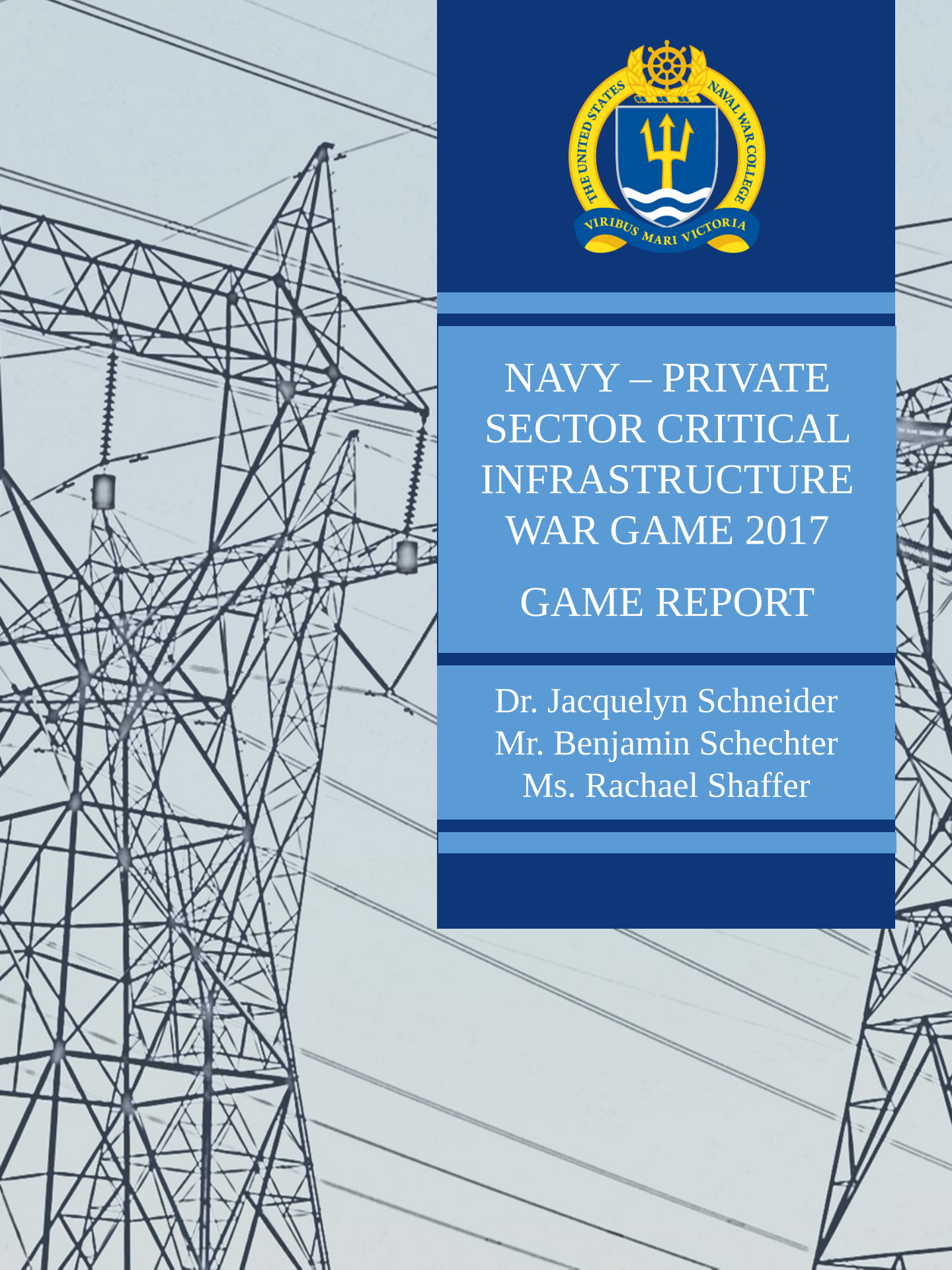


NAVY – PRIVATE SECTOR CRITICAL INFRASTRUCTURE WAR GAME 2017

GAME REPORT

Dr. Jacquelyn Schneider
Mr. Benjamin Schechter
Ms. Rachael Shaffer

About the Game Team

Dr. Jacquelyn Schneider is an Assistant Professor in the Strategic & Operational Research Department and is a core faculty of the Center for Cyber Conflict Studies at the U.S. Naval War College. She was the Game Director and the Lead Game Analyst for this war game.

Mr. Benjamin Schechter is a Research Associate in the Center for Cyber Conflict Studies at the U.S. Naval War College. He was the Lead Game Designer and part of the Analysis Team for this war game.

Ms. Rachael Shaffer is a Research Assistant in the Strategic & Operational Research Department at the U.S. Naval War College. She was the Logistics Lead and part of the Analysis Team for this war game.

CDR Marc Fryman is military faculty and a cyber subject matter expert in the War Gaming Department at the U.S. Naval War College. He was the War Gaming Department Lead for this war game.

LCDR Kevin Davis is part of the War Gaming Department at the U.S. Naval War College**.** He was the War Gaming Department Support Lead for this war game.

Mr. John Hanus is an Associate Professor in the War Gaming Department at the U.S. Naval War College. He was the Game Developer for this war game.

Mr. Pete Pellegrino is a Senior Military Analyst in the War Gaming Department at the U.S. Naval War College**.** He was a Game Designer for this war game.

Acknowledgements
We would like to acknowledge the generous support of the Naval War College Foundation. Their efforts were instrumental in recruiting our private sector participants and without their financial support of the Center for Cyber Conflict Studies events like these would not be possible. We also want to commend the joint efforts of the War Gaming Department and the Strategic and Operational Research Department who partnered to make this event so successful.

Navy-Private Sector Critical Infrastructure War Game

July 10-11, 2017

Contents:

I. Executive Summary

The unclassified Navy-Private Sector Critical Infrastructure Game took place over July 10th and 11th, 2017. It included 125 players from 14 critical infrastructure sectors, local and state government, and the federal government. The game was designed to answer two main research questions: when do cyber attacks reach the level of a national security incident? When should the Department of Defense (DOD) be involved and in what capacity? It hypothesized that the answer to these questions would be influenced by three primary variables: the effects created by cyber attacks, the targets of cyber attacks, and the actor conducting the cyber attack.

In our war game, the attacks that were most likely to escalate to a national security incident were those on the civilian nuclear sector and sectors that had strong linkages across the national economy. Attacks on these sectors with strong linkages within the rest of critical infrastructure created cascading effects, many of which had life or death implications beyond the initial scope of the cyber attack. Therefore, results from the war game suggest that U.S. government resources and policies should focus on the energy, transportation, communications, water/wastewater, and nuclear sectors. While there were other sectors that experienced loss of life, the effects from these cyber attacks were largely confined to their sector and therefore were less likely to create a national security crisis.

Our war game also provided insight into the desires of the private sector from local, state, and federal government. In our event, private sector companies largely sought to remediate impacts on their own networks without government support (the exception may be highly-regulated industries such as energy or nuclear), but looked to the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) for information sharing about threats. Once physical damage or loss of life occurred, private sector leaned heavily on local emergency management and state resources, such as the National Guard, as the first line of defense. This meant that the primary role desired for the DOD was to counter cyber attacks prior to a major campaign as well as to ensure a credible deterrence by punishment strategy through a wide range of cross-domain capabilities.

This leads to the following policy recommendations:

- For the Federal Government: Create declaratory deterrence strategies focused on deterring attacks on a smaller number of critical infrastructure sectors, perhaps energy, transportation, nuclear, water/wastewater, and communications.

- For the Navy: Better understand dependencies on civilian infrastructure. Partner with National Guard units to ensure these industries have support for cyber remediation in a potential cyber attack. Lead in planning and execution of counter-cyber operations prior to conflict and utilize Navy assets across domain for deterrence by punishment options.

- For Private Sector: Create informal networks of information sharing across critical infrastructure sectors. Pro-actively work with federal, state, and local government to create crisis action plans for major cyber attacks.

- For Local/State Governance: Better train and resource first-line responders to consider cyber attacks as a threat vector. At the same time, integrate these personnel with local DHS and FBI representatives for better information sharing. For the state governments, consider allocating additional resources to Guard units dedicated to cyber defense missions.

As with all games, the findings from this war game should not be taken as the final word on these issues. Games are a moment in time with a small sample of the population. We made some choices to sacrifice realism for the sake of exploring our question (for instance, providing attribution for all the attacks). We have tried to caveat our findings based on these limitations.

II. Background and Motivations of the Game

In January 2017, the leaders of U.S. intelligence and cyber organizations issued a joint statement to the Senate Armed Services Committee. The statement voiced a dire warning about the vulnerability of U.S. critical infrastructure to cyber attack, declaring that "the cyber threat cannot be eliminated . . . our adversaries have capabilities to hold at risk U.S. critical infrastructure."[i] In the months following these intelligence leaders' testimony, a spate of cyber attacks and successful network exploitations against critical infrastructure occurred across the globe. The Wannacry ransomware attacks of spring 2017 debilitated the British hospital system, disrupted shipping systems at Fedex, impacted German railroad systems, affected automotive manufacturing in Japan and France, and impeded operations at Spain's telecoms giant, Telefonica.[ii] Only a short time later, a similar ransomware strain, Petya, attacked Ukranian banks and power companies, Danish transportation and energy, and U.S. pharmaceutical manufacturing.[iii] At the same time, evidence of Russian hacking in the U.S. and French elections continues to mount and reports have surfaced of Russian exploitation attempts in the U.S. civilian nuclear sector.[iv]

These attacks are examples of what has been an extraordinary increase in cyber attacks and network exploitation attempts against critical infrastructure. According to the DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the organization has never seen so many successful exploitation attempts on the control system layer of industrial systems.[v] Meanwhile, the United Kingdom (UK) Department for Culture, Media, and Sport, almost 50% of UK businesses reported cyber exploitations in 2016.[vi] Cumulatively, these attacks are having large impacts on global economies. Although cost estimates are difficult to determine, reports range from half a billion upwards to three trillion U.S. dollars in cost and lost productivity.[vii] Analysis conducted by the largest cybersecurity insurer, Lloyd's of London, calculated that an extreme cyber attack could cost major economies $50 billion—roughly the cost of Superstorm Sandy.[viii]

These cyber vulnerabilities in critical infrastructure have created an interesting dynamic for international security. First, these cyber attacks present a way of waging economic warfare on adversary nations that does not require a robust conventional military presence or significant stake in the international economy. Cyber attacks on and cyber exploitation of states' critical infrastructure can be conducted by a host of actors ranging from criminal organizations and mercenary militias to developed and developing nation-states. As such, cyber attacks on critical infrastructure provide a potential new tool for coercion and a prolific threat to the resources of a national economy. Historically, there is precedent for economic warfare as a precursor or motivation for larger conventional conflict (see for example naval blockades, state-sponsored piracy, and resource-motivated land grabs). The scope of cyber attacks on critical infrastructure suggest that these attacks could be tools for the economic warfare of the near future and therefore pose a significant threat to the economic viability of a state.

Secondly, the use of cyber attacks against critical infrastructure introduces novel threats for states that would otherwise be buffeted by natural geographic boundaries. This is especially true for the United States—a nation that has had to devote limited efforts to homeland defense

because of its friendly neighbors and large oceanic borders. For the first time in modern American history, multiple adversaries can target the homeland.[ix] Further, they can conduct these attacks with little warning and at low cost, making vulnerabilities to U.S. critical infrastructure a soft-underbelly target for a prolific set of actors motivated by greed, opportunism, radical beliefs, or good old-fashioned state coercion. To make the problem more complicated (and more dangerous), many of these critical infrastructure industries support — directly or indirectly — U.S. military operations. Civilian energy sources often supply military bases and ports. Service members' livelihoods reside in private banking institutions, and food is sourced from private-sector companies. These dual-use critical infrastructure sectors could be opportune first-strike targets for conventionally asymmetric adversaries looking to increase their chances of victory against U.S. conventional military forces in a crisis.[x]

The puzzle is that despite the large economic threat posed by these cyber attacks, as well as the danger civilian dependencies pose to military power, there is little to no precedence of national security crises that were created by cyber attacks. In fact, an analysis of unclassified cyber incidents over the last ten years reveals almost no significant state responses to cyber attacks.[xi] Anecdotally, the findings from this research seems to have face validity. The large-scale cyber campaigns conducted by Russia on U.S. and French elections have so far resulted in no use of military power. Major attacks by the Iranians on the Saudi oil industry giant, ARAMCO, led to no conventional crisis between Iran and Saudi Arabia. This is despite the fact that the cyber attack wiped out over 30,000 of the business' computers and caused significant profit losses for ARAMCO.[xii] Even the most well know example of a cyber attack that caused physical damage—the Stuxnet virus—resulted in no conventional escalation between the U.S. and Iran. Further, evidence from strategic crisis war gaming at the Naval War College suggests that American decision-makers do not view cyber attacks—even those with physical and even nuclear effects—as events worthy of government response.[xiii]

This leads us to ask—when do cyber attacks against critical infrastructure reach a "hurt point" in which societies or governments believe cyber attacks reach the level of a significant national security incident? Current U.S. cybersecurity policies that call for the use of federal government resources hinge on cyber attacks reaching the threshold of "national security incidents."[xiv] However, the definition of what would constitute a cyber attack of that magnitude is largely open to interpretation. More concretely, at what point do societies believe that cyber attacks are serious enough to warrant the utilization of national defense resources—whether for defense, crisis mitigation, information, deterrence, or retaliation? For U.S. national security decision-makers, when and how should the DOD be used to combat cyber attacks on civilian critical infrastructure?

Despite the large role played by the private sector in U.S. critical infrastructure (all but one sector are majority or completely populated by private companies), their perspective on these questions has been largely under-studied. And while policy prescriptions call for more public-private integration, the "hurt point" at which private sector believes cyber attacks warrant government or DoD intervention is unknown. This is an important omission in the development of current policies because the private sector controls most of these resources, has unique

information about the vulnerabilities of these resources, and makes the initial decision about how and when to involve the U.S. government in any post-hoc efforts. Our war game uses the private sector as the primary sample of interest and therefore focuses on private sector responses and interactions with local and federal government.

III. Current State of U.S. Policies vis-à-vis Cyber Attacks on Critical Infrastructure

The mid 1990s saw both the first Federal use of the term critical infrastructure and a role for federal government in its protection. *EO 13010 - Critical Infrastructure Protection* established government's roles in protecting critical infrastructure, defined and designated critical infrastructure sectors, and emphasized the need for public-private cooperation. The order also began outlining the threats, "threats to these critical infrastructures fall into two categories… physical threats to tangible property... and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ('cyber threats')." From the outset cyber was understood as a threat vector.[xv]

The 9/11 attacks and the creation of the DHS made protecting critical infrastructure a key priority.[xvi] The 2003 *National Strategy to Secure Cyberspace* outlined government efforts to secure critical infrastructure against cyber threats. This document also limited DoD to protecting government networks and the Defense Industrial Base.[xvii] Gradually DHS would undergo restructuring to better achieve its new cyber responsibilities, including the creation of the National Cybersecurity and Communications Integration Center (NCCIC) in 2009.[xviii]

During this time the DOD also advanced and clarified its capabilities and role, standing up U.S. Cyber Command in 2009 and publishing the 2011 *DOD Strategy for Operating in Cyberspace*.[xix] Although U.S. Cyber Command provided new formidable tools to the DOD, it was not clear when and how to use those capabilities outside armed conflict. Nonetheless, the DOD strategy acknowledges the critical infrastructure interdependencies and the need for secure critical infrastructure, asserting that "DOD operations—both at home and abroad—are dependent on this critical infrastructure." To defend these important interdependencies, the DOD stood up 13 Cyber National Mission Teams tasked to "defend the United States and its interests against cyberattacks of significant consequence."[xx]

EO 13636 -- Improving Critical Infrastructure Cybersecurity and *PPD-21 -- Critical Infrastructure Security and Resilience* implemented concurrently in 2013 provided much needed organization, clarity, and tools. The executive order called upon agencies to improve information sharing by providing timely, high quality information on cyber threats to the private sector to bolster critical infrastructure cybersecurity. Additionally, it directed the National Institute of Standards and Technology (NIST) to "develop a technology-neutral voluntary cybersecurity framework."[xxi] The resulting NIST Cybersecurity Framework pulls from best-practices, to provide standards, procedures, and processes to help the private industry manage cyber risk. PPD-21 updated existing policies and plans to create greater governmental unity of effort, including specifying the current 16 critical infrastructures and mapping interdependencies. The directive established the current 16 critical infrastructure sectors. EO 13636 and PPD-21 ultimately seeks to strengthen and formalize the federal government's relationship with the private sector.[xxii] [xxiii]

While the majority of executive actions have been direct towards hardening critical infrastructure and facilitating coordination and information, efforts have been made towards deterrence through punishment. *EO 13694 - Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* was one of the first orders that outlined retaliatory measures against cyber attackers. The order allows for the direct sanctioning of any persons outside the US who "have engaged in, directly or indirectly, cyber-enabled activities… that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States…"[xxiv] This allows the federal government to impose direct financial costs on the person or persons responsible for cyber attacks on US critical infrastructure. In 2016 this was expanded to include cyber-enabled attacks on electoral systems and processes.[xxv]

The recent 2017 *EO 13800 - Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* builds on the work of the previous EO 13636. The new order addresses both securing critical infrastructure and federal networks, as well as public cybersecurity. In supporting critical infrastructure, the order directs specific efforts be made to assist those sectors identified in EO 13636 as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security," under Section 9[xxvi]. Additionally the order directs efforts towards addressing "automated and distributed attacks (e.g., botnets)." On the federal level, the order also directs federal agencies to become compliant with the NIST Cybersecurity Framework.[xxvii]

This brief review of the policies that currently exist highlight the difficulties the U.S. government has in focusing resources and efforts towards cyber attacks on critical infrastructure—especially with no empirical precedent of attacks that have triggered a "national security" incident. This is especially problematic because the U.S. government is already developing cyber capabilities and institutions without a clear understanding about the point at which attacks might warrant different types of government support. Our game is meant to provide insight for these policy and capability developments.

IV. Game Design

On July 10th and 11th, 2017, the U.S. Naval War College conducted the Navy-Private Sector Critical Infrastructure War Game. The unclassified war game included approximately 125 participants, including senior leaders from 15 critical infrastructure sectors, representatives from local emergency management and government, state governance, federal government, and subject matter experts from industry, academia, and government. The strategic-level decision-making game included two scenarios with 66 different cyber attacks across 14 critical infrastructure sectors.

We designed the game to answer a primary research question: when do attacks against U.S. critical infrastructure rise to the level of national security threats? Secondarily, when do these national security threats warrant action by the DOD and in what capacity? We hypothesized that three variables would drive participants' answers to our questions: the effect of the attack (virtual, physical damage, physical damage with loss of life, nuclear), the target of the attack (critical infrastructure sectors), and the actor conducting the attack (state actor, non-state actor).

Variable 1: Effect	Variable 2: Target	Variable 3: Actor
Virtual	Energy	State Actor
Physical Damage	Communications	Non-State Actor
Loss of Life	Transportation	
Nuclear	Commercial Facilities	
	Chemical	
	Healthcare	
	Nuclear	
	Dams	
	Water/Wastewater	
	Finance	
	Information Technologies	
	Food and Agriculture	
	Critical Manufacturing	
	Defense Industrial Base	

Table 1. Variables

In order to test these hypotheses, we crafted two iterations of the war game using a quasi-experimental method. The first scenario was a hypothetical non-nuclear state actor. This state actor was motivated by a need for resources embargoed by our hypothetical blue state as well as pressure from regional states seeking territorial claims. Together, this dynamic created a state that sought to cripple blue conventional superiority through attacks on civilian inter-dependencies as well as to inflict significant damage on blue civilians (thereby decreasing support for the resource embargo on red state).

The second day followed the same design but with a notional non-state actor with extremist ideologies and a desire to secure territory for a future state. This notional non-state actor was primarily motivated by a need for revenue to support their insurgency. Additionally, they were interested in creating terror in blue populations and therefore cyber attacks focused on creating cash for their cause as well as enabling conventional terrorist attacks that caused fear.

Both scenarios included 33 attacks ranging in effect from virtual to nuclear across 14 critical infrastructure sectors. Ideally we would be able to include all level of effects for each of the sectors, but during our war game development we found that this over-saturated players. Additionally, there were concerns about players' ability to suspend disbelief for unrealistic effects. Therefore, if an effect was highly unlikely for a particular sector, we removed it from the attack matrix. This led us to take out all scenarios with a loss of life in all but the chemical, energy, healthcare, transportation, and nuclear sectors. Only the nuclear sector received a scenario with nuclear effects (see table below). We randomized the order of attacks in order to minimize the chance of bias towards escalation and submitted the attacks to players in two waves, one at the beginning of the game and the second half-way through game play. Where necessary, we deleted inputs in the second wave if players took actions that made subsequent injects unlikely (this only occurred in the second game to four injects).

Actor	State (Non-Nuclear)				Non-State (Extremist)			
Sector \ Effect	Virtual	Physical	Physical (Loss of Life)	Nuclear	Virtual	Physical	Physical (Loss of Life)	Nuclear
Chemical	Y	Y	Y	N	Y	Y	Y	N
Commercial Facilities	Y	Y	N	N	Y	Y	N	N
Communications	Y	Y	N	N	Y(np)	Y	N	N
Critical Manufacturing	Y	Y(np)	N	N	Y(np)	Y	N	N
Dams	Y	Y	N	N	Y	Y	N	N
Defense Industrial Base	Y(np)	Y	N	N	Y	Y(np)	N	N
Emergency Services	N	N	N	N	N	N	N	N
Energy	Y(np)	Y	Y	N	Y	Y	Y	N
Financial Services	Y	Y	N	N	Y	Y	N	N
Food and Agriculture	Y(np)	Y	N	N	Y	Y	N	N
Government Facilities	N	N	N	N	N	N	N	N
Healthcare and Public Health	Y	Y	Y	N	Y	Y	Y	N
Information Technology Sector	Y	N	N	N	Y	N	N	N
Nuclear Reactors, Materials, and Waste	Y	Y	Y	Y	Y	Y	Y	Y
Transportation Systems	Y	Y(np)	Y	N	Y	Y	Y	N
Waste and Wastewater Systems	Y	Y	N	N	Y	Y	N	N

Y = was deployed in the war game
Y(np) = was planned to be deployed, but was not deployed due to player action
N = was not planned to be deployed in war game

Table 2. Matrix of Injects

Players were divided into four cells of activity. The first, a private sector cell, included teams ranging in size from two to 12 participants of senior leaders within the energy, defense industrial base, communications, transportation, healthcare, waste and wastewater, dams, nuclear, finance, commercial facilities, critical manufacturing, chemical, and food and agriculture critical infrastructure sectors. The second cell, a local and state governance cell, included participants that represented state government (governor's office, state-level emergency management and

infrastructure, National Guard, attorney general) and local government (mayor's office, local police, local fire, local emergency management). The third cell represented the federal government and included representatives playing the DOD, DHS, Department of Treasury, Department of Transportation, Department of Energy (DOE), FBI, and National Security Council (NSC). The final cell included subject matter experts and war gaming professionals who answered requests for information from players, adjudicated decisions made by players, and submitted public opinion, stock market, and international opinion updates based on player actions.

PRIVATE SECTOR PLAYERS	**LOCAL & FEDERAL GOVERNMENT AND WHITE CELL PLAYERS**
Applied Control Solutions	Army Cyber Institute
AT&T/Chief Security Organization/Enterprise Security	Atlantic Council
Bechtel Global Corporation	Citywide Cybersecurity Division, Department of Info Tech & Telecom
Bessemer Trust	Columbia Law School
Campbell Soup Company	Crawford Associates
Cargill, Inc.	Cyber National Mission Force (CNMF)
Center for Financial Services, Depaul University	Cybersecurity and Networking, Roger Williams University
Citi	Defense Security Cooperation Agency
Columbia University	DFCSC, University of Rhode Island
ComEd	DHS
Consolidated Edison	FAA
Decision Resources Group	FBI
Duke Energy	Federal Aviation Administration (FAA)
DuPont	FEMA
Electricity Information Sharing and Analysis Center	Fire Department of New York (FDNY)
Entergy Services, Inc.	Former Secretary of the Navy
Exelon	Former United States Attorney for the District of Rhode Island
Federal Reserve Bank of Dallas	Idaho National Laboratory
Financial Systemic Analysis & Resilience Center	J.P. Morgan Chase
Fiserv	National Guard Bureau
FM Global	NATO
General Dynamics/Electric Boat Division	Naval Information Force Reserve
Hospital Corporation of America	Naval Postgraduate School
Huntington Ingalls Industries	Navy Cyber Defense Operations Command
Independent Consultant	New York City Department of Environmental Protection
JetBlue	New York City Emergency Management

Kinder Morgan	New York Police Department (NYPD)
Kirby Capital Advisors	National Security Agency (NSA)
Lone Star Analysis	NY/NJ Port Authority
Midwest Reliability	Office of Congressman Jim Langevin
National Grid	Office of Management and Budget, Cyber and National Security Unit
Navy Federal Credit Union	OPNAV
OGE Energy Corp.	Pell Center, Salve Regina University
Shield Capital Partners/Harbourvest	R.I. Air National Guard
Southern Company	R.I. National Guard
Starwood Capital Group	Rhode Island Department of Health
t4 Spatial	State of Rhode Island
Tennessee Valley Authority	U.S. Chamber of Commerce
The Boeing Company	U.S. Department of State
The Mount Sinai Hospital	U.S. Department of the Treasury
Tyson	U.S. Secret Service
U.S. Naval War College	U.S. Cyber Command
USBank	U.S. Northern Command
Westinghouse Government Services	Versive
ZRG Partners LLC	Wensing Enterprises LLC

Table 3. List of Player Organizations

On the first day, players responded to incidents, received updates, and provided information via an online gaming tool and outlook-based webmail. This tool allowed for near real time response to incidents and computer-based coordination within and among cells. On the second day, network capabilities were degraded and players performed the same function without the use of the gaming software. Instead, players sent and received information via word documents and files saved in a shared network. This slowed down the sending of information requests and actions and made face to face conversations more prevalent than emails or on-line communications. Consequently, we saw a significant reduction in information-sharing or questions via the computer. Actions were still conducted via the shared network access and word documents, but less internal actions or information-sharing actions were conducted on day two.

Information was collected in three ways. First, players on both days submitted action forms and request for support forms. Action forms detailed actions they would take within their company or agency while request for support forms asked for request from specific governmental agencies. All cells were given access to action forms; only the private sector cell and local/state government cell were given request for support forms. These forms allowed us to track when government support was requested and from whom. Within the game, these forms were sent either to the white cell (action forms) or to the agencies themselves (request for support forms). Action forms were adjudicated by the white cell and updates sent to the pertinent players. Request for support forms were responded to by the pertinent federal government agencies. We

also generated data from ethnographer notes. Each cell of players included two assigned individuals who took notes on discussions within the cell and in the two plenary sessions. These notes provided data about the motivations behind the actions and requests taken in forms.

Finally, data was collected through a survey form presented to the players at the end of both days. The survey included demographic questions about gender, education, military experience, civilian experience, and political affiliation. Players were then asked to identify which sectors they believed experienced an attack that reached the level of a national security incident and to detail these attacks. They were also asked to choose what they believed to be the primary factor that made this incident a national security threat. Finally, the last section of the survey asked players whether or not they requested support from the DOD and why or why not. In scenario one, 91 respondents completed the survey for a completion rate of 96%. In scenario two, 82 respondents completed the survey for a slightly lower completion rate of 85%.[xxviii]

Like all war games, there are limitations to the generalizability of the findings we derived from this war game. First, we included representatives from private sector companies within critical infrastructure but these are large sectors and our players do not represent the totality of views within their industries. Therefore, actions and ideas voiced within the game should be considered a microcosm of the interests of the sectors and not be generalized throughout the entire private sector. Secondly, we gave attribution and context to all players at the beginning of each scenario. This allowed us to conduct the game at the unclassified level and focus on responses to cyber effects, but it is not a realistic display of the uncertainty that characterizes most cyber attacks. Our game down-played the important role of information sharing and therefore we should expect that in a real cyber attack scenario, more requests for information between our various organizations would likely occur. Finally, our game was explicitly a cyber game and therefore players were likely more focused on mitigating cyber incidents than they might be in a game that was more largely framed around business profits, electability, or a national security crisis with conventional conflict dynamics (i.e. air strikes, special operations missions, or naval engagements).

V. Data

We compiled all the actions taken by the private sector cell (our primary sample of interest) as well as local/state government across both days of the war game. We categorized the actions within eight possible genres: 1) internal, 2) public affairs, 3) request for government support (information), 4) request for government support (emergency management), 5) request for government support (cyber defense), 6) request for government support (cyber remediation), 7) request for government support (policy), and finally 8) request for government support (retribution). Internal actions include personnel decisions, operational changes, internal policy reviews, or cyber or physical security actions taken within the notional company. In general, these actions did not include offensive actions with the exception of one "hack-back" by the water/wastewater sector. Public affairs include any media or communications activities associated with an external audience. The following six categories cover requests for government support, ranging from information all the way to retribution (either punishment, retaliation, or counter-cyber operations). After generalizing the actions within these categories,

we found that the dominant actions were internal to the private sector, with 67% of all actions either internally driven or public affairs. Of the remaining 33%, most requests for government support were for emergency management (16%) with only 1% requesting retribution-type support. There were no requests for external (local, state, or federal government) support for cyber defense or policy. This could be because of a genuine lack of desire for government support within these areas. Private sector companies may not trust government ability to defend their own networks or to control proprietary information and may believe more policy generates greater regulation without more capability. However, it could also be a product of the strategic crisis nature of game which prioritizes short-term decisions (i.e. not policy) and strategic level trade-offs (i.e. not technical decisions about cyber defense).

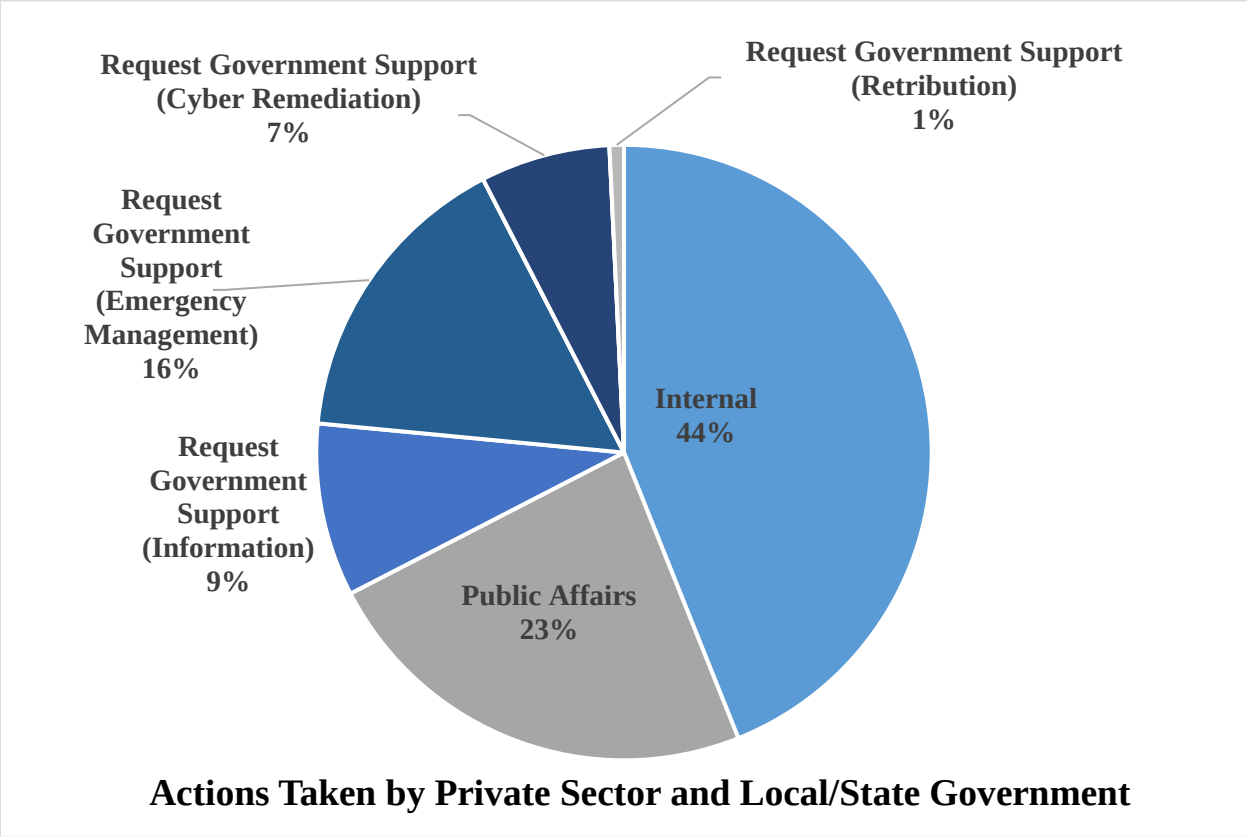


Figure 1. Actions Taken by Private Sector and Local/State Government

We also categorized the agencies from which the private sector requested support. The primary agencies the private sector reached out to were the FBI/DOJ, DHS, and local government in that order. Together, these three entities made up 57% of the requests for support. The remaining 43% of support was mainly made up of requests to the State Government, the DOD, and the DOE. Certain sectors were more likely to reach out to the remaining agencies, including Transportation Sector requests from the Department of Transportation and finance engagement with Treasury and State Department. The data from these requests for support suggest that the primary federal government agencies called on for support in a significant cyber attack on

critical infrastructure would be DHS and FBI/DOJ (a behavior which is consistent with the general delegation of current roles and responsibilities in the federal government).

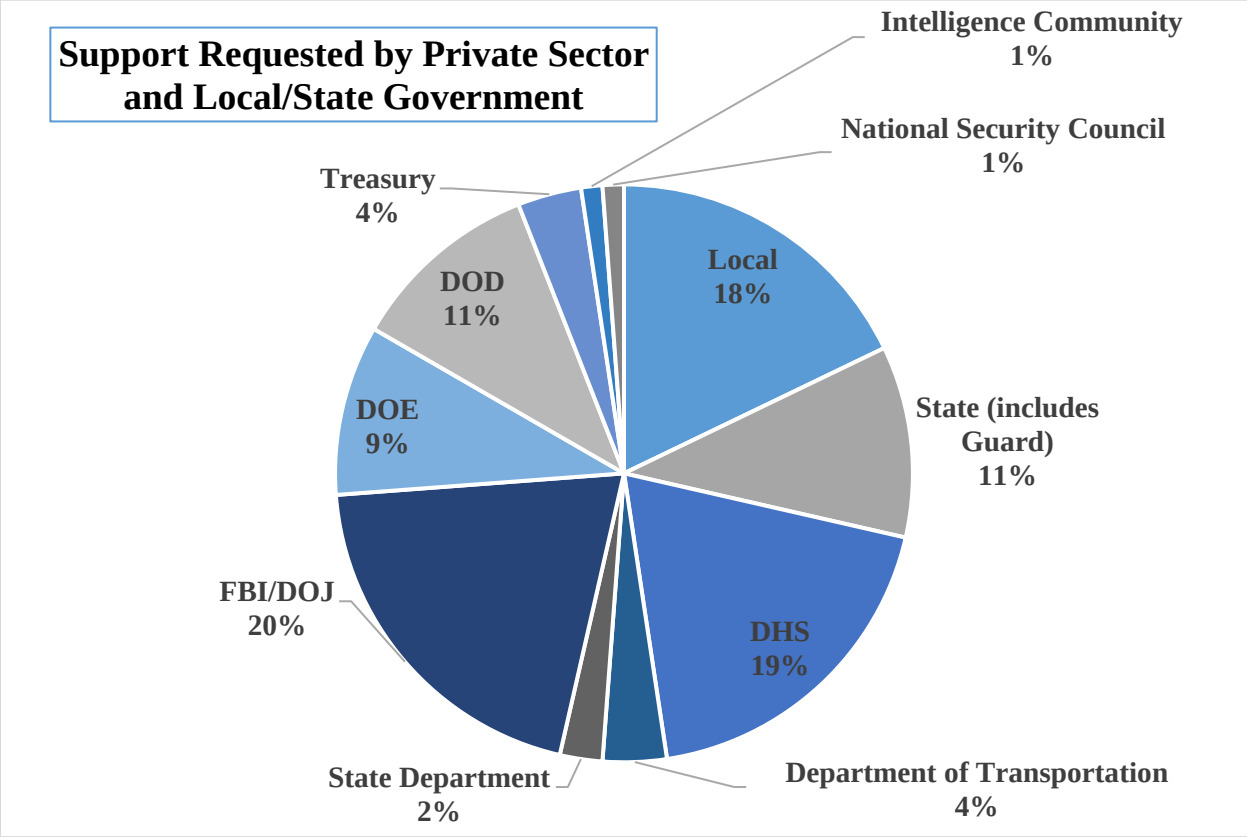


Figure 2. Break-out of Support Requested by Agency

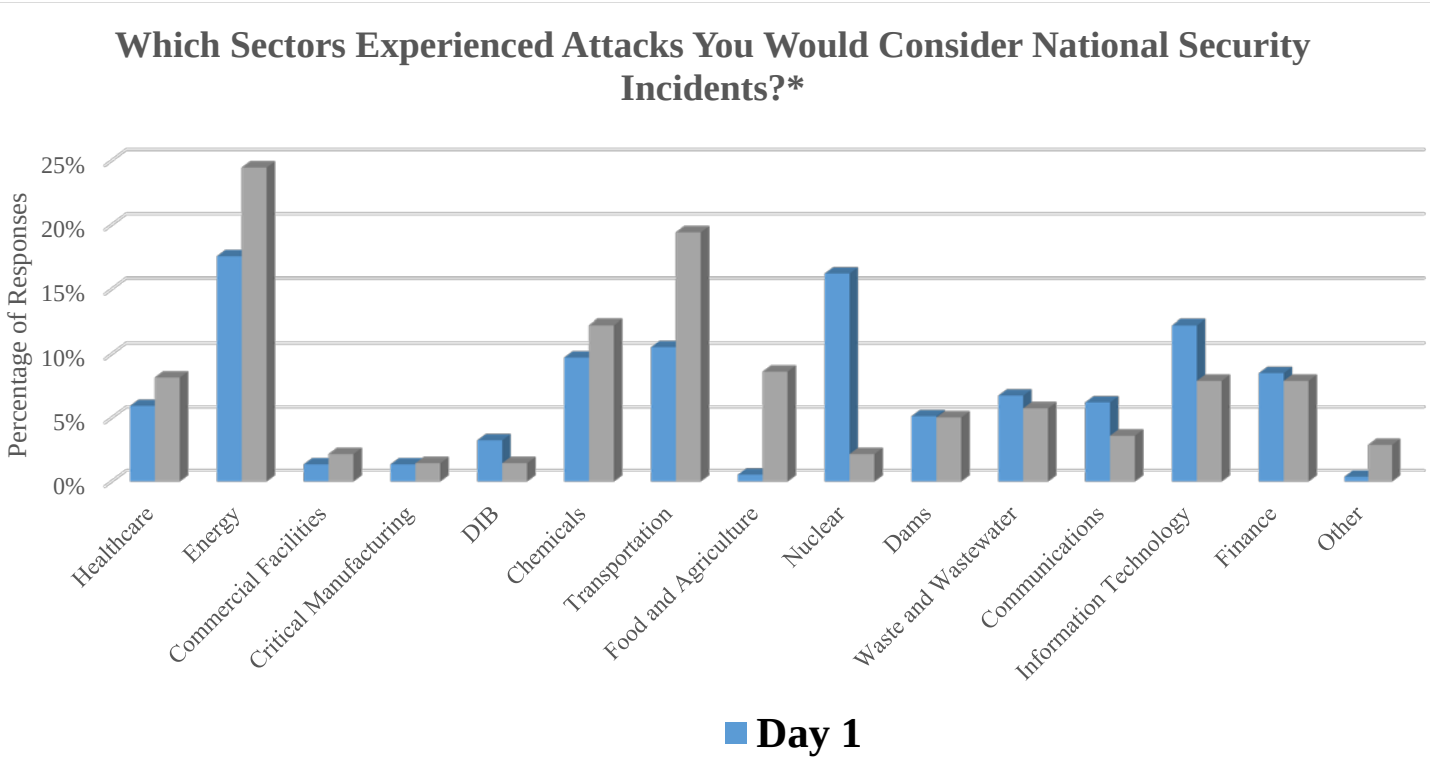
This was not a game designed to understand federal government decision-making. However, it can be helpful to understand whether government action was driven by requests from the private sector or local/state authorities or was instead pushed from the government to the private sector. The data from private sector actions shows that the primary requests for government support were either for information or emergency management. Emergency management was largely covered by the local authorities and the National Guard. This means that the primary requests for federal government action concerned sharing information (which was also the primary action taken by the federal government). This suggests that there was a very equitable push and pull between federal government and the other players to share information.

Only a very small percentage of requests concerned government support for cyber remediation and retaliation and no requests were for government support to cyber defense. That did not stop the federal government from proactively providing some of these capabilities, including deploying hunt teams and cyber defense capabilities to the private sector. In one instance, DOJ/FBI pushed a patch forward to private industries which was designed to combat adversary ransomware. This action met with stiff resistance from the private sector players, who were concerned that the federal government did not have enough understanding of their networks, information technology, and operating systems to push technical solutions across companies.

Federal agencies, particularly the DOD and Cyber Command, were also highly proactive in putting forth options for both conventional and cyber retaliation against the adversary. And, while this was not a large focus of government support requests in the game, discussion in the plenary suggested that players appreciated the willingness of the federal government to seek these options even absent strong calls from the private sector.

In addition to categorizing the actions taken by players in the game, we wanted to understand what cyber attacks private sector players believed reached a level that would trigger the "national security" incident used as a threshold for government action in both the Obama and Trump executive orders. Therefore, we used a survey at the end of each day to measure the perceptions of game players about the national security implications of the cyber attacks. In the survey we asked the game players to select all the critical infrastructure sectors they believed had attacks that would be characterized as national security incidents. We then asked them to detail these attacks for each sector and finally to identify the primary reason they believed the attack reached the level of a national security incident.

On Day 1, the sectors most likely to be classified as the recipients of an attack that reached the level of a national security incident were Energy, Chemicals, Transportation, Nuclear, and Information Technology. We noticed a statistically significant difference on the second day with Energy, Chemicals, and Transportation as the primary selections in the non-state actor scenario. Nuclear, which was a leading national security sector in the first day, was one of the least selected sectors in the second day (we will discuss this more, but this could be in part because the nuclear inputs occurred late in Day 2 and therefore were overlooked by many players responding to previous incidents). Despite this difference, there were commonalities across both days of play. In both days, attacks on commercial facilities, critical manufacturing, and the defense industrial base were least likely to reach a threshold of national security incidents for the players. We also saw consistent rank-ordering of damns, waste and wastewater, and finance across both days.



*Unpaired t-test of difference between Day 1 and Day 2 was significant at $p \leq .01$

Figure 3. Perceptions of National Security Incidents by Day

Our second round of questions asked individuals to identify what they believed to be the primary characteristic that made that event a national security incident. Here we saw more commonality between Day 1 and Day 2 (t-test statistic, p=.12) than we saw in the previous question. We gave the game players eight different choices. The first four roughly aligned with our original hypotheses: the actor, the magnitude of the effect (which we presented as two different types of magnitude—how much physical or monetary damage vs. how many people or businesses affected), and the target of the attack. Additionally, we included responses related to particular types of effects (stock market, public opinion), and existing government policy. On both days, the magnitude of the effect dominated people's determinations about national security incidents. On day one, 46% of respondents chose effect as the primary characteristic, with actor and target of attack tied at 23% a piece. Similarly, on day two, 50% of respondents selected an effect explanation, while only 11% believed the actor was a primary consideration and instead 30% viewed the target of the attack as the most important factor.

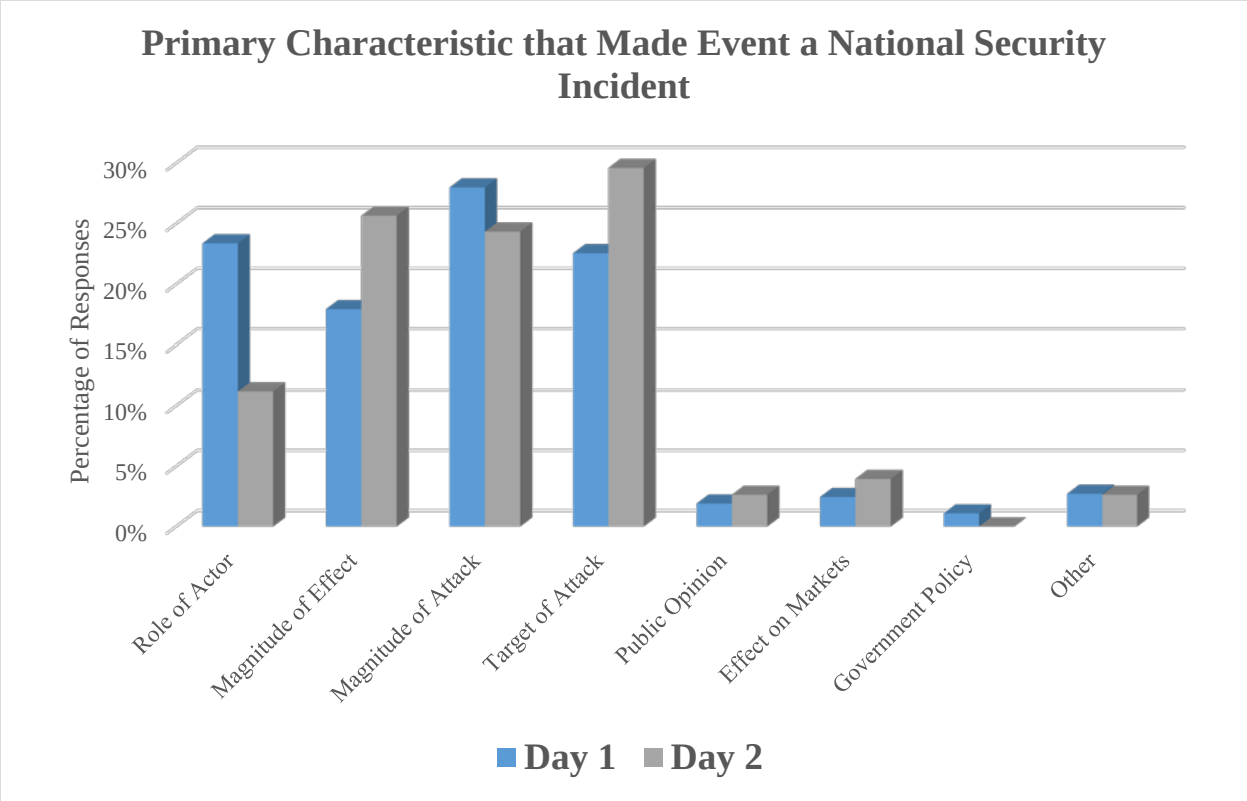


Figure 4. Perceptions of the Characteristics of National Security Incidents

VI. Discussion

What does this data suggest about our original hypotheses? What was the most important variable in driving cyber attacks to a national security incident in our war game—effects, targets, or actors?

Hypothesis 1: The Effect Drives Perceptions of National Security Implications of Cyber Attack
Our first hypothesis was that the effects of the cyber attacks would be the dominant consideration that elevated cyber attacks to a national security incident. We categorized the attacks within four genres of effects ranging from virtual, physical, loss of life, to nuclear. If effects were most important to escalation considerations, then we would expect that across both days and all target sectors, the attacks most likely to be perceived in our survey as national security incidents—as well as the attacks most likely to generate requests for government support—would be those that were nuclear, followed by loss of life, physical, and then virtual.

Results from our survey certainly suggest that the magnitude of effects played a significant role in the perception of cyber attacks. Magnitude of effect was the primary characteristic—across both days—identified as the primary characteristic of a national security- level attack. Actions taken within the game reveal a slightly more nuanced story than the pronounced findings reported in our survey. As effects moved from virtual to nuclear, we saw players were less

focused on internal actions and more focused on government support for emergency management, cyber remediation, and retaliation. Despite this pattern, the only statistically significant difference in the actions taken, when categorized by effects, was in actions taken in response to attacks that created nuclear effects. Actions taken in response to nuclear effects were significantly different than actions taken after any other type of effects. This suggests that effects do matter, but there may be little difference between actions taken in response to attacks until the effects reach the highest order of magnitude.

	Internal	**Public Affairs**	**Request for Gov. Support (Info)**	**Request for Gov. Support (Emergency Management)**	**Request for Government Support (Cyber Remediation)**	**Request for Government Support (Retaliation)**
Virtual	53%	20%	9%	9%	9%	0%
Physical	46%	24%	12%	12%	4%	2%
Loss of Life	31%	28%	5%	25%	8%	3%
Nuclear	25%	25%	0%	50%	0%	0%
t-test between virtual and physical=not significant t-test between virtual and loss of life= not significant t-test between virtual and nuclear= .09 (significant at .1) t-test between physical and loss of life= not significant t-test between physical and nuclear= .0598 (significant at .05) t-test between loss of life and nuclear= .0320 (significant at .05)						

Table 4. Actions Taken by Non-Federal Players, Divided by Effect

Indeed, when pressed in plenary for the point at which monetary damages due to a cyber attack would reach the level of a national security incident, none of the players could provide a threshold. This was especially apparent in how players ranked the gravity of threats to the financial sector. These attacks essentially shut down the financial markets with banking and stock markets completely closed in both days. Despite these large monetary effects, attacks on the finance sector were deemed national security incidents by only seven to eight percent of survey respondents. Additionally, less than 5% of survey respondents believed effects on the stock market elevated cyber attacks to a national security incident.

The data presented by the actions taken in the game did not necessarily reflect the consensus of discussions with players in the plenary. In the plenary, participants were asked to identify when they believed the cyber attacks reached the threshold of national security incidents. They argued that loss of life constituted a national security incident . . . *any* loss of life associated with a cyber attack. This was not what their actions suggested. The slight dissonance between what the players were prepared to deem a national security incident and their subsequent actions to these attacks mat be generalizable beyond our game. We see this dilemma in U.S. policies toward cyber attacks. While decision-makers may declare an incident a national security threat (for example, the Sony attack), the actual actions taken in response to the attack may be more limited

than national security incidents caused by conventional means of war (for example a terrorist bombing, a missile launch, or an air strike). In our war game, therefore, the players' actions and survey responses suggest that effects matter towards perception of the importance of a cyber attack, but may only significantly influence actions when the magnitude of the effect is quite large.

Hypothesis 2: The Target Drives Perceptions of National Security Implications of Cyber Attack

Our second hypothesis was that the target of the cyber attack would be the primary consideration for classifying an attack as a national security incident. Data from our survey suggests that the target of the attack was largely secondary to other considerations. On both days, target of attack was the second most selected determinant of national security incidents, following behind effects. The exception to this is in two sectors. Those sectors were nuclear and transportation. On Day 1 nuclear was the second-most selected sector for national security incidents and on Day 2 transportation was the second-most selected. There are important difference about each sector's vignettes that may help illustrate what role the target of cyber attacks plays in overall determinants of national security significance.

Nuclear was the only sector in the first day in which players identified the target of the attack as the primary reason to classify a cyber attack as a national security incident. Attacks on the civilian nuclear sector provide an interesting case. On day one, players were given a scenario in which cyber attacks were conducted on the nuclear facility and created a fall out event within the nuclear reactor. The adversary was clearly targeting that nuclear facility and the cyber exploitation was within the operating systems of the facility. On the second day, a day in which only two respondents believed the nuclear sector had experienced a national security incident, the cyber attack was not on the facility itself but instead on an internet-of-things system embedded in a truck that was transporting nuclear waste just outside of the facility. In the second case, it was unclear whether the adversary intended to target the nuclear facility or if instead the nuclear effect was a fortuitous coincidence. The divergence in perceptions of national security relevance for these two scenarios may suggest that physical nuclear facilities carry greater emotional significance than other non-nuclear targets that may nonetheless have second or third order nuclear effects.

Transportation was the only sector identified the second day in which the target of the cyber attack was the most important characteristic raising the threat to the level of a national security incident. In the previous day, survey responses that cyber attack effects had played a larger role for the transportation sector than the target of the attack. This is interesting because in Day 1, the attacks culminated in the loss of four lives. In Day 2, the effects were actually larger and 12 lives were lost. But perhaps the greatest difference—beyond even the immediate deaths—in the two days was that in Day 2 the FAA grounded all flights in response to the cyber attack whereas in Day 1 the effect was limited to the airport and a handful of flights. On Day 1, the impacts from cyber attacks on transportation were largely isolated to the transportation sector while in day two, the attacks impacted almost all of the other critical infrastructure sectors. This significantly increased the perception of the gravity of attacks on the transportation sector. As

the players explained, the primary reason they viewed the attack as significant was because of the subsequent grounding of flights. As they explained in survey responses:

> *"grounding all the flights and hack to electronic flight control system that could impact passenger safety"*

> *"Airplane crash, question of cyber event, the fact that planes were grounded"*

The discussion about attacks on the transportation sector reveals something very important about the relationship between certain kinds of effects and particular sectors. The sectors that were most likely to create national security incidents were not only those that had loss of life, but those that created cascading effects to other sectors. Energy was the number one most likely sector to be classified as a national security incident on both days. While this was certainly related to the physical loss of life created by the attacks on the energy sector, players were more concerned with the cascading effects of the attacks on other critical infrastructure sectors than the amount of people killed in the initial attack. As players explained in the survey about their perception of the severity of the attacks:

> *"The lack of power output effected many other industries and sectors"*

> *"Energy sector experienced a disruption of service which impacts every other sector."*

Compare these responses with chemical, a sector whose attacks did not have strong cascading effects on other dependent industries. On both days, cyber attacks on the chemical sector caused loss of life (six dead on day one, four dead on day two). This is comparable with energy, which had four direct deaths on both days. However, energy boasted the majority of respondents' national security incident selections on both days while chemical trailed seven percentage points on day one and 12 percentage points on day two. Examining players' write-in explanations of their choices demonstrates a different focus than the attacks on the energy sector, which emphasized the importance of cascading effects. Instead, for attacks on the chemical sector, the focus was on the immediate first order effects from destruction within the chemical facility.

> *"Explosion releasing toxins into the atmosphere and leading to possible contamination. Evoking fear."*

> *"Release of chemicals could cause massive number of casualties."*

Our data shows that the targets of cyber attacks matter most when it is a nuclear facility but otherwise the importance placed on the target of the cyber attack is secondary to the types of effects created. In particular, for sectors that have strong linkages across critical infrastructure, first order effects did not need to be as large in order to classify an attack as a national security incident. Instead, cascading effects magnified concerns that a cyber attack would lead to a larger incident. It is for that reason that attacks on energy—even more than nuclear—were characterized as a national security concern. Therefore, we should expect that sectors like transportation, communications, water/wastewater, and energy may be more likely to lead to

major security incidents than sectors that may have the potential for large first-order effects (including deaths), but are less likely to create cascading effects across other sectors.

Hypothesis 3: The Actor Drives Perceptions of National Security Implications of Cyber Attack

Our final primary hypothesis was that the actor conducting the attack drove perceptions of the national security implications of a cyber attack. To test for this, we devised two separate scenarios with the same number of attacks and varied the actor conducting the attacks. If there were large differences in actions between these two days, then the quantitative data would suggest that the actor was a major determinant. The data suggests that this is not the case. First, we conducted a t-test between the actions taken and support requested in day one (state actor) versus day two (non-state actor) and found no statistically significant difference in the two days. We then looked at how survey respondents ranked the role of the actor in their determinants for classifying a national security incident. Here we found that in Day 1, 23% of responses believed the actor was the most important consideration for national security elevation (tied for second place with the target) while on Day 2 it was only 11% (fourth place selection). This suggests that players at least perceived that the actor played an important role in their actions, but that the non-state actor was less of a consideration in Day 2. The similarity of actions between the two games indicates that this belief did not translate to how the private sector players behaved in the game, though it may explain the great use of conventional military power by the federal government in Day 1 versus Day 2.

Hypothesis 4: Demographics Drive Perceptions of National Security Implications of Cyber Attack

We found no statistical relationship between age, education, veteran status, or political affiliation and perceptions of national security implications or requests for government support.

The Role of the DOD

The data presented above showed that only 11% of the requests for support in this game went to the DOD. Similarly, results from our survey suggest that in Day 1, only 39% of the private sector and state/local players reached out to the DOD, while only 33% reached out in Day 2. The limited call for support from the DOD that occurred within this game generates an important question from our research puzzle—when do the attacks generate a desire for DOD involvement and in what capacity?

Requests for Support from the DoD By Actor, Effects, and Target	
Actor	**Number of Requests for Support**
Scenario 1	4
Scenario 2	5
Effects	
Virtual	1
Physical	4
Loss of Life	1
Nuclear	1
Sectors	
Energy	1
DIB	1
Nuclear	2
Dams	1
Waste and Wastewater	1

Table 5. Requests for DOD Support

The data generated from action forms suggest that desire to call in the DOD was agnostic to the actor and instead was more closely related to the effects and targets of a cyber attack. In particular, the DOD was called on in half of the nuclear incidents created in the war game. It is likely not a coincidence that the industries most likely to request support from the DoD are also those that are more highly regulated. They are also industries that have the potential for significant loss of life—a factor that correlates with the cyber attacks that created higher level effects. These findings are particular to the Active Duty DOD. The National Guard, in comparison to the active DoD, was called in early on both days to conduct both crisis management and cyber remediation activities.

Why was the DOD not a larger part of the support requested from the private sector and local/state government cell? In the last question of our survey, we asked those who did not request support from the DOD to identify why they used other agencies or non-governmental entities instead of the DOD. The responses suggest that players were largely agnostic to the capabilities, personnel, and resources of the DOD and instead did not believe the DOD currently has (or should have) the primary role in first response to cyber attacks. This is consistent with federal policy over the last eight years.

Plenary discussions with players revealed desire for a larger role for the DOD both prior to and after cyber attacks. First, private sector players vehemently believed the DOD and the U.S. government in general should take more actions prior to a large-scale cyber attack to degrade adversary offensive cyber capabilities. Additionally, after significant cyber attacks, players looked to the federal government cell for credible retaliation options. The focus on retaliation was primarily to use levers of national power to counter-cyber activity (i.e. stop the hurt), but also to provide credible punishment for effective deterrence. The focus here was on state actors, which players believed to hold the greatest potential for attacks with large-scale effects and also were the most susceptible to conventional uses of state power.

VII. Recommendations

Federal Government

Under both the Obama and Trump administrations, executive orders have called for more "deterrence" of cyber attacks on critical infrastructure. However, it is difficult to gauge how effective U.S. efforts at cyber deterrence have been so far. The success of deterrence depends on adversaries' perceptions of how the United States will respond to cyber attacks, but current U.S. policies ambiguously threaten unspecified action for "significant" attacks on the various critical infrastructure sectors. That list of sectors (which does not include the electoral system) is so expansive that it becomes difficult to credibly threaten punishment. If everything matters, then adversaries may believe that nothing matters. Over the next few years, the Trump administration should think about making cyber deterrence policies more declaratory with a much more limited list of critical infrastructure sectors. Being clear about what we care about may enhance the credibility of punishment across domains and therefore bolster deterrence.

Additionally, the United States may be able to exercise counter-cyber actions to stem the tide of other cyber attacks not explicitly deterred through punishment policies. This could include offensive cyber operations against adversary cyber infrastructure, as well as economic sanctions, cross-domain military operations against cyber nodes, diplomatic activities, or DOJ/FBI prosecutions. The Obama administration appeared to successfully employ these capabilities to reduce Chinese intellectual property theft. Similar campaigns that pair threats with counter-cyber activities could stymie significant cyber attacks (especially against known and sophisticated state actors). Our war game indicated there is a greater appetite within the private sector for these type of actions that degrade adversary cyber capabilities prior to attack. During the Obama administration, policymakers seemed reluctant to use these kinds of operations because of concerns about escalation. However, the exponential rise in cyber attacks and exploitations on critical infrastructure vulnerabilities—along with the anecdotal evidence from our war game—suggests that the risk of waiting to respond until after a major attack may be as dangerous to U.S. national security interests as the hypothetical risk of escalation. Future policymakers contemplating the use of cyber operations need to do a better job of understanding both sides of this risk equation to build more effective cyber policies.

Navy

While this game didn't explicitly explore Navy dependencies on civilian infrastructure, many of the vignettes within the game highlighted the cascading effects that cyber attacks on critical infrastructure might have on core Navy missions. This builds on the findings of last year's similar game that highlighted the very large role that cyber attacks on civilian infrastructure would have on Navy mission effectiveness. The Navy, unlike the Army and the Air Force, does not have a National Guard role. In states in which the Navy is heavily dependent on civilian infrastructure for its mission (for example Hawaii), the Navy will have to rely on its sister services for National Guard provided cyber assistance to critical infrastructure. The Navy should work closely with those units to make sure they have existing relationship with industry and are

trained on the networks and operating systems specific to the civilian sectors that the Navy relies on in those states.

This game highlighted the important role that DOD could play in countering cyber operations through the use of weaponry across domains. The Navy could play a leading role in devising and implementing these types of operations, whether they be cable-cutting operations that degrade the network lifelines of adversary offensive cyber units, offensive cyber operations, or the posturing of U.S. maritime vessels near adversary cyber centers of gravity. Further, the Navy's conventional arsenal and ability to project power globally make the Navy one of the primary means of credible deterrence by punishment against offensive cyber operations.

Private Sector

Our war game suggested that the most dangerous cyber attacks were those that caused cascading effects across sectors. Cross-sector dependencies on electricity, transportation, and wastewater systems made significant attacks on these sectors exponentially more deleterious than attacks on stand-alone sectors such as commercial facilities or the defense industrial base. Unfortunately, the complex interdependence of sectors makes these attacks not only the most likely to create catastrophic consequences, but also the least conducive to current information-sharing and crisis management techniques. While sector-specific Information Sharing and Analysis Centers may facilitate information sharing within a single sector, they may have the unintended consequence of creating stovepipes that impede our understanding of the effects of attacks across sectors. Our industry players called for more informal means of communicating across sectors and levels of government in order to solve these problems. This could include working groups of executives across industry sectors, advisory boards, and routine gatherings between government officials and the private sector about cyber vulnerabilities and dependencies.

State and Local Government

For any cyber attack that created physical effects, local responders were generally the first (and quite often the only) government aid requested to remediate the effects of these cyber attacks. This put an enormous onus of responsibility on local responders to not only remediate the effects of the attack, but also to provide information to national-level agencies for greater coordination. Additionally, dependence on emergency management at the local and state level as the first lines in cyber attack response means any attacks on police, fire, health, or environmental management will be especially dangerous and may make a routine cyber attack escalate quickly to a national security incident.

The National Guard played a significant role in emergency management within our game and were the only defense assets used for cyber tasks within private sector networks. Our game has only highlighted the very large role that the National Guard would play in any major cyber incident. This may pose a revolutionary incentive for how states apportion its assets for the National Guard. Should Governors reallocate resources from other conventional National Guard units to network warfare or cyber protection team units? This may be a particularly relevant question for states with uncontested borders but which house major centers of industry. It seems highly unlikely that there will be large scale air or ground invasions of a state's borders.

However, it seems highly likely that the critical infrastructure within states will be increasingly bombarded with cyber attacks, potentially with large economic implications for states. This would suggest that more investment in cyber capabilities within the National Guard and concerted efforts to recruit, train, and retain cyber talent will be a future priority for state governments.

VIII. Conclusion and Further Research Recommendations

In our war game, the attacks that were most likely to escalate to a national security incident were those on the civilian nuclear sector and sectors that had strong linkages across the national economy. Attacks on these sectors with strong linkages within the rest of critical infrastructure created cascading effects, many of which had life or death implications beyond the initial scope of the cyber attack. Therefore, results from the war game suggest that U.S. government resources and policies should focus on the energy, transportation, communications, water/wastewater, and nuclear sectors. While there were other sectors that experienced loss of life, the effects from these cyber attacks were largely confined to their sector and therefore were less likely to create a national security crisis.

Our war game also provided insight into the desires of the private sector from local, state, and federal government. In our event, private sector companies largely sought to remediate impacts on their own networks without government support (the exception may be highly-regulated industries such as energy or nuclear), but looked to the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) for information sharing about threats. Once physical damage or loss of life occurred, private sector leaned heavily on local emergency management and state resources, such as the National Guard, as the first line of defense. This meant that the primary role desired for the DOD was to counter cyber attacks prior to a major campaign as well as to ensure a credible deterrence by punishment strategy through a wide range of cross-domain capabilities.

This war game has highlighted the extraordinary dependencies between critical infrastructure sectors and the U.S. economy and military power. Further research will explore the dependencies between U.S. military missions and civilian infrastructure and will create an understanding of the potential vulnerabilities that these dependencies have to cyber attacks.

Finally, as with all games, the findings from this war game should not be taken as the final word on these issues. Games are a moment in time with a small sample of the population. We made some choices to sacrifice realism for the sake of exploring our question (for instance, providing attribution for all the attacks). We have tried to caveat our findings based on these limitations.

IX. Appendices

Appendix A: Overview of BLUE

The war game participants all played as leaders within BLUE, a notional advanced state modeled on U.S.

- **Government**
  - For purposes of game, identical to U.S. with comparable agencies, departments, and capabilities.
- **Economy**
  - Large and diverse economy with major multinational companies in most sectors
  - Extremely digitally reliant
    - Highly integrated Internet of Things (IoT), networks
  - Resource rich, major large oil and gas exporter
  - GDP of ~$18 trillion, largest global economy
- **Military Capabilities**
  - Global military power
    - Advanced blue-water navy
    - 5th-generation aircraft
    - Moderately sized, well trained and equipped land forces
    - Advanced special operations capabilities
  - Full strategic nuclear capacities
  - Global forward deployed forces
    - Able to exert military force globally
  - Extensive cyber capabilities
  - For game purposes, able to engage in offensive and defensive operations
- **BLUE State**
  - Large coastal state
  - Well-developed and integrated infrastructure
- **BLUE City**
  - Largest city in BLUE, population ~9 million
  - Hub of economic activity in BLUE
  - Not the capital of BLUE

Appendix B: Overview of RED and Scenario 1

Adversarial power controlled by the White Cell. RED represented a hostile state and was presented in Scenario 1. An overview of RED is provided followed by the Crisis Scenario that precipitated Scenario 1, followed by RED's stated objectives.

RED State

- **Economy:**
  - Developing state, resource-poor
    - Highly dependent on oil for energy
  - Large technical sector, highly educated population
    - Under-employed in private sector

    - GDP $375,000 (millions of US$)
        - #30 in the world
- **Government: Authoritarian**
    - Ethnic separatists
    - Internal dissidents
    - Young population
- **Military:**
    - Regional power
        - Strong conventional capabilities within region
            - Brown-water navy
            - 4th-generation aircraft
            - Modern integrated air defenses (ranges out to 50NM+)
            - Large army and special operations forces
        - No ability to reach BLUE with conventional weapons
        - No nuclear capability
- **Geopolitics:**
    - Antagonistic relationship with BLUE allies in the region
        - Disputed territories currently controlled by RED
    - Aggressive push to secure oil and decrease dependency on BLUE without success
- **Cyber Capabilities:**
    - Large focus on cyber capabilities
    - Known successes with infiltrating supply chains, unconventional accesses, and new cyber tactics

RED Crisis Situation

- **RED recently conducted crack-down on ethnic/religious groups**
    - Possibilities of chemical weapon use
    - Concerns about genocide
- **Triggered domestic legislation in BLUE**
    - Created a total oil embargo/sanctions by BLUE and BLUE allied-countries on oil-dependent RED
    - Oil embargo and sanctions cannot be revoked without Congressional and Presidential approval
- **Without oil, RED is experiencing significant unrest**
    - Limited power in cities has led to riots
    - Military unable to conduct significant defensive or offensive operations
    - Oil reserves being siphoned to military
- **RED enemies in the region massing at RED's borders**
    - RED concerned neighbors may conduct strike to take advantage of RED's current weakness
    - RED unable to sustain forces in disputed territories for more than a week
- **RED Foreign ministry statement: "we will conduct an asymmetric attack at the heart of BLUE society" if BLUE does not lift oil embargo**
- **Intelligence indicates increases in cyber network intrusions from RED**

- All source intelligence shows increase in RED military cyber force activity

RED Objectives

- Quell internal unrest
- Deter regional adversaries from attacking disputed territories
- Convince BLUE to lift oil embargo
- Conduct information operations to convince international community to drop support for oil embargo

Appendix B: Overview of REO and Scenario 2

REO was an adversarial power controlled by the White Cell. REO represented a hostile non-state, violent extremist organization and was presented in Scenario 2. An overview of REO is provided followed by the Crisis Scenario that precipitated Scenario 1, followed by REO's stated objectives.

REO Non-State Actor

- **Extremist trans-national terrorist organization**
  - Large contingent of non-affiliated lone actors
- **Wants to create its own religious state**
  - Supports social services and governance within occupied territories in PURPLE
- **History of bombings, hijackings, shootings across the world**
- **Currently in a civil war with BLUE's Ally, PURPLE**
  - BLUE has no forces in PURPLE, but does train PURPLE military personnel and provides weapons and aid to PURPLE
- **Military:**
  - Trans-national terrorist cells
    - Explosive ordnances, snipers, suicide operations
  - Irregular forces in Purple with small arms and light vehicles
- **Economic:**
  - Trying to amass significant resources via drug trade, bank robberies, and extortion
  - Economic resources vital to REO objectives—requires funding in order to support territories and conduct terrorist attacks and irregular warfare within PURPLE
- **Cyber:**
  - Significant focus on building capabilities and recruiting talent
  - Focus on insider threat for access (sleeper terrorist cells)
  - Extensive use of ransomware

REO Crisis Situation

- **BLUE leading international campaign to cut off REO's funds**
  - Frozen bank accounts
  - BLUE companies refusing to work with REO associated companies
    - Banks that work with REO
    - Food and healthcare conglomerates that REO has contracted for support
    - Energy companies
- **REO has launched a "Down with BLUE" campaign**
  - Promised attacks "to the soft-belly of BLUE"
  - Increase in propaganda operations
- **Purple initiating major ground campaign to take down REO strongholds within PURPLE**

REO Objectives:

- **Create REO state within PURPLE territories**
- **Generate money**
- **Conduct information propaganda**
- **Deter/defeat PURPLE attacks**
- **Punish BLUE and inflict terror on BLUE population**

Appendix C: Company Profiles

- **Private Sector Cell**
  - The Private Sector Cell consisted of 14 companies, each in a different sector
  - Each sector represented a designated critical infrastructure sector
- **Company overviews**
  - Each company was an industry leader, one of largest companies in their sector
  - Each company was publicly traded, is subject to the market
  - All companies were headquartered in BLUE
  - The companies were headquartered, or had substantial operations, in BLUE City

Company Name	Company Profile
Chemical Company	Chemical Company is a publicly traded multinational chemical manufacturer headquartered in Blue City. An industry leader with over 45,000 employees globally, Chemical Company manufactures plastics, chemicals, and agricultural products. They operate many manufacturing facilities in the Blue City area, particularly from their agricultural products division.
Com-Fac Company	Com-Fac Company is a publicly traded, industry leading hospitality company based in Blue City. The company also owns the largest chain of affordable midrange accommodations throughout the country, Villa Hotels. In addition to owning many profitable subsidiary companies, Com-Fac Company owns and operates some of the most exclusive hotels in BLUE, including The Ascension and the Grand Nimitz Hotel in Blue City.
Communications Company	Communications Company is an industry leading, publicly traded cellular provider headquartered in Blue City. A Fortune 500 company, Communication Company operates the largest cellular network in Blue, with over 145 million customers. The Communications Company has invested heavily in infrastructure, boasting the most cell sites in Blue City and frequently ranked the most reliable in the country.
Manufacturing Company	Manufacturing Company is a publicly traded manufacturing conglomerate headquartered in Blue City. A Fortune 500 company, Manufacturing Company is primarily engaged in capital and energy intensive manufacturing, including heavy machinery production. The company is diversified and has extensive light industry and mineral refining operations.
Dam Company	Dams Company is the largest dam owner and hydroelectric producer in the Blue City region, and a leading hydroelectric company that has invested heavily in modernizing its infrastructure. Operating over 42 dams, including Blackwater Dam, the largest regional dam. Dams Company sells its power output to Energy Company for transmission and distribution.

Defense Company	Defense Company is publicly traded, aerospace, defense, and security company. A Fortune 500 company, Defense Company is a leader in military aircraft design, development, and manufacturing, for which it is most well-known. The company boasts extensive international operations, with its 120,000 employees dispersed across the globe. However, the company is headquartered in Blue City.
Energy Company	Energy Company is a publicly traded Fortune 500 power production, transmission, and distributer in BLUE, and the largest electricity provider in Blue City. The company owns and operates conventional fossil fuel power stations, but has diversified in renewables. Energy company also purchases wattage from Nuclear Company's Raven Island Power Station, which accounts for approximately 30% of the Blue City's power, and Dam Company's hydroelectric dams.
Finance Company	Finance Company is a Fortune 100 publicly traded investment and financial services institution. Finance Company largest banking service provider in BLUE, and operates over 5000 banking branches across the country. The company has invested heavily in its internal network infrastructure and is widely regarded as a leader in online banking and wealth management.
Agriculture Company	Agriculture Company is a publicly traded and highly diversified multinational food and agricultural conglomerate. A Fortune 500 company producing a wide range of consumer goods, ranging from organic produce to canned foods, from soft drinks to soap, the company has invested heavily in its network infrastructure and logistics.
Healthcare Company	Healthcare Company is a for-profit publicly traded healthcare management company based in BLUE. The company operates over 130 hospitals nationally, and 27 hospitals in the Blue City area. This includes 4 Level I Trauma centers, Mercy Regional, Blue City Memorial Hospital, and Maxwell Wood Medical Center, and New Providence Hospital. The company also manages a series of community clinics throughout Blue City.
IT Company	IT Company a publicly traded company and global leader in software development. The company specializes in developing high-end enterprise application software (EAS) solution for large corporate clients. The company has clients and office around the globe, but is based in Blue City.
Nuclear Company	Nuclear Company is one of the largest publicly traded national nuclear power stations operators, with power stations across BLUE. Nuclear Company owns and manages Raven Island Power Station near Blue City, which operates four Pressurized water reactors (PWR). One reactor is currently offline. The facility is the single largest energy producer and power seller to Energy Company. Raven Island provides approximately 30% of Blue City's power.

Transportation Company	Transportation Company is the largest publicly traded commercial airline in BLUE, and an industry leader in both passenger air travel and cargo. The company operates a fleet of over 1200 aircraft supporting its passenger and cargo operations. Transportation Company operates out of Blue City International Airport (NWW), which is their main hub, and uses Mahan International Airport (NWN) as its hub for cargo.
Wastewater Company	Wastewater Company is a multi-national company that serves 8 million people in Blue and treats 900 million gallons of wastewater a day. The company has over 4,000 employees and is the sole wastewater service provider for Blue City.

Appendix E: Player Actions

Game play considered of player taking actions. The four player action types are described below.

Player Options	Description
Action	Players took specific actions in the form of issuing orders to their organizational subordinates. When a player took any actions, they were directed to state the objective of the action, what subordinates the order applied to (IT team, legal department, etc.) the perceived best and worst outcomes of the action, and a justification for why they were taking the action. These orders were received by the White Team, which adjudicated the results. Any results from the action would be reported back to the player from the perspective of their subordinates. For example, the player could take an action by directing their company IT team to take the company webmail offline. The White Cell adjudicated the action and reported back the success (or failure) of the action.
Request Government Aid (Req. Govt. Aid or RFGA)	Private Sector Cell players could formally request support from agencies and departments within the Federal and State/Local Cells. Additionally, the Governor and Mayor from the State/Local Cell could also request assistance from the Federal Cell. Players would specify what form of support they were requesting (emergency management, cyber mitigation, etc.), specifics of what they wanted to accomplish, the perceived best and worst outcomes, and why they were requesting the support. The request would be pasted directly to the relevant player cell and the Federal Cell and/or State/Local Cell could take an action (give orders to their subordinates) to execute the request. The player could then reply directly to the request.
Press Release (Media)	The players could make press release, official statements from the player's organization. These press releases would be distributed to all players along with other media reports. Additionally, the press statements potentially affected game play in other ways, depending on how the public responds to the statements.
Request for Information (RFI)	Request for Information allowed players a basic question-and-answer with the organization's subordinates. These requests were used to clarify information about the organization or a situation. For example, a player could ask their subordinates to clarify the severity of a server crash or the amount of reserve fuel remaining for backup generators.

Appendix F: Injects for Scenario 1 and Scenario 2

Below are the pre-designed injects for Scenarios 1 and 2. These injects were scripted to be sent directly to players at predetermined times, at either the outset of the scenario (part A) or at the midway point (part B). For convenience, each inject is labeled with the intended effect categorization. For further reference, all pre-scripted "informational" injects are also included.

Due to system problems during Scenario 2 the finalized game injects were not available. Instead players were presented with an earlier draft of the injects. Effects and framing remained constant between the intended finalized injects and the draft versions that were utilized. However, there were some minor phrasing differences, such as the references to "New Washington" instead of "BLUE City."

Player Injects for Scenario 1

Part	Status	Sector	Effect	Event
A	Sent	Chemical	Physical (Loss of Life)	Staff report there was an explosion at a BLUE CITY Chemical Company facility. The facility produces a range of agricultural products, but primarily pesticides. Six Facility employees are missing, and are presumed dead. The media is aware of the explosion. It appears that the explosion was caused by an error in the storage control system. The error caused chemicals to be stored improperly and created an unstable reaction. Initial incident reports show no leakage of hazardous chemical agents, and the explosions did not compromise any other in-use storage tanks.
A	Sent	Chemical	Info	Staff report that despite the recent brownouts, operations have been minimally affected. As a major Energy Company customer with high energy demands, Chemical Company facilities draw power directly from the transmission grid and were unaffected by disruptions to the distribution grid.
A	Sent	Chemical	Virtual	Staff report that Chemical Company is being hit by a large, and concerted DDoS attack. The attack has knocked the most outward facing sites offline, including some employee and remote access portals. The attack is disrupting the day-to-day remote operation of Chemical Company facilities and systems. So far there have been no physical effects of the DDoS, but there have been significant employee cost overruns as additional staff have had to work over-time and production has slowed.

A	Sent	Chemical	Physical	Staff report severe damage at a Chemical Company facility that manufactures industrial grade plastics. The facility experienced multiple water line ruptures after valves were abruptly and unsafely closed during normal operation. No personnel were injured, although operations have been greatly degraded and staff are concerned for the potential risks of water damage to other parts of the facility. System engineers have located an extensive array of deeply embedded malware in the facility command systems.
A	Sent	Communications	Physical	Technicians report fires at cellular sites across the BLUE CITY region. The transmission equipment at the cell sites suffered power surges above safe thresholds resulting in equipment damage. The damage at affected towers is significant. Staff report degraded cellular connectivity in the region on Communications Company networks, although not total loss of operations. Customers are operating with reduced or no data access and may experience connectivity issues. Media has picked up the story.
A	Sent	Communications	Virtual	Staff are reporting a major incident with customer subscription management. The primary subscription management database was tampered with and over 2 million customers were automatically notified that their subscriptions, and coverage, were being terminated. Coverage to these customers has not yet been restored. The customers, primarily in the BLUE CITY region, are outraged and have taken to social media to complain. The media has not yet take up the story, and some are even calling the incident an elaborate hoax.
A	Sent	Critical Manufacturing	Info	Staff report that despite the recent brownouts operations have been minimally affected. As a major Energy Company customer with high energy demands, the Manufacturing Company facilities draw power directly from the transmission grid and were not the affected distribution grid.

A	Sent	Critical Manufacturing	Virtual	Staff are reporting a major disruption with the company manufacturing inventory management system. Inventory levels of crucial manufacturing inputs for a range of Manufacturing Company products have been manipulated, and production has been adversely impacted. Power turbine and transmission equipment manufacturing units are currently the most impacted with a nearly complete loss of inventory information. Floor staff are unsure if they can proceed with assembly. Staff have temporarily halted the automated logistics system to prevent unnecessary procurement.
A	Sent	Dams	Virtual	Staff report that Dam Company data system have been compromised. The compromised systems are responsible for monitoring hydroelectric power demand, electrical output, and automatically managing the sale of electrical output to the electrical grid. The system has been infected with malware that subtly manipulated data to under-report demand, output, and sales, but still be within normal bounds. The result could have been a substantial impact on profits and lower power output into the grid.
A	Sent	Defense Industrial Base	Virtual	Staff are reporting signs that large volumes of extremely sensitive financial data and business strategy documents have been exfiltrated from Defense Company. Documents pertained to ongoing programs, as well as projections for follow-on and future programs, including potential new business avenues and bidding information for potential contracts. If made public or shared with competitors this information could result in substantial lost revenue. Additionally, the stolen program material relates directly to BLUE military weapon research and development and could compromise the technological competition between BLUE and RED.
A	Sent	Defense Industrial Base	Info	Staff report that despite the recent brownouts operations have been minimally affected. As a major Energy Company customer with high energy demands, Defense Company facilities draw power directly from the transmission grid and not the affected distribution grid.

A	Sent	Energy	Physical	Workers reported explosions and fires at company facilities. Technicians report extensive physical damage to many distribution substations and transformers, as well as damage to some step-down stations. There have been no reported injuries, but the substations, transformers, and step-down stations have been physically damaged and will require repair or replacement before the grid will return to normal functioning. Industrial and large corporate customers who draw power directly from the transmission grid have not been impacted. Customers have been complaining of unreliable access to power as the city suffers widespread outages. BLUE CITY suburbs are also reporting power outages. The repair cost estimates are soaring and initial lost revenue is estimated in the multi-millions of dollars and rising.
A	Sent	Energy	Virtual	Staff report that the data that underlies the Energy Company's smart grid have been subtly modified. The altered data is used to inform potential heightened and peak usage times that would require increased capacity. The data alterations would make the grid considerably more susceptible to failure during peak usage times. Staff are working to recover the data, but the process will take considerable staff hours and time.
A	Sent	Federal Government	Info	RED's neighbors, GREEN and PURPLE, who are friendly with BLUE are asking BLUE State Department to hold firm on the oil embargo and sanctions. They are also asking that BLUE make a statement about redlines for cyber incidents, as they are worried about potential cyber attacks from RED.
A	Not Sent	Federal Government	Info	BLUE CITY's major military base is reporting difficulty making phone calls outside of the base. While running a recall exercise, they were unable to contact 33% of assigned personnel. This includes members of the National Guard tasked with combat air patrols of BLUE CITY and the Cyber National Mission teams associated with the State Guard unit.

A	Sent	Federal Government	Info	RED's Ministry of Foreign Affairs reached out representatives at BLUE State Department with a statement: "You may have thought in the past that you could conduct economic warfare against us without repercussions. But oceans cannot protect you now. We demand an immediate roll-back of sanctions and actions taken that threaten our access to oil. If you do not, there will be consequences."
A	Sent	Federal Government	Info	Intelligence sources are reporting that RED has established a dedicated cell to target BLUE nuclear facilities. They have already successfully gathering critical information on employees and their roles for a large nuclear power company, Nuclear Company.
A	Sent	Federal Government	Info	FAA staff reporting that there have been substantial ATC equipment difficulties at Mahan International Airport (NWN). Technicians report that the air control system was apparently targeted by a malicious cyber attack. Before air traffic controllers were aware of the situation, a Transportation Company cargo plane crashed during an attempted landing at the airport while on approach.
A	Sent	Financial Services	Physical	Staff reports there was a fire at a major BLUE CITY mainframe facility that processes financial transactions. The fire caused moderate damage to two floors of the facility before fire suppression systems ended the blaze. It appears that sensors for the facilities cooling system were tampered with and failed to provide accurate temperature control, leading to the blaze. There were no reported injuries. The building is currently evacuated and financial transactions are being transferred to another facility, causing intermittent service outages for customers. Customers are already complaining about the spike in processing times and incomplete transactions, particularly at ATM and debit transactions. The media has not yet picked up the story, although customers are complaining on social media.

A	Sent	Financial Services	Virtual	Staff have discovered a complex suite of malware throughout the company's operations. The malware appears to have been surveilling the company and capturing sensitive information on Finance Company strategic plans, trading and investments strategies, and holdings. The malware also appears to have the capability to facilitate further network intrusions and data manipulation. The information captured by the malware would provide considerable financial advantages to an individual or state.
A	Sent	Food and Agriculture	Info	Staff report that despite the recent brownouts operations have been minimally affected. As a major Energy Company customer with high energy demands, the Agriculture Company facilities draw power directly from the transmission grid and not the affected distribution grid.
A	Sent	Food and Agriculture	Physical	Staff report that a BLUE CITY vegetable canning facility was forced to halt operations. The facility's autoclaves overheated and resulted in damage to the autoclave and the facility's integrated canning system. The autoclave control systems report that the autoclave was operating at a safe temperature. However, the facility engineering team have discovered that the autoclave temperatures readings were tampered with to read below the target range.
A	Sent	Healthcare and Public Health	Info	Staff are reporting that despite the recent brownouts all Healthcare Company hospitals are operational and have their emergency generators on standby. Some Community Clinics, however, have seen service disruptions.
A	Sent	Healthcare and Public Health	Virtual	Staff at 13 Healthcare Company hospitals across BLUE CITY are reporting that the patient management system is currently experiencing substantial computer access issues. Although critical patient information and medical records currently in use, including in-patients and those records that have been recently accessed (including most-outpatients) are not affected. Patients are complaining about "service disruptions" and some have taken to social media. In these social media posts, some of these patients are complaining about loss of care, long wait times, and discussing grounds for a class action suit.

A	Sent	Healthcare and Public Health	Physical (Loss of Life)	Staff report a serious cyber incident at Mercy Regional hospital. The hospital's integrated healthcare monitoring system has been effectively locked down, with medical staff shutout of terminals, unable to access patient records, or operate medical equipment connected to the network. This incident is beginning to cause a panic, and there have been 2 reported deaths related to the lockout. All scheduled, non-critical, medical procedures have already been cancelled. There have so far been no media reports related to the incident.
A	Sent	Nuclear Reactors, Materials, and Waste	Virtual	Security staff are reporting signs the HR Department network was breached and that large volumes of sensitive employee information and PII was taken. This includes the positions, roles, and site access rights of employees at Nuclear Company.
A	Sent	Nuclear Reactors, Materials, and Waste	Physical (Loss of Life)	Staff are reporting that 5 technicians have died, and 3 other employees are in critical condition, following a serious generator fire. The team was conducting routine tests and repairs of the diesel generators for the auxiliary coolant pumps at Raven Island Power Station. The team began with the generators for reactor 4, which is currently offline. When the maintenance team performed a test start on the generator it malfunctioned, and a fire ensued. The fire is currently under control. The media has not yet picked-up the incident. The generator has been critically damaged and will need a full replacement. There were no radiological materials exposed or at risk. Network technicians report that the generators generator safe operating procedures had been altered remotely.
A	Sent	State & Local Govt.	Info	Staff are reporting an influx of calls from concerned residents in the area around the Chemical Company facility following a loud explosion and smoke rising from the facility. The facility is known to produce pesticides and area residents are concerned and want assurances that they're safe.

A	Sent	State & Local Govt.	Info	BLUE CITY's major military base is reporting difficulty making phone calls outside of the base. While running a recall exercise, they were unable to contact 33% of assigned personnel. This includes members of the National Guard tasked with combat air patrols of BLUE CITY and the Cyber National Mission teams associated with the State Guard unit.
A	Sent	Transportation Systems	Virtual	Staff are reporting that Transportation Company flights have reached a standstill at BLUE CITY International Airport (NWA) as flight information has suddenly been lost following a severe network breach. Staff are trying to manage flight connections, luggage routing, and the thousands of stranded passengers.
A	Sent	Transportation Systems	Physical (Loss of Life)	Staff report a Boeing 767 cargo plane for Transportation Company suffered a fatal error while on approach at Mahan International Airport (NWN) and landed short of the runway. The crew of 4 perished in the crash and the airport has been at least temporarily shut down. Initial reporting suggests that at the time of the incident air traffic control was experiencing serious anomalies with air traffic control systems in concert with bad weather and pilots new on the airframe. Due to the anomalies and the subsequent aircraft crash, all flights to and from the airport have been grounded. Hundreds of flights have been cancelled. Thousands of passengers are stranded.
A	Sent	Waste and Wastewater Systems	Virtual	Staff report inability to access integrated control system at wastewater plants throughout BLUE CITY following a complex cyber attack on the system. Currently all systems are running as set prior to the system malfunction, but the system is unable to adapt or execute commands issued remotely.
B	Sent	Commercial Facilities	Virtual	Staff report that information in the central reservation system (CRS) for Villa Hotels has been manipulated, with reservations being moved, deleted, or altered in some way. Management at Villa Hotel locations across BLUE CITY are reporting customers claiming to have reservations (most with confirmation emails) and complaining that they aren't getting their rooms. Frustrated customers have already taken to social media to air their grievances.

B	Sent	Commercial Facilities	Physical	Staff report that all fire suppression systems at the Com-Fac Company flagships BLUE CITY property, The Ascension, have been activated. This includes in every zone and in every room. The all-clear message was nonfunctioning and staff were forced to cut power to the fire pump. The hotel has been forced to conduct a total evacuation, and angry patrons have already taken to social media.
B	Sent	Critical Manufacturing	Physical	Staff report that the newly opened BLUE CITY Steel Mill has just suffered major damage. The furnaces were going through a routine power down following prolonged use, but the power down order failed. The staff were forced to initiate a full emergency shutdown, which severely damaged the furnaces. There is evidence of extensive tampering with the furnace SCADA. The damage is extensive. No workers were harmed, but are uncertain what to do with the active furnaces that are approaching a necessary power down.
B	Sent	Defense Industrial Base	Physical	Engineering staff are reporting a subtle defect in a critical component for an advanced BLUE air platform. The defect was remotely inserted into the manufacturing CAD used directly by the industrial robots. The defect was detected during a quality control review, and is clearly intentional and well enough engineered to be hard to detect. Staff only identified the issue because of newly implement quality control processes.
B	Not Sent	Energy	Physical (Loss of Life)	Staff report the death of four employees. The four engineers were part of a team working on a substation following earlier incidents when a power surge struck the station, resulting in a minor detonation. The part of the substation the engineers were repairing was supposed to be offline, but the automated grid was tampered with causing a surge at station and the resulting accident.
B	Sent	Federal Government	Info	Intelligence sources report that RED leadership has directed their cyber forces to target energy infrastructure in BLUE CITY. While the scope and target of cyber attacks remains unknown, reporting suggests that there will be a concerted cyber campaign to coerce BLUE to drop their support for the oil embargo and sanctions. High confidence assessment is that RED has the capabilities to successful execute large scale cyber operations against BLUE and the energy sector.

B	Not Sent	Federal Government	Info	Intelligence sources reports that behind closed doors hardliners within RED are calling for a more heavy-handed approach to dealing with the economic aggression of BLUE. They demand the country's cyber forces strike out at the supposed energy "life blood" of BLUE, nuclear power, in retaliation for the oil embargo. Meanwhile, satellite imagery has shown forces massing at the disputed border-line between RED and two other nations. Both countries appear to be calling up reserves and placing fighter jets on alert.
B	Sent	Financial Services	Info	Despite the recent brownouts staff are reporting stable operations. The company's most sensitive systems, such as transaction mainframes and data centers, have backup generators in case of such an emergency.
B	Sent	Food and Agriculture	Virtual	Staff reporting that after a routine internal audit that financial records have been altered. The records appear to have been altered remotely, and there are no signs the alterations were fraudulent. Staff attempted to draw data from backups and found that data had also been affected. The records can be restored, but it will take considerable effort and staff hours.
B	Not Sent	Healthcare and Public Health	Physical	Staff at 7 BLUE CITY hospitals, including Mercy Regional and BLUE CITY Memorial Hospital, are reporting that temperatures of the units used to store sensitive medical supplies have risen substantially above safe levels. Readings coming from the storage units still report normal temperatures. Although substantial stores of medical supplies have been damaged, resulting in thousands of dollars or more in lost supplies, none of the tainted medical supplies have been used, and there have no casualties so far related to this incident.
B	Sent	Information Technology	Virtual	Security staff identified a serious breach into the system that has resulted in the theft of a digital certificate. This certification may have been used against IT Company's cutting-edge enterprise application software. It is primarily used when pushing updates to customer systems. Staff are uncertain how long the certificate has been held by the intruders, but based on the intrusion pattern it may have been a considerable length of time.

B	Sent	Nuclear Reactors, Materials, and Waste	Physical	Staff report damage at the Raven Island Power Station. The facility has experienced multiple water line ruptures after valves were abruptly and unsafely closed during normal operation. No personnel were injured, although engineering staff are concerned. The water mains were part of the water feed to the auxiliary systems for the three operational reactors. System engineers have located an extensive array of deeply embedded malware in the facilities SCADA.
B	Sent	Nuclear Reactors, Materials, and Waste	Nuclear	Staff report a critical emergency at the Raven Island Power Station. The facility reactor coolant pumps have gone offline for all three active reactors. Staff immediately activated the auxiliary pumps for reactor 1 and 2 operational, however the auxiliary pump for reactor 3 failed. Reactor 3 experienced a rapid hydrogen gas buildup and a serious explosion that resulted in a breach of the containment building. The explosion has left 2 on-site engineers missing, and presumed dead, and exposed 3 employees to a potentially lethal dose of radiation. The reactor 3 containment building is currently releasing low level of airborne low-grade radiological material. There are significant quantities of radiological material within the facility. Initial projections are placing this accident at a INES level 4, with a rise to level 5 depending on the severity of the airborne contaminants. None of the reactors were operating at peak output, technicians report that the other two reactors are compensating for the power loss...
B	Sent	State & Local Govt.	Info	The Mayor's staff are reporting anxiety and heightened concern from the public regarding the brownouts due to the damage at the power distribution facilities, citizens have been calling nonstop. People are concerned that the brown out might be the result of terrorism, or worse, an attack by RED. Emergency dispatch is also reporting a higher call rate in response to the brownouts. So far, the increased demand for emergency services have been manageable. However, the number of calls to report looting and vandalism is rising.

B	Sent	State & Local Govt.	Info	Emergency responders have been called to Com-Fac Company's the Ascension, one of BLUE CITY's premier hotels. The hotel's fire suppression system is reporting fire in every zone in the hotel. Every fire suppression measure has been activated.
B	Not Sent	Transportation Systems	Physical	Staff report that a commercial passenger aircraft has crash landed at BLUE CITY International Airport (NWW). Thankfully there were only minor injuries. The flight was making the final approach in weather and runway lights and indicators had been tampered with. Initial reporting from the airport suggests that the light and indicator malfunction was the result of a cyber attack. The flight managed to adjust in time to avert a tragedy, but did skid off the runway. The landing severely damaged the aircraft's landing gears. The craft is currently stranded partly on the main runway and the median strip.
B	Sent	Waste and Wastewater Systems	Physical	Staff were unable to bring the integrated control system back up at two wastewater plants in BLUE CITY. The prolonged inability to control the system led to pump failure at two plants and sewage is currently flooding the primary treatment tank.

Player Injects for Scenario 2

Part	Status	Sector	Effect	Event
A	Sent	Chemical	Virtual	Staff have received a message from REO. They claim to have accessed senior level email accounts and downloaded thousands of correspondences. They claim to have embarrassing emails regarding unsafe working conditions and illegal chemical sales to sanctioned states. They included several "examples," including some which have been subtly altered to appear highly incriminating. REO is demanding $10 million or they will share the emails with the world. Staff have confirmed that the email accounts in question were breached.
A	Sent	Chemical	Physical	Staff report that a Chemical Company New Washington chemical plant has been targeted by SCADA attack. The attack forced open the valves of two benzene storage tanks which have leaked thousands of gallons of the noxious and highly flammable liquid. Staff could manually seal the tanks after they confirmed that the controls were being nonresponsive. The chemical is currently contained to the facility, but staff are concerned about containment. The media has not been alerted to incident.
A	Sent	Chemical	Physical (Loss of Life)	Staff report a fire has broken out at Chemical Company manufacturing facility. The fire began at an isolated petrochemical storage area at the facility. Fire suppression systems are in effect, although emergency services have not yet been notified. Staff are reporting that 4 facility employees are currently missing and are believed dead, 7 others have suffered severe burns. System engineers believe the fire was started when a pump overheated and malfunctioned, it appears that the pumps standard operating processes and limiters were altered. However, there doesn't appear to be external access to the system SCADA. Corporate security staff believe they may be dealing with an insider.

A	Sent	Commercial Facilities	Virtual	Staff received an email from REO with the following threat: "We have access to the locks in your hotels. All your customers should be afraid. We have REO operatives inside New Washington and will randomly take your customers hostage and behead them. We will release this information on social media if you do not pay us $10 million." Initial reporting from staff confirms that the locking system has been breached.
A	Sent	Communications	Physical	Staff are reporting a fire at one of the Communications Company's 7 New Washington central exchanges. The fire has nearly destroyed the site's main distribution frame, and while redundancies mitigated some of the effect, the fire has resulted in a temporary loss of connectivity and telephone access for tens of thousands of New Washington residents. The fire was apparently caused by an attack on the facilities heating control system, and ultimately resulted in a large blaze. The media has picked up the story.
A	Sent	Critical Manufacturing	Physical	Staff report there is a fire at a Manufacturing Company manufacturing plant. The facility was producing locomotives and rail equipment in support of a multimillion order rail order for a Purple infrastructure program. No employees were seriously harmed by the fire, but the damage is severe. The fire was triggered by an electrical malfunction, however, tampering with the manufacturing facilities fire suppression system fire pumps allowed the blaze to spread. The fire suppression system was manually activated, but the fire is not yet under control. Staff are estimating that the facility has suffered millions of dollars in damage.

A	Sent	Dams	Physical	Staff report that main spillway gate actuators, the mechanism that operates the dam gates, at Blackwater Dam have been damaged following an improper attempt to remotely open the gates. The damage is substantial and the actuators will require extensive and expensive repairs or full replacement. The spillway gates were open for a significant period before the operators could manually fix the problem. Significant flooding has occurred south of the Dam. No people appear to have been injured, but soy fields were flooded and there is expected be extensive economic impact.
A	Sent	Energy	Physical (Loss of Life)	Staff report that 4 employees are missing, presumed dead, and 3 others are in critical condition following a natural gas storage unit explosion at a New Washington area natural gas power station. The tank's control mechanisms were remotely tampered. When technicians were dispatched to investigate the tank, the tank exploded with several staff in the blast radius. The power station is still operational.
A	Sent	Federal Government	Info	Federal law enforcement elements monitoring and tracking illicit activity on several darknet forums have reported a spike in activity related to a new ransomware called LOCKMAGEDDON. The malware was developed by a radical hacker collective supporting REO. Posters claim to have seen the cryptoware deployed against many companies, almost exclusively in Blue.
A	Sent	Federal Government	Info	The Ambassador of Purple Informed Blue State and Blue SecDef that Purple will be initiating a large-scale military operation against REO-held territories in Purple. Purple would like Blue to increase financial actions against REO and supply more weapons to Purple. Additionally, Purple would like to discuss the possibility of augmenting Blue "special advisors" within front-line troops and potentially supplying air cover for Purple operations.
A	Sent	Federal Government	Info	SIGINT suggests that REO is planning a large-scale campaign against Blue up to and including attacks on nuclear facilities.

A	Sent	Financial Services	Virtual	Staff report that $24 million in fund transfers have been incorrectly authorized from over 13 accounts. The accounts belong to human rights and humanitarian NGOs that operate in REO's region.
A	Sent	Financial Services	Physical	Staff report that over 2200 computer terminals have been damaged as a result of a coordinated attack on the company's Federal Employee and Veteran Banking Services division. The attack resulted in the near total wiping of the affected machines, and many will need to be completely replaced. Most of the data hosted on the damaged machines was backed up, although any items employees were working on at the time were lost. It will take a substantial number of staff hours to normalize operations. The damage also resulted in a severe disruption in services to federal employees and veterans; many customers have taken to social media to air their grievances.
A	Sent	Food and Agriculture	Virtual	Staff report that Agriculture Company's financial records, including the backups, have been hit by LOCKMAGEDDON, a new strain of ransomware. The malware appears to have been dormant and only triggered when it migrated into the backup system. LOCKMAGEDDON is demanding $10 million for the data to be released. The news of the attack has not left the company.
A	Sent	Healthcare and Public Health	Virtual	Healthcare Company's main website, as well individual hospital websites and Community Clinic websites, have been defaced. The front pages have been replaced with REO messages and propaganda. Most worryingly, the defacements threaten that "This is only the beginning for Healthcare Company... Pray for your patients, we are coming for you! The halls of your hospitals will be our next battlefield" The media has picked up the story and patients are worried for their safety.

A	Sent	Information Technology	Virtual	Security staff have discovered a substantial data breach in an IT Company research and development unit. The breach was discovered after an anomalous data transmission from the unit. A review of the breach suggest that the attackers managed to exfiltrate large volumes of extremely valuable company IP. Staff are valuing the potential loss in the millions.
A	Sent	State & Local Govt.	Info	Staff report a dramatic spike in reports of suspicious activity and "unattended packages" hospitals and healthcare facilities following the REO defacement of the Healthcare Company's website.
A	Sent	State & Local Govt.	Info	The New Washington Health Department has received reports of people developing severe food poisoning, with symptoms of botulism. The commonality is that reported victims had consumed an Agriculture Company Canned Beef Product.
A	Sent	Transportation Systems	Physical	A commercial passenger aircraft with 192 passengers onboard reports a potential hack into the auto-pilot system. The aircraft was inbound to New Washington International Airport (NWW) when pilots reported that autopilot appeared to not be working appropriately. The pilots, who had been using autopilot to maneuver through weather, overrode the system and conducted an emergency landing manually. The landing moderately damaged the aircraft and the aircraft will have to be sent to maintenance. REO sent a message to the media about the incident threatening that worse would come.
A	Sent	Waste and Wastewater Systems	Virtual	IT staff report that emails for company executives have been accessed and downloaded by REO, including potentially harmful emails between wastewater plant managers about hiding the full environmental impact of the previous cyber attack. REO has sent a message to the company demanding $10 million dollars to keep REO from releasing the emails.

A	Sent	Waste and Wastewater Systems	Physical	Staff report that the control system of a tank at one of the New Washington wastewater facilities reported erroneous data about the tank's current capacity and therefore the automated overfill function failed. The tank flooded and sewage has spilled out of the facility. Crews are attempting to manually stop pumping, but the damage is currently not maintained. Staff are concerned that there may be costly and dangerous environmental repercussions for the neighboring community of industrial companies and large farms.
B	Sent	Commercial Facilities	Physical	Staff report that emergency fire suppression systems have been activated in the common areas of ten of the largest hotels owned by Commercial Facilities Company. Staff so far have been unable to turn off the system using any automated systems and so each hotel is attempting to turn the systems down locally. The common areas have so far received substantial damage from the water. Staff have received an additional email from REO asking for another $10 million or more attacks on fire suppression systems at hotels internationally will occur.
B	Not Sent	Communications	Virtual	Security staff are reporting a massive breach of the Communications Company subscriber database. Attackers managed to exfiltrate the account information of over 80 million Communications Company customers, but only stole the credit card information of 50 million customers. The attack was detected and staff were able to halt the data exfiltration. However, security staff report that they are already seeing the stolen credit card information appearing for sale on the Dark Web. The media has not been alerted to the incident.
B	Not Sent	Critical Manufacturing	Virtual	Staff report that Manufacturing Company's employee records, including payroll and other sensitive information, have been hit by a new strain of ransomware, LOCKMAGEDDON. The malware appears to have been dormant and only triggered when it migrated into the backup system. LOCKMAGEDDON is demanding a $10 million ransom be paid for the data to be released. The news of the attack has not left the company.

B	Sent	Dams	Virtual	The CEO of Dams Company is an avid runner and fitness tracker and wears a fitbit at all times. Recently, he received an email with a map of all his travel and a detailed log of activity. The email included a picture of REO beheading a hostage and a threat, "We know where you are at all times. We will find you and kill you if you do not send us $10 million. Enjoy your run today."
B	Sent	Defense Industrial Base	Virtual	Defense Company has received a message from REO. The message claims that REO has stolen thousands of employee records, including sensitive PII. REO is demanding that unless Defense Company pays $10 million, they will release the residential information for over 25,000 employees, including those living and working in high-threat locations, and will send their follower to kill them. "They will be butchered in their beds." REO provided full profiles of 10 employees as proof. Staff have confirmed the veracity of the 10 employee accounts, including a senior project manager currently working in a high-threat environment. However, staff are uncertain which of the company's' 120,000 employees might be at risk.
B	Not Sent	Defense Industrial Base	Physical	Staff report that Defense Company's New Washington military aircraft manufacturing facility has been forced to enact an emergency shutdown and cease operations. A series of industrial robotic arms used at the facility began acting erratically, endangering factory employees and causing damage to themselves and the military platforms being manufactured. The damage to two heavy aircraft under construction was substantial. However, the most severe damage was to the industrial robots themselves. Repairs are expected to be costly. No employees were injured. REO is taking credit and warning Defense Company not to provide weapons to Purple in their fight against REO.

B	Sent	Energy	Virtual	Staff report system problems with the Energy Company smart grid. The company's monitoring and reading department has lost connection with 100,000 deployed smart meters. The smart meters are in the trial stage and have been deployed to residential customers at considerable expense. An initial investigation revealed that the meters were infected with malware that restricted their signal transmission. Each meter will need to be individually serviced to restore functionality.
B	Sent	Energy	Physical	Staff report a major generator fire at the Northpoint Power Station, a 3 unit, 1300-megawatt natural gas power plant. The fire was caused by an unauthorized alteration to the Unit 2 fuel injection rate. Although turbine was severely damaged, and will need to be replaced, the fire is being contained by the facility's fire suppression systems.
B	Sent	Federal Government	Info	Federal law enforcement elements monitoring and tracking illicit activity on several darknet forums report that a cyber criminal group is claiming to possess extremely sensitive IP from the IT Company. The criminals are attempting to auction off the information and the current highest bid is $500,000. They released a handful of sensitive documents that appear to verify their claims. The criminal group is a known affiliate of REO.
B	Sent	Food and Agriculture	Physical	Staff report that as part of a routine quality check on canned food stuffs technicians discovered the dangerous bacteria C. botulinum in a can of Canned Beef Product. They executed an investigation and found that the sterilization systems were not operating as intended and had not been properly sterilizing the canned meats. The sterilization device had been remotely tampered with and its operating temperatures lowered to unsafe levels. Staff are uncertain if any of the contaminated cans left the facility. There have not yet been any media reports of botulism thus far.

B	Sent	Healthcare and Public Health	Physical	Staff report IT equipment problems at 13 Healthcare Company Community Clinics in the New Washington area, with vital computer systems unresponsive. The clinics are outfitted with a common suite of equipment, network equipment, and patient management software. On-site technicians confirm that machines have been reformatted and effectively wiped by a severe malware attack. The malware is encoded with anti-BLUE messages. Technicians believe they could restore the systems, but it may be less cost effective than replacement. Regardless, they expect the process to be time consuming and costly.
B	Sent	Healthcare and Public Health	Physical (Loss of Life)	Two Healthcare Company Hospitals are in crisis following a sudden spike in facility temperatures. New Providence Hospital, a Level 1 trauma center with 1500 beds, and Armistice Memorial Hospital, a Level III trauma center with 700 beds, were both affected. The hospitals experienced a sudden and rapid rise in temperatures above safe operating limits, approaching 102 degrees as the facility HVAC emergency heating was activated. The HVAC was unresponsive to commands and on-site technics cut power. However, the hospitals still both require extensive cooling during the summer season and temperatures are dangerously high. During the unprecedented temperature swing, 6 highly vulnerable individuals died due to the excessive heat. Many others have seen their conditions deteriorating. Staff report REO has sent a message to the Healthcare Company. They demand $10 million or "your other hospitals will suffer a similar fate!"
B	Sent	Nuclear Reactors, Materials, and Waste	Virtual	IT staff report that emails for company executives have been accessed and downloaded by REO, including potentially harmful emails between managers at the nuclear site about hiding the full environmental impact of the truck crash. REO has sent a message to the company demanding $10 million dollars to keep REO from releasing the emails.

B	Sent	Nuclear Reactors, Materials, and Waste	Physical	Additional reporting from the scene of the truck accident at the nuclear reactor indicate that when the truck veered off the road at the facility entrance, it ran into the guard post and destroyed the main entry/exit security apparatus at the facility.
B	Sent	Nuclear Reactors, Materials, and Waste	Physical (Loss of Life)	Updates from the scene of the truck crash report that the truck driver has passed away due to injuries received in the crash as well as at least one guard that was in the security post when the truck crashed.
B	Sent	Nuclear Reactors, Materials, and Waste	Nuclear	Staff report a significant accident involving a truck carrying radioactive waste that was leaving one of Nuclear Company's reactor sites. It appears that the truck transporting the material hosts a new system that sends information back to headquarters. This IOT (internet of things) system may have provided an access point for REO to control the brakes and truck accelerator, causing the truck to veer off the road and crash just outside the entrance of the nuclear reactor. At least one of the radioactive canisters appears to have been damaged and there are concerns about leakage of the radioactive waste.
B	Sent	Transportation Systems	Virtual	REO has conducted a major DDOS attack on Transportation Company's outward facing website and customers are unable to access travel information or conduct on-line travel requests. When individuals try to log on to the website, a large photograph of REO terrorists and threats to customers comes up on the website reading, "Infidels who fly business with Transportation Company will know the wrath of REO." An email has been received from REO that requests $10 million to cease the DDOS and web page defacement.

B	Sent	Transportation Systems	Physical (Loss of Life)	A commercial passenger aircraft with 75 passengers onboard has had to make an emergency landing with reports a potential hack into the autopilot system. The aircraft was inbound to New Washington International Airport (NWW) when the tower realized that the aircraft was not within the approved approach corridor. The tower notified the pilots. The pilots, who were relying on instruments in the weather, were unaware of the potentially faulty readings that had affected their approach. The pilots were unable to pull up in time and landed short of the runway. Reports from the scene are ongoing but at least a dozen passengers are presumed dead. REO has claimed responsibility for the incident.

[i] James R. Clapper, Marcel Lettre, and Michael S. Rogers. "Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States." January 5, 2017: https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

[ii] Chris Graham, "NHS cyber attack: everything you need to know about 'biggest ransomware' offensive in history," *The Telegraph*, May 20, 2017: http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/; Felix Palazuelos, "How the WannaCry ransomware attack affected businesses in Spain," *El Pais*, May 19, 2017: https://elpais.com/elpais/2017/05/19/inenglish/1495181037_555348.html; John Kennedy, "Impact of WannaCry: Major disruption as organizations go back to work," *Siliconrepublic*, May 15, 2017: https://www.siliconrepublic.com/enterprise/wannacry-impact-organisations-attack.

[iii] Healthcare IT News, "Petya cyberattack halts Merck production, hurts profit" http://www.healthcareitnews.com/news/petya-cyberattack-halts-merck-production-hurts-profits. Krebs on Security, "'Petya' Ransomware Outbreak Goes Global," June 17, 2018: https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/.

[iv] Office of Director of National Intelligence, "Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution," January 6, 2017: https://www.dni.gov/files/documents/ICA_2017_01.pdf; Andy Greenberg, "The NSA Confirms It: Russia Hacked French Election 'Infrastructure,'" *Wired*, May 9, 2017: https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/; Ellen Nakashima, "U.S. Officials say Russian government hackers have penetrated energy and nuclear company business netowrks," *The Washington Post*, July 8, 2017: https://www.washingtonpost.com/world/national-security/us-officials-say-russian-government-hackers-have-penetrated-energy-and-nuclear-company-business-networks/2017/07/08/bbfde9a2-638b-11e7-8adc-fea80e32bf47_story.html?utm_term=.ffa1aa48edb9.

[v] NCCIC, *ICS-CERT Annual Assessment Report*, FY 2016, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

[vi] Cara McGoogan, "Cyber attacks hit half of UK businesses in 2016," *The* Telegraph, April 19, 2017: http://www.telegraph.co.uk/technology/2017/04/19/cyber-attacks-hit-half-uk-businesses-2016/

[vii] Luke Graham, "Cybercrime costs the global economy $450 billion: CEO," *CNBC*, February 7, 2017: https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html; John Gilligan, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment* (AFCEA International Cyber Committee, October 2013: https://www.afcea.org/committees/cyber/documents/CyberEconfinal.pdf); Brian Taylor,

"Cyberattacks fallout could cost the global economy $3 trillion by 2020," *TechRepublic*, February 20, 2014: http://www.techrepublic.com/article/cyberattacks-fallout-could-cost-the-global-economy-3-trillion-by-2020/;
[viii] *Counting the Cost: Cyber exposure decoded*, Lloyd's Emerging Risks Report 2017, July 10, 2017: https://www.lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost.
[ix] Bret Basso, "Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories," *Fireeye*, April 29, 2016: https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html.
[x] Jacquelyn Schneider, "Digitally-Enabled Warfare: The Capability-Vulnerability Paradox," *Center for a New American Security*, August 29, 2016: https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox.
[xi] Valeriano, Brandon, and Ryan C. Maness. *Cyber war versus cyber realities: cyber conflict in the international system*. Oxford University Press, USA, 2015.
[xii] Christopher Bronk and Enekien Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* no. 2, 55 (81-96), 2013.
[xiii] Schneider, Jacquelyn. *The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict*. Diss. The George Washington University, 2017
[xiv] See section on executive orders.
[xv] Office of the President, "Executive Order 13010—Critical Infrastructure Protection", July 1996: http://www.presidency.ucsb.edu/ws/?pid=53066.
[xvi] The Department of Homeland Security, "National Strategy for Homeland Security," July 2002: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf.
[xvii] The Department of Homeland Security, "National Strategy for Secure Cyberspace," February 2003: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[xviii] Office of the Press Secretary, "Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center," October, 39 2009: https://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened.
[xix] Office of the Secretary of Defense, "Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," June 23, 2009: http://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-029.pdf.
[xx] The Department of Defense, "The DOD Cyber Strategy," April 2015: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
[xxi] Department of Homeland Security, "EO 13636 and PPD-21 Fact Sheet," March 2013: https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf.
[xxii] Office of the President, "Executive Order 13635 -- Improving Critical Infrastructure Cybersecurity," February 12, 2013: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[xxiii] Office of the President, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities", December 29, 2016: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency
[xxiv] Office of the President, "Executive Order 13694 -- Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf.
[xxv] Office of the President, "Issuance of Amended Executive Order 13694; Cyber-Related Sanctions Designations," December 12, 2016: https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20161229.aspx.
[xxvi] Office of the President, "Executive Order 13635 -- Improving Critical Infrastructure Cybersecurity," February 12, 2013: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[xxvii] Office of the President, "Executive Order 13800 -- Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", May 11, 2017: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal.
[xxviii] The second day had a smaller completion rate because players in the private sector cell used survey time to finish action forms they were unable to complete due to network degradation.