IMPACT RESISTANCE: CyOTE AND CCE

FEBRUARY 10, 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL Idaho National Laboratory

Contents

EXECUTIVE SUMMARY

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) works to enhance the security of U.S. critical energy infrastructure and mitigate the impacts of disruptive events and risks to the sector through preparedness and innovation. To further this mission, CESER and Idaho National Laboratory (INL) developed the interrelated Consequence-driven Cyber-informed Engineering (CCE) and Cybersecurity for the Operational Technology Environment (CyOTE^{TM}) programs. Outputs from the CCE process can help focus Asset Owners and Operators' (AOOs) efforts when applying the CyOTE methodology. The CCE methodology streamlines the CyOTE process, by pointing to observed areas of unverified trust in the AOO's people, processes and technologies, that if exploited by an adversary, could lead to high-consequence events that could disrupt the AOO's ability to deliver their critical function. Further, when implemented together CCE and CyOTE accelerate impactful change within an organization, resulting in more effective protection from cyber-enabled sabotage.

CyOTE partners with energy sector AOOs to enhance AOO capabilities to independently identify indications of malicious cyber activity within their operational technology (OT) environments. Different from and complementing the approach taken by commercial security solutions, CyOTE emphasizes building context around anomalies perceived in the OT environment. As such, CyOTE and CCE build upon existing fundamentals in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (see Figure 1 [a]) and MITRE ATT&CK for Framework for Industrial Control Systems (ICS). The NIST Cybersecurity Framework is a best practice, enabling organizations to manage cybersecurity risk through five functions: Identify, Protect, Detect, Respond, and Recover.

CCE helps AOOs identify critical functions that need to be protected and prioritize solutions to do so. CCE primarily focuses on Protection strategies which aim to remove the risk through engineering, design, or process changes. However, if protection mechanisms are not an option, CCE focuses on identifying mitigating options which can significantly limit the effect of the identified High Consequence Event (HCE).

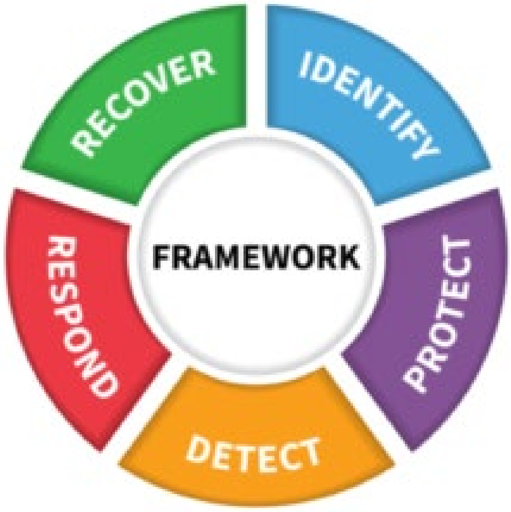

Figure 1: NIST Cybersecurity Framework

In alignment with CCE, the CyOTE methodology provides an approach for an AOO to use when an anomalous event or condition is detected or arises. Leveraging available detection methods and operational information, the methodology enables the AOO to comprehend the event in the context of their own environment and determine whether there has been a reliability failure that can be fixed, or if there is adversarial behavior/misuse requiring a response by the AOO to prevent the impact or impediment to a critical function.

[a] Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

INTRODUCTION

Since 2016, CyOTE has partnered with industry to develop targeted strategies to increase the cybersecurity resiliency of the nation's energy sector. The CyOTE methodology, released in 2021, provides a general approach for an AOO to use, starting from the point in time and space an anomalous event or condition meriting investigation is perceived, and continues to the point where the anomaly is comprehended with sufficient confidence to make a business risk decision on the appropriate resolution.[1] CyOTE enables AOOs to enhance their comprehension abilities resulting in accelerated response to potential incidents, reduced impact, and increased cyber resilience or the energy grid.

Since 2015, CCE has provided both private and public organizations with the steps necessary to thwart cyber-attacks from highly resourced adversaries that could result in a catastrophic physical effect. The CCE process helps critical infrastructure owners, operators, and their security practitioners make demonstrable improvements in securing their most critical functions and processes. The CCE program has successfully engaged with critical infrastructure and military partners, with numerous inquiries from around the world. CCE has provided the following opportunities to teach fundamental concepts of the CCE process.

- ACCELERATE: provides critical infrastructure companies with a self-guided approach to conducting their own CCE effort.
- Partner Training: designed to provide an in-depth, team-based training for select individuals who will participate in the execution of a Tier 1 engagement[b].
- Workforce Development: designed to provide in-depth, team-based training for select individuals who will help guide Tier 1 partners in the execution of a CCE engagement. "Countering Cyber Sabotage": informative book introducing the CCE methodology, released in 2020.[2]

CCE's primary goal is to apply strategic mitigations and protections to an organization's most essential operations, processes, and technologies. CyOTE's goal is to enable AOOs to detect threats in order to implement appropriate mitigations earlier in an attack campaign. Per the NIST Cybersecurity Framework, detection focuses on the timely discovery of cybersecurity events, while protection and mitigation focus on deterrence and limiting factors. These approaches are complementary, not mutually exclusive. The CyOTE methodology identifies existing data sources and information available from OT and IT sources, as well as data from sensors placed to gather security information specific to an AOO's OT infrastructure. Implementing the CyOTE methodology provides additional capabilities to the AOO in analyzing malicious actors or equipment/process failures.

Synergistic implementation of the CyOTE methodology and CCE process can increase protection and visibility within AOOs environments to improve their operational cybersecurity. The amalgamation of these two essential processes are further described in the remainder of this report.

[b] INL conducts Tier 1 CCE engagements with companies or organizations that deliver functions or services deemed highly critical to national security—making them prime targets for cyber sabotage.

CCE METHODOLOGY AND PURPOSE

CCE seeks to secure the nation's critical infrastructure systems by thinking like the adversary. CCE assumes that if critical infrastructure is targeted by a skilled, determined, and well-resourced adversary, the targeted operation can—and will—be compromised. This process, encompassing the four phases listed below, generates a new way of thinking about strategic cyber risk.

- Phase 1, Consequence Prioritization, identifies critical systems and associated events that would trigger failure of those critical functions.[3]
- Phase 2, System-of-Systems Analysis, identifies, collects, and organizes all information regarding critical systems identified in Phase 1.[4]
- Phase 3, Consequence-based Targeting, develops Attack Scenarios to determine paths, targets, access, and information an adversary would need to achieve identified events.[5]
- Phase 4, Mitigations and Protections, focuses on preventing, limiting, responding to, and recovering from an adversary carrying out the Attack Scenarios.[6]

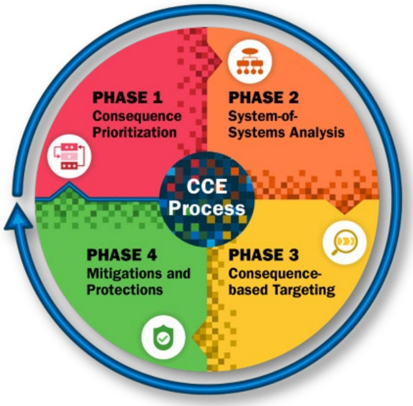
PHASE 1
Consequence Prioritization
PHASE 2
System-of-Systems Analysis
CCE Process
PHASE 4
Mitigations and Protections
PHASE 3
Consequence-based Targeting

Figure 2: Four Phases of the CCE Process

CyOTE METHODOLOGY AND PURPOSE

The CyOTE methodology applies fundamental concepts of perception and comprehension to expand what is known and shrink the unknown realm. By seeking to comprehend the observables and anomalies in the OT environment, an AOO can move from visibility alone to *understanding.* When an anomaly prompts investigation to help the AOO understand what caused it, that particular event becomes the triggering event. If sufficient evidence of a malicious nexus is found through investigating a triggering event, the situation is addressed through existing organizational incident response procedures. Failure to find sufficient evidence of malicious activity defaults to existing organizational corrective maintenance and work management procedures.

By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables that could represent a faint signal of an attack requiring a defense response. Over time, AOOs' triggering events will move towards earlier detection to interdict incidents. As explained in the CyOTE "Sensor Placement and Capability Recommendations" paper, data captured for operational purposes may not contain some of the data/information that would enable the perception and comprehension of whether an anomaly was from a malicious cyber activity or a mechanical/maintenance issue. The AOO may determine that additional sensors are needed to precisely capture cybersecurity related data.

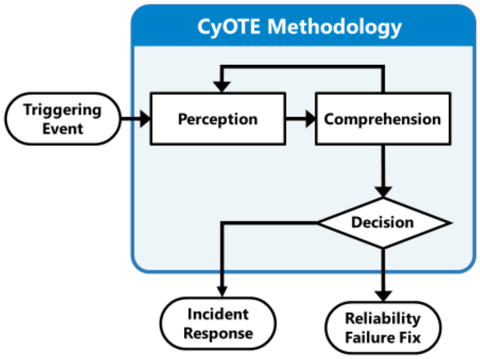

Figure 3: The CyOTE Methodology

Figure 3 shows the CyOTE methodology.[7] The first step is perception, where a human consciously recognizes the existence of a triggering event and elevates that awareness from individual to organizational level. Three common ways to perceive a triggering event are 1) programmed alarms and alerts, 2) human pattern matching, and 3) business process exception.

The second step, comprehension, is the organizational process of gathering available information from traditional networks and device monitoring approaches, information from the energy infrastructure (e.g., telemetered physical quantities like voltage, current, or pressure, and discrete equipment indications like breaker or switch positions), individuals (including operators, engineers, technicians, and maintainers), and the business processes by which humans monitor and control the OT and interconnected infrastructure to accomplish the organization's critical and enabling functions. The gathered information is used to increase understanding and comprehension of what caused the triggering event and other related anomalous observations.

As comprehension increases, an AOO can better determine and characterize the event as either a cyberattack or a reliability failure. Thus, informed business risk-decisions can be made, resulting in either the activation of incident responders for malicious cyber activity or maintenance dispatch for identified reliability failure(s).

CyOTE METHODOLOGY IMPLEMENTATION

There are at least three ways an AOO can employ the CyOTE methodology. First, AOOs can apply CyOTE to investigate anomalies within their own production systems, starting from the perception of a triggering event, through iterative comprehension to determine whether it is reliability failure or malicious activity.

Second, CyOTE can be used to retrospectively analyze relevant incidents (i.e., Case Studies) using available information. These Case Studies identify opportunities to detect and understand the chain of adversary activity earlier, where anomalies created by adversary techniques were either not perceived, or not sufficiently or accurately comprehended earlier, before the impact occurred. By identifying anomalies earlier in a chain of adversary activity, an AOO can assess how to improve their own processes to comprehend and respond to earlier indicators in a similar situation.

The third way an AOO can employ the CyOTE methodology is to proactively build a perception and comprehension capability for consequential cyber-events, as described in the next section. This starts with taking the identified High Consequence Event (HCE) from the CCE process and mapping it to adversarial techniques needed to carry out that event with the CyOTE methodology. As a result, AOOs can implement procedures, methods, and sensors that can identify or observe those related people, processes, and technologies.

SYNERGY BETWEEN CCE AND CyOTE METHODOLOGIES

Through the creation of logical connections between the CCE and CyOTE programs, AOOs can apply the outputs derived from the CCE process to inform the CyOTE methodology to detect malicious cyber actions within their environment(s). The output from the CCE process can help focus an AOO's efforts when applying the CyOTE methodology. The CCE methodology streamlines the CyOTE process by pointing to observed areas of unverified trust in the AOO's people, processes and technologies, that if exploited by an adversary, could lead to high-consequence events that could disrupt the AOO's ability to deliver their critical function. Parallel use of these approaches increases the speed to impactful change within an organization. This more effectively and quickly protects the AOO from cyber-enabled sabotage. Figure 4 provides a visual representation of opportunities for an AOO to leverage the four phases of the CCE process and CyOTE methodology simultaneously.

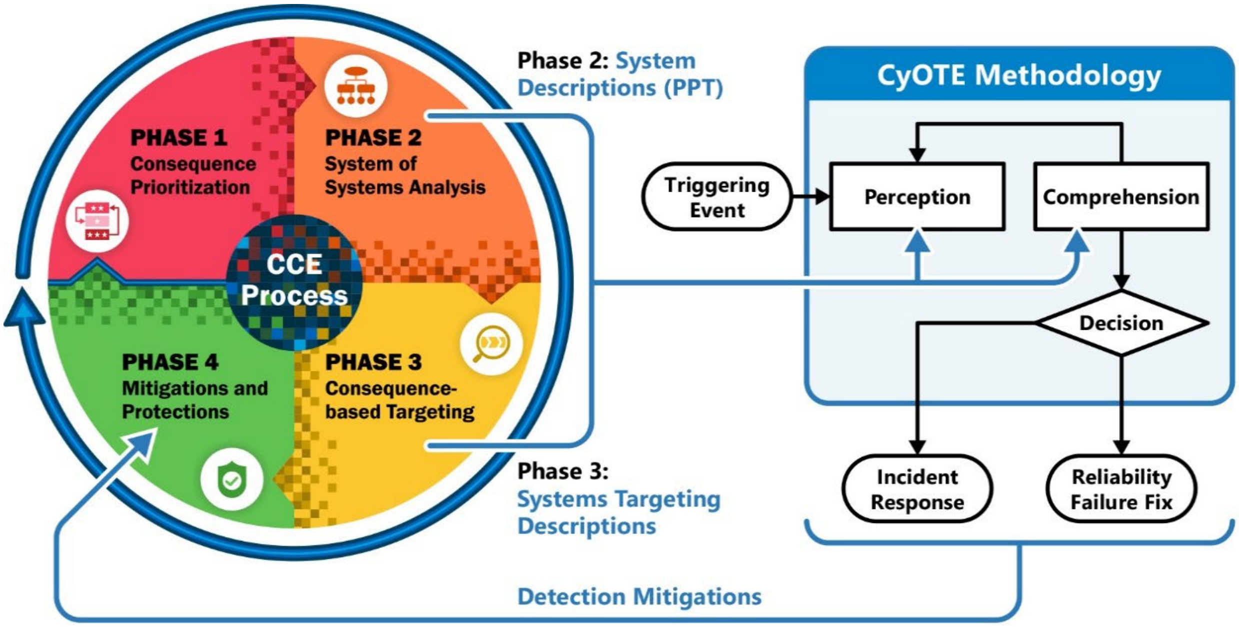
PHASE 1
Consequence Prioritization
PHASE 2
System of Systems Analysis
CCE Process
PHASE 4
Mitigations and Protections
PHASE 3
Consequence-based Targeting
Phase 2: System Descriptions (PPT)
Phase 3: Systems Targeting Descriptions
CyOTE Methodology
Triggering Event
Perception
Comprehension
Decision
Incident Response
Reliability Failure Fix
Detection Mitigations

Figure 4: CyOTE Methodology Leveraging the 4 Phases of CCE

CCE **Phase 1** focuses on identifying HCEs that are of greatest impact to the organization's critical functions. To develop an HCE, AOOs identify cyber-events, described as possible disruptive events that could be achieved via cyber-means and that impact critical functions, services, or processes. The event identified in Phase 1 is what the AOO works to prevent or mitigate through the remainder of the CCE Process. By identifying relevant anomalous activity that would triggering further investigation, an AOO can employ the CyOTE methodology to comprehend early indicators prior to the impact of the identified HCE.

Phase 2 conducts a systematic review and analysis of information related to the equipment, systems, processes, operations, maintenance, testing, and procurement practices based on the identified HCE. This step includes collecting all relevant information particular to the given HCE to produce a System Description of people, processes, and technologies that functionally describes all aspects of the HCE. CCE Phase 2 provides a big picture of how a system or function operates, how people interact with the system, and how the controls work.

The information and knowledge gained in Phase 2 of the CCE process is the same information and knowledge that is needed to build a framework for the Comprehension stage in the CyOTE methodology. Knowledge of how the system works, where people are involved, what the process is, and how technologies are used is critical when trying to explain an anomalous event. Documentation of these elements will help ensure early indicators are not missed or ignored and streamline the comprehension process if a triggering event occurs

The goal of **Phase 3**, Consequence-based Targeting, is to develop Attack Scenarios. The System Targeting Description is used to summarize and reference all the key details that are required for the Attack Scenarios. This development is also supported by the data collected and organized during the comprehension stage. Both steps aim to identify plausible ways to carry out the HCE. Phase 3 provides the details of an envisioned attack, such as what tactics, techniques, and procedures (TTPs) would be employed and the chain of events that could conclude in an HCE.

The identified TTPs are key for the CyOTE methodology. Organizations will monitor and analyze specific data sources and fields to detect the occurrence of TTPs. The aim is to map source data and information that will detect adversarial behaviors as they use those techniques. To accomplish this, the CyOTE program uses a node and link diagram, as shown in Figure 5, to organize and visualize the discovered information. The usage of node and link diagrams becomes exponentially more important as the triggering event expands into a web of postulated, confirmed, or denied relationships between anomalies.

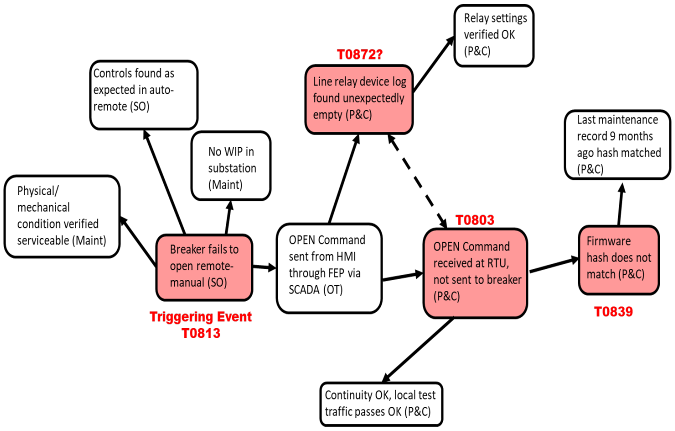
Relay settings verified OK (P&C)
T0872?
Line relay device log found unexpectedly empty (P&C)
Controls found as expected in auto-remote (SO)
No WIP in substation (Maint)
Last maintenance record 9 months ago hash matched (P&C)
Physical/ mechanical condition verified serviceable (Maint)
Breaker fails to open remote-manual (SO)
Triggering Event
T0813
OPEN Command sent from HMI through FEP via SCADA (OT)
T0803
OPEN Command received at RTU, not sent to breaker (P&C)
Firmware hash does not match (P&C)
T0839
Continuity OK, local test traffic passes OK (P&C)

Figure 5: Node and Link Diagram Example

The CyOTE methodology can be used to work through how AOOs perceive and comprehend triggering events related to information gathered from the entire CCE process, in which they can identify observables in people, process, and technologies related to each possible investigation. This involves significant efforts of data and information collection with the taxonomy linking functions and categories. Figure 6 shows that attack techniques can potentially be identified by analyzing one or more data source; however, in each data source a utility has the option to collect various data fields. The data fields contain operational and security information. Often technicians collect operational data, but security information such as state and configuration changes is not collected, as it could congest the network. AOOs may need to implement sensors to monitor, analyze, and alert to unexpected or anomalous behavior.

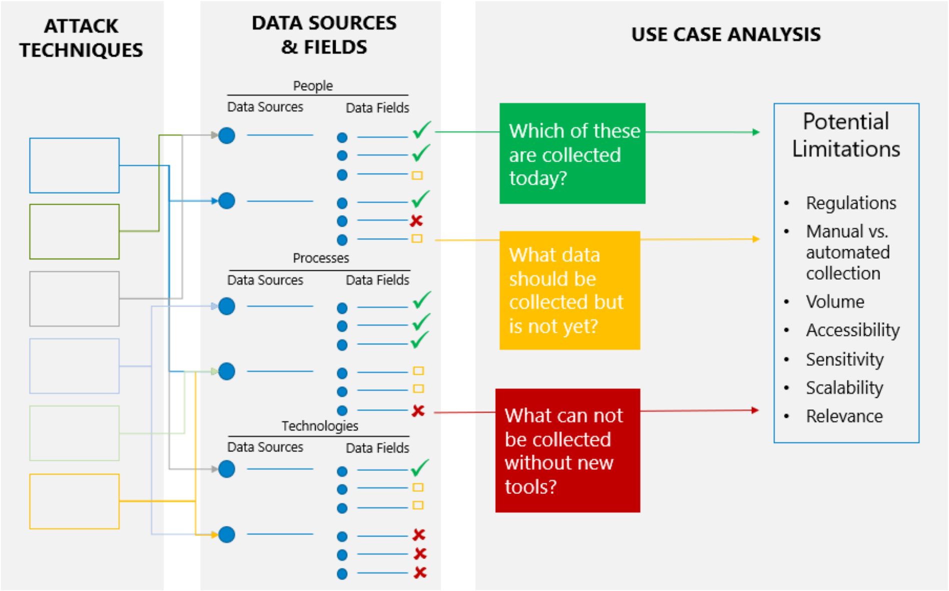

Figure 6: Demonstrating how Data Fields are Combined into Data Sources, which can be Used to Identify Attack Techniques

Phase 4 of CCE, Mitigations and Protections, focuses on leveraging engineering to remove the possibility of the end effect or developing means or mechanisms ("protections") that will ensure an adversary cannot achieve their objective via cyber means. However, even the best protections may not guarantee complete security and in some situations, the implementation of protections may not be feasible or possible. Thus, the next measure focuses on putting an organization in a better position to detect adversary activities directed against it and respond or recover from the attack. The CyOTE methodology focuses on detecting potential adversarial activity, encouraging vigilance in all phases of organizational maturity. By identifying the presence of a chain of techniques, an AOO can establish compelling evidence of malicious cyber activity and act earlier by employing incident response. Alternatively, if investigation of a triggering event results in no plausible indication of cyber activity, or the confident disproval of such, the anomaly can be resolved using a Corrective Maintenance Program. Both outcomes increase overall awareness of the OT environment and thus increase the challenge of cyber-enabled sabotage for the adversary and increases the AOO's resilience.

Through following the CCE and CyOTE processes, AOOs identify, protect, detect, respond, and recover. The tasks conducted through the CCE process to protect against an HCE complements the work needed to support the CyOTE methodology to detect adversarial activity working to execute that HCE. These activities may be repeated to identify protections and detections for other HCEs.

CONCLUSION

This document addresses the correlation of two programs, CCE and CyOTE. Together, these two programs provide complementary processes that AOOs can incorporate to protect their environment from cyber-enabled sabotage, detect (perceive) any anomalous event, and comprehend whether that anomaly is indicative of a cyber-attack or mechanical/maintenance issues. The decisions made and information gathered throughout the CCE process feed directly into the CyOTE methodology. The same systems and functions that the AOO is working to protect through the CCE process are the same the CyOTE methodology is working to detect anomalous events that may identify a cyberattack. When both methodologies are applied with deliberate understanding and selected incorporation of the other, AOOs can better defend their systems than with either methodology alone.

NEXT STEPS: AVAILABLE TRAINING AND SUPPORT

ACCELERATE training provides critical infrastructure companies with a guided approach to conducting their own CCE effort. It includes 16 hours of training on the CCE process, plus a detailed guide and templates participants can use to facilitate a CCE engagement within their organization. With this training, participants gain a fundamental overview of CCE concepts, a structured set of process steps to implement the methodology, and a combination of trainer instruction and group exercises that use realistic case studies to practice implementing each phase of the CCE process. Further plans to incorporate CCE and CyOTE are under development.

CYOTE Program: *Promoting protection of the U.S. energy grid through research, development, and asset owner/operator engagement resulting in a layered approach to increasing America's cybersecurity and resiliency. Find out how you can be part of the solution by e-mailing cyote.program@hq.doe.gov .*

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov

[1] ["CyOTE-Methodology_2021.pdf" | Accessed: 07 Oct 2021. [Online]. Available: https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf | Overall classification is UNCLASSIFIED]

[2] ["Counter Cyber Sabotage" | Accessed: 07 Oct 2021. [Online]. Available: https://www.routledge.com/Countering-Cyber-Sabotage-Introducing-Consequence-Driven-Cyber-Informed/Bochman-Freeman/p/book/9780367491154 | Overall classification is UNCLASSIFIED]

[3] [S. Freeman, C. St. Michel, and N. Johnson | "CCE Phase 1: Consequence Prioritization" | INL/EXT--20-58089-Rev000, 1617458 | May 2020. doi: 10.2172/1617458 | Overall classification is UNCLASSIFIED]

[4] [D. Buddenbohm and S. G. Freeman | "CCE Phase 2: System-of-Systems Analysis" | p. 9]

[5] [S. Cook, S. Freeman, and C. St. Michel | "CCE Phase 3: Consequence-based Targeting" | INL/EXT-20-58090-Rev000, 1617456 | May 2020. doi: 10.2172/1617456]

[6] [T. Miller, S. Freeman, and C. St. Michel | "CCE Phase 4: Mitigations and Protections" | INL/EXT--20-58091-Rev000, 1617455 | May 2020. doi: 10.2172/1617455]

[7] ["CyOTE-Methodology_2021.pdf" | Accessed: 07 Oct 2021. [Online]. Available: https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf]