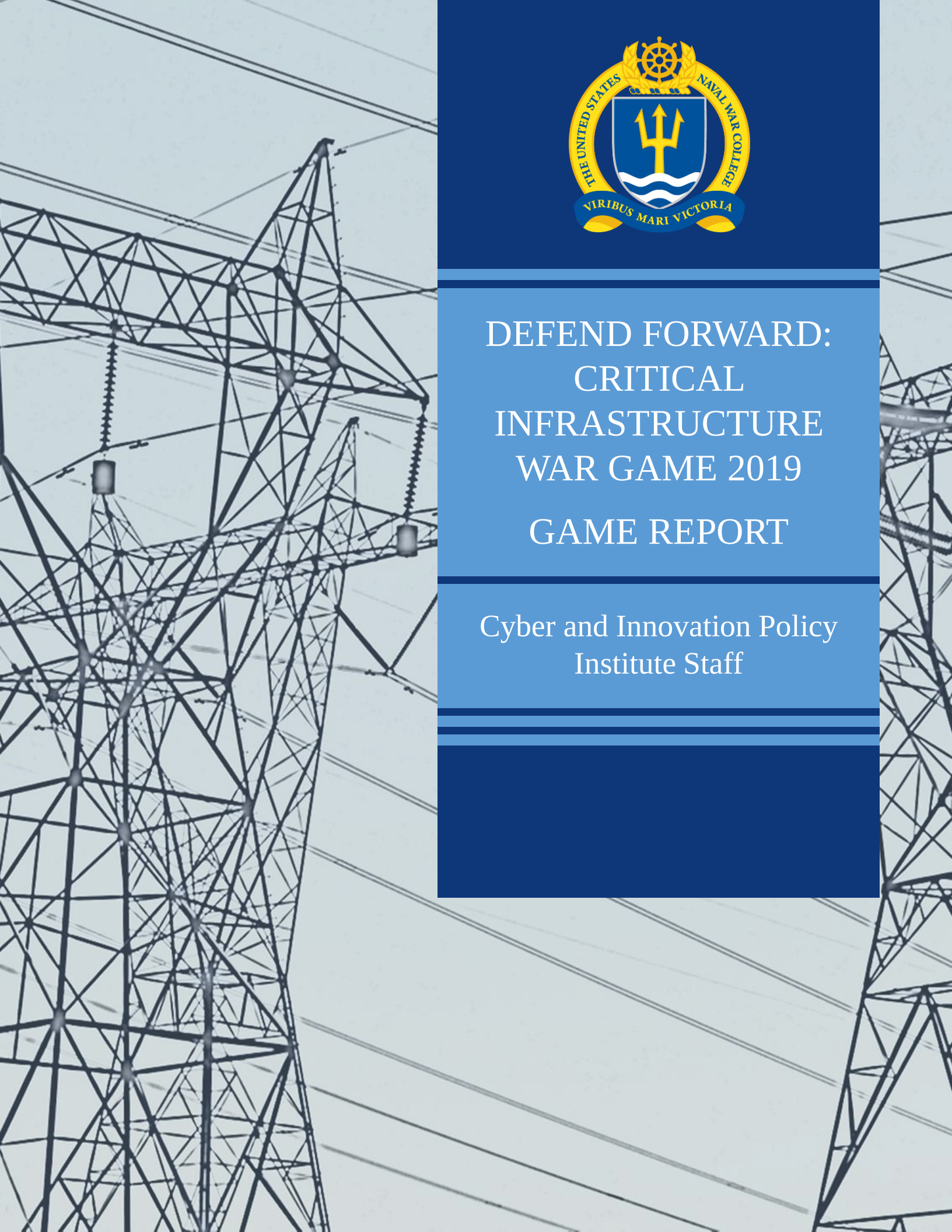


DEFEND FORWARD: CRITICAL INFRASTRUCTURE WAR GAME 2019

GAME REPORT

Cyber and Innovation Policy Institute Staff

Table of Contents

I. Defending Forward: Wargaming a Cyber Strategy

The publicly released, unclassified summary of 2018 Department of Defense Cyber Strategy introduced an important shift in Department of Defense (DoD) thinking about its roles in securing the United States against cyber attacks. The new strategy transitions DoD's cyber posture from a "be prepared" stance to defending forward, "to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[1] The introduction of Defend Forward also elevated the importance of the DoD within the U.S. government for defending the nation and critical infrastructure against foreign cyber attacks. Since its introduction, however, the DoD has struggled to explain Defend Forward. Illustrations of the strategy range from private sector intelligence sharing to forward deployment of cyber protection teams in allied nations to unconfirmed reports that the U.S. has inserted malware into adversary electrical grids. The significant array of activities that could fall under the umbrella of Defend Forward make the concept difficult to implement and introduces uncertainty about the DoD's role in combatting cyber attacks on critical infrastructure. It is unclear what is and is not possible under the new strategy both for adversaries and for private sector seeking help from the U.S. government to stem the rising tide of sophisticated cyber attacks.

The strategy was released at a time when cyber attacks on critical infrastructure were becoming more numerous, sophisticated and, perhaps, a normalized tool of state coercion. For example, the 2016 Russian cyber-enabled operations influenced the U.S. elections, Russian attacks on Ukrainian power grids that accompanied military operations along the border, and

[1] Department of Defense, *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: The Pentagon, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

North Korean and Iranian attempts to extort money from the U.S. financial sector all demonstrate the increasingly front line role of critical infrastructure in state-led cyber attacks.[2] Critical infrastructure from transportation nodes to power grids and the globally interconnected financial sector are among the linchpins of modern digitally-enabled societies. The success of the DoD's implementation of Defend Forward and its relationship with private sector infrastructure is vital not only for future military campaign successes but also for ensuring U.S. economic prosperity.

Defend Forward therefore merits further analysis, especially regarding if, and how, cyber operations in support of the strategy might affect the nation's critical infrastructure. What are the geographic boundaries of Defend Forward? What are the conceptual parameters of the new approach? What is Defend Forward's relationship the broader federal cyber security efforts? How do the unique needs of the different critical infrastructure sectors affect the way Defend Forward is operationalized?

The need to address these questions motivated the Naval War College's (NWC) Cyber and Innovation Policy Institute (CIPI) to design and execute an unclassified wargame. The two-day wargame held in July 2019 convened leaders from the finance and energy sectors with cyber practitioners. It served as a venue for strategy experimentation, revealing potential approaches to

[2] Examples from the 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; Brian Krebs, "'Petya' Ransomware Outbreak Goes Global," Krebs on Security, June 27, 2017, https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/; Erica Borghard, Protecting Financial Institutions Against Cyber Threats: A National Security Issue" (paper, Carnegie Endowment for International Peace, September 24, 2018), https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324.

implementing Defend Forward as well as challenges and opportunities for the strategy as it moves forward.

This report proceeds as follows. The first presents the NWC wargame design and play among fictional states using policies and theoretical capabilities. The second section discusses the findings of wargame using data gathered from game play, focusing on the actions by, and effecting, the private sector. The brief conclusion presents the potential implications for the cyber strategies as well as issues for further research, analysis, and wargaming.

II. The Defend Forward Wargame

To examine the implications of the different conceptualization of Defend Forward, operational implementation, as well their domestic impacts, the Naval War College developed The Defend Forward: Critical Infrastructure Wargame, a two-day event hosted in Newport. The focus of the wargame was the financial and energy critical infrastructure sectors, which were selected for two primary reasons. First, previous analyses and wargames, identified these sectors as essential for the security and prosperity of the United States. Second, both sectors have mature relationships with the U.S. government and participate in special pathfinder information sharing projects with both the Department of Homeland Security (DHS) and the DoD.[3]

The wargame was designed as a three-move, move-step, free play game, with a two private sector cells (Finance and Electric, each with four companies), a Blue State cell, and a Red

[3] Gopal Ratnam, "Pentagon, Homeland Security Helping Private Companies Defend Against Cyber Threats," *Roll Call*, November 15, 2018, https://www.rollcall.com/news/politics/pentagon-homeland-security-cyber-threats.

State cell.[4] Additionally, a White cell consisting of experts on domestic politics, military operations, cyber capabilities, economics, and electric or finance operations was created to asses, evaluate, and adjudicate the implications of actions taken by the players cells. The White Cell was responsible for simulating other global functions, such public perception, market activity, and also played Green State, an ally of Blue State. Finally, the White Cell was also responsible for providing updates on results of player actions in between moves.

The wargame involved the participation of over 100 subject matter experts, practitioners, and business leaders. Participants were organized into teams, or cells, based on the roles they played. CIPI collaborated with the Naval War College Foundation to recruit approximately 50 senior business people from the finance and energy sectors. The private sector participants were asked to play senior executive roles, CEO, CIO, CISO, COO, and government liaison, within notional companies in the fictional Blue State. We created four such notional companies for each of the two included critical infrastructure sector cells. Private sector players were asked to self-organize including assigning the roles and responsibilities among their team members.

We also recruited experienced practitioners to serve in a notional Blue State government—role playing for example, fictional analogs of DoD, DHS, the National Security Council (NSC), and other governmental agencies[5]—as well as a team of experts playing the adversarial Red State government, made up of cyber, military, and regional subject matter experts.

[4] Using colors to distinguish between cells is a norm in many gaming communities. In this case, readers should NOT equate one color or another with specific actors in the real world.

[5] We used U.S. department and agency titles to avoid confusion amongst players about the responsibilities and authorities of the various participants in cells. In the scenario and game play, these components of the fictional Blue States should not be equated with actual U.S. executive branch organizations.

Within each of the three moves participants played the game by submitting requests for government aid, offers of aid, or productions of media statements interacting with other cells through GameNet, a specialized computer software that facilitated all player actions and communications (see Appendices). A GameNet terminal was provided to each player. Players communicated with each other via email and chatrooms built to simulate the Energy-ISAC (Information Sharing and Analysis Center) and Financial Services-ISAC, also through GameNet.

In this wargame, the data underpinning later analysis was collected in three ways. First, each player cell included note takers who summarized conversations and dynamics within the cell. Second, all player actions taken via the GameNet terminals including chat, communications, and action forms were collected in a database. Third, after every move players completed a survey about the motivations behind their behaviors and perceptions of game play.

Game Scenario

The unclassified and hypothetical scenario developed for the wargame involved economic competition between two peer competitor states, and in which Red State was conducting a cyber campaign to gain economic leverage and expose vulnerabilities for potential use in a future conflict. This first move of the three game moves lasted 180 days (in game time); player actions in this move were meant to mirror day-to-day competition in a status quo political environment. The second and third moves represented the period before and the period after a pre-scripted political crisis in in which an ally of Blue State—Green State—held an election that Red State viewed as a significant national security priority. Both Move Two and Move Three were each 30 days long. Move Two was intended to capture activity by players leading up to the Green State election, and Move Three captured the fallout and follow on actions post-election.

Game play began with an initial array of Red State and Blue State cyber campaigns already occurring, in order to simulate the environment preceding forward defense actions. Most of these cyber capabilities focused on espionage, but presented the means to generate effects against leadership in both Blue State and Red State, as well as against critical infrastructure and military networks (see Appendix). Finally the game organizers explicitly gave Blue State and Red State "counter-cyber" capabilities.

During the three moves, predesigned "noise" cyber attacks from other non-state actors (not represented by players) were introduced. These noise cyber attacks included IP (intellectual property) theft, ransomware, as well as data exfiltration. These were meant to simulate the kinds of day–to-day cyber activity that businesses within the finance and energy sector experience from criminals, hacktivists, and less-capable state actors. The White Cell provided players with attribution for some of the cyber attacks, also making it hard to differentiate between state and noise attacks. In other cases certain players (private sector or government) had attribution for attacks but others did not.

Game Play Overview

Before delving into how Defend Forward manifested within the game in the next section, it is helpful to get a brief overview of what occurred in the game. The first move presented players with a scenario in which Red State was already conducting cyber campaigns against Blue State Government and Blue State's energy and finance sectors. These operations sought accesses to infrastructure, potentially for future kinetic military operations, or to obtain information about Blue State leadership in order to blackmail or influence Blue State leaders in case of a future need. Players in the Blue State Government Cell were given some strategic level information

about the intent behind the cyber campaigns while private sector players had the brunt of information about the characteristics of attacks on critical infrastructure.

In response to these opening conditions in Move One, private sector players focused on mitigating vulnerabilities and restoring business operations. Blue State Government responded with offensive cyber actions, initiated a series of cyber attacks into Red State's finance and energy infrastructure, and began information operations campaigns against both Red State and Green State decision-makers. Blue State Government also facilitated domestic intelligence sharing and prepared to support civilian authorities. Meanwhile, Red State focused on creative actions to influence the Green State election, restrained further attacks against Blue State critical infrastructure, and utilized other economic and political means towards its objectives.

In Move Two, Blue State Government increased its offensive cyber operations and cyber-enabled influence operations. This included operations to disrupt a prominent website known for sharing leaked government documents (which was sharing Red State fabricated anti-Blue State reports) and Green State-based public information outlets. Blue State Government also leveraged other diplomatic, economic, and military support incentives with Green State. The end of Move Two witnessed the backfiring of Red State's influence operations leading to the controversial election of a Blue State-friendly opposition candidate within Green State.

In Move Three Blue State Government reduced its offensive cyberspace operation, both at home and in Green State, but deployed cyber protection teams to support Green State and other regional allies. There were some limited Red State cyber attacks against Blue State critical infrastructure, but Red State refocused on diplomatic and economic outreach to Green State. Overall, there was a significant increase in tensions and state hostilities between Blue State and Red State in other domains.

III. Moving Forward with Defend Forward

Based on the game play data collected and post-game analysis, the CIPI-led game organizers have generated a small number of findings. The findings from this wargames are suggestive not definitive. At some later date, wargame iteration and other social science and operations research techniques may increase confidence in the insights below. In combination with data of the two previous NWC critical infrastructure games, research and analysis of many of these findings will continue in the coming years to contribute to the understanding of cyber operations and strategy, especially at the intersection of public-private interests and capabilities.

In the game, the Blue State Government played a Defend Forward strategy that focused on creating mutual vulnerabilities within critical infrastructure and then conducting offensive operations on these infrastructures in both allied and adversary nations to deter further escalation. Secondarily, the Blue State DoD took actions to increase the defensive capability of its allied partner and employed counter-cyber operations a final leg of their strategy. While this game cannot assess the effectiveness of this strategy against a real adversary, it does find that private sector players were sometimes frustrated with the way the Blue State Government players implemented the Defend Forward strategy. In surveys and plenary, players voiced concern about implications to global infrastructures and were frustrated about actions taken against Red State and Green State critical infrastructure in the game that could have had negative implications for consumer confidence and global markets. Meanwhile, players indicated that they had no clear way to request or advocate for counter-cyber operations that would degrade adversary capabilities to conduct cyber operations against their infrastructure.

The preceding discussion should not be read as a private sector critique of counter-cyber operations. Players consistently voiced support for counter-cyber operations throughout the game. This is an important distinction for the Blue State DoD because it delineates between operations taken (primarily within cyberspace) to degrade an adversary's ability to conduct cyber operations and operations undertaken to deter an adversary by holding the adversary's own critical infrastructure at risk. Players seemed to believe that counter-cyber operations could be less escalatory and less destabilizing than sometimes thought by policy analysts and scholars. Instead, they assume that the mutual vulnerability strategy of attacking critical infrastructure would create escalation dynamics that could be more harmful to national critical infrastructures than the attacks themselves. If the success of Defend Forward-like cyber strategies is based on its ability to degrade adversary abilities without escalating to thresholds of strategic or significant attacks, then practitioners should be conscious of how operations aimed specifically at creating mutual vulnerabilities within infrastructure might undermine the intent of forward defense approaches.

Recommendations

- Focus Defend Forward on counter-cyber operations and distinguish—both publicly and within the government—between operations meant to deter strategic cyber attacks versus those meant to degrade adversary cyber capability.
- Work with the private sector to determine measures of success for Defend Forward.
- Clearly define what activities fall under Defend Forward and work with the private sector to develop these and to circulate them for private sector awareness.

- Identify at what point (if any) Defend Forward transitions to crisis response and actions at a higher intensity of scope or potential violence.
- Government actors should take into to account for differences between infrastructures that are primarily domestic and those that are tied to global infrastructure.
- Game play suggests that the implications of actions taken to respond to cyber operations have greater repercussions for long-term critical infrastructures than the immediate effect of adversary cyber operations.
- Determine how, and if, all other government agencies support or are supported by Defend Forward like strategies and operations. In general, cyber strategies cannot be successful without full partnerships, but sometimes unclear to private sector players what part of the Blue State government was leading, in what circumstance, and how.
- To better implement Defend Forward like strategies and operations while taking account private sector stakeholder, governments should strengthen mechanisms for providing input on potential counter-cyber operations (both for and against).

IV. APPENDICES

Appendix A: Overview of Actors

All players were briefed the profiles for Blue State, Red State, and Green State, as well as other non-state actors, at the beginning of the war game and had access to the information throughout the game. That information, included in this appendix, was available to all players and represented a common, ground knowledge of the states. The private sector briefings are not included here, but are included separately in Appendix B

Privileged information, not available to all players, was also provide to the Red State and Blue State Government Cell and is available in Appendix C. The briefings also included maps, which were extremely abstracted to support game objectives.

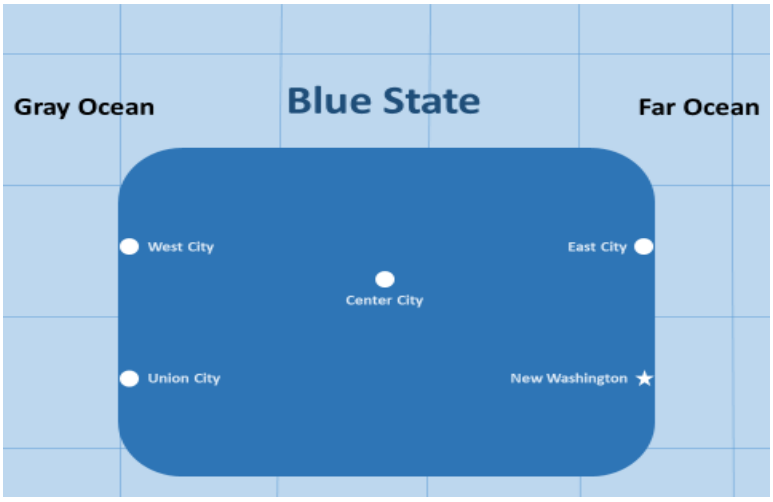
The information was primarily presented through briefing slides, but has been condensed here for ease of reference.

Appendix A.1: Blue State

This information represents all the common, ground knowledge on Blue State that all players had received. The section includes a general overview, as well as broad information, on the economy, military, and diplomatic aspects of the country. An abstracted map was also provided.

Blue State Overview

- **Notional state roughly modeled on the U.S.**
- **Government**
    - For purposes of game, identical to U.S. with comparable agencies, departments, and capabilities.
- **Overview**
    - Population of 330 million, with 80% living in urban areas
    - There are five major cities in Blue State
        - New Washington, Blue State capital
        - East City, largest city, a cultural and financial hub
        - New Union, a technology hub, called the "Silicon Coast"
        - West City, largest west coast city and a major port
        - Center City, largest non-coastal city and am industrial hub



Map of Blue State, including the 5 prominent cities.

Economy

- **Overview**
  - GDP of $19 trillion, with 3% growth rate
    - Growth rate is projected to remain steady barring any unforeseen shocks
  - Steady unemployment and consumer confidence
- **Diversified**
  - Sizable agricultural and energy sectors
  - Some advanced manufacturing, primarily capital goods and high-tech goods (such as ICT products)
    - Heavy, capital goods manufacturing in decline
  - Services account for roughly 75% of GDP
    - Blue State boasts the largest and most globally integrated financial services sector
- **Advanced Tech**
  - Educated workforce and premier educational institutions
  - Global leader in R&D, at 2.8% of GDP (>$500 billion)
  - Highly dependent on proprietary IP and data
    - Critical for high-tech manufacturing and service sectors
  - Reliant on imported components and hardware from Red State
- **Globally integrated**
  - Exports of goods and services account for 13% of GDP
  - Red State is Blue State's largest trade partner
  - Reliant on global supply chains
    - Large portion of Blue State supply chains are in Red State

Diplomacy

- **Overview**
  - A global leader, playing a prominent role in range of organizations and diplomatic efforts
  - Large, experienced diplomatic corps

    - Maintains sizable diplomatic missions in most countries
    - Supports a wide range of humanitarian, human rights, and civil society programs and organizations
- **International Organizations**
    - Permanent member of the United Nations Security Council
    - Largest shareholder and veto holder in the World Bank
    - Member of the World Trade Organization

Military

- **Global military power**
    - Advanced blue-water navy
    - Air force comprised of primarily 5th-generation aircraft
    - Moderately sized, well trained and equipped land forces
    - Well-developed special operations capabilities
- **Strategic nuclear capabilities**
    - Fully developed nuclear triad with secure second strike
- **Extensive presence in Gray Ocean under GRAYCOM**
- **Cyber capabilities**
    - Highly developed offensive capability
    - Mission ready cyber defensive teams

Major Cities in Blue State

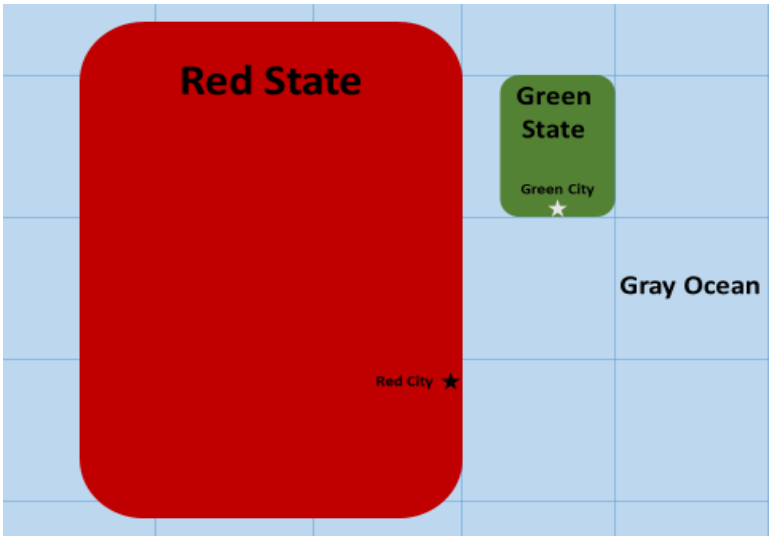
- **New Washington**
    - Capital of Blue State and seat of government
    - East coast city with a population of 2 million people
- **East City**
    - East coast city with a population of 9 million people
    - Largest city in Blue State, by population
    - Home to most major Blue State financial institutions
    - Extremely capable city services
- **Union City**
    - West coast city with a population of 1.5 million people
    - The current center of high-tech industry and innovation in Blue State, sometimes called the “Silicon Coast”
- **West City**
    - Largest city on the west coast, and third largest in Blue State, with a population of 4 million people
    - Largest port in Blue State and primary access to the Grey Ocean
- **Center City**
    - Second largest city in Blue State, by population
    - Located in the Blue State heartland with a population of 3 million people
    - Home to many financial institutions and one of the few major manufacturing hubs in Blue State

Appendix A.2: Red State

This information represents all the common, ground knowledge on Red State that all players had received. The section includes a general overview, as well as broad information, on the economy, military, and diplomatic aspects of the country. The Red State briefing also included an overview of the Red State domestic political situation. An abstracted map was also provided.

Government

- Semi-authoritarian, classified as Unfree by Freedom House
  - prioritizes stability over individual freedom
- Highly centralized with a strong president and loyal leadership cadre
- Rampant, state institutionalized corruption
- Elections are held, but serve as a propaganda tool with little political opposition



Map of Red State and Green State.

Economy

- **Overview**
  - GDP of $12 trillion, with 5% growth rate
  - Extraordinary efforts taken to maintain growth and stability
- **Rapidly developing economy**
  - Transitioning from agriculture and heavy industry to IP intensive, high-tech manufacturing, and services
  - Substantial foreign investment
  - Massive state investments in infrastructure and R&D
  - Agriculture and manufacturing still significant share of GDP
- **Large manufacturing sector**
  - Global leader in hardware and component manufacturing
  - Deeply integrated into global supply chains
- **Export driven economy**

    - Red State's domestic market is emerging, but there is still insufficient domestic demand to support economic growth
        - Exports of over $2 trillion
        - Blue State is Red State's largest trade partner and largest export market
    - Reliant on shipping through the Gray Ocean
- **Government intervention in the private sector**
    - Government pressure on the domestic financial services sector to support strategic industries and specific firms
    - Creation of "state champion" firms
        - Leverages favorable policies, trade barriers, and investments
        - Believed to provide government support through espionage
- **Corruption and crime**
    - Corruption is a reality at every level of government through complex patronage systems that goes up to the President
    - Large firms pay a "tax" for protection and intelligence, as well as opportunities domestically and abroad
    - Government indirectly and directly supporting organized crime and black markets domestically and abroad

Military

- **Rising global power**
- **Strong conventional capabilities**
    - Large mixed capability green/blue water navy
    - Mix of 5th and 4th-generation aircraft
    - Large army and special operations forces
    - Heavy use of military contractors
- **Strong defensive capabilities**
    - Military posture focused on regional defense
    - Advanced air and maritime defense systems
- **Diverse nuclear capabilities**
- **limited ability to project power globally**
- **Cyber Capabilities:**
    - Large focus on cyber capabilities in military, special forces, and intelligence
    - Primarily uses cyber operations in peacetime for:
        - Pre-staging accesses/exploits for later use in crisis
        - General situational awareness intelligence
        - Intellectual-property theft
    - For game purposes, assume both offensive and defensive cyber capabilities
        - Known successes with infiltrating supply chains, unconventional accesses, and large scale data breaches
        - Does not typically use cyber-enabled information operations

Domestic Politics

- **Public unrest**

    - Public pressure to maintain economic growth
    - Growing discontent with widespread corruption
        - Some civil society activists and organizations have come out against the government corruption
        - Some government crackdowns and limited media converge (state friendly media firms)
- **Broad support for "Red State rising" narrative**
    - Desire to protect and expand Red State's influence
    - Hostility towards those perceived as undermining or blocking this rise
    - Perceptions of Blue State hostility to Red State ambitions
- **Rise of domestic ultra-nationalist groups**
    - Rapidly growing
    - Open contempt and hostility towards those viewed as thwarting Red State's assent (i.e. Blue State)
    - Groups calling for more forceful Red State actions to secure and protect state interests
    - Putting pressure on leadership

Appendix A.3: Green State

This information represents all the common, ground knowledge on Green State that all players had received. Green State was run by the White Cell and had no players. However, it played a significant role in the scenario and crisis, and was briefed as part of the Scenario Overview. In particular, the elections in Green State (information included below) was crucial to scenario.

Overview

- **Large island country off the coast of Red State**
- **Government**
    - Democratic, classified as Free by Freedom House
- **Bilateral treaty ally of Blue State**
    - Mutual security agreement
    - Extensive free trade agreements
- **Within Red State's geographic area of interest**
    - Red State considers Green State's close relationship with Blue State to be national security risk
    - Red State has made efforts, diplomatic and economic, to draw Green State closer
    - Shares a common language with Red State
- **Current governing party is friendly to Red State**
- **Ruling party's government viewed as corrupt**
    - Population has favorable view of Blue State
- **Ruling party is more engaged with Red State, despite public preferences**
    - Has implemented policies and passed laws that favor Red State businesses and interests
    - This extends to the Green State civil servants and military

Economy

- **Overview**
    - GDP of $600 billion, with average growth of 4%
    - Extremely digitally reliant economy and population
    - Engaged in high-tech manufacturing and services
        - Substantial financial services sector
    - Largest trade partner is Red State, but the second largest is Blue State
    - Red State is currently the largest source FDI

Military

- **Overview**
    - Small elite force, uses Blue State military hardware
        - Military forces focused on defending the homeland
    - Non-nuclear state

Green State Elections

- Green State is preparing to hold highly contested national elections
    - Elections are slated to be held in 210 days
- A Pro-Blue nationalist party is expected to win and remove the current governing party
- Red State Foreign Ministry spokesperson:
    - "The provocative and sensationalist Green State opposition party will destabilize the region and bring hardship on the Green State. We hope that the Green State people make a wise decision in the elections…"

Green State Political Overview

- **Deference to Red State**
    - The current ruling party in Green State has been seen as too accommodating to Red State
    - It has implemented numerous economic and diplomatic policies that favored Red State firms and interests
- **Rising corruption and crime**
    - Green State has been rocked by a series of national corruption scandals, many related to Red State firms
    - There has been a marked increase in crime across Green State, believed to be tied to organized crime
    - The Green State public is blaming their leaders and Red State for the corruption and crime

Appendix A.4: Non-State Actors

The non-state actors profile was intended to provide context to the "noise" cyber attacks that players would be subjected to throughout the game.

Non-state Actors

- Wide range of cyber capabilities
- Ranges from lone actors to large organizations
    - Could be supported by or working for a state actor
- Motivated by ideology or profit, or just as likely, boredom and reputation
- Example of non-state actor actions and campaigns
    - Accessing sensitive networks to sell access or for fame
    - Stealing sensitive information or data to sell
    - DDoS attacks and web defacements for fun, for hire, or for ideological purposes
    - Deploying malware, such as ransomware, for profit
    - Developing tools to support other malicious actors

Appendix B: Overview of Private Sector Critical Infrastructure Firms

Two critical infrastructures sectors were played in the game, the Financial Services Sector and the Electricity Subsector. Players where given an overview of the private sector firms in the initial briefing along with the states.

That information, included in this appendix, was available to all players and represented a common, ground knowledge of the private sector critical infrastructure firms. All players had access to the information throughout the game. The briefings also included maps, which were extremely abstracted to support game objectives.

The information was primarily presented through briefing slides, but has been condensed here for ease of reference.

Appendix B.1: Financial Services Sector Firm

Players in the Financial Services Sector Cell were assigned to one of four identical firms (numbered 1 thru 4). This Appendix includes information for Finance 1, which was identical to the other three firms, Finance 2, etc.

Overview

Finance 1 is a publicly traded, Fortune 100 banking and financial services company, and 1 of the 4 largest financial services companies in Blue State.

- Headquartered in East City, Blue State
- Finance 1 operations are geographically dispersed
- Over 200,000 employees across Blue and globally
- ~$100 Billion revenue, ~$33 Billion net income
- Structured around four core lines of business
- Operates a hybrid IT infrastructure strategy

Lines of Business (LoB)

Finance 1 offers services domestically and globally, divided into four lines of business:

- Consumer and community banking
- Commercial banking
- Corporate and Investment Banking
- Asset and wealth management

  Corporate, investment banking and asset/wealth management have extensive global activity particularly in Red State's developing economy.

Infrastructure and IT Overview

Finance 1 has a hybrid IT infrastructure strategy, utilizing public (external) and private (internal) cloud systems, and legacy systems.

- **Public cloud system**
  - Managed by Tongass Web Services (TWS), recognized as a leader in cloud services
  - Provides some security services, on call 24/7
  - Hosts a range of less sensitive data and applications
- **Private cloud system**
  - Managed internally by Finance 1
  - Hosts data, applications, and processes too important or sensitive to host on public cloud systems
- **Legacy IT system**
  - Support functions and operations that have not (yet) been moved to the cloud for practical, security, technical, and/or cost reasons, this includes some complex core applications
- **Geographic dispersion and IT hubs**
  - Servers and other physical IT infrastructure are dispersed across the Blue State in centralized hubs
  - IT infrastructure hubs are generally geographically co-located with the business hub they support
  - Primarily reliant on ground based (cable) transmission methods, satellite backups for intercontinental transmissions

IT Processes Overview

Finance 1 has implemented controls in line with, or surpassing, industry standards

- **Data and system classifications**
  - Data, applications, and systems are identified by their criticality to Finance 1 operations, they are: routine, moderate, high, or vital
  - This determines a security requirements, this enforced across internally and externally (with contractors)
- **Access security and encryption**
  - All data is encrypted in line with its classification
  - Processes for handling and transmitting of data is determined by classification

Contractors and external venders

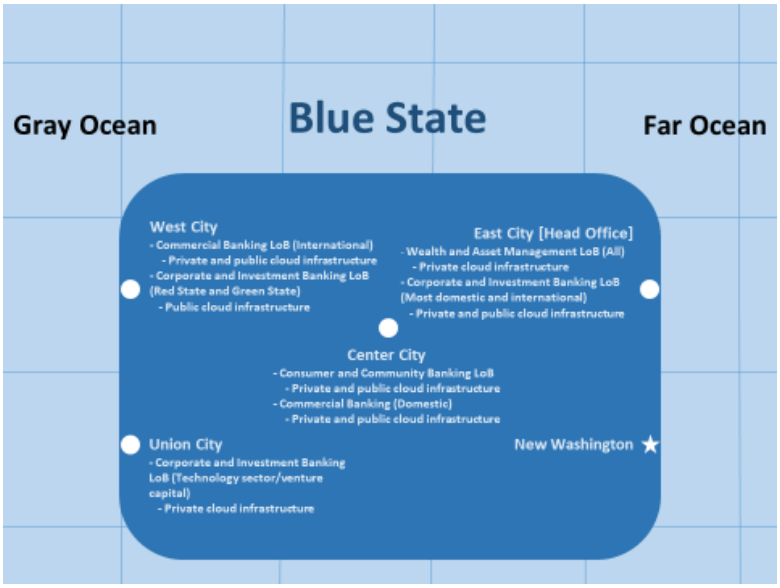
- **Payments Clearing Services (BPCS)**
  - 3rd party firm that processes payments across the financial services sector
  - Used by all major Blue State banks, interfaces with foreign payment processing firms (including in Red State)
- **Tongass Web Services (TWS)**
  - Largest cloud services company in Blue State
  - Based in Union City
- **Decker Cybersecurity**

- External, private cybersecurity firm specializing in financial institutions, widely used across the financial services sector
- On call 24/7 to support cyber incident response and mitigation

LoB and Cloud Services

- **IT Networks**
  - Divided between public and private cloud infrastructure
    - Private cloud infrastructure based in East City
    - Public cloud services provided by TWS in East City
- **Asset and wealth management**
  - Includes both international and domestic operations
  - Hosted primarily on private cloud infrastructure
    - Physical infrastructure based in East City
    - Interfaces with international offices
- **Consumer and community banking**
  - Divided between public and private cloud infrastructure
    - Private cloud infrastructure based in Center City
    - Public cloud services provided by TWS in Center City
- **Commercial banking**
  - Domestic commercial banking LoB divided between public and private cloud infrastructure
    - Private cloud infrastructure based in Center City
    - Public cloud services provided by TWS in Center City
  - International commercial banking LoB primarily public cloud
    - Public cloud services provided by TWS in West City
    - Interfaces with international offices
- **Corporate and Investment Banking**
  - For international and some domestic operations EXCLUDING Red State and Green State
    - Divided between public and private cloud infrastructure
      - Private cloud infrastructure based in East City
      - Public cloud services provided by TWS in East City
  - For Red State and Green State operations
    - Public cloud services provided by TWS in East City
  - Specialized services for technology companies in Union City uses private cloud
    - Private cloud infrastructure based in Union City, shared with financial technology R&D

IT and Infrastructure Geography



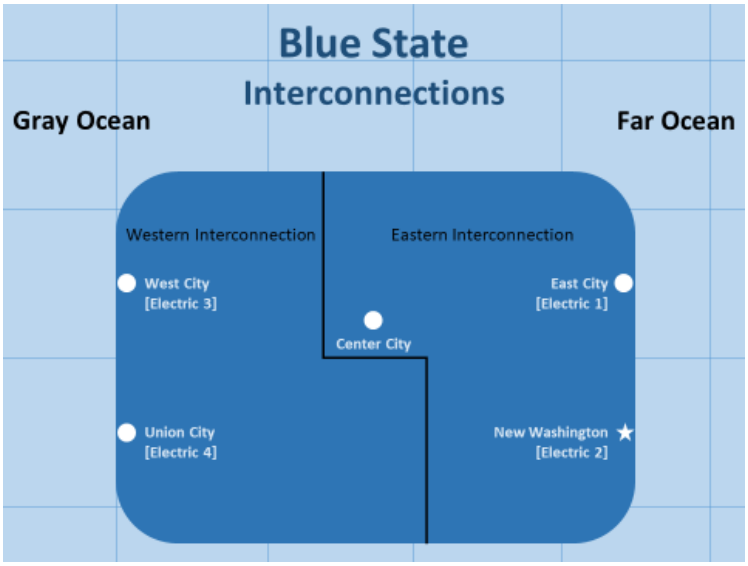
Map of Blue State with Financial Services hubs

- **East City**
  - Executive officers and operations HQ for Finance 1
  - Primary hub for Wealth and Asset Management LoB
  - Primary hub for domestic Corporate and Investment Banking LoB
  - Contractors
    - TWS offices and cloud infrastructure for local LoBs
    - Payments Clearing Services primary offices
- **New Washington**
  - Offices for government engagement
- **Center City**
  - Primary hub for Consumer and Community Banking LoB
  - Primary hub for Commercial Banking LoB, particularly for domestic operations and midsize industrial ventures
  - Contractors
    - TWS offices and cloud infrastructure for local LoBs
- **West City**
  - Central offices for Red State and Green State business
  - Large hub for Commercial Banking and Corporate and Investment banking in Red State and Green State
  - Contractors
    - TWS offices and cloud infrastructure for local LoBs
- **Union City**
  - Primary center for FinTech R&D
  - Investment and Corporate Banking officer servicing Union City, primarily engaged in venture capital
  - Contractors
    - Tongass Web Services central offices and primary infrastructure for the west coast

        - Decker Cybersecurity primary offices
- **Green City**
    - Head office for Green State operations
    - Majority of data on Green State citizens localized
- **Red City**
    - Head office for Red State operations
    - All data on Red State citizens localized
        - Heavy restrictions on what data pertaining to Red State firms can be gathered, stored, or transported abroad

Appendix B.2: Electricity Subsector Utility

Players in the Electricity Subsector Cell were assigned to one of four electric utilities. While the electric utilities were extremely similar, they were differentiated slightly by necessity, each serving a different major metropolitan area (and in a different intersections) within Blue State. This appendix includes information on the Electrical 1. The other electrical utilities were also in either the Eastern or Western Interconnect. Each utility also served a different one of the major cities identified in the Blue State profile (West City, Union City, etc.) as identified in the player map. All four utilities were large and varied only slightly in size (in terms of customers, generation, and service area) based on the size of the city they served.



Map of Blue State identifying which city and in which interconnection each utility operated.

Overview

Electric 1 is a vertically integrated generation, transmission, and distribution, Investor-Owned Utility (IOU). Electric 1 is also the primary electrical utility for East City.

- Headquartered in East City, Blue State
- Part of the Eastern Interconnection
- Services over 11 million end user customers in East City and the East Coast region
- Service territory of roughly 100,000 square miles

- One of the largest electric utilities by capacity

Generation

- Generating capacity of 35,500 MW
- Operates 88 generating plants
- Diverse generation mix

Source	Percentage
Coal	27%
Natural gas	31%
Nuclear	20%
Hydroelectric	15%
Wind and solar	2%
Other	5%

Transmission and Distribution

- Primary distributor to East City, the largest city on the east coast
- Operates 240 transmission substations
- Operates 1015 distribution stations
- Overview of transmission lines (by kV)

Transmission lines by kV	
HVDC	0
500kV	16
345kV	145
230kV	15
138 kV	202
115kV	31
<100 kV subtransmission	177

IT Network Overview

Electric 1 operates two sets of networks, a business network and OT networks

- **Business network**
  - Hosts internal business processes and data
  - Contains outward, customer facing, applications
- **Operations networks**
  - Separate networks that control and monitor various aspects of Electric 1's operations
    - Generation control and monitoring network
    - Transmission control and monitoring network
    - Distribution control and monitoring network

    - These wide-area networks connect to local networks at generating stations and substations

IT Contractors and Personnel Overview

- **Electric 1 cybersecurity personnel**
    - Cybersecurity teams, including a 24/7 SOC
    - Security audit teams
    - Incident response teams
- **Contractors**
    - Arclight Security
        - External, private cybersecurity firm specializing in electrical utilities, used across the electrical subsector
        - On call 24/7 to support cyber incident response and mitigation

Appendix C: Private Information Provided to Players

The majority of player information was in the initial briefing and was public, common knowledge. However, both Red State Cell and Blue State Government Cell received private, specific information. This information included information regarding ongoing cyberspace operations and other military capabilities, assets, and operations.

The information was primarily presented through briefing slides, but has been condensed here for ease of reference.

Appendix C.1: Blue State Government Cell Briefing

The Blue State Government Cell received information on suspected Red State activities in Green State and information on their cyber capabilities. Additionally, they received a list of ongoing operations against Red State. These cyberspace operations are highly abstract and non-technical, derived entirely from unclassified, open source research.

Red State Activities in Green State

- **Organized crime**
  - Organized crime is prolific in Green State
  - Active in money laundering, smuggling, and trafficking
  - Believed to serve as a liaison and support for Red State's Green State government allies and other interests
  - Widely believed to have ties to Red State (an open secret)
- **Corporate partners**
  - Large Red State corporate presence in Green State, supports pro-Red State interests and political candidates

Cyber Capabilities

- **Offensive and defensive capable**
  - Standalone and integrated offensive cyber capability
    - Can be utilized in conjunction with or independently of military operations
    - Integrated into military operations
  - Integrated defensive cyber capability
    - Cyber defensive operations are routine
    - Integrated into military operations
    - Capability to protect and support select civilian networks

Defensive Cyber Capabilities

- **Managed by a range of Blue State Government departments and agencies**
  - Department of Homeland Security (DHS)
  - Department of Energy (DOE)
  - Department of the Treasury (DOT)

- Department of Defense (DOD)
- Department of Justice/FBI (DOJ/FBI)

- **Blue State Cyber Campaigns (vs. Red State)**

#	Target	Effect	Covert	Duration	Utility
Alpha	Classified networks of the Red State Foreign Ministry	Espionage	Yes, moderate probability of detection, moderate probability of attribution	Until detected	High quality source for Intelligence on Red State intent and diplomatic activities, leverage to potentially gain access to other networks
Beta	Unclassified networks of Red State Office of the President	Espionage	Yes, moderate probability of detection, low probability of attribution	Until detected	Source for Intelligence, potentially including leadership intent and personal activities, potential to leverage information for information operations and/or blackmail
Charlie	Unclassified networks of the Red State Military Logistics Agency, which manages military lift and logistics for Red State forces	Espionage, degrade or disrupt	Yes, low probability of detection, moderate probability of attribution	Until detected	High quality source for Intelligence on Red State military activity and force movements, leverage to potentially gain access to other networks (including military and civilian logistics elements), use to disrupt or degrade military logistics,
Delta	Classified command and control networks of Red State Navy	Espionage, degrade or disrupt	Yes, high probability of detection, moderate probability of attribution	Until detected	High quality source for Intelligence on Red State naval activity, leverage to potentially gain access to other military networks, use to disrupt naval operations and degrade trust in networks/C2
Echo	Red State electrical critical infrastructure, primarily for generation that serves areas with military installations	Degrade or disrupt, potentially destroy	Yes, low probability of detection, low probability of attribution	Until detected	Ability to delay or disrupt Red State force mobilization by disrupting power generation to military installations, will impact civilians, potential unintended cascading effects
Foxtrot	Classified networks for Red State's Intelligence Services, Cyber Operations Command Element	Espionage, degrade or disrupt	Yes, high probability of detection, high probability of attribution	Until detected	High quality source for Intelligence on Red State cyber operations, leverage to potentially disrupt Red State cyber operations

Appendix C.2: Red State Cell Briefing

Red State players received objectives and considerations from a national command authority (NCA) as part of their briefing. Additionally, they received information on their cyber capabilities and list of ongoing operations against Blue State and Green State. These cyberspace operations are highly abstract and non-technical, derived entirely from unclassified, open source research.

Objectives

NCA has authorized the use of all reasonable [loosely defined] means to achieve objectives, within specified limitations

1. **Maintain internal stability and regime survival**
   - Manage and/or placate ultra-nationalist elements
   - Prevent and, if necessary, suppress domestic unrest
2. **Maintain economic stability and growth**
   - Protect domestic businesses
   - Develop and secure access to markets and resources
   - Facilitate economic espionage, IP and data theft
3. **Maintain and expand influence over Green State**
   - Prevent a change in Green State leadership that would undermining Red State interests in the country
   - Prevent closer ties between Green State and Blue State, and as possible, disrupt the existing relationship
4. **Collect intelligence on Blue State**
   - Develop and maintain means to understand and influence Blue State decision-making

Constraints

NCA has specified these constraints on actions

1. **Avoid direct armed conflict with Blue State or actions that will clearly result in armed conflict**
   - Provocative actions are acceptable, and potentially necessary, to achieve objectives
   - If Blue State initiates armed conflict, further guidance will be given
2. **Avoid embarrassment of Red State or Red State leadership**
   - Take actions and precautions to prevent or disrupt the spread of disparaging information

Red State activities in Green State

- **Organized crime**
  - Organized crime tied to Red State is prolific in Green State
  - Active in money laundering, smuggling, and trafficking
  - Serves as a liaison and support for Green State government allies and other interests

    - Widely believed to have ties to Red State (an open secret)
- **Corporate partners**
    - Large Red State corporate presence in Green State, supports pro-Red State interests and political candidates
- **Special operations forces**
    - Small, persistent special forces presence in Green State
        - Green State is NOT aware of their presence
        - Supported by friendly organized crime

Cyber Capabilities

Large focus on cyber capabilities in military, special forces, and intelligence

- **Large focus on cyber capabilities in military, special forces, and intelligence**
    - Works across government and with select firms
- **Current operational usage includes:**
    - Pre-staging accesses/exploits for later use in crisis
    - General intelligence
    - Intellectual-property theft
- **Well-developed offensive and defensive cyber capabilities**
    - Operates effectively independent of military operations
    - Untested ability to use cyber operations conjunction with military operations
    - Ability to support and protect select civilian networks

Red State Cyber Campaigns (vs. Blue State)

#	Target	Effect	Covert	Duration	Utility
R01	Unclassified DOD/OSD networks	Espionage	Yes, high probability of detection, moderate probability of attribution	Until detected	High quality source for Intelligence on Blue State intent and strategy, leverage to potentially gain access to other networks
R02	OPM databases	Espionage, gained information on individuals for follow on actions	Yes, moderate probability of detection, moderate probability of attribution	Until detected, data already stolen	Access person data that can be used for targeting, to facilitate other attacks (social engineering, spear phishing, etc.), and for blackmail/asset recruitment
R03	Office of the Trade Rep. networks	Espionage	Yes, moderate probability of detection, low probability of attribution	Until detected	High quality source for Intelligence on Blue State economic activities, negotiations, and strategy, leverage to potentially gain access to other networks
R04	Unclassified networks of the Executive Office of the President	Espionage, degrade or disrupt	Yes, high probability of detection, low	Until detected	High quality source for Intelligence on Blue State leadership intent, potentially

			probability of attribution		leverage for information operation and/or political blackmail
R05	Classified networks of GRAYCOM (Gray Ocean AoR GCC)	Espionage, degrade or disrupt	Yes, high probability of detection, moderate probability of attribution	Until detected	Exquisite source for Intelligence on Blue State current and future operation in the Gray Ocean AOR, potentially leverage to degrade or disrupt Blue State operations in theater
R06	Classified networks of Blue Systems Engineering (BSA), developer of the Advanced Combat Fighter system	Supply chain attack, espionage	Yes, low probability of detection, high probability of attribution	Until detected/supply chain attack executed	Intelligence on Advanced Combat Fighter system, introduced a critical vulnerability into an essential hardware component, the component has been integrated into the aircraft. It's effectiveness is unknown
R07	Business operations/engineering IT networks of electrical utilities	Espionage	Yes, low probability of detection, moderate probability of attribution	Until detected	Intelligence on the functionality and architecture of the electrical infrastructure, including OT networks, SCADA, and physical machinery of electricity generation and transmission systems
R08	Electrical utilities' OT networks and SCADA of power generation for areas near Blue State bases	Degrade or disrupt, potentially destroy	Yes, low probability of detection, moderate probability of attribution	Until detected or activated, duration of effects variable but estimated to be days to weeks depending on mitigating factors	Potential to degrade, disrupt, or, potentially, destroy power generating capacity in critical power stations. Degrading or disrupting electrical generation is reversible, but may require substantial downtime depending on the severity. Destruction is non-reversible
R09	Electrical utilities' OT networks for transmission infrastructure	Degrade or disrupt, potentially destroy	Yes, moderate probability of detection, low probability of attribution	Until detected or activated, duration of effects variable but estimated to be days depending on mitigating factors	Potential to degrade, disrupt, or, potentially, destroy power transmission, with the potential to cause widespread power loss and potential cascading effect. Degrading or disrupting transmission infrastructure is reversible, but may require substantial downtime depending on the severity. Destruction is non-reversible
R10	Financial services FinTech R&D cloud	Espionage	Yes, high probability of detection, low probability of attribution	Until detected	Economic espionage, stolen technology can either be given to domestic firms or exploited to develop further attacks

R11	Financial services firm Customers Database (for Blue citizens)	Espionage, gained information on individuals for follow on actions	Yes, low probability of detection, low probability of attribution	Until detected, data already stolen	Access person data that can be used for information operation, intel collection targeting, to facilitate other attacks (social engineering, spear phishing, etc.), and for blackmail/asset recruitment
R12	Financial services firm Customers Database (for Green citizens)	Espionage, gained information on individuals for follow on actions	Yes, low probability of detection, low probability of attribution	Until detected, data already stolen	Access person data that can be used for information operation, intel collection targeting, to facilitate other attacks (social engineering, spear phishing, etc.), and for blackmail/asset recruitment
R13	Green State opposition leadership	Espionage	Yes, moderate probability of detection, low probability of attribution	Until detected	High quality source for Intelligence on Green State opposition intent, election strategy, potentially leverage for information operation and/or political blackmail
R14	Green State Ministry of Defense	Espionage	Yes, moderate probability of detection, low probability of attribution	Until detected	High quality source for Intelligence on Green State intent and strategy, leverage to potentially gain access to other networks

Appendix D: Player Actions

All players had the same core mechanisms to communicate and take actions within the wargame utilizing a digital wargaming tool. Player had the ability to take actions, send communications, and issue press releases. The majority of actions required text responses. The only variation was the private sector players had a Request Government Aid option, the Blue State Government Cell had a Respond to Request for Government Aid option, and the Red Cell had neither. Additionally, the use of a chat faction varied slightly for the private sector players.

Actions

Players took specific actions in the form of issuing orders (through a digital form) to their subordinates. This allowed players to remain at the strategic level and leave minute details to their staff.

When players took actions they had to describe the entity or component executing the action. This might be a legal staff, public relations office, or an IT services for the Private Sector. Because the Blue State Government Cell was subdivided by department and agency it varied greatly. For example, the Blue State DoD may have directed its Navy to take an action.

Players then described what the action was, broadly how it would be accomplished, and why they were taking that action. For example, “we are using X capability to do Y for Z reasons.” Finally, player specified what they perceived the ideal and worst outcomes of the action to be.

Communications

All players had the ability to send messages to any other groups through the communications function. There messages appeared roughly as emails, and were routed from one group to another group. For example, a player in Finance 1 (one of the four financial services companies) could send a message to Electric 3. Electric 3 (and all the players in that utility) would receive a communication from Finance 1. Players could not use communications to directly message another player.

If players sent messages to recipients not represented by any players (such a Green State) responses would be managed by the White Cell.

Press Release

The players could create press releases, official statements from the player's organization. These press releases would be viewable by all players. Additionally, the press statements potentially affected game play in other ways, depending on how the public (played by the White Cell) responded to the statements.

Chat Function

Players could also communicate within one of two chatrooms, the FS-ISAC and the E-ISAC. These chatrooms were meant to very roughly simulate the mechanisms of coordination and information sharing of those organization. Only the Financial Services Sector Cell and DHS players were in the FS-ISAC and only the Electricity Subsector Cell; and DHS players were in the E-ISAC. Players, through actions, could establish other chatrooms to simulate other coordination and information sharing entities.

Request for Government Aid

Private Sector Cell players could formally request support from agencies and departments in the Blue State Government Cell. Players had to specify what form of support they were requesting:

- Cyber Defense
- Cyber Forensics
- Cyber Remediation
- Counter Cyber Actions
- Emergency Management
- Domestic Policy Creation
- Foreign Policy Actions

Players also had to specify why they were requesting specific government aid and the objective of that aid. They had to provide what they perceived as a best case outcome and a worse case outcome of that aid.

The request would be passed to the relevant government body as indicated by the player, which would then decide how to proceed. Any repose the government would take would have to be

submitted as a separate action. For example, Electric 1 requests emergency management from DHS. DHS then would have to take an Action (see above) saying they were providing emergency management support for Finance 1, otherwise nothing would happen.

Respond to Request for Government Aid

Blue State Government Cell players could respond to Request for Government Aid. This functioned similarly to a traditional communication. However, responses would be delivered to a separate tab for private sector players, differentiating it from other communications. However, even if Blue State Government responded, they would have to take an action to generate the aid requested. Thus Blue State Government players could respond, but fail to actually take the corresponding actions.