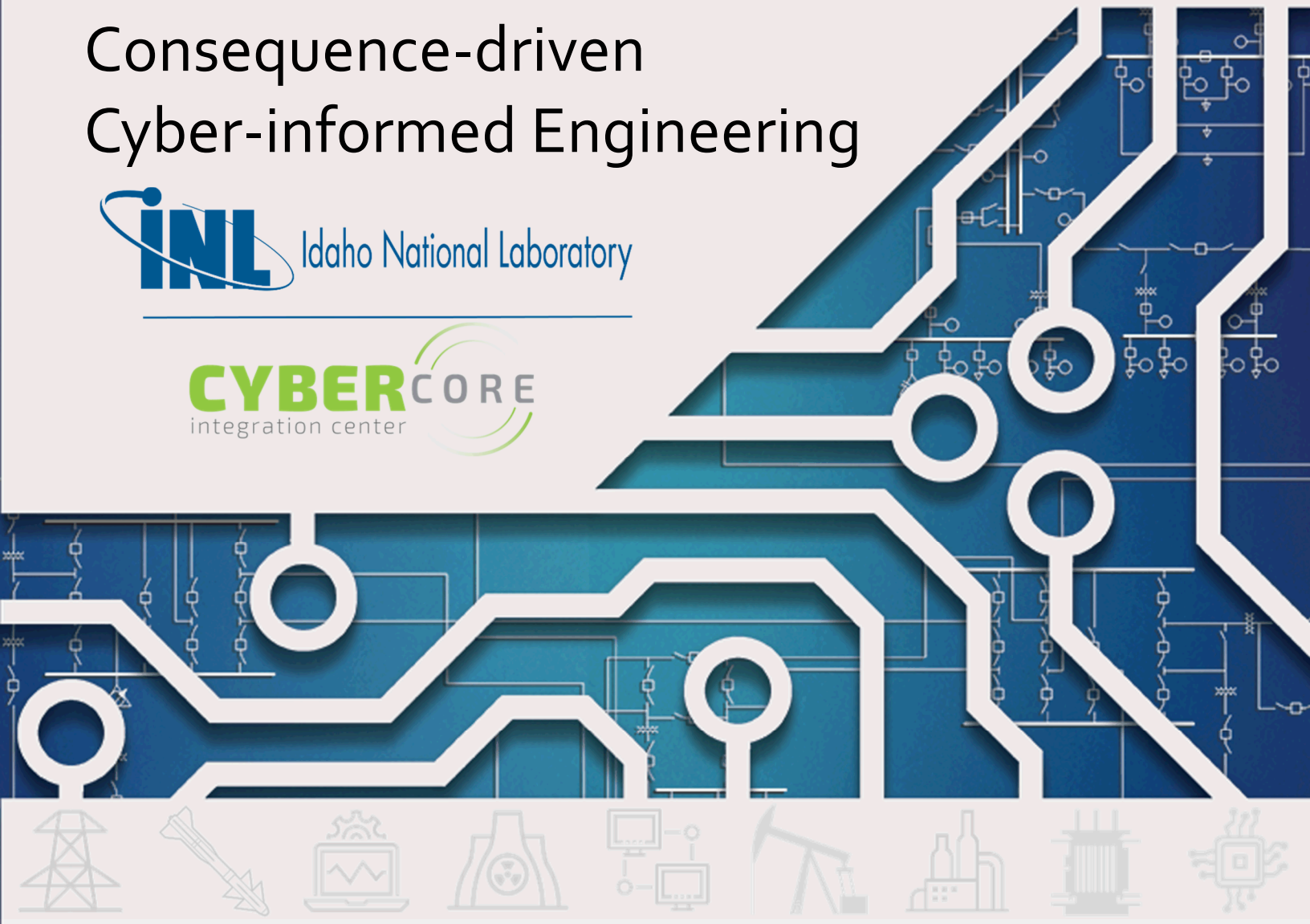
CCE Phase 3: Consequence-based Targeting

Consequence-driven Cyber-informed Engineering



Prepared By: Stacey Cook and Sarah G. Freeman
Cybercore Integration Center
Idaho National Laboratory

May 5, 2020

INL-EXT-20-58090

CCE Phase 3: Consequence-based Targeting

Consequence-driven Cyber-informed Engineering

Stacey Cook
Lead Author

Sarah G. Freeman
Co-Author

Idaho National Laboratory
Cybercore Integration Center
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of National & Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

CCE Phase 3: Consequence-based Targeting

Introduction

During Phase 1, Consequence Prioritization, the CCE Team identified High Consequence Events (HCEs) that could be accomplished through cyber means to impact critical functions, services, and processes. During Phase 2, System-of-Systems Analysis, the CCE Team conducted a systematic review and analysis of information related to the equipment, systems, processes, operations, maintenance, testing, and procurement practices based on the HCEs identified in Phase 1.

A summary of the HCE-relevant information collected in Phase 2 was drafted into a System Description, which serves as the starting point for the targeting analysis performed during Phase 3, Consequence-based Targeting. The goal of Phase 3 is to develop plausible **Attack Scenarios**. The CCE Team examines the data from Phase 2 with an adversarial perspective to brainstorm different ways to achieve the HCE. The **System Targeting Description** is used to summarize and reference all the key details that are required for the Attack Scenarios.

It should be noted that the findings in Phase 3 are not all-inclusive; they represent a set of *possible* approaches, called **Technical Approaches** in CCE, that can disrupt critical systems or functions. At the same time, these identified Attack Scenarios may be limited or informed by the Boundary Conditions defined in Phase 1. The **Target Details** describe each location where manipulation or compromise occurs in an Attack Scenario to make the HCE possible. Target Details include all the technical details an adversary would need.

While Phase 2 was a data collection effort, Phase 3 is a targeting effort. In Phase 3, organizations systematically identify the necessary steps for adversary success—all from the adversary's perspective. A key component to this approach is identifying the critical information needs, targets, access, and actions required for the adversary to achieve the HCE. These **Critical Needs** are tied to accomplishing the HCE, such as the technical requirements for the payload (**Development**), or the access required to deliver a payload (**Deployment**).

Critical Needs can and will be identified outside of an entity's network boundary or direct control (vendors, suppliers, subcontractors, regulatory, or financial filings) as well as through publicly available, open-source resources found in various places. An entity's ability to identify what these Critical Needs are, where they reside, and who has access to them is a crucial step in understanding—and ultimately mitigating—risk.

For the CCE Team, the definition of critical information should extend well beyond documentation because an adversary will need to understand precisely how a process or piece of equipment functions to achieve a specific effect. To gain this type of knowledge, the adversary may need to acquire equipment, software, configuration files, or even access somewhere in the supply chain. An understanding of Critical Needs can also be used as the basis for "tripwires" that flag adversary activity related to the HCE.

Visualizing Cyber-enabled Sabotage with the CCE Kill Chain

The CCE Kill Chain (see Figure 1 on the next page) was developed to help illustrate the activities an adversary must accomplish in order to cause cyber-enabled sabotage. Assembling the cumulative knowledge, capability, and access that is needed to maliciously manipulate a system requires a long term "campaign" of iterative targeting and information collection activities. The results achieved by these efforts are required for the associated payload Development and Deployment activities. They also directly relate to the success of a cyber sabotage campaign. Therefore, if a roadblock is met in payload Development, or new information or accesses become available, all the activities in the campaign will adjust to the new requirements.

The main reason for using the CCE Kill Chain is CCE's focus on understanding (and ultimately disrupting) the requirements an adversary needs to achieve the HCE. For example, adversaries may target vendors and subcontractors through supply chain or human recruitment tactics in conjunction with a cyber campaign.[1] This is done to both obtain critical information and gain necessary access for the deployment of capabilities. A highly resourced and motivated attacker may insert corrupt components or software several layers into the supply chain. An attacker might also investigate co-opting insiders or have their own agents apply for critical positions at the target organization, a subcontractor, or a vendor.

Rather than focusing on the network and cyber hygiene details for every possible cyber access point, the CCE Kill Chain will identify areas of unverified trust in the implementation, operation, or maintenance of a targeted control system. These instances of unverified trust are sources for Critical Needs an adversary requires.

[1] One concerning example of supply chain manipulation was demonstrated during the Havex campaign in 2014. During this infection campaign, the adversary intercepted and altered update packages for ICS and auxiliary equipment. This effort directly targeted the operations of its victims by piggybacking on the update process for non-internet facing and air-gapped machines.

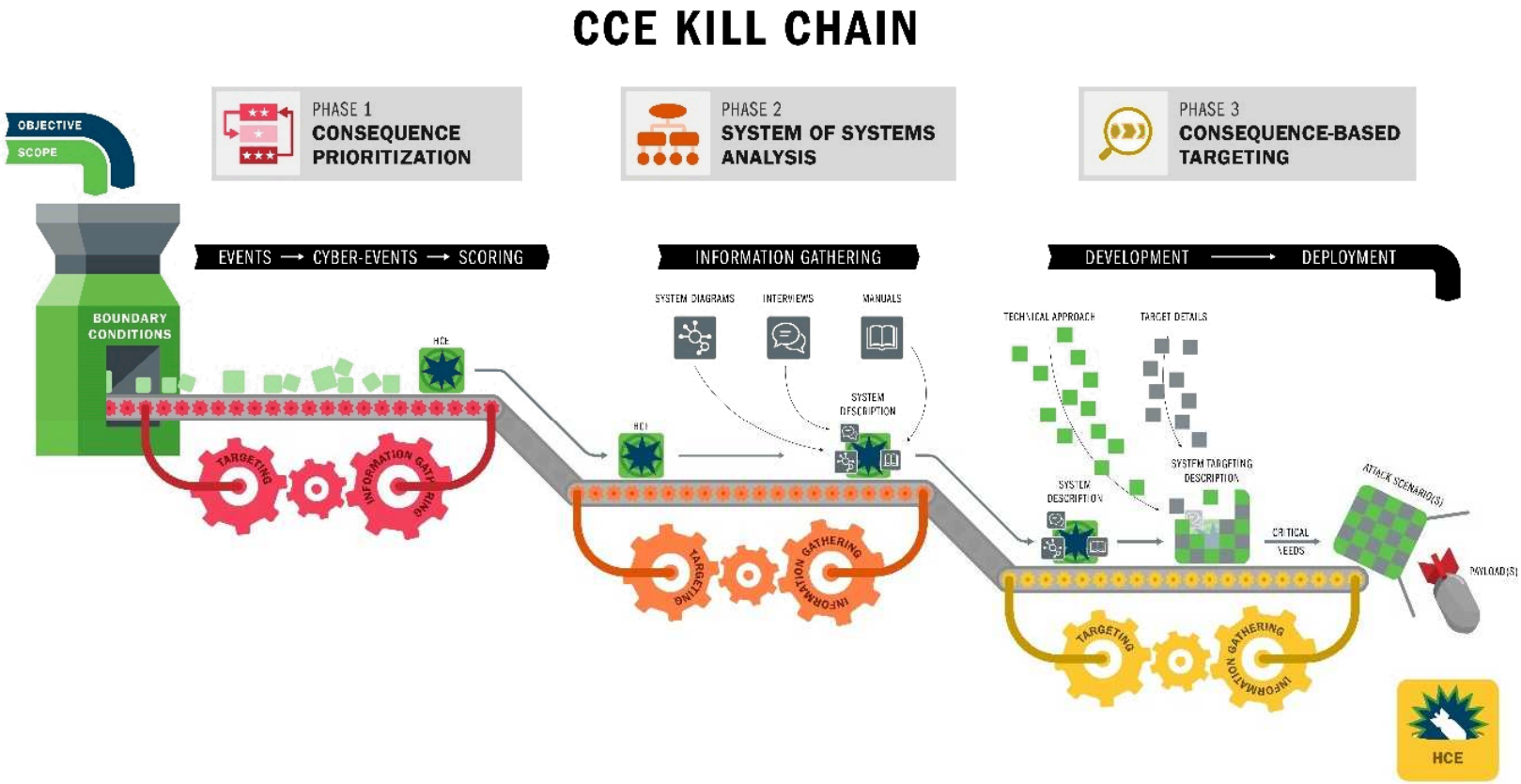


Figure 1. The CCE Kill Chain describing Phase 1 through Phase 3.

Identifying Choke Points

Think of a tree as a representation of every possible way to achieve a specific effect. The goal is to go from the tips of the branches to the roots of the tree. The branches represent all the different vectors an adversary can use to reach the goal. Even within the branches, there are many forks and possibilities. There are choke points where the branches come together—especially the trunk. These choke points are the specific locations that need to be identified by a targeting exercise.

By following the different branches of the tree down to the trunk, it is obvious there are many different pathways an adversary could take to compromise a system. Through Consequence-based Targeting exercises, these choke points an adversary must traverse are identified. These locations help narrow the areas for defenders to focus their protections to keep adversaries from reaching their goal.

Figure 2. Visual representation of choke points.

As discussed in the tree analogy, there are many different approaches an adversary could take to reach their goal of achieving the HCE. To take that concept a bit deeper, there may be multiple targets and multiple actions done to those targets, and there most likely will be multiple ways to access those targets. It is important to narrow down these numerous Attack Scenarios to the most plausible scenarios. Try to not get caught up in the countless possibilities.

Requirements for an Industrial Control System Attack

To successfully execute cyber-enabled sabotage on a critical function controlled by an industrial control system (ICS), an adversary must accomplish three basic tasks. They must develop the payload(s) required to cause the desired HCE, they must achieve access to the target ICS(s),[2] and they must get the payload(s) to the target device(s) in the ICS(s).

Like developing software, a customer provides requirements to the software developer detailing what the software must be able to do. The software developer would also need to know what kind of system the software will be running on with all the technical details. Once the software is developed, it needs to be delivered to the customer on the designated system.

While developing the criteria necessary for an adversary to cause an HCE, there are several questions that need to be answered, such as:

- "What do we have to do to achieve the HCE?"
- "Where do we have to be to achieve the HCE?"
- "How do we get to the Target(s)?"

[2] Access can be obtained through an initial access vector and/or any required network traversal.

The answers to these questions help define what the adversary needs to know, where on the ICS they need to be, what equipment or software they must access for development, and what kind of exploit they need to develop to cause the HCE.

System Targeting Description

The System Description from Phase 2 will be the groundwork that becomes the System Targeting Description in Phase 3. The System Targeting Description includes additional key details that are identified during targeting analysis and complete the summary of information required for the Attack Scenarios to cause the HCE. Adversaries have many different vectors or scenarios they could use to reach their goal. Just like the previously discussed tree analogy, there are a myriad of branches or pathways available, but the most plausible routes and choke points need to be the focus during this targeting exercise.

References are crucial in this step. Every piece of information documented in the System Targeting Description should also be referenced to the easiest accessible location. For example, if the fact that an organization uses a specific model of equipment can be found in both internal engineering documents and from the equipment vendor's website, the vendor's website should be referenced. The public-facing website is the easier path for the adversary to collect the needed critical information because it does not require breaching the company's network.

In addition, if information can be found in several locations, the reference that contains more than one piece of critical information should be cited. Again, thinking like the adversary, it is more advantageous to find several pieces of information in one location than it is several spread out. This gives the entity a good place to start with mitigations.

Consequence-based Targeting Process

The complex process of completing Phase 3 involves recording all the different Attack Scenarios possible to cause the HCE. Within these Attack Scenarios, there will be numerous targets that require specific actions and payloads based on their technical details. These targets also have numerous ways to be accessed. In building out the details required for each target, one possible Attack Scenario is synthesized. The different accesses to each target construct a possible pathway the adversary could take to reach the final goal of the HCE.

The technical details of the targets identified in the Technical Approach are described in the Target Details, which include the details of each specific element that would need to be manipulated or compromised to achieve the HCE. All information required for the different Attack Scenarios (each with a completed Technical Approach and Target Details) would be included in the System Targeting Description with complete references for each piece of information. This is an iterative process and will likely require revisiting Phase 2 activities in order to collect the pertinent information for targeting. Figure 3 illustrates the entire Phase 3 process.

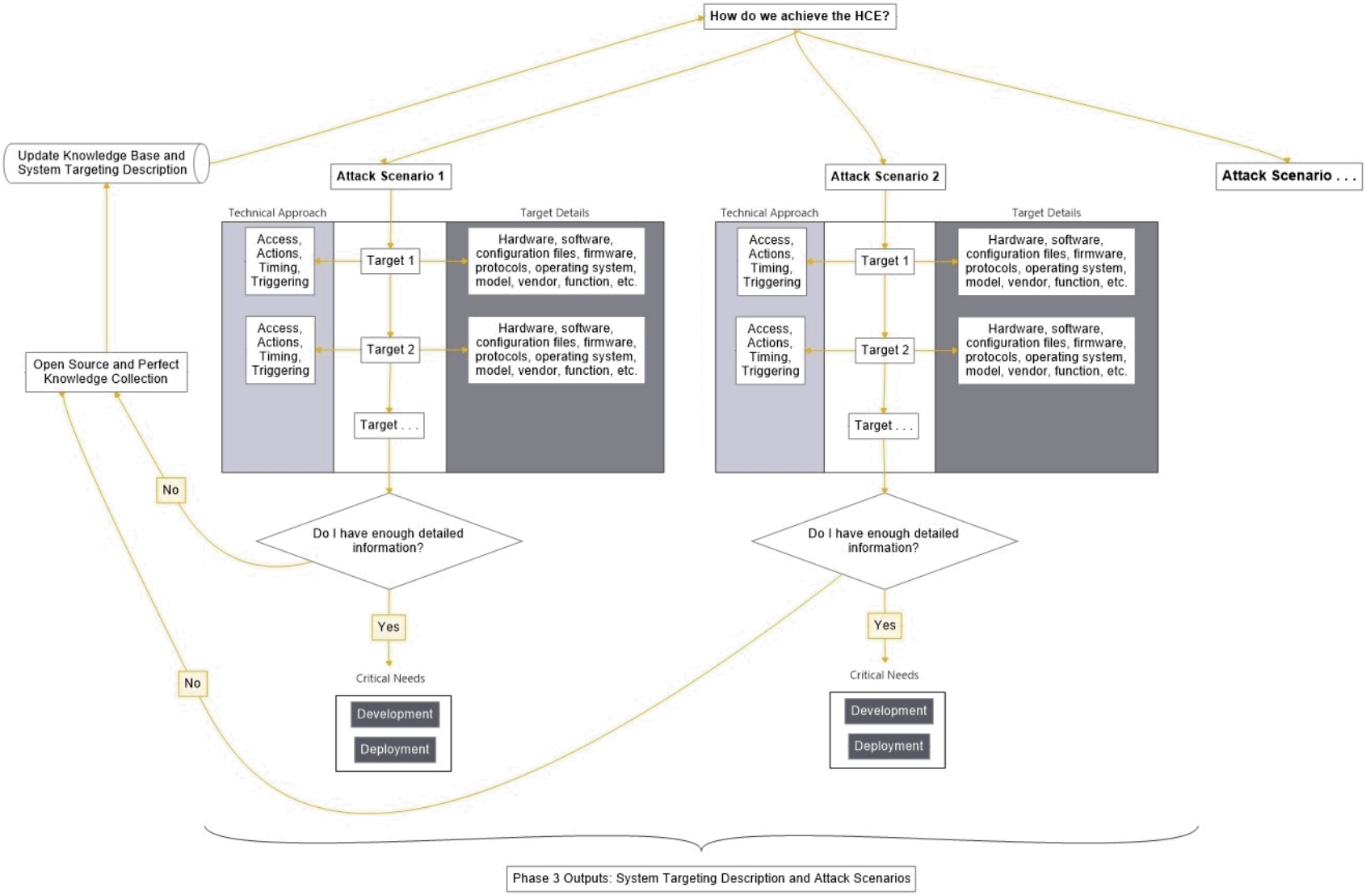


Figure 3. Phase 3 process flow chart.

Technical Approach

The Technical Approach is a detailed set of requirements. It defines a series of steps required for the exploitation of a target ICS environment to achieve a cyber-enabled sabotage effect. These individual steps will be tailored to the implementation of the targeted ICS. They will also describe how to get to each ICS element that the adversary needs to manipulate or compromise to enable the final cyber-enabled sabotage goal.

Each element in the Technical Approach will be identified by the **Target** ICS element. This specific Target might be a device component, system process, memory module, programmable chip, or logic circuit. The Target can also be non-cyber or human components of the process, like personnel with direct access to the system. Each element will define the **Access** to the target, what **Actions** need to occur at the target, and when (**Timing**) and how (**Triggering**) the payload will be triggered.

TECHNICAL APPROACH ELEMENTS

Access are the steps, movements, and actions an adversary performs to reach a target. This can occur by several pathways, but it is important for the CCE Team to choose one (either the easiest path for the adversary, or one that highlights a "blind spot" of unverified trust). It will be easy to get bogged down with all the different pathways, but it is important to focus on the most plausible pathway to discover critical choke points. In the case of extremely well-resourced adversaries, like nation-states, Access can be achieved in a variety of ways. These can include network-based, human-enabled, and supply chain methods. Keep in mind people can be either wittingly or unwittingly involved in the adversary's Technical Approach.

Actions are the conditions or steps that need to be accomplished to cause the HCE. This includes what conditions need to be met to initiate the payload, as well as what the payload actions will be once initiated. This can be anything from manipulating a control valve, opening a breaker, "spoofing" a value on a human machine interface (HMI), installing malware, escalating privileges, or even having an insider insert a USB drive into the targeted system.

Timing refers to both the *order of operations* and *sequence* of an attack, as well as the actual or "machine cycle" time in which steps must occur during an attack. These steps may be taken to avoid detection or to achieve maximum damage. The details of the timing depend on the objective of the attack.

Triggering is *how* a payload is activated, and it is always tailor-made to the process or target. Attacks are most often initiated one of two ways. They can be initiated by an attacker who is interfacing with a system or device in real time or, alternatively, by an agent operating on behalf of the attacker. These agents, also known as smart triggers, can be programmed to initiate attacks at various predetermined and defined points. The simplest triggers, and arguably not smart at all, execute a payload code based on a specific date or time input. Historically, these have been referred to as logic bombs.

TYPES OF TRIGGERS

More complex trigger designs can be used, such as conditional or process state triggers. The first trigger type, **conditional trigger**, is a trigger that initiates sections of code based on predefined and programmed requirements within the trigger's logic. For example, a trigger may "arm" the payload, but it may not proceed to the next stage of an attack until a "go" signal has been received. In this case the condition is whether the "go" signal has been received.

State triggers make up the second type of triggers. State triggers initiate the attack when the target process reaches a required state. State triggers are designed around manipulating a process. As previously highlighted, these triggers are always tailor-made to the specific component and process (they cannot be applied to a similar target without code modifications) and may require subject matter expertise to design.

Keep in mind that Triggering and Timing may occur in parallel, but this is not always the case. Adversaries may choose to trigger different parts of an attack at different times or at the same time.

Target Details

The Target Details is the section that describes the operating position(s) for a cyber-attacker; it is the "where" in the question. Where does an adversary need to be to control and execute the attack?

In some cases, it may be possible for a cyber-attacker to operate from multiple locations. For example, an adversary seeking to target electric distribution infrastructure with the effect of causing an outage may be able to attack a utility from the regional distribution management system (DMS) level. This was the case during the December 2015 attacks in Ukraine. Or, they may be able to target equipment in the substation (such as a remote terminal unit [RTU]) to be effective in causing an outage from the field device level.

If the Technical Approach is thought of as the requirements for a hacker to develop the payload, the Target Details describe the software and hardware platforms (e.g., device component, system process, memory module, programmable chip, logic circuit) that will be exploited or manipulated to implement the requirements. An adversary's terminal goal is achieved by the compromise of the items described in the Target Details via the Technical Approach and payload Deployment. The details an adversary would need about each individual Target to accomplish their goal is included in this section: make, model, software, firmware, configuration files, vendor, function, model, operating system, and protocols.

It is helpful to clearly delineate these Target Details because it may be possible to disrupt adversary activity at these nodes. In some cases, reengineered solutions, additional security measures, or improved procedures may limit the attack progression or make a target too expensive (in terms of time, money, or resources). This lessens the target's "attractiveness."

Critical Needs

Critical Needs are key pieces of data (information, equipment, or software) an adversary must acquire in order to successfully sabotage a system. By identifying this data, the CCE Team determines information that can serve as indicators or tripwires of adversary activity. These Critical Needs should be documented. Be sure to include a list of the key documents, each document's location(s), and all the personnel who have access to it. Even if a key piece of information is out of the control of the organization, that should be documented. It is important to document everything so unverified trust can be identified and addressed.

One thing to keep in mind is a Critical Need can be more than a document. Critical Needs can be pieces of equipment the adversary acquires to reverse-engineer. This allows the adversary to know exactly what will occur if the payload is triggered. It can also be crucial information that is needed. Key questions to answer:

- What you need?
- Where you can get it?
- Who has access?

Development of the Payload

Critical Needs for Development include all the information, equipment, and software needed to develop a payload. The payload is the mechanism an adversary will use to maliciously manipulate or attack a system to cause the HCE. Often, the payload is designed to target the basic functions of a system and render these functions unavailable, or maliciously use available design features.

The goal of payload Development—and its corresponding cyber-attack—is a physical effect accomplished via cyber means. In contrast to many (if not all) information technology (IT)-centric attacks, a cyber-physical attack is directed against the base functions of a system, instead of access to sensitive information. For example, adversaries targeting the wicket gate of a hydro generation station may be successful in limiting or stopping the flow of water through a dam, thereby limiting the generation output of the site.

Adversaries interested in designing payloads to sabotage physical systems need a detailed level of understanding of the target process to manipulate it for disruptive purposes. Because of the additional knowledge required, engineering design documents and other technical specifications will be a key element of the targeting process. Another exceptionally useful source of information is mechanical failure analysis or similar documentation; this information can provide valuable insight for the adversary seeking to achieve damaging or destructive attacks via cyber means.

Reid Wightman illustrated the usefulness of these design specifications when he identified a common vulnerability in a key engineering component. Wightman designed a hypothetical attack against a variable frequency drive (VFD) by rewriting the skip frequency[3] so that dangerous conditions would be obtained by the VFD during operation.[a] Wightman also noted that in many cases the skip frequency field was read/writable, allowing for potential malicious alteration by an adversary.

Deployment of the Payload

Critical Needs for Deployment of the payload include the pieces of critical information the adversary needs to deliver the payload to the intended location. Delivery of the payload often requires different accesses than those that were used during payload Development. Other considerations include the desired scale of the attack and how many systems will need to be sabotaged to achieve the HCE.

For example, if an adversary wants to affect an entire fleet of ships—and not just one ship—the Critical Needs for Deployment will be different. They will need to figure out how to deploy their payload to all the ships and not just one. This may be achievable through the supply chain. If the entire fleet relies on one common vendor for a target component, the adversary may only need to interrupt the supply chain in one location. However, if the ships used different suppliers for the target component, the Deployment may require access to the supply chain in more than just one location.

Documentation and Reporting

Each Attack Scenario should be drafted with the key collected information summarized in the System Targeting Description. This will help inform a thorough and knowledgeable presentation for the company's C-Suite. Being able to translate targeting information into their language (risk, cost, efficacy, consequence, etc.) will help them understand the risk to their business, generate their buy in, and facilitate the implementation of mitigations in Phase 4.

Outputs and Next Steps

The output of Phase 3 and input to Phase 4 are fully developed Attack Scenarios that can accomplish the HCE and a fully documented and referenced System Targeting Description. Each identified Attack Scenario will include:

- Technical Approach with the requirements for each target including the Access to the target, the Actions needed to be taken, and the Timing and Triggering of the payload.
- Target Details which describe the technical details of each target that will be exploited or manipulated in order to implement the requirements from the Technical Approach.
- Critical Needs, which describe what an adversary requires (information, access, components, software, etc.) for both payload Development and Deployment, including the "easiest" place to obtain them.

With all the Attack Scenario details and choke points compiled into a Phase 3 summary document, the CCE Team can use them in Phase 4 to articulate specific mitigations and protections to secure those choke points.

[3] A skip frequency is a designated frequency for a specific piece of equipment at which unsafe vibrations and other damage can occur.

See Idaho National Laboratory's document titled "CCE Case Study: Ukraine Substation Power Outage" (INL-EXT-20-58092) for more Phase 3 examples on defining Attack Scenarios, creating a System Targeting Description, and developing Critical Needs.

[a] Zetter, Kim. "An Easy Way for Hackers to Remotely Burn Industrial Motors." Wired Magazine, January 12, 2016, https://www.wired.com/2016/01/an-easy-way-for-hackers-to-remotely-burn-industrial-motors/.