THE BLUE BOOK PROJECT: LESSONS LEARNED FROM PHASE ONE

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 (US) have become more frequent, coordinated, and severe. Foreign adversaries are increasingly targeting and exploiting US critical infrastructure through network and supply chain vulnerabilities. Although these attacks most often have consequences such as financial loss and data and intellectual property theft, cyberattacks can also result in physical damage to critical infrastructure that can cause severe, long-term disruptions in services.

In fiscal year 2023, the Commonwealth of Virginia was awarded Regional Catastrophic Grant Program funding for the Virginia Department of Emergency Management (along with state agency experts like VSP and VITA) to develop a plan for responding to a nationally significant cyberattack on critical infrastructure. Subsequently, the VDEM initiated the Blue Book Project. The goal of the Blue Book Project is to ensure the Commonwealth is positioned to manage the consequences of a sophisticated nation-state cyberattack across critical infrastructure. Through this effort, the Commonwealth will establish and organize opportunities to support critical infrastructure partners during attacks, ensure residents' basic needs can be met, and support the military so that it can continue its mission to protect the homeland and project forces globally when systems are disrupted.

The cyber 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 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. The Blue Book Project has four objectives:

a. Leverage the expertise of stakeholders from the federal, state, local, and private sector.
b. Maintain awareness of the evolving threat environment to inform preparedness and response planning and strategies.
c. Develop strategies and plans that define an overall coordination framework (operations and management) needed to protect Virginia's critical infrastructure and people, outline processes to respond and recover from unavoidable attacks that damage or destroy systems, while supporting the Department of Defense (DOD) in restoring mission critical functions.
d. Test and assess resilience to threats by implementing games and exercises.

This white paper outlines a framework for other states to replicate the Blue Book Project across the nation and offers support and guidance for executing Phase 1: Project Initiation. The Blue Book Project has four phases; Phases 2, 3, and 4 will be covered in subsequent papers.

PHASE 1 OVERVIEW

The first phase of the Blue Book Project focused on developing a project charter and establishing cohesive working groups that can contribute to the project teams' understanding of threats and vulnerabilities, anticipated impacts, and plans for consequence management. Phase 1 activities establish an important foundation of knowledge, support, and partnership that will set the project up for success in later phases.

Develop Charter

The project charter serves as an authoritative document that will guide the execution of the Blue Book Project. The charter specifies the goals of the Blue Book Project, details the project timeline, sets expectations for how members will collaborate with each other and with project leaders throughout the entirety of the project, and serves as the primary reference for decision-making through the project life cycle. The charter is a living document that can be adapted and amended as needed throughout the course of the project.

Identify Participants and Stakeholder Groups

The Blue Book Project team identified a broad cross section of participants to represent key stakeholders from federal, state, and local governments; private sector and critical infrastructure owners and operators; and community groups and nongovernment organizations (NGOs). Within those stakeholder groups, the team further endeavored to identify participants with the knowledge and expertise needed to support the planning and execution of the Blue Book Project, including, but not limited to, expertise in cybersecurity, cyber risk, and emergency response and management.

Local government	State government	Federal government	Critical infrastructure	Military	NGO
• Emergency management • Fire/EMS • Law enforcement • Information technology • Water treatment	• Emergency management • Law enforcement • Fusion Center • Energy • Environmental quality • Agriculture • Health • Social Services • Transportation • Regulatory agencies • Information Technology	• FEMA • DOE • FBI • TSA • CISA • USACE • Federal Reserve Bank	• Major utilities, (e.g., water, electricity, gas) • Transportation providers • Telecom service providers • Financial companies • Private sector associations	• US Coast Guard • National Guard • NORTHCOM/ Army North • DOD/Office of the Secretary of Defense • Military installations	• American Red Cross • Voluntary Organizations Active in Disaster (VOAD) leadership

Conduct Kickoff Meeting

The Blue Book Project team brought all members together for a day-long in person kickoff meeting. The objectives of the kickoff meeting included the following:

a. Project overview: The project team outlined the project goals, the threat of nation-state cyberattacks, the importance of strengthening the state's cybersecurity posture, and details on how the Blue Book Project will better prepare the state for an attack. Included were the project timeline and deliverables of each phase.
b. Threat presentations: Multiple subject matter experts (SMEs) briefed the assembled members on the threats from nation-state actors to critical infrastructure, including defining cyberattacks, discussing what they look like in practice and why they are appealing to foreign adversaries, and describing the damage that a cyberattack on critical infrastructure could cause. The threat briefings covered the strategic goals, capabilities, actors, and examples of cyberattacks from China, Iran, North Korea, and Russia. Finally, a SME delivered a briefing defining and distinguishing between mis-, dis- and mal-information, describing how foreign adversaries employ it and how we can counter it.
c. Small group discussions: Participants conducted the first working group breakout sessions with scenario examples of an attack on critical infrastructure. Discussions included the direct and cascading effects, response actions, plans and roles, and parallel planning efforts that should take place in that scenario. Outbriefs were shared after reconvening with the full group.
d. Charter approval: Members received the charter in advance as a read ahead and were invited to ask questions and provide feedback on the proposed charter. Pending suggested edits, the assembled members voted to approve and adopt the charter.

Establish Working Groups

Invitations for participation in the Blue Book Project were issued to organizations representing the groups described above. Each organization was provided a background on the project and asked to select one primary and one alternate member who could best meet the needs of the project.

The Blue Book Project established five functional working groups:

a. The Intelligence and Analysis Working Group brings together experts from intelligence agencies, law enforcement agencies, and other government organizations. The primary objective of this working group is to gather, analyze, and share information related to cyber threats, vulnerabilities, and adversaries to inform decision-making.
b. The Critical Infrastructure Working Group brings together representatives from government agencies, infrastructure owners and operators, members of regulatory bodies, and members of other relevant private sector organizations. The primary objective of this working group is to discuss the effects of a prolonged outage on Virginia's critical infrastructure following a

cyberattack on target sectors, including water and wastewater, energy, transportation, telecommunications, and finance.

c. The Military Requirements and Support Working Group brings together representatives from various military branches and facilities in the Commonwealth of Virginia. The primary objective of this working group is to address the unique cybersecurity needs and challenges faced by the military, especially if resources are divided by mobilization in response to the cyberattack.
d. The Community Vulnerabilities Working Group brings together experts in potentially vulnerable populations during disasters, such as those with disabilities and access and functional needs, those requiring both acute and long-term medical care, and other vulnerable communities. The primary objective of this working group is to address the human needs of a coordinated emergency response to a major cyber incident with real-world, long-term consequences.
e. The Consequence Management Working Group brings together representatives from law enforcement, emergency communications, emergency management, and other government organizations. The primary objective of this working group is to identify the activities necessary to support community lifelines and to coordinate managing the consequences from a prolonged outage of critical infrastructure sectors.

The working groups are organized into three parallel tracks, and the outcomes of each track will contribute to the development of the concept of operations (CONOPS) in Phase 3, as shown in Figure 1. The Intelligence and Analysis Working Group was asked to identify potential threats, including how nation-state adversaries might exploit vulnerabilities in Virginia's critical infrastructure. The Critical Infrastructure Working Group was asked to identify the outcomes of a cyberattack on critical infrastructure, including hard to anticipate second and third order cascading effects. And finally, the Military Requirements and Support, Consequence Management, and Community Vulnerabilities Working Groups were tasked with identifying likely actions to manage consequences from a cyberattack on critical infrastructure, as well as the material needs that would support such a response effort.

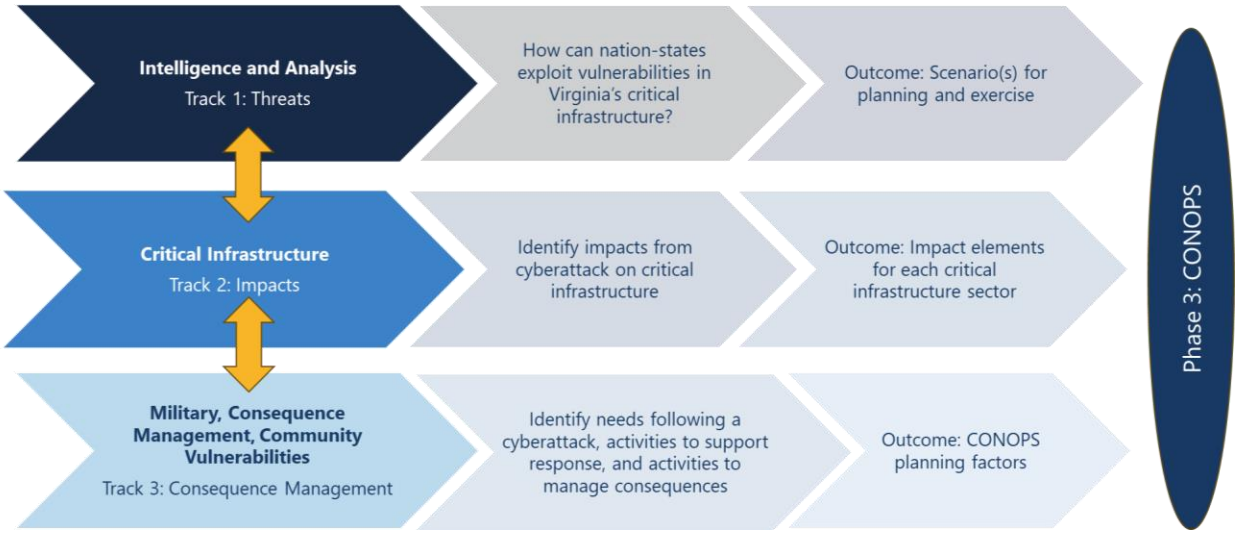

Figure 1: Working group parallel lines of effort

CONCLUSION

The Blue Book Project is a first-in-nation effort to develop a plan that arranges a coordinated, cohesive response to a major cyberattack across critical infrastructure by a sophisticated nation-state actor. Although many of the specific activities conducted will be specific to Virginia, the goals, objectives, and methodologies may be of interest to others across the country to develop a similar product. The steps outlined in this white paper may assist other states or jurisdictions in replicating the Phase 1 process of the Blue Book Project. Each of the steps described, from identifying stakeholders to the approving the charter, will ensure that a representative cross section of stakeholders is identified and that each participant is knowledgeable about the process and expectations of them throughout the project. The steps will also set up the team and participants for success from the onset to ensure an efficient and productive planning process.

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