cybereason

BLACKOUT

PROTECT THE VOTE

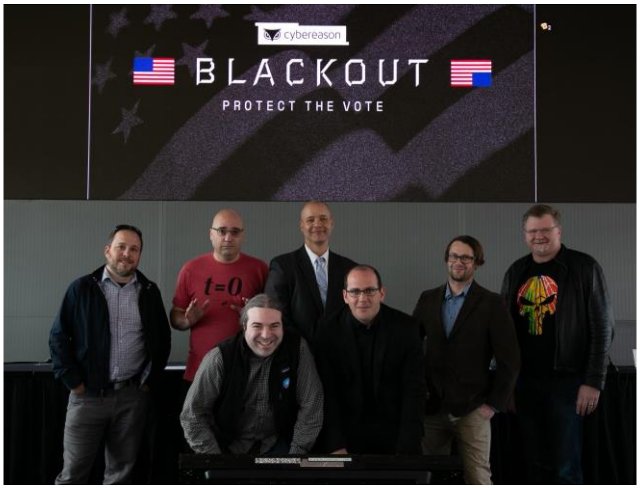
# Operation Blackout Summary of Events

Washington, DC

November 5, 2019

Recent times have seen election tampering by special interest groups and foreign powers in the United States, Europe and Asia. With a looming 2020 presidential election in the United States, Cybereason hosted an election hacking tabletop exercise on **November 5, 2019** in Washington, DC.

The goal of the tabletop exercise was to examine and advance the organizational responsiveness of government entities to an anarchic group’s attempts to undermine democratic institutions and systems of governance in the republic. Most election hacking discussions and exercises focus on the mechanics and minutiae of hacking election equipment or contaminating and violating the integrity of voter rolls. This exercise **explicitly excluded hacking election equipment** from consideration to focus instead on everything else in the electoral system.



## The Teams

The scenario pitted a team of veteran law enforcement officers from the US Secret Service, Department of Homeland Security, the FBI, and the Arlington, VA police against a group of ethical hackers, academics and security professionals from the private sector. The law enforcement team was the *Blue Team: Adversaria Task Force*, and the white hat hackers were known as the *Red Team: Kill Organized Systems (K-OS)* hacktivist group.

The game administration and control as well as *ad hoc* role needs in the game sequence was controlled by a *White Team*, run by industry veteran and CSO Sam Curry, as well as Managing Director of Cybersecurity Services at Venable Ari Schwartz. Sam's Cybereason-staffed team both adjudicated the event and provided US Federal support options as appropriate. The *White Team* also benefited from both experience with federal and state governance processes and the presence of seasoned government officials as observers of the event.

## The Setup

The event took place in the fictional city of *Adversaria* on a typical November election day. Turns in the simulation lasted 20 minutes of real time, each modeling 4 hours in the simulated autumn day. The event started with a short strategy turn and was followed by three additional turns. Once both teams had submitted their turn moves, the white team decided how these moves impacted the simulation. They then informed the teams of any changes to the environment, and teams pursued the next round of moves.

Each team is allowed a set of two actions and one development per turn, known as their turn moves.

**Red Team Moves:**

- **Development:** A development is a capability the team wishes to develop so they may use it on subsequent turns. For example, Red Team may wish to develop the capability to use deep fake technology. They would need to expend a development turn to develop the capability, then they may use the capability on the next turn in the game.

- **Action:** An action is a capability the team wishes to expend during a turn. For example, the Red Team may wish to gain access to the social media accounts of the local government. They would need to expend an action turn to use this action.

**Blue Team Moves:**

- **Development:** A development is a capability the team wishes to develop, typically by asking for assistance by calling up reserves, calling on other agencies, or by getting assistance in other ways. For example, Blue Team may wish to call the federal government (the White Team) for additional support if they need more boots on the ground. They would need to expend a development turn to develop the capability, then they may use the capability on the next turn in the game.

- **Action:** An action is an assignment of a group of officers to a task. For example, the Blue Team may wish to deploy 100 police officers to polling stations at zones 3, 4, and 7. They would need to use an action to deploy the officers during a turn.

There is a lot of leeway for what makes up an action or development. In a single action, one may accomplish several goals. For example, the Blue Team may expend one action to deploy 100 police officers to polling stations at zones 3, 4, and 7, while also using the same action to send harbor patrol to watch bridges. For both teams, action turns can be turned into Development turns if so desired, but the reverse was not allowed.

The *White Team* determines what moves are too far out of scope for the turn.

<table>
<tr><th colspan="2">TURNS</th></tr>
<tr><td colspan="2"><i>Introduction for All Participants by White Team</i></td></tr>
<tr><td colspan="2"><b>Turn 1: Strategy</b></td></tr>
<tr><td>Red Team Submits<br>1 Development and 2 Actions</td><td>Blue Team Submits<br>1 Development and 2 Actions</td></tr>
<tr><td colspan="2"><i>White Team Updates the Environment to Reflect Red and Blue Team Actions</i></td></tr>
<tr><td colspan="2"><b>Turn 2</b></td></tr>
<tr><td>Red Team Submits<br>1 Development and 2 Actions</td><td>Blue Team Submits<br>1 Development and 2 Actions</td></tr>
<tr><td colspan="2"><i>White Team Updates the Environment to Reflect Red and Blue Team Actions</i></td></tr>
<tr><td colspan="2"><b>Turn 3</b></td></tr>
<tr><td>Red Team Submits<br>1 Development and 2 Actions</td><td>Blue Team Submits<br>1 Development and 2 Actions</td></tr>
</table>

| | |
|---|---|
| *White Team Updates the Environment to Reflect Red and Blue Team Actions* | |
| **Turn 4** | |
| Red Team Submits<br>2 Actions | Blue Team Submits<br>2 Actions |
| *White Team Updates the Environment to Reflect Red and Blue Team Actions* | |
| *Hot Wash and Distribution of Final Results* | |

*An outline of the schedule for the exercise.*

## Expectations

Cybereason conducted two similar exercises preceding the US midterm elections, one in September 2018 and one earlier in the year, both held in Boston. The results of those elections were expected to be reflected at least partially in this exercise.

In the previous Autumn exercise, the system was not designed for this sort of threat, local law enforcement was not comfortable calling for help beyond their jurisdiction, and law enforcement was mostly reactive and flat footed during the day.

The Red Team was able to dominate by feeding the Blue Team what it expected and using the expected results for anarchy, mayhem, and controversy in the political sphere. The decisive Red Team victory was expected to be less one-sided in 2019, but the outcome was expected to still lean to the Red Team rather than the Blue Team.
The second exercise saw a marginal victory for the Blue Team. The Blue Team was prepared and asked for help when needed, and the Red Team didn't put up a challenge soon enough to develop significantly enough for the end of the day.

## Results

This tabletop event showed excellent preparation and execution by members of both the Red Team and the Blue Team.

The Red Team implemented a fantastic set of moves that demonstrated daring and creativity. They developed capabilities early on that they could use throughout the day for multiple scenarios and took impactful actions at each turn. However, the primary mission of the Red Team failed due to overkill. Instead of undermining the election, they forced the Blue Team to cancel the election and they caused a terrorist attack. The aftermath of the Red Team's efforts increased the fear of terrorism overall and started conspiracies about potential government collusion.

The Blue Team made decisive, immediate action and expanded their capabilities early in the day. They focused on what they could control and called for federal aid at all the right points. However, the public did get hurt, with 200 people injured and 32 dead, and the election was cancelled. The only thing the Blue Team could have done sooner was address the autonomous vehicle systems earlier in the day, but overall, they gave a solid performance and addressed the Red Team's actions quickly.

It is fair to say each team denied the other victory in the final turn. The Red Team causing the death of civilians at the polls prevented the Blue Team from winning, and the Blue Team being forced to reschedule the election prevented the Red Team from winning. Regardless of the outcome, both teams played aggressively, well and enjoyed the immersive experience.

# Lessons Learned

## Communications are the New Battleground

- Recognizing that having clear channels of information or *dis*information was very important for affecting public sentiment for both sides.
- Control of social media networks for journalists, influencers, and political figures allowed the Red Team to easily spread misinformation through supposedly "legitimate" channels.
- **Lesson Learned**: Law enforcement must create open lines of communication between government departments and media sources and social media companies. The government can only extend their capabilities so far without the support of the platforms upon which misinformation is spread.

## Developing Technology Poses Threats that are Difficult to Predict

- Autonomous vehicles were leveraged by the Red Team to wreak havoc at polling stations and cause many deaths and injuries. These vehicles can be used by attackers as a new set of weapons in their operation with no consequences to the Red Team.
- Deep fakes were used by the Red Team to impersonate the superiors of pollsters and law enforcement officers and direct them to execute actions that benefited the Red Team. In addition, deep fakes were used to create fake videos and spread misinformation about the candidates in the race.
- **Lesson Learned**: As we develop advanced technology for user convenience, we must consider the consequences of the technology and ways to prevent its misuse and abuse. Additionally, we must work to construct fail safes to prevent this technology from being abused so significantly that it results in the death or severe injury of others. Open lines of communication between the government and technology companies will also help in this effort.

### You Can’t Prepare for Every Scenario

- To this day, the adversary still has the advantage over the defender. They can take actions across a huge spectrum of possibilities, whereas law enforcement must work within the bounds of the law. It is impossible for law enforcement to prepare for every scenario an attacker might implement.
- **Lesson Learned**: It’s critical for law enforcement to proactively prepare and be aware of the potential actions an attacker may take.  These tabletop exercises give law enforcement a deeper understanding of what can go wrong and how, so they may use that information to develop processes that prepare them for the worst outcomes.

## Actionable Insights for Law Enforcement

### Communication is Key

- **Use Media Effectively:** Broadcast media is the bully pulpit. Make sure it's used effectively to help counteract the effects of misinformation through other channels.
- **Use Multiple Channels**: Have several alternate means of communication.  Assume that cell phones can be compromised, social media is unreliable, and that radios have weaknesses like jamming. Make sure to practice out-of-band communications and have a default contingency to establish central communications and coordination.
- **Don’t Forget Radio**: The amateur radio service can provide alternate means of communications in the event of an issue with the main communication channels. Having a local amateur operator part of the ARRL at precincts or dispatch can help tremendously in the event main communication channels fail.

### Developing Technology Poses Unknown Threats

- **Coordinate with the Private Sector:** Coordinate with major providers of infrastructure and transportation ahead of time, including private companies that provide the technical aspects of that infrastructure. Understanding where things like the power grid and self-driving cars are vulnerable can help prevent potential attacks on key utilities.
- **Take Care with Smart Vehicles:** Make sure that *smart city* and *smart vehicle* programs are known by law enforcement. Educate law enforcement on smart equipment and provide the means for liaison in the event of a crisis.

### You Can’t Prepare for Every Scenario

- **Collaborate with Other Government Agencies:** Take advantage of state and federal resources to augment existing law enforcement and provide additional intelligence. Use peacetime to establish relationships with cyber centers and other levels of government. Make sure that the police department has a means to communicate with the State Secretary of State and has existing relationships with the city communications office.

The police department and the city press officers should be coordinated in the event of an incident and should convene with the Governor's office in the event of a crisis.

- **Develop Playbooks**: Run specific-to-your city tabletop exercises that account for existing idiosyncrasies in your community, city, state and federal relationships. In a crisis, you don't want to be thinking about "how" to do things or what your options are but should be running playbooks like a well-oiled machine. If professional sports teams work this way on the field, local government and law enforcement should be just as prepared around elections.
- **Take Region into Account:** As with any good police work, understand the regional nuances and sensitivities in the community to adequately prepare for when they will be manipulated or put at odds.
- **Consider Non-conventional Scenarios**: Law Enforcement should always try to think outside the box.  Even though their role is limited to public safety, crime prevention, and law enforcement, recognizing that there are possibilities for physical safety issues from infrastructure is key.
- **Deploy Early:** Ensure good resource deployment prior to the elections by having a police presence in place before the event. This will lead to less of a psychological impact on civilians if more officers must be deployed, especially in areas where law enforcement is viewed with distrust.

## Feedback

While each subsequent election hacking simulation improves on the one before, the consensus was that this was a solid immersive experience for practicing cyber incident readiness much as war games prepare the military in times of peace.

The law enforcement participants on the Blue Team appreciated the utility of the exercise and how applicable it is to coordination, orchestration, and preparedness for future elections. There is an understanding in the law enforcement community that their reach may only extend so far, and they must address and control what they can.

The security professionals on the Red Team felt confident in their moves and the results. Despite the election being cancelled, they felt the events that occurred during the exercise would be enough to sway public opinion, prevent voter turnout, and undermine any future election.

## Next Steps

Cybereason will likely hold a follow up event in early 2020 closer to the US Presidential elections. In future years, we will likely hold similar events in other cities and states to see regional variation, and in other countries, especially those with a parliamentary system of government rather than republican.

# Final Comment

Cybereason would like to thank all participants for their willingness to dedicate valuable time and energy to this event, and for their faith in suspending disbelief to engage in an immersive tabletop experience. Finally, no actual hacking was performed and no innocent bystanders, hackers, networks, systems, police officers, students, social networks, or republics were harmed in the course of this simulation or its aftermath.

# Appendix: Event Record

<table>
<tr><th colspan="2">TURNS</th></tr>
<tr><td colspan="2"><i>Introduction for All Participants by White Team</i></td></tr>
<tr><td colspan="2"><b>Turn 1: Strategy</b></td></tr>
<tr><td>Red Team Move<br><b>STRATEGY</b><br>- Deploy Stingray.<br><b>DEVELOPMENT</b><br>- Develop deep fake ability for video and audio on demand.<br><b>ACTION 1</b><br>- Gain access to social media accounts of any influencers and press.<br><b>ACTION 2</b><br>- Inform the public that voting machines were hacked with pictures of unattended voting booths in purple and blue districts.</td><td>Blue Team Move<br><b>DEVELOPMENT</b><br>- Restore 911 services.<br><b>ACTION 1</b><br>- Distribute officers to polling places, traffic enforcement, incident response, and to schools and fire stations.<br><b>ACTION 2</b><br>- Inform the public that emergencies can be reported to any police station or fire station and may call #77 State Police intake for emergencies.<br>- Bring in CISA resources.<br>- Send preemptive Canine EOD and officers to bridges and polling places.</td></tr>
<tr><td colspan="2"><i>White Team Updates the Environment to Reflect Red and Blue Team Actions</i><br><br><b><i>UPDATE FOR BOTH TEAMS</i></b><br><i>911 is restored.</i><br><i>Police officers are at polling and fire stations, and K-9 units are on bridges and at polling stations.</i><br><br><b><i>UPDATE FOR RED TEAM</i></b><br><i>The Stingray has been deployed and is now available.</i><br><i>You now control the Fox News website and CNN’s Twitter account, and Facebook and Twitter accounts for city hall and the mayor.</i><br><br><b><i>UPDATE FOR BLUE TEAM</i></b><br><i>CISA is now on call.</i><br><i>The FBI and NCCIC notifies you an attempt to hack into voting machines occurred. Pictures of suspects were sent to local law enforcement.</i></td></tr>
</table>

**Turn 2**

*White Team Updates the Environment During Turn 2*

***UPDATE FOR BOTH TEAMS***

*Pictures of polling stations taken yesterday are circulating.*
*Hacking of voting machines remains unattributed but is on social media.*
*Protests have started at IMF.*

***UPDATE FOR BLUE TEAM***

*CISA dispatches a fly-away team.*
*Rumors of Stingray vulnerabilities and dark web credential purchases for social media accounts.*

Red Team Move

**DEVELOPMENT**

- Develop control of as many of the autonomous vehicles in the city as possible.

**ACTION 1**

- Cause accidents by controlling the traffic lights.

**ACTION 2**

- Distribute a deep fake video of the democratic candidate committing racial and domestic violence from the past year.

Blue Team Move

**DEVELOPMENT**

- Establish a unified command center and resource assignment center.

**ACTION 1**

- Place National Guard on standby.
- Initiate incident response through the FBI and Secret Service and deploy additional officers to IMF.
- Request femtocells for each district.

**ACTION 2**

- Inform the public no signs of hacking have taken place.
- Request social media companies identify hacked accounts.

*White Team Updates the Environment to Reflect Red and Blue Team Actions*

***UPDATE FOR BOTH TEAMS***

*Traffic lights are causing havoc and accidents.*
*There is a moderate concern for public safety.*
*There are concerns of anti-democrat election interference.*
*A video is spreading on Fox News and CNN of a racially charged incident of domestic violence by the democratic candidate.*

***UPDATE FOR BLUE TEAM***

*500 more officers have been made available.*
*The unified command center is established.*

**Turn 3**

*White Team Updates the Environment During Turn 3*

***UPDATE FOR RED TEAM***

*The Stingray is live.*
*50 cars and 5 buses are under your control.*

***UPDATE FOR BLUE TEAM***

*Femtocells have been deployed.*
*Domestic terrorist bombing was stopped in major Blue State Metropolis on the eastern seaboard. This is not public knowledge.*
*The National Guard is available.*

### Red Team Move

**DEVELOPMENT**

- Take over telecommunications providers and develop DDoS capability.

**ACTION 1**

- Initiate a phishing campaign to create deep fake voices of pollsters' superiors and convince them to reset the DRE systems.

**ACTION 2**

- Crash the autonomous buses and cars into the polling lines and polling locations.

### Blue Team Move

**DEVELOPMENT**

- Request extended polling hours and hospital preparedness.

**ACTION 1**

- Request the public limit travel to voting and emergencies.

**ACTION 2**

- Deploy portable traffic lights.
- Send 100 plain clothes officers to polling locations.
- Send a helicopter to monitor protests.

*White Team Updates the Environment to Reflect Red and Blue Team Actions*

***UPDATE FOR BOTH TEAMS***

*Chaos at polling stations as officials reset DRE voting systems.*
*Public is informed trips should be limited due to traffic system compromise.*
*Concern on social media of anti-democrat bias with police.*
*Portable traffic lights deployed.*
*Polls will stay open late.*

***UPDATE FOR RED TEAM***

*Attack against telecommunications providers is underway and may or may not produce results.*
*5 additional buses are under your control.*
*Femtocells have been deployed.*

***UPDATE FOR BLUE TEAM***

*The FBI has identified two suspected ring leaders of K-OS YONATAN STRIEM-AMIT and JEFF TAYLOR living in District 9.*
*A Stingray device was discovered.*
*Helicopters are up.*

**Turn 4**

*White Team Updates the Environment During Turn 4*

***UPDATE FOR BOTH TEAMS***

*Compromised buses with innocent passengers slam into polling lines.*
*Cars have been abandoned around the city.*
*Riots have started.*
*Hospitals are filling.*
*The National Guard is on site.*
*Wanted posters are appearing for YONATAN STRIEM-AMIT and JEFF TAYLOR.*

***UPDATE FOR RED TEAM***

*A Stingray has gone offline.*

Red Team Move

**ACTION 1**

- Fake commanding officers report a compromise in the digital systems and send them to control traffic for a bomb threat in the North.

**ACTION 2:**

- Video leaks of cars and buses crashing into polling stations and the reset of the systems and previous hack have failed.
- ISIS claims responsibility.

Blue Team Move

**ACTION 1**

- Deploy additional officers in various zones.
- Switch to manual drivers only.
- Reschedule the election.

**ACTION 2**

- Arrest Yonatan and Jeff Taylor and identify co-conspirators.
- Take down any additional Stingray devices.

*Final White Team Updates the Environment to Reflect Red and Blue Team Actions*

*The election has been cancelled and people are told to go home.*
*The Governor and Secretary of State address the city and the nation.*
*They declare a state of emergency, martial law, and how this is a tragic day for Adversaria. Many have been hurt, and a manhunt is on for the ring leaders and associates of K-OS.*
*A new election day will be announced.*
*Fear over terrorism increases.*
*The primary mission for the Red Team failed due to overkill.*
*The FBI starts an investigation into the entire incident at the state's request.*
*Yonatan Striem-Amit and Jeff Taylor are arrested at the airport.*
*Extra Stingrays are discovered and removed.*
*Rumors persist in echo chambers about government collusion, although the investigation exonerates all involved.*
*Other members of K-OS are arrested over the course of 6 months and trials begin.*
*The final casualty count is 200 wounded, 32 dead.*
*November 5th becomes Adversaria Strong Day.*

*Hot Wash and Distribution of Final Results*