toughest deepfakes to fight will be of high-trust local figures who have content of themselves online.

Voters in several large counties get text messages telling them they need to register with the county in order to vote in the upcoming election. Clicking the link leads to a personal information form, which can be printed and mailed to the county or submitted online for a \$20 TicketMaster-like online convenience fee. The payment gateway offers multiple means, including cryptocurrency, to pay, all of which are routed to a bank in Macau, and ultimately to North Korea's overseas business development wing of the Korean People's Army.

PLAYERS INVOLVED:

4, 20, 22, 26, 28, 45

KEY LESSON:

Not all election interference is political. Many organizations and governments may just want to make money, even if illegal.

4

All The News That Isn't Fit To Print

A network of fake online newspapers with AI-generated articles started publishing in late 2023 in so-called news deserts in major battleground states. Social media traffic has picked up tremendously, and in a handful of cases, former reporters have joined the sites as local writers. Recently, the newspapers have been offering more opinionated content and telling certain voters details about polling information that isn't accurate ("Early voters are wasted votes"). The ultimate origin of these sites is unknown.

PLAYERS INVOLVED:

8, 12, 33, 37, 39, 51

KEY LESSON:

Vetting news sites is nearly impossible today given the rise of citizen journalism and the shrinking of traditional media.

Freedom of Disinformation Request (Primary)

A well-known metro newspaper reporter files a freedom of information request (FOIA) to the secretary of state's office in a major battleground after receiving a shadowy tip that the office is attempting to undermine the local election. The reporter unearths a set of emails and replies from members of the staff under the subject line, "Confidential: Election Suppression Plan" detailing changes to polling sites to limit the turnout of certain voters. These emails were planted on the servers by hackers using an unpatched version of a popular email exchange server software and recent GenAI text platforms.

PLAYERS INVOLVED:

11, 15, 23, 30, 46

KEY LESSON:

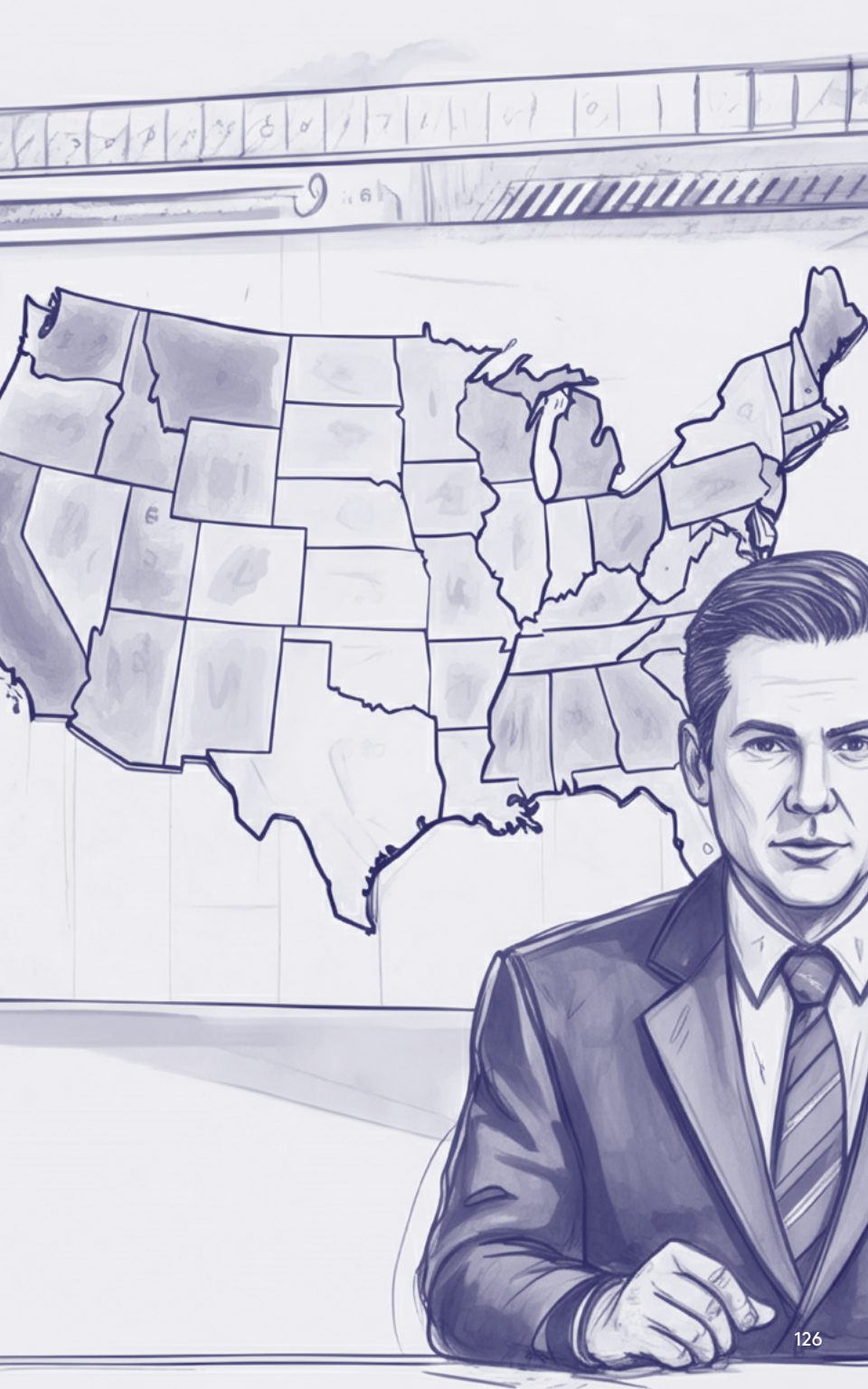
Hackers don't always try to exfiltrate information out of an organization — they can also plant information to embarrass someone or cause fear, uncertainty and doubt.

Video ads on popular social media networks show what purports to be the staff of a major presidential candidate offering "citizenship certificates" to recent migrants to the United States along with instructions on how to vote for a specific candidate. The videos have been posted as news, and amplified through payment, without triggering the networks' elections or politics rules.

PLAYERS INVOLVED:**6, 13, 31, 35, 38****KEY LESSON:**

Media economics have only gotten worse in the past decade, with greater and greater incentive to focus on controversy over verification.

Scene 2: During and After Election



1

Fear Factor (Primary)

Voters over the age of 65 in Maricopa County, Arizona are targeted with interactive deepfake AI robo-calls placed by Russia's new agency about their polling places being closed because of threats from militia groups. The calls describe how the "Citizen Election Security Brigade" is involved, and warn voters not to visit their polling places. The Brigade is not involved at all, but is just being named since it has been circulating in the news media.

PLAYERS INVOLVED:

9, 21, 26, 29, 33, 40

KEY LESSON:

Foreign forces can usurp the name and identity of domestic groups to pursue their own agendas.

While livestreaming on Twitch, a high school student hacks into the Secretary of State offices of Michigan and Minnesota and posts fake election results data a few minutes after the polls close. Major newspapers and outlets programmatically report the results in their online visualizations, and are prepared to call the election early given the swing of Electoral College votes.

PLAYERS INVOLVED:

23, 24, 27, 31, 36, 46

KEY LESSON:

The motivations of some attackers of U.S. elections are just for the "lolz." Also, the media's election coverage is increasingly automated in the competition to call an election first, risking uncertainty about elections if early calls are wrong.

An extremist political group calls in fake "active shooter" threats to multiple busy polling sites in swing states during the busy early morning voting period. SWAT Police shut down the polling sites and clear them quickly, but people waiting in line have already left and may not return. News coverage of the potential shootings are covered in all national publications, and several fake AI videos circulate showing victims running and screaming that are mashups of other mass shooting events.

PLAYERS INVOLVED:

4, 7, 10, 37, 42

KEY LESSON:

AI can accentuate concerns about physical security to diminish voter turnout.

Audio clips are published across social media purporting to be the campaign manager of a major senatorial candidate admitting to accepting money via Bitcoin and other cryptocurrencies from Iran. Disinformation analysts speculate that it is deepfaked given how blunt the campaign manager speaks about the bribes, and computer scientists and algorithms identify the clip as a deepfake as well due to specific distortions in the audio file. However, the clip is actually real and was just compressed badly upon upload. The senator did indeed take money from Iran.

PLAYERS INVOLVED:

2, 3, 19, 41, 50, 54

KEY LESSON:

Verification algorithms are in their infancy and can be wrong. Extraordinary scandals might also be true.

Reduce, Reuse, Revote (Primary)

A series of images and videos goes rapidly viral across social media showing what appears to be poll workers disposing ballots in Miami-Dade County, Florida. The virality was triggered by a bot-texting campaign that originated in Russia. Analysts are split on whether the material is real or fake. Several key media outlets lose access to their social media accounts, which are used to post stories reinforcing the bot-texting campaign by an offshoot of Iran's Islamic Revolutionary Guard Corps. The reality is that the scene was actually staged by actors, but then enhanced with AI to look more realistic. The group posted it as a joke on a darkweb forum, where Russian operatives saw it and began spreading it.

PLAYERS INVOLVED:

16, 17, 22, 25, 38, 49, 52

KEY LESSON:

Foreign influence may reuse domestic content in order to increase its authenticity. Stories around AI use can be quite complicated with multiple steps and actors involved.

A surge of mail-in ballots and bad early-November weather has stymied the Postal Service and slowed delivery across large swaths of the country. Rumors circulate on social media that the Postal Service is purposely attempting to adjust the vote by opening ballots and switching them out. The "Citizen Election Security Brigade" begins breaking into postal processing centers looking for potential malfeasance. The Postal Service, caught unprepared, loses chain of custody on some boxes of mail-in ballots, exacerbating doubt about the election's outcome on whether all ballots were counted or whether some were changed.

PLAYERS INVOLVED:

5, 8, 12, 28, 35

KEY LESSON:

A cascade of unfortunate events and reactions can quickly undermine the integrity of the election in the eyes of the typical U.S. voter.

There is a spike in TV and digital advertising calling for a day of action in several states with election results that are too close to call. The ads use menacing tones urging Americans to descend on the contested states and "bring protection in case it gets ugly." Online organizers begin putting together lists of ballot recount sites, and voicemail and SMS messages threaten violence against anyone who shows up at the sites. Ballot counters, afraid for their safety, don't arrive, slowing the counting process.

PLAYERS INVOLVED:

32, 34, 44, 51, 53

KEY LESSON:

Counting the vote accurately is just as important as ensuring the safety of voters on Election Day.

Players with Unused Clues

In the first scene, the following players' clues weren't used for any threat: 1, 2, 5, 7, 10, 14, 16, 18, 19, 25, 32, 34, 40, 42, 44, 48, 50, 53, 54.

In the second scene, the following players' clues weren't used for any threat: 1, 6, 11, 13, 14, 15, 18, 20, 30, 39, 43, 45, 47, 48.

Contact

Contact Us

For questions or comments related to riskgaming or this scenario, please email riskgaming@luxcapital.com.

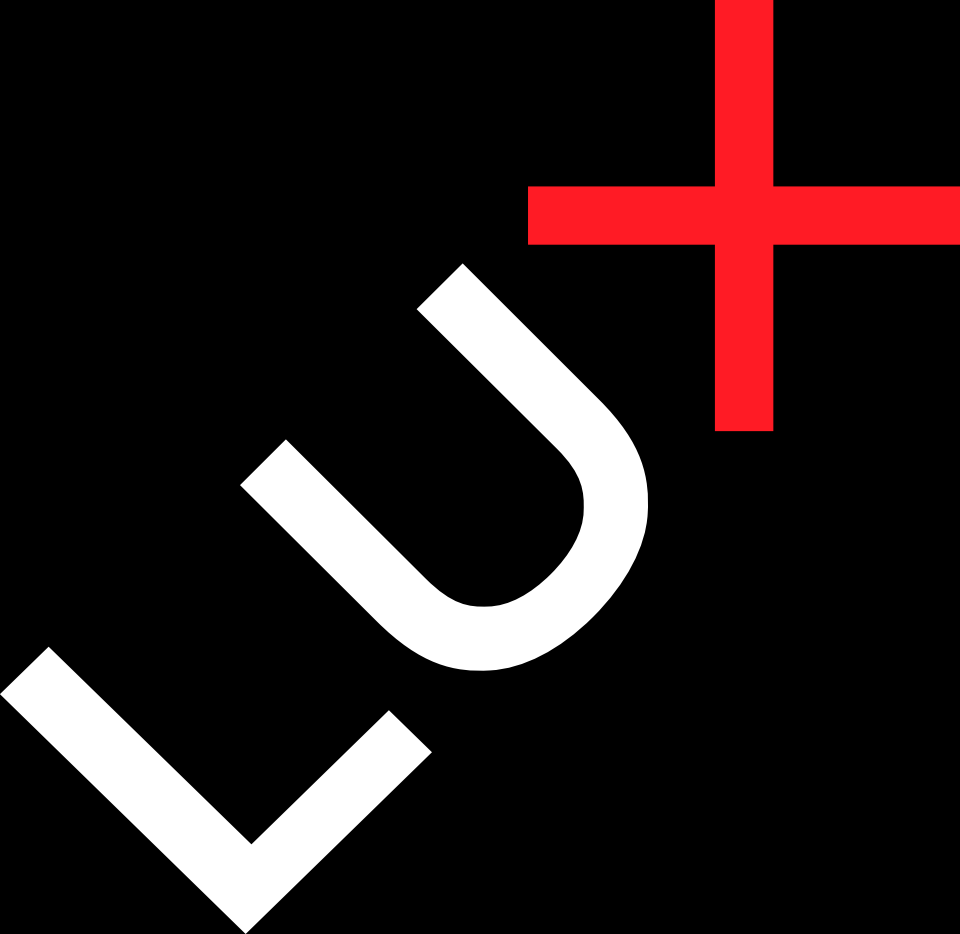
For press inquiries, please email comms@luxcapital.com.

New York

920 BROADWAY 11TH FLOOR
NEW YORK, NY 10010
[P] 646.475.4385

Silicon Valley

1600 EL CAMINO REAL, STE 290
MENLO PARK, CA 94025
[P] 646.475.4385



New York
920 BROADWAY 11TH FLOOR
NEW YORK, NY 10010

Silicon Valley
1600 EL CAMINO REAL, STE 290
MENLO PARK, CA 94025