THE BLUE BOOK PROJECT: LESSONS LEARNED FROM PHASE 2

BACKGROUND

In an era of escalating geopolitical tensions and advanced cybersecurity threats from foreign adversaries, safeguarding critical infrastructure has become a paramount concern for national security. In recent years, cyber threats and attacks against the United States have become more frequent, coordinated, and severe. Foreign adversaries are increasingly targeting and exploiting US critical infrastructure through network and supply chain vulnerabilities. These attacks most often result in financial loss and the theft of data and intellectual property, but cyberattacks can also physically damage critical infrastructure—potentially causing severe, long-term disruptions in services.

In fiscal year (FY) 2023, the Virginia Department of Emergency Management (VDEM) was awarded Regional Catastrophic Grant Program funding to develop a plan for responding to a cyberattack of national significance on its critical infrastructure. In response, the VDEM team initiated the "Blue Book Project."[1] The goal of the Blue Book Project is to ensure the Commonwealth is best positioned to manage the consequences of a sophisticated nation-state cyberattack on critical infrastructure. Through this effort, the Commonwealth seeks to establish and organize opportunities to support critical infrastructure partners during attacks, ensure residents' basic needs are met, and ensure the military can protect the homeland and project forces globally while systems are disrupted. This threat is not unique to Virginia. Critical infrastructure across the nation is vulnerable to exploitation by sophisticated adversaries, potentially resulting in significant consequences to communities and residents. Although some of the Blue Book Project's activities may be specific to its risk profile, many of its methods can be replicated by other states, regions, counties, or cities looking to implement a similar planning process. To this end, this white paper highlights the outcomes and lessons learned from executing Phase 2: Intelligence Assessment.

[1] For more background on this project, please see the project charter, the project overview, and lessons learned from Phase 1, which can be downloaded from the VDEM Blue Book Project webpage.

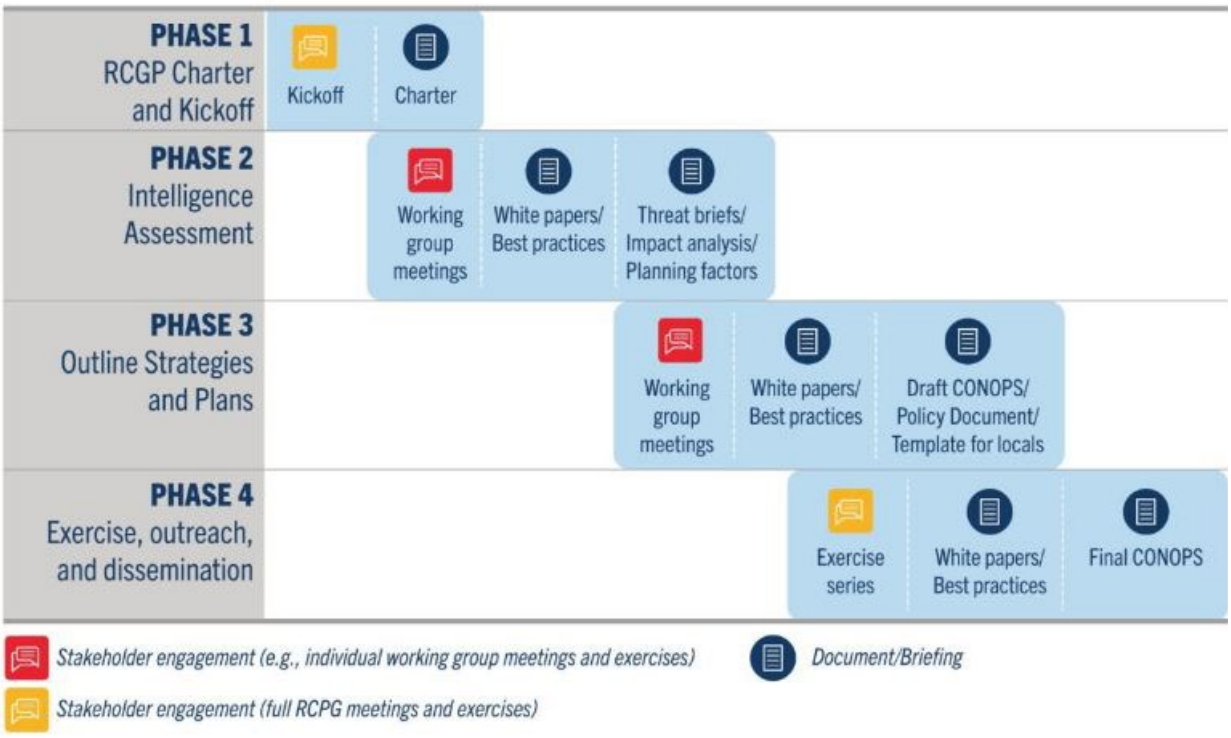

Figure 1: Blue Book Project timeline

PHRASE TWO OVERVIEW

During Phase Two, the project team emphasized cross-sector and intra-agency collaboration through a series of working group meetings designed to foster intelligence sharing, scenario development, and operational planning—establishing a foundation for Phase 3 deliverables. As a major focus of the Phase Two working group meetings, participants identified and discussed the impacts and consequences of a cyberattack on critical infrastructure, as well as the consequence management activities that will be necessary to respond. Table 1 provides definitions of key terms used in the Blue Book and by the working group.

Table 1. Blue Book terms and definitions

Terms	Definition
Impacts	The significant or major effects of a targeted attack
Consequences	The situations or challenges resulting from an impact
Consequence management activities	Public sector activities employed to meet the immediate and ongoing needs of the affected community and stabilize the affected community lifelines

Working Group Meetings

The working group meetings in Phase Two facilitated focused discussions among experts from various sectors and communities—each contributing unique insights and perspectives to the project. In addition to facilitated discussions, these sessions incorporated collaborative tools to enable participants to explore critical aspects of vulnerabilities to cyberattacks and the impacts and consequences following a cyberattack on critical infrastructure.

Figure 1 depicts how the five working groups functioned along parallel lines of effort that allowed the planning team to capture the information that each working group was best positioned to provide (i.e., the impacts, consequences, or resource needs following a cyberattack). The outcomes of these working groups will contribute to the development of the concept of operations (CONOPS), described in further detail in the following subsections.

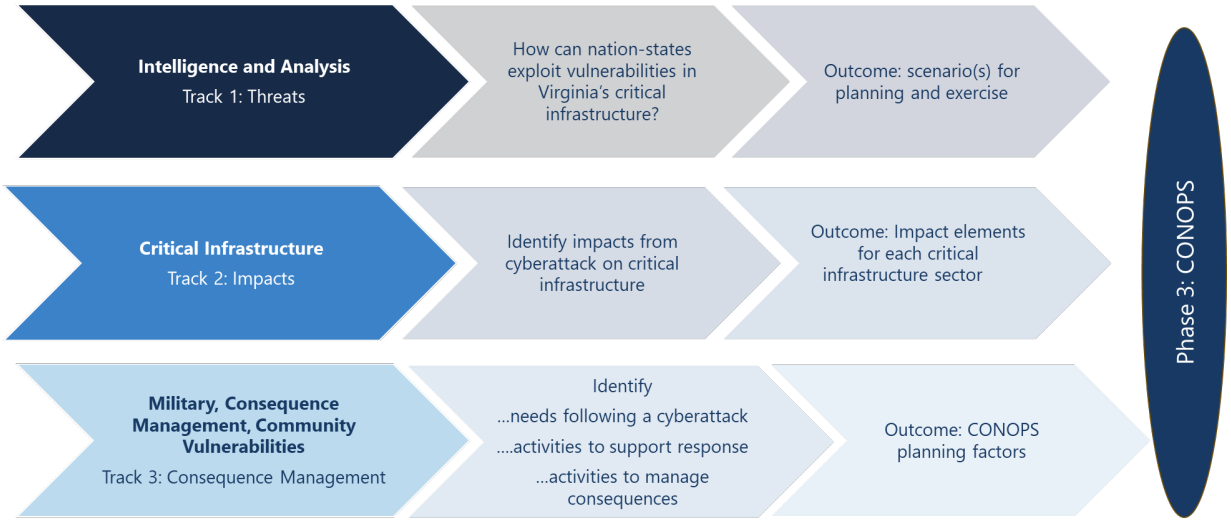

Figure 2: Working group parallel lines of effort

Analysis of Threats, Impacts, Consequences, and Resource Needs

Following the working group meetings, the planning team compiled the data and insights collected from the working groups and analyzed and categorized the findings. These efforts resulted in a consolidated list of vulnerabilities (Table 2) and potential impacts, anticipated consequences, and predicted resource needs (Table 3).

Table 2. Most consequential target sector vulnerabilities, as identified by the working groups

Target Sector	Vulnerability Scenarios
Energy	• An insider threat, or a person recruited by a nation-state actor, is coerced to upload malware to the energy grid. • An attack targets essential grid reliability services from out-of-service generators.

	• A coordinated disruptive cyberattack targets power generation facilities and the "black start" sites supporting them.
Water Systems	• A cyberattack on water treatment plan system operations alters chemical levels and is compounded by a misinformation campaign to undermine public trust in the water supply. • An attack compromises water dam SCADA (Supervisory Control and Data Acquisition) systems leading to the flooding of adjacent municipal centers. • Hacking and disruption of industrial control systems halt the delivery of fresh water to consumers.
Communications	• A cyberattack damages major telecommunication hubs in urban areas such as Richmond, degrading communications and internet for the state government and the governor's office. • Official IT-based communications platforms or social media accounts are hacked, and disinformation is disseminated via "official" channels about an ongoing cyberattack. • A cyberattack causes disruptions to GPS capabilities. • A cyberattack on trans-oceanic internet cables out of Virginia Beach interrupts internet and data traffic to Europe, South America, and South Africa.
Transportation	• A supply chain attack focuses on disrupting other sectors (energy and water) by targeting rail supply of fuels or chemicals. • A cyberattack disrupts critical rail functions, such as signals, switching, and safety systems, on routes supplying bulk fuel or coal to the Norfolk coal terminal. • Intermittent hacking of traffic lights in urban areas creates accidents and traffic jams, stretching the capacity of first responders. Mis-, dis-, and mal-information (MDM) following the cyberattack creates confusion and loss of confidence in the reliability of traffic control systems.
Financial Systems	• A nation-state actor accesses credit card processing systems and prompts false payments, while MDM drives loss of confidence. • MDM induces panic-buying and hoarding of critical items. • A bad actor leverages prior incidents of bank failures and possible bad financial news to create disinformation regarding bank failures and entice a run on a bank.

Table 3. Sampling of impacts, consequences, resources, and activities for each target sector, as identified by the working groups

Target Sector	**Impacts**	**Consequences**	**Resource Needs**	**Consequence Management Activities**
Energy	- Loss of heating and cooling - Prolonged power outages - Traffic light outages	- Increased fatality rate - Increased crime - Military operations reduced to essential	- Fuel for generators - Alternative energy sources such as solar panels	- Consolidate 911 centers - Implement additional staff for security

	- Reliance on limited generators	operations and personnel	- IT resources to restore networks	- Create areas for shelter - Prioritized fuel distribution plans
Water	- No potable or non-potable water - Lack of clean, usable water	- Disruptions to medical facility operations - Waste buildup - No cooling to power infrastructure and systems	- Portable water treatment units - Emergency drinking water supplies - Supply and distribution system for chlorine tablets	- Activate public alert and warning plan - Coordinate pumps to collect water from natural bodies of water - Increase production and distribution of bottled water
Communications	- Loss of communication capabilities - No cellphone service - Impacts on GPS communications	- Inability to coordinate emergency management activities - Navigational challenges - Limitations in dispatch capabilities	- Satellite phones - Radios compatible with law enforcement and emergency management - Additional staff for inspections	- Establish emergency communication channels - Coordinate with private sector partners to support the repair and restoration of communications - Activate backup systems such as SATCOM
Transportation	- Loss of rail service - Loss of port operations - Loss of traffic control signals	- Supply chain disruptions - Inability to transport critical resources efficiently - Increased traffic - Overwhelmed local police	- Alternative transportation modalities such as ships, rail, or car - Transportation waivers to those transporting essential resources - DMAT deployment	- Activate contingency plans - Deploy additional security to roads, airports, and stations - Establish alternative supply chain routes

A more detailed discussion of the analysis from Phase 2 will be documented in the CONOPS as a series of Sector-Specific Appendices. These appendices will provide in-depth, threat-based analyses of the cyber risk landscape for each of the five target sectors (energy, water systems, transportation, telecommunications, and financial systems), including vulnerabilities that could be exploited by nation-state actors known for their cyber activities. The appendices will serve as a resource for stakeholders and will help to foster informed decision-making and holistic preparedness.

Mission Areas

Based on the information collected from the working group discussions, the project team identified a set of mission areas that Virginia state agencies and partners will need to support to manage the consequences of a cyberattack resulting in a critical infrastructure outage. These mission areas will enable responders to meet immediate and ongoing community needs and stabilize essential community lifelines, as depicted in Figure 2.

Figure 2: Derivation of mission areas from Phase 2 findings

These mission areas (see Figure 3) will provide the framework for focused planning in Phase 3, enabling smaller, mission-focused groups to engage in concentrated discussions and planning. The Blue Book Project will facilitate these efforts through virtual meetings, workshops, and scenario-based planning sessions, identifying what is needed to successfully support each mission area in a degraded environment. This approach will draw out potential challenges and explore solutions, workarounds, and adjustments in accomplishing the mission area, ensuring the continued delivery of essential services despite the anticipated compromised conditions.

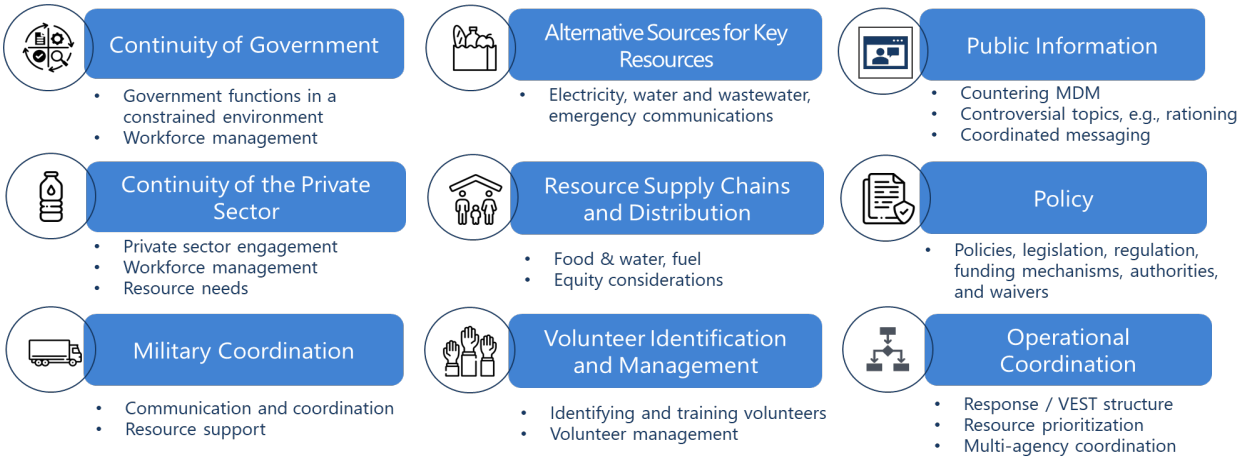

Figure 3: Phase 2 mission areas and their subcomponents

Interdependencies

During Phase 2 of the Blue Book Project, the planning team also initiated an in-depth research effort examining how the target sectors and their vulnerabilities are interconnected and mutually reliant to better understand the potential impacts of a cyberattack and its associated consequences on community lifelines. The insights and findings from the interdependencies research of Phase 2 will be detailed in another white paper, which will serve as a valuable resource for future planning efforts.

White Papers

Phase 2 also focused on the development of white papers to explore key subjects related to the management of consequences following a cyberattack on critical infrastructure. Topics explored thus far include civil defense strategies from the Cold War, use of the Defense Production Act, law enforcement support to military operations, and mis-, dis-, and mal-information (MDM). These documents will help emergency managers cultivate a proactive approach to similar threats and will equip them with the tools and ideas necessary to effectively navigate the evolving cyber threat landscape. Ultimately, these resources will contribute to building a more knowledgeable and resilient nation and will empower states to plan and respond to cyberattacks more effectively. The white papers, as well as additional information pertaining to the Blue Book Project, can be downloaded from the Blue Book website.

CONCLUSION

The steps outlined in this white paper may assist other states or jurisdictions in replicating the Phase 2 process of the Blue Book Project. Phase 2 provided a method for working groups to successfully identify and discuss critical infrastructure vulnerabilities to a cyberattack and the resulting impacts and consequences, as well as the resources communities may need to maintain lifelines during a prolonged outage of critical services. This information is the basis for the development of a series of mission areas that will need to be supported following a cyberattack on critical infrastructure, which will be the focus of research and exploration during Phase 3.

For more information, please contact the project planning team at BlueBookProject@vdem.virginia.gov.