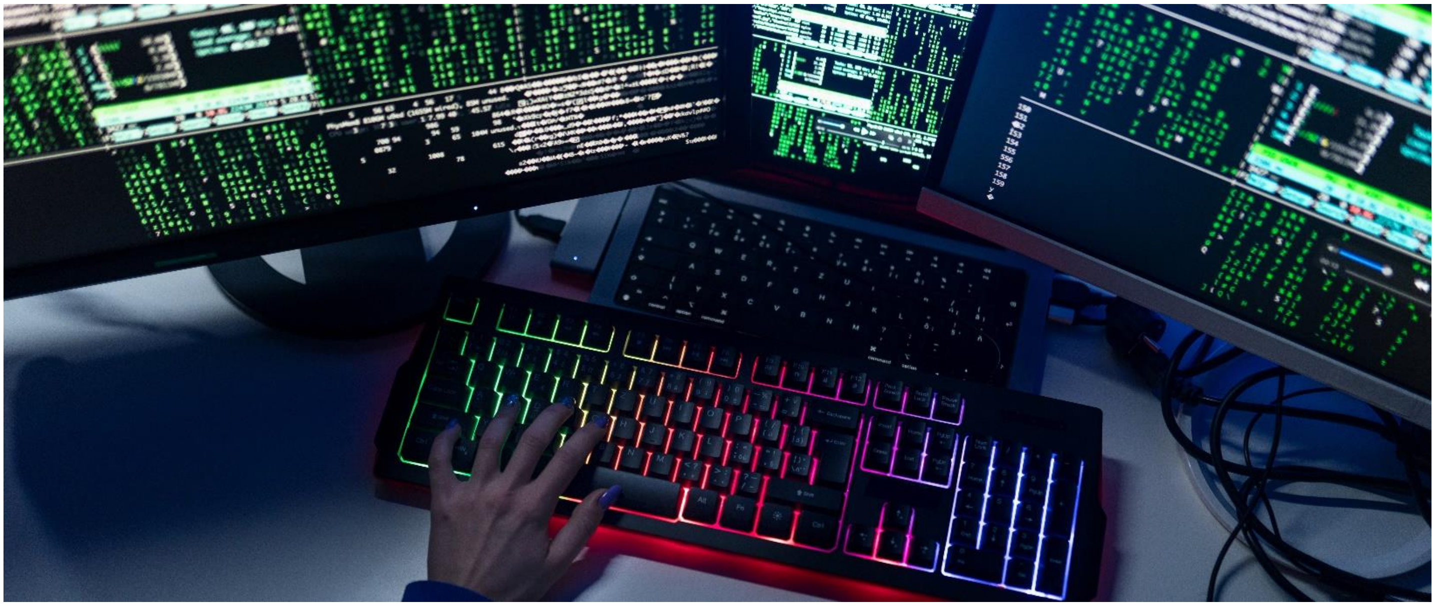
CYBERSECURITY RPG

• BLUE TEAM •

WARGAMING FRAMEWORK



DEFEND NETWORKS AGAINST ATTACK

– CONTENTS –

CYBERSECURITY RPG

• BLUE TEAM •

The blue team cybersecurity role playing game (RPG) is designed to facilitate defensive security assessment and learning about defensive cybersecurity technologies. Blue team cybersecurity role playing game (CRPG) is a tabletop roleplaying game that, unlike some tabletop exercises, aims for balance between attacker and defensive actions. The goal is to provide a realistic environment to consider organizational risks and learn about cybersecurity techniques within.

[I. Introduction]

A number of games related to cybersecurity exist. These include cyber competitions, card games and even escape rooms. In many cases, these games are designed to impart a message (such as showing organizational leaders that more investment into cybersecurity is needed). Some other games have educational purposes or seek to prompt organizational thoughts about areas of risk.

In spite of all of this, there are few mechanisms that show IT professionals, students, managers and others how to assemble the components of a defensive security program and operate them. This systems-level thinking is critical – and learning about processes, technologies and techniques in isolation doesn't produce it.

Exercises for organizational assessment and preparation have a different, but somewhat related problem: they need to be accurate, as opposed to beginning with an end message in mind. Not only are unrealistic games unhelpful for determining whether more resources are needed (and even more unhelpful for assessing where they should be devoted to), they are also not useful for planning or threat assessment purposes.

CRPG is designed to be a solution to these problems. It is a fun and balanced game that pits blue team defenders (the players) against red team attackers, who are played by the incident master (IM). It is designed to simulate cybersecurity systems and to do so accurately, to facilitate assessment, planning and learning.

The remainder of this chapter discusses the basics of CRPG. An overview of the game is provided and the dice required for it are briefly discussed. Following this, the roles within the game and possible modes of play are discussed. Subsequent chapters will provide more details on how individual parts of the game are played and describe the techniques that can be used by the player-defenders and IM controlled-attackers.

| The Game

To play CRPG, an incident master (IM) creates (or uses a pre-created) scenario. Players create (or use pre-created) characters to play that scenario. The players also establish a turn order.

Then the game begins. Typically, the game will start with the IM describing the current situation. Gameplay uses a turn-based protocol and continues until the red team has accomplished its goal, as set by the IM, or is prevented from doing so. In some cases, games may be time-limited – either by the nature of the scenario or players' availability.

| Dice

The only dice needed to play *CRPG* are a four-sided die (referred to as a d4), a six-sided die (referred to as a d6) and a twenty-sided die, (referred to as a d20). Each player should have their own dice to speed up gameplay.

| Roles

Players take one of two roles: incident master or blue team member. The incident master (IM) takes the place of a game master in a tabletop role playing game. The rest of the players will make up the blue team. For the rest of the document, the term "players" will refer to the members of the blue team. In cybersecurity, the term blue team refers to a defensive team which is attempting to protect a network or system. The IM takes the lead and establishes a scenario for the players to then participate in. With this, the game begins.

[INCIDENT MANAGER]

The IM is responsible for setting the scene for the blue team. To fulfill this role, the IM has constant access to all relevant information. Primarily, this means that they possess information regarding the entire network in question as well as all relevant details surrounding the target facility and personnel.

All rules described within this document are subject to the decisions of the IM. These rules provide guidelines for the IM to follow so that a realistic attack can be simulated, but complete adherence to the rules outlined here is not strictly necessary. For example, if the rules dictate that a certain network change should be hidden from the players, but the IM would like them to have access, then that access can be provided.

Additionally, because of the freedom allowed to the players in deciding what actions they will take, it is impossible to describe how to handle every possible scenario that players will encounter. In any scenario not described by this document, the IM is the final authority and must decide what will take place. The role of IM is the most critical role as they are the one who guides the blue team through a realistic attack simulation. A knowledgeable IM is preferable for a smooth playing experience. Typically, the IM should be the most knowledgeable participant.

[BLUE TEAM]

The blue team is the team of players that are protecting a computing system or network. At the beginning of the game, the players will, thus, have a good knowledge of the configuration and state of the network; however, as the red team makes changes to it, during their attack, the players' knowledge will become more limited. For example, the blue team will only have access to the visualization of network devices in the state that they last interacted with them in. Players' knowledge of facilities and any threats is provided at the discretion of the IM or as dictated by the game scenario.

Once the IM has described the current situation, the players have access to and the background information of the scenario, the players take turns doing actions. These include physical movement and performing the techniques described in Chapter VII.

| Modes of Play

This document describes the mode of play where the incident manager plays the red team and other players take the roles of blue team members. See Chapter X for details about other modes of play.

[II. Network]

Networks are integral to CRPG gameplay. This section discusses network nodes' properties, such as their security modifiers, access levels and services.

| Network Nodes

The players are provided a visual representation of the network they are defending. Each computer or network device is represented by a node, which defines the characteristics of the device. Nodes are also linked to other nodes to represent network connections between computers. A node's characteristics include its access level, security modifier, and any running services.

Defenders will typically be given a network diagram that accurately depicts the network at the start of the game, while the IM should simulate the red team having to explore it. Over time, the players' understanding of the network may grow inaccurate due to red team activities.

| Security Modifier

One of the characteristics of each network device is its security modifier. This value represents the security measures a computer or device has, such as a device firewall and antivirus software.

When a player rolls a skill check in order to perform a technique, the security modifier is *subtracted* from the roll value to reflect this. The security modifier is available to players as relevant. The security modifier can range from -3 to +3.

Positive levels indicate a higher penalty and, thus, better security measures. Negative levels indicate an insecure node. Because the modifier value is subtracted, a negative value provides an addition to the skill check value. The security modifier for each node is determined by the IM when developing a scenario.

| Access Levels

Access levels (ALs) represent the extent to which a computer or network device is accessible by attackers and defenders / IT personnel. The AL is comprised of two parts: a number and a letter.

For the numeric component, the levels are on an ascending numeric scale. Red team members receive the benefit from all levels below the current AL of a node. For example, having admin access also provides the required access for any technique requiring the user, traffic, or secure levels. The access level is readily available to players.

The following are descriptions of each level:

0–Secure: The target node is not accessible by the red team. They can only view it and use limited techniques.

1–Filtered Traffic: The red team can send some types of traffic through the node, but have no access permissions and not all traffic will be allowed through. This access level is provided by filtering devices such as firewalls. The IM should identify the types of traffic allowed and disallowed when designing the network. When traffic is sent through the device, the IM should roll to determine if traffic is allowed and for attack detection.

2–Traffic: The red team can send traffic through the target node but have no device access permissions.

3–User: The red team has user level account permissions on the target node (and can therefore run some attacks), but cannot make system wide changes.

4–Restricted Admin: The red team has access to a limited-purpose administrative account on the system with limited permissions which are defined by the IM.

5–Admin: The red team has admin account permissions on the target and can make system wide changes. Little functionality remains out of reach.

6–Kernel: The red team has direct kernel access and can change anything they want on the target. This level is difficult to reach and very few techniques require it. The players can attempt to make custom changes using this access level.

The letter component indicates whether existing user accounts are still valid on the device and, thus, whether blue team members still have access to it. Six letters are used:

N – Normal access available: All user accounts still work and have their normal permission levels.

A – Admin accounts unavailable: User accounts are still accessible but admin accounts have been disabled, deleted or had their passwords changed.

U – User accounts unavailable: All accounts are unavailable due to having been disabled, deleted or having their passwords changed.

R – Random accounts unavailable: Some accounts are unavailable or have degraded permissions. Roll >3 on a d6 for access to an account. Roll >2 on a d6 for administrative permissions to be retained on an account that is accessible.

D – Degraded administrative accounts: Administrative accounts are available but only have user-level permissions.

T – Targeted: The attackers have taken specific actions beyond those described above.

|Services

Each node can have one or more services associated with it that represent the running programs or uses of a target. Most techniques require certain services in order to be performed. Some services are specific protocols used in the real world while others are abstractions of types of common programs. There is no limit to how many services a node can have except that nodes cannot have two instances of the same service. The IM determines whether a service can logically run on a specific node. Scenarios will typically include predetermined services running on network nodes.

[LIST OF SERVICES]

Web Server

Computer software which uses protocols like HTTP and HTTPS to respond to client requests. This service stores, processes, and delivers information or webpages to the user.

Email Server

Computer server software for sending and receiving emails. It ensures that emails reach their recipients, acting as a virtual post office.

Database Server

Computer software that houses and maintains database files as well as provides access to it. Provides clients with access to data over a network.

DNS Name Server

The domain name system (DNS) and its protocols are run on this server. It is able to translate domain names into internet protocol (IP) addresses following a DNS query.

Hypervisor

Computer software which is used to create, run, monitor, and manage virtual machines on a server.

SSH

Secure shell (SSH) is a network communications protocol used to operate network services (remote access and communication between computers, for example) securely over an unsecured network.

FTP

The file transfer protocol (FTP) is a communication protocol used to transfer files between computers over a network.

Telnet

A network protocol used to log into another computer on the same network. It provides a communications interface with the remote device.

RDP

The remote desktop protocol (RDP) creates secure remote connection between clients and workstations or servers (including virtual machines). Users are able to remotely access and control physical and virtual devices through a graphical interface.

RPC

Remote procedure call (RPC) is used by a client to request (call) processes on a remote server.

Proxy Services

A proxy service is an intermediary application between a client and server. It retrieves data from the server on the client's behalf using its own IP address. It may filter requests or responses to them.

REDIS Database

Remote dictionary server (REDIS) is a key-value database for housing data structures. Its in-memory cache and quick response time makes it popular for storing and managing data.

Remote Config

A remote management mechanism that is present on a device allowing a system administrator to configure it remotely.

VoIP

A service that allows users to make and receive telephone calls over TCP/IP networks.

DHCP

The dynamic host configuration protocol. Provides IP addresses, gateway, DNS and other information to clients.

[III. Setup]

This chapter describes how an incident master prepares to run an *CRPG* game and the steps that players take to prepare to play it.

| Designing the Scenario

The first job of the IM is to design or model an existing network and/or organization facility and prepare the scenario. As IM, it is important to have a clear vision of what the scenario consists of before gameplay begins. It is wise to have a solid understanding of the network model and all relevant characteristics of the target. There should also be a goal for the players to accomplish. Typically, for blue team members, this goal will be to protect the network from a red team attack. This goal should be defined in terms of a duration and the types of attacks the IM expects to deliver to the players.

In Chapter II, we covered the parts of the network and how they work. The following sections discuss how to create a network that can be used to run a successful game.

[OBJECTIVE]

Each scenario should have an objective. Typically, this objective will affect the model network in some way. In most cases, the goal of the blue team / players will be resisting and responding to the attack of the red team, as played by the IM. This can be done through preparation, response and recovery activities. In some cases, a scenario may include multiple periods of attack interspersed by non-attack periods.

The red team attackers may have a goal. For example, they may be seeking to exfiltrate data from the defenders' computers. This goal could be something that could be satisfied through a single attack or it could be something that requires disablement of certain functionality for a period of time – or something else.

In many cases, the IM will tell the players the goal of the scenario as part of their initial briefing. However, this could, at the option of the IM, be incomplete or change. Additionally, the scenario briefing could describe the need to resist attackers, in general, without describing the specific threats that the players are expected to face and their rationale.

Some scenarios may seek to test the defenses of real-world networks. Others may seek to model real-world phenomena of other types. Yet others may have educational or analysis goals.

[NETWORK SECURITY]

One key decision that the IM (or scenario designer) must make is what level of security that the network that the blue team is defending should have. While players will, typically, have a short amount of time to (hopefully) enhance the network's security, most of the security (or insecurity) of the network will be based on IM (or scenario designer) decisions.

When modeling a real-world network for testing, the decisions are simple, as the goal is to replicate the actual network to the greatest extent possible. For instructional or other scenarios, the level of network security is a key IM/scenario designer consideration.

[FIREWALLS AND ROUTERS]

Firewalls and routers play an important role within enterprise networks. They also have an important role in gameplay. Firewalls can act as a first line of defense against some red team activities and both firewalls and routers can limit what information the attacking red team can access.

When defining the scenario, the IM (or scenario designer) will need to ensure that (at least approximate) firewall and routing rules are developed. Players may wish to modify these rules during the preparation, operations or attack and response phases. The IM will need to take note of the impact of the initial rules and any modifications on red team attacks. Additionally, to simulate advanced firewall features, such as artificial intelligence, the IM may wish to roll for attack detection and blocking against red team attacks that would otherwise pass through the operational ruleset.

Firewall and routing rules can be defined in the technical manner that they would actually be implemented within the actual devices. They can also be defined in terms of particular attacks that work (or don't work) through a device or in terms of ports and protocols that are open. The IM should also determine (and track player and red team-produced changes to) what network or networks the firewall or router's management interface is available from.

[ATTACK PATHS & SYSTEM FUNCTIONALITY]

The IM will want to ensure that the players do not impair the scenario through denying attack paths in an unrealistic way. Specifically, the IM should ensure that the system is required to remain functional throughout any changes that are made by the players during the preparation and operations phases. Changes that break this functionality may change a scenario to initially focus on having to repair this, due to IM-supplied user complaints.

When using CRPG to simulate actual networks, this required functionality should be defined based on actual organizational requirements. When developing a scenario for learning or analysis purposes, the IM will want to use functional requirements to ensure that key elements of the scenario can be carried out. Of course, care should be taken, in these cases, to ensure that the operational requirements are realistic, make sense and don't make the scenario impossible or unintentionally more difficult for the players.

[NETWORK SIZE]

Whether simulating a real-world network or developing a network for instructional or analysis purposes, network size is a key consideration as it will impact how long a simulation takes. Real-world elements and player decisions also have a key role in duration, as well, so network size to time correlation is imprecise. That being said, a network with 3 to 5 subnets with about 4 to 8 nodes in each subnet will take about an hour to play, in network mode. The complexity of the network, the number of red team attacks, attack effectiveness and the players' luck with die roles will all impact upon this. Note that time may increase at a greater-than-proportionate rate, as networks expand, due to the increased complexity. Because of this, 20-30 nodes is a good size for many simulations.

Each node is a type of networking or network-connected device. The services that are running on the device (which provide requisite organizational functionality and present the targets for the red team to attack) depend on the device's type and role within the network. These are discussed in a later chapter. IMs should also feel free to create their own device types and services to model real-world networks or fit their scenarios, if desired. In doing this, it is important to be realistic and to ensure that they are designed to be proportionate to the network devices discussed herein.

| Creating a Character

The first step for a blue team player is creating a character. In the network game mode, characters have a set of skills. While other TTRPGs include characteristics inventory, character names, and appearance, purely network gameplay only cares about a character's skills. Other characteristics are used in the physical game mode.

[SELECT ROLE]

The role of a character describes their skillset, gained through education and experience. Certain techniques can only be carried out by individuals of certain roles. Other techniques have a positive or negative modifier, depending on the role of the character that is attempting to perform it. This manual only covers the role of blue team members and all techniques presented include the applicable modifiers for blue team members.

[ASSIGN SKILL POINTS]

Each player has a set of eight skills. Six of these are primary skills that relate to the ability to perform a particular type of technique: preparation (PRP), vulnerability identification (VI), network reconfiguration (NR), attack detection (AD), cleanup (CU), communications (COM) and organizational response (OR). One score, other (OTH), is computed based on other scores. Characters' scores can be assigned as part of scenario development or based upon characters' levels.

If characters will be manually created, the six primary scores each start at -2 and can be increased by players applying points to them.

As a general rule, beginner-level characters should start with 12 points that they can use to increase scores. Intermediate-level characters should receive 15 points and advanced should receive 18 points. The number of skill points available, in a given instance, is selected by the IM during scenario creation.

Each point adds 1 to the score up to a maximum of +3. Thus, each player has seven skill scores ranging from -2 to +3. For example, a character could have skills of: PRP:-1, VI:+1, NR:+2, AD:+2, COM:-2 and OR: +1.

The OTH score is calculated by averaging all six of the primary scores. If averages result in a fraction, this is rounded down.

The more skill points assigned to it, the more proficient the player is at executing a skill's techniques. The skill scores modify the probability of success for a technique of a certain skill, so it can be important to have well rounded skills and a well-rounded team. Players should write down and label all eight skill scores for reference during gameplay.

[CHARACTER LEVEL]

The level indicates the experience and skill level of the character. The incident master should inform players of the levels of character that they can create, based on the scenario that they will be playing. Characters can be beginners, intermediate or advanced.

A character's level defines the number of technique skills that a character knows and can perform. The skill points allowed by the IM should also be proportional to the characters' level.

[CHOOSE TECHNIQUE SKILLS]

Since not everyone knows how to do everything, characters must identify the techniques that they know. Techniques are categorized and also characterized as trivial (T), simple (S), moderate (M), difficult (D) or very difficult (VD). The techniques that a character knows and can use is determined by the character's level.

Beginners:

- Trivial techniques in all categories
- All moderate and simple techniques in one (primary) category
- All simple techniques in a second (secondary) category
- 3 additional technique points

Intermediate:

- Trivial and simple techniques in all categories
- All difficult, moderate and simple techniques in one (primary) category
- All moderate and simple techniques in two more (secondary) categories
- 6 additional technique points

Advanced:

- Trivial, simple and moderate techniques in all categories
- All very difficult, difficult, moderate and simple techniques in one (primary) category
- All difficult, moderate and simple techniques in three more (secondary) categories
- 9 additional technique points

A character's primary category is the one that they have the highest modifier for. Their secondary category or categories are the ones that they have the next highest modifiers for (e.g., an advanced character would have the category with their highest modifier as their primary category and the categories with the next three highest modifiers as their secondary categories).

Note that techniques marked as specialty (e.g., S-S, M-S, D-S or VD-S) are not learned automatically with any category but must be learned using additional technique points (ATPs). ATPs can also be used to learn techniques outside the entitlements from a character's level and categories of primary and secondary specialty. ATP costs are as follows:

Level	ATP Cost
Simple	1
Moderate	2
Difficult	3
Very Difficult	4

Characters can also attempt to perform a technique that they have not learned; however, a time and success penalty are assessed, as listed below.

Level	Time	Modifier
Simple	6	-2
Moderate	12	-3
Difficult	18	-4
Very Difficult	24	-5

The time cost must be expended before the technique can be attempted, each time. The modifier is applied to the success roll for the technique. Note that this presumes that the character has internet or another suitable reference to use in learning a technique. The IM can disallow the use of a non-learned technique, increase the time required or increase the modifier if reference material is not available.

[CHOOSE GEAR]

Characters need gear to perform certain techniques. Gear is described in Chapter IX and techniques indicate what gear they need, if gear is required, when they are presented. Gear can be held or carried in characters' pockets.

Gear has weight and size, which define how it can be carried. As this system does not deal with the physical capabilities of characters, it is presumed that characters can carry no more than 50 pounds of total gear, no more than 20 pounds per hand, and no more than 3 pounds per pocket. Characters are able to carry two very small (VS) or one small (S) or medium (M) item per hand. They can carry up to four VS items or one S item per pocket. Carrying a large (L) item requires both hands. Interactions with very large (VL) items are described in the item description. Some items can carry other items and their description describes what they can carry.

Software is a type of gear that requires no weight or physical space to carry. Instead, it requires a device with software storage space. Software is defined in terms of the electronic storage (ES) space required to store it. Devices that provide electronic storage indicate how much they can store.

Electronic storage may be important to track and manage for campaigns that involve large amounts of backed up data or if the IM wants to limit the amount of different types of software or data that players have access to. In many cases, though, electronic storage can be disregarded, if it is not critical to the campaign.

[IV. PLAYING THE GAME]

With characters created and the network planned out, you are ready to play. This chapter breaks down how the game is played.

| GAME PHASES

To model the activities of information technology and defensive security personnel, the game includes periods prior to attack and an attack period. At the IM's option, the pre-attack period can be very short (or non-existent). Additionally, the game can cycle through multiple periods of attack and non-attack.

To model this, CRPG includes three phases. The ***preparation phase*** is a short optional (at the IM's discretion) period at the beginning of the game where the players can make changes to their network's beginning state. The IM will typically limit how much time can be spent during this phase, if including it in a scenario. The ***operations phase*** represents normal network operations when not under attack. Notably, players must detect an attack, so they may believe they are in the operations phase while an attack has commenced. Finally, the ***attack and response phase*** is where the blue team players attempt to prevent, counter and respond to attack from the red team.

It is important to note that while some techniques are only relevant during the attack and response phase, most techniques that can be performed during the preparation phase can be conducted during the following phases. Also, most operations phase techniques can be performed during the attack and response phase. However, while performing techniques during what they believe is the operations phase, the blue team runs the risk that they are already under attack and that they may be aiding the attackers. Techniques performed while under attack must be assessed to see what opportunities they may provide the attackers such as to see if they may aid in spreading malware.

[PREPARATION PHASE]

The preparation phase is designed to give the players an opportunity to modify the network that they will be defending to better align with their network management and configuration approaches and their defense strategy. Basically, this phase represents the actions that IT and defensive professionals would have taken over an extended period of time prior to an attack beginning. It is, unlike the other parts of the game, not tied to specific rounds of time.

During this phase, the IM should provide the players with a pool of system time (ST) and human time (HT) units that they can spend on preparation. This pool is provided to the players as a group and they should agree on how it is spent. Notably, this phase may not be included (or may be very short) for scenarios that model existing networks (as allowing the players to change the network would defeat the point of the scenario).

The IM may apply other scenario-specific restrictions on this phase, such as disallowing changes to some areas of the network, for operational or functional reasons relevant to the scenario. The IM could also limit the techniques available to the blue team. Because of the timelessness of this period, skill checks are not generally needed. However, the IM may still require a skill check (potentially with a modifier applied) for unlikely or risky actions. All changes are also subject to the feasibility assessment and agreement of the IM.

During this phase, the players don't need to worry about a concurrent red team attack; however, the IM could prospectively start a scenario with a long-term red team compromise's persistence mechanism pre-existing on the network.

[OPERATIONS PHASE]

The operations phase represents normal network operations. In some scenarios, this phase may be important to validating that changes made by the players during the preparation phase are functional (and the IM, in the role of users or organization management, may require changes to the network, if they are not). During this phase, the IM may make typical requests of the blue team related to ongoing operations.

At some point during the operations phase, the game will switch into the attack and response phase, when the red team's attack commences. A key aspect of CRPG is that players must detect the attack in order to begin to combat it. The players may think that they are in the operations phase while the attack and response phase has commenced. Thus, the players will want to conduct activities during this phase to attempt to detect the any activities of an attacker. The speed at which the blue team detects an attack may have a pronounced impact on how successful the red team may be.

The IM may provide the blue team with indirect information about red team activities in the form of user reports or requests. For example, what appears to be a typical password reset due to a user forgetting a password may actually be an outcome of a red team compromise.

It is important to note that the blue team can make longer-term changes during the operations phase, similar to or building on those that are made in the preparation phase. This may be the only time to make these changes, if a scenario doesn't include a preparation phase or the preparation phase isn't long enough for the players to make all of their targeted changes. However, the network may be under attack during this time, so the IM should consider what opportunities the change-making process may provide to the red team and if it may spread malware or other effects of an attack.

[ATTACK & RESPONSE PHASE]

The attack and response phase begins when the IM decides (potentially based on scenario plans or an arbitrary decision) that the red team's attack has commenced. Of course, the IM may decide that the attack and response phase has commenced while the blue team still believes they are in the operations phase.

During the attack and response phase, the IM simulates red team attacks using the techniques specified for red team actions in Chapter VIII. The players can take actions as specified in Chapter VII to detect, prepare for or respond to the red team activities.

This phase continues until the red team attack stops. This could be because the red team has been successful in achieving their objective, due to an arbitrary or scenario-based decision of the IM, or because the blue team has been effective in preventing the red team from having the ongoing access to the network that they need to complete their objective.

[ITERATION]

In some cases, the game may end at the end of the attack and response phase. However, other games may include multiple phases of operations and attack and response. As the players don't know for sure whether they are in the operations phase or attack and response phase at any given time, this distinction is primarily for the IM.

Games may include iterations of operations and attack and defense phases to simulate longer-term attack strategies or as part of other scenario design goals. As the blue team's goal is always to defend the network, the IM may want to set expectations regarding the length of the scenario at the beginning; however, this may or may not include defining specific duration conditions, such as specifying that the blue team would need to defend against a single red team attack or for a specific period of time.

| Turns and Initiative Rolls

CRPG is split up into rounds. A round consists of the IM taking red team actions and every player taking their turn. During each turn, players have six human time units to spend which correspond to approximately six 10-second periods of human action. Everything happening during each round is considered to be happening at the same time.

The IM's period for red team actions is always at the top of the turn order. They can use attack points to any desired take red team actions, which are described later in the section.

After this, players take their turns. After all players have taken a turn, the attack points pool is increased, as described below.

[PLAYER TURN ORDER]

To facilitate smooth game play, a turn order is determined at the beginning of the game and is used throughout the game, as needed. In many cases, the turn order will provide a convenient order to poll players for their characters' actions each turn. However, because all turns are concurrent in game universe-time, there is no reason why turn order must be maintained.

To determine the turn order, each blue team player rolls a d20. The turn order is determined by the rolls of the players from highest to lowest. Ties are broken by a reroll to find who, among those tied, goes before to the other.

In some games, it may make sense to ignore turn order and let players take their turns in any order desired. Players should also feel free to swap turns, defer their turn to the end of the round or 'cut in line' (with the IM and other players' consent) and take their turn early. Generally, players who are collaborating should describe their actions and take their turn at the same time or consecutively, to facilitate the implementation of the collaboration and interaction rules which are described in the next section.

[CHARACTER COLLABORATION & INTERACTION]

In some cases, players may wish for their characters to collaborate on a task or interact with each other or each other's equipment. Ideally, collaborative activities should be announced at the beginning of the first participating player's turn. However, they could, potentially, be announced later on.

As turns represent concurrent periods of time, player collaboration should be assessed for feasibility within this context. For example, results from a scan or attack that took one player five human time units to setup couldn't be available to another player at the start of their turn during the same round. The location of the characters and any required gear should also be considered. Gear being used by one character would not (typically) be available for use by other characters at the same time.

In addition to addressing concurrency considerations, a requested collaboration should be reasonable in terms of the characters having an in-universe way to communicate or interact, as required. Time for coordinating the collaboration should also be allowed. At a minimum, one human time unit should be used, from each participating player, for coordination; however, more may be required for complex actions or activities. An activity that crosses multiple rounds would not need to be assessed a coordination cost each round, unless coordination was required during that round.

[NETWORK & WORLD CHANGES]

Because turn activities are concurrent, typically all changes to the network (and any real-world object changes) can be taken to take effect at the beginning of the next round. This includes both red team and blue team activities. This approach simplifies tracking of when changes occur.

In some cases, though, more granularity will be needed. For example, a player that takes one action to prepare for the next shouldn't need to wait for the beginning of the next turn to do the second action if they have enough human time units to do it in a single round. Similarly, more granularity may be needed for the activities of collaborating players. In these cases, the IM can track how many human time units are consumed by an activity and make its results available to others at this point during the turn.

When using points-based red team actions, these always take effect at the beginning of the next turn.

| Rolling Skill Checks

When players want to take an action, they pick a technique and roll a corresponding skill check. The player rolling the skill check rolls a d20. Then they add their corresponding skill score. The total is the result of the skill check. Depending on the difficulty value (DV) of the technique the player is rolling for, the check can result in a success, stall, or failure.

For example, if a player is asked to make a COM skill check, the player rolls a d20 and adds their COM skill modifier to the value. A roll of 12 and a modifier of +2 results in an end score of 14.

Some techniques (discussed later) also include a critical success or critical failure. A critical success is when the d20 rolls a 20 before modifiers. A critical failure is when the d20 rolls a 1 before modifiers. A critical success automatically succeeds and a critical failure automatically fails. Effects specified in the techs for a critical success or critical failure override the normal effects.

If the rolled skill check value is equal to or greater than the difficulty value, the skill check succeeds. If the value is less than the difficulty value but above the failure value, the skill check results in a stall. If the value is less than the failure value, the technique fails. The difference between stalling and failing is explained in the next section and the results of techniques stalling and failing are described in the technique descriptions.

| Techniques

Actions that can be performed by the players are called techniques. Each technique is associated with one of the character's skills. When rolling a skill check to use a tech, add the character's associated skill modifier to the roll and subtract the security modifier. A list of all techniques and their characteristics can be found in Chapter VII.

Before attempting to perform a technique, it is important to review the technique's description. When the player initiates the technique they then make a skill check. The skill check that the player makes depends on the category of the technique. For example, if a technique was part of the communications category, the player would make a COM check. To do this, the player rolls a d20 and adds their modifier to this. For example, if the payer rolled a 13 and had a COM modifier of +2, their total would be 15. If that is equal to or higher than the tech's DV, it would succeed and the benefit of the technique would be enjoyed.

If the player does not roll high enough to succeed, the technique either stalls or fails. Rolling under the fail value (FV) of the technique results in a failure. Stalling occurs if the player rolls a value between the success and failure values. Stalling usually means that an action is wasted and nothing happens, unless otherwise indicated for a particular technique. Failing often has a negative effect. Both are described in the technique description.

| Role of the Incident Master

The incident master performs a key role within the game. They keep the story moving and keep the players engaged. They are also responsible for determining whether players' actions are successful or not. To do this, they use a difficulty level system and dice rolls.

[DIFFICULTY LEVEL SYSTEM]

Techniques' difficulty levels determine how likely they are to succeed or fail. They are defined for each technique. They can also be modified by circumstance, such as a characteristic of a node that makes it more or less susceptible to a particular technique being performed. They can also be modified by the IM, to improve gameplay and enhance realism.

As with anything else in this document, this difficulty level system can be adapted, modified or ignored by the IM. For example, if the IM would prefer to have a skill check be a bit easier or more challenging they can require a lower or higher roll, respectively.

The reason for having this system of difficulty is simply to provide the IM with consistent values to quickly reference when having a player make a skill check. It functions to allow an IM to decide if an action would be relatively easy or hard to successfully perform, or if an average IT staffer would have a reasonable level of success, without feeling the skill check represents anything that is particularly easy or challenging.

The IM is welcome to adapt the values as needed. The IM can also entirely use values that they determine on their own for each skill check. This is acceptable as long as the IM can maintain consistency with these values.

In any case it is important for the IM to keep the purpose of the game they are running in mind and consider the realism of the decisions that they are making. Having a note sheet (and additional blank paper) handy can be helpful for the game to run smoothly.

Protecting the Network

The goal of the players will typically be to protect one or more networks or network-connected devices. For some scenarios, this protection objective may be in support of a broader mission that provides context for it.

Red Team Actions

At the start of every turn, the IM can take one or more red team actions by spending points from the attack points pool. The techniques that they can use for red team actions are listed in Chapter VIII. These attacks are taken before any player actions, but do not take effect until the beginning of the next round. IMs may wish to note the techniques they have performed on a piece of paper or a whiteboard, both to remember them and to assure the players that the techniques were chosen at the beginning of the round.

Most red team techniques require only a single round; however, some techniques (or some complex uses of a technique) may require multiple rounds. The IM should determine the amount of time required for a technique based on the attack pathway and methods that they identify. Note that red team techniques typically target a single computer or device and, thus, several iterations of attack may be required to reach a particular target device within a network.

The attack points pool is managed by the IM and its value and the changes to it will typically only be known to the IM. It is replenished in several ways. First, the pool receives one point per round per attacker (as defined by the scenario). Generally, a single pool can be used; however, if attackers are in different locations (e.g., some are on-site at a facility and some are remote), multiple pools may be needed to prevent points from being generated in one location and used in another (which would be unrealistic, in the vast majority of cases). Points are also generated by failed blue team techniques which provide an advantage to the red team. If multiple pools are being used, these can be applied to any relevant pool.

Finishing the Game

The IM should discuss the game completion conditions with players as part of their initial briefing about the scenario. In most cases, the goal of a CRPG scenario will be for the players to withstand, prevent or respond to one or more cyberattacks. Given this, it will be important for players to know what will determine when the scenario is done. This could be defined in terms of a number of attacks (or attack components) that may need to be withstood, prevented or responded to (in which case, the specifics wouldn't be given to the players, instead a general notion would be provided). Completion could also be defined in terms of a certain amount of game time or real-world time.

The success condition will depend on the nature of the scenario being run. A scenario may end if a network becomes irreparably compromised or a key milestone or objective is missed or is no longer possible to achieve.

[V. Network Devices]

The nodes on the network that is used for gameplay are called network devices. These devices are comprised of physical hardware and virtualized systems. Some are used to interconnect the network itself, while others are servers that provide services to users. The following is an example of how network devices are presented and described:

Router (Name)

ALs: Secure | Traffic | User | Admin (Supported Levels)

Services: NNN (Services running)

W: 1 (Weight) **PS:** 0 (Physical Storage) **ES: 0** (Electronic Storage) **Type**: M (size of device)

Routers interconnect areas of a network and can also filter traffic. If traffic filtering is enabled, devices that the red team accesses through the router will have a AL of filtered traffic. (Description)

[DEVICE DEFINITION ELEMENTS]

Name: Device name

ALs : Access Levels: The supported access levels of the device.

Services: The supported services of the device.

W : Weight: The weight of the item

PS : Physical Storage: An indication of the physical storage capability (in weight) of a container item.

ES : Electronic Storage: An indication of the data storage capability (in GB) provided by or required. When listed for an electronic storage container, it indicates the amount of storage provided. When listed for software, it indicates the amount of storage required.

Type: Indicates the type of item, including its size and other characteristics.

Description: The description of the item, including any applicable restrictions on its use.

| Networking Devices

This section describes devices that are used as part of an IT network.

Firewall

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | SSH | Telnet | FTP | Remote Config

W: 1 **PS:** 0 **ES:** 0 **Type**: M

Firewalls are used to protect areas of a network by filtering traffic. When traffic filtering is enabled (a default condition), devices that the red team accesses through the router will have a AL of filtered traffic.

Rack-Mount Router

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | SSH | Telnet | FTP | Remote Config

W: 5 **PS:** 0 **ES:** 0 **Type**: M

Routers interconnect areas of a network and can also filter traffic. If traffic filtering is enabled, devices that the red team accesses through the router will have an AL of filtered traffic.

Workgroup Router

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | FTP

W: 1 **PS:** 0 **ES:** 0 **Type**: S

Routers interconnect areas of a network and can also filter traffic. If traffic filtering is enabled, devices that the red team accesses through the router will have an AL of filtered traffic.

Hub

ALs: Traffic

Services: None

W: 1 **PS:** 0 **ES:** 0 **Type**: S

Hubs interconnect computers and provide a local area network; however, they don't direct traffic to only targeted ports (like switches do) meaning that all traffic on the workgroup can be seen by any host. Hubs don't have a management interface and cannot be attacked directly.

Rack-Mount Switch

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | SSH | Telnet | Remote Config

W: 5 **PS:** 0 **ES:** 0 **Type**: M

Switches interconnect computers and provide a local area network. When the port that a computer or device is connected to is known, traffic is sent only to that port. This switch is designed to be installed in a computing equipment rack.

Workgroup Switch

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | Remote Config

W: 1 **PS:** 0 **ES:** 0 **Type**: S

Switches interconnect computers and provide a local area network. When the port that a computer or device is connected to is known, traffic is sent only to that port.

Wi-Fi Access Point

ALs: Secure | Traffic | Restricted Admin | Admin

Services: SSH | Telnet | Remote Config

W: 3 **PS:** 0 **ES:** 0 **Type**: M

Wi-Fi access points provide wireless network access to an area of a building. They are connected to a wired network and provide an interconnection to it.

Virtualized Switch

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | SSH | Telnet | Remote Config

W: 0 **PS:** 0 **ES:** 0 **Type**: SW

Switches interconnect computers and provide a local area network. When the port that a computer or device is connected to is known, traffic is sent only to that port. This switch runs within a hypervisor on a virtual machine server.

Virtualized Router

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | SSH | Telnet | FTP | Remote Config

W: 0 **PS:** 0 **ES:** 0 **Type**: SW

Routers interconnect areas of a network and can also filter traffic. A virtualized router runs on a virtual machine server. If traffic filtering is enabled, devices that the red team accesses through the router will have a AL of filtered traffic. This router runs within a hypervisor on a virtual machine server.

Virtualized Firewall

ALs: Secure | Traffic | Restricted Admin | Admin

Services: Web Server | SSH | Telnet | FTP | Remote Config

W: 0 **PS:** 0 **ES:** 0 **Type**: SW

Firewalls are used to protect areas of a network by filtering traffic. When traffic filtering is enabled (a default condition), devices that the red team accesses through the router will have an AL of filtered traffic. This firewall runs within a hypervisor on a virtual machine server.

| Computers

Rack-Mount Server

ALs: Secure | Traffic | User | Admin | Kernel

Services: All Services

W: 20 PS: 0 **ES:** 20 **Type**: L

A higher-capacity server that can be used to provide all types of services to users.

Workgroup Server

ALs: Secure | Traffic | User | Admin | Kernel

Services: All Services

W: 15 **PS:** 0 **ES:** 15 **Type**: L

A lower-capacity server that can be used to provide all types of services to small groups of users.

Virtualized Server

ALs: Secure | Traffic | User | Admin | Kernel

Services: All Services Except Hypervisor

W: N **PS:** 0 **ES:** V* **Type**: SW

A server that can be used to provide all types of services to users. This server runs within a hypervisor on a virtual machine server. *Varies based on physical server and configuration.

VoIP Phone Server

ALs: Secure | Traffic | User | Admin | Kernel

Services: VoIP, SSH, FTP, Telnet, Web Server

W: 10 **PS:** 0 **ES:** 15 **Type**: M

A server used to provide voice over internet protocol (VoIP) telephone services. Connects to the telephone (PSTN) network and one or more VoIP phones connect (via TCP/IP) to it.

Desktop Workstation

ALs: Secure | Traffic | User | Admin | Kernel

Services: Services Applicable to Operating System (IM discretion)

W: 10 **PS:** 0 **ES:** 15 **Type**: M

A desktop computer that may be commonly located in an office or other workspace.

Virtualized Desktop

ALs: Secure | Traffic | User | Admin | Kernel

Services: Services Applicable to Operating System (IM discretion)

W: N **PS:** 0 **ES:** V* **Type**: SW

A virtual image of a desktop operating system that allows users to work on a virtual server. This runs within a hypervisor on a virtual machine server and can be accessed via a physical server, physical desktop workstation or thin client.

Thin Client

ALs: Secure | Traffic | User | Admin

Services: Remote Config | SSH | FTP

W: 2 **PS:** 0 **ES:** 2 **Type**: S

A device that allows a user to access a virtual machine running within a hypervisor on a virtual server. The thin client provides a user interface, including a keyboard, mouse and monitor.

VoIP Phone

ALs: Secure | Traffic | User | Admin | Kernel

Services: VoIP, Remote Config, Web Server

W: 3 **PS:** 0 **ES:** 15 **Type**: S

A desktop telephone that provides users with voice over internet protocol (VoIP) telephone services. Connects to a VoIP phone server.

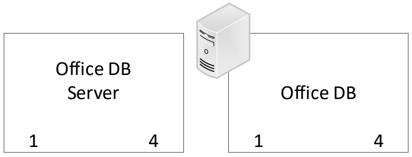
Please note that other network-connected devices, which are mobile – such as laptops and mobile devices, are discussed in the gear section.

[V. Scenario Maps]

The creation of a scenario and gameplay both require a way of recording and conveying information to players regarding the network and, if applicable, physical layout of a facility. This chapter discusses two different types of maps that can be used to play CRPG. First, we'll discuss network maps. Then, we'll look at facility mapping.

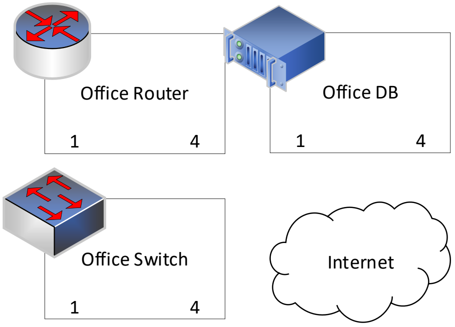
| Network Maps

Network maps are designed to show the interactions between servers, workstations, networking devices and other network-connected devices. They draw from the network devices discussed in Chapter V and devices created by the IM for a particular scenario.

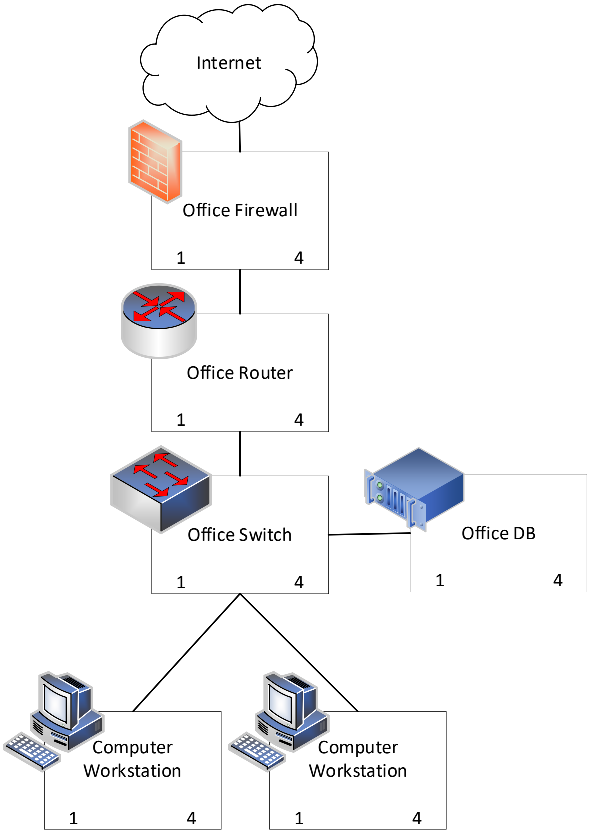


For each device, we'll want the map to contain its name and device type. Devices are represented by boxes in our network maps. The name is always the topmost line of text in the box. There are two ways to represent the device type. The most basic, shown on the left below, is to simply indicate the type of device (e.g., server). This would be appropriate for any type of network map and can be readily used for maps that are hand-drawn – either on paper or on a whiteboard. For computer-generated maps, an icon can be used to indicate the device type, as shown on the right. We also need to include two key numbers: the access level (left) and security level (right).

When using different types of devices with the basic depiction, the device type name is used to represent the particular type of device. Each device should have a unique name; however, device type names should be consistent (and match with the devices discussed in the previous chapter or created by the IM). Different icons can be used to indicate different device types, when using computer-generated maps. Three additional device types and the symbol for the internet connection are shown below.

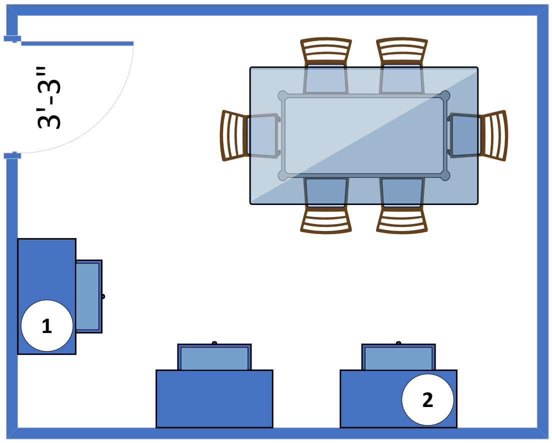


In the top row, a router and rack-mounted server are shown. The second row shows a switch and the internet cloud. The use of these devices to create a basic network, that could be a single internet-connected subnet in CRPG, is shown below.



| Facility Maps

In addition to making maps of the IT network, IMs and players will also need to create maps of facilities. Common architectural mapping techniques can be used to depict facilities for use with CRPG. An example is shown below.



In this diagram, standard shapes are used to represent a door, a conference table and desks. There are numerous shapes that can be used to represent office environments – as well as residential and other environments. The IM should include a key for each map that contains, at a minimum, a definition for any shapes which are not obvious. Including a definition for all shapes can help avoid potential confusion.

On this map, we also include numbered circles to indicate where devices that are located on the IT network can be found in the physical environment. For example, circles 1 and 2 could represent the two computer workstations shown in the previous network map. Dimensions can also be included on the map, but are not strictly necessary.

| Making and Using Maps

There are a wide variety of tools that can be used to make maps. The maps included in this section were created using Microsoft Visio, which has a shape collection that can be used for making network maps and the architectural drawing capability to support making facility maps.

Note that, while it is beneficial to the IM to have a complete network and facility map, the IM will need to determine what information is available to the players. Blue team members can be assumed to have familiarity with the initial state of the offices that they work within regularly and the initial network configuration. However, they may not be familiar with all areas of a facility and would not know about changes to facilities and networks that are made by the red team.

The IM can reveal parts of a network or facility that are unknown to the players and changes as players explore. This can be accomplished by manually transferring parts of a map to a whiteboard (or other drawing surface), as they are discovered by players. Alternately, tiles can be used to create rooms and network areas on a table or maps can be folded or cropped and displayed on a screen.

[VI. Blue Team Techniques]

Actions that can be performed by the players are called techniques. They are described in this section.

| Technique Description

The following is an example of how techniques are presented and described:

Perform Backup (Name)

DL: Trivial (Difficulty Level)

RES: N (Resources)

SV: N (Setup Value) **DV:** N (Difficulty Value)

FV: N (Fail Value)

ST: V* (System Time) **HT**: V* (Human Time)

Gear: Backup software (Required Gear)

Services: None (Required Services)

An attempt to perform a backup of files on a computer. Players should specify the computer that is being backed up and whether all files (including OS and software files) or only certain files are backed up. *Varies depending on the size of files being backed up. (Description)

[TECHNIQUE DEFINITION ELEMENTS]

Name: Technique name

DL: Difficulty Level: the difficulty level of the technique, which determines whether and which characters can use it.

RES: Represents the level of resources on a computer that the technique requires in order to run. Some techniques do not require resources (either due to not using a computer or because they have minimal requirements that are abstracted to 0). Typically, if a computer and software is required to run a technique, resources are required.

SV: Setup Value: the required roll to meet or beat to have a technique started.

DV: Difficulty Value: the required roll to meet or beat to have a technique activate

FV: Fail Value: When the activation check rolls under this value, the technique fails and often increases the attack points.

HT: Human Time: every round, players get 6 action points to spend. These can be done to setup techniques or effect the physical world. Each action is considered to take about 10 seconds with each round then being a minute long. It is highly encouraged to use all your action points each round.

ST: System Time: every round, one system time unit passes. Techniques that are currently running count down their ST corresponding to when they were set up; on the player's turn. Once the technique's ST reaches zero, the player that set up the technique makes an activation check. If the technique does not stop after activating, the ST resets to its original value and can begin counting down again.

Services: Required services that must be on the target node in order to perform the technique.

Gear: List of required gear a player must have in order to execute the technique.

Description: Describes the tech and the and effects the tech will have.

[TECHNIQUE PHASES]

There are several phases that a technique can be in. Not all techniques have all phases. In some cases, phases are abstracted for gameplay and do not require the players to roll skill checks. Relevant checks required for each technique are included in the technique description.

Setup: When wanting to start a technique, a player will choose a technique and spend the amount of HT and, if required, roll a setup check.

Setup Check: If a technique requires a setup check, the player rolls a d20 plus the relevant STAT modifier against the setup value on a technique. On success, meaning rolling equal to or higher to the startup check value (SV), the technique is started. Otherwise, the time spent is wasted, unless specified otherwise in the technique. SV values of N listed for techniques indicate that a setup check roll is not required.

If a setup check is required and the player rolls under the FV, the failure effects in the technique apply. Techniques may have a special failure effect for failing at the startup check or use the same failure effect for both startup and outcome check failures.

Running: After setup succeeds, the technique begins its ST countdown. At the end of the ST (when the count reaches zero), the player rolls an outcome check for the technique. This determines if the technique succeeds or not (with a result of success, stall, or fail).

Outcome Check: The player rolls a d20 plus the applicable STAT modifier against the DV of a technique. The technique will provide information as to what will happen on a success, stall, or failure. Notably, most techniques will have nothing happen on a stall and some techniques will stop after a certain number of outcome checks are made.

Success: Success means rolling, with modifiers the difficulty value (DV) or above. This usually has a positive outcome for the roller. Some techniques automatically stop after succeeding.

Stall: Stalling means not succeeding in a check by rolling a number, with modifiers, under the difficulty value (DV), but not under the fail value (FV). This usually has a neutral outcome for the roller, often nothing but wasting the time spent.

Fail: Failing means rolling under, with modifiers, the difficulty value (DV) for a check. This usually has a negative outcome for the player.

Stopped: Some techniques will stop on their own, while others will run infinitely and must be stopped by a player. After being stopped, it is no longer necessary to keep track of the technique.

| PREPARATION

Preparation techniques relate to general network setup and maintenance activities. They are used during the preparation phase and can also be used during the operations and attack and response phases.

When used during the preparation phase, skill roles are typically not required (as the phase is timeless and a failed technique is presumed to be reattempted successfully). IMs may still require skill checks for unusual uses of techniques or particularly difficult circumstances (potentially with a modifier). Success, difficulty and failure values are included for these techniques principally for when they are used during the operations and attack and response phases.

[INFORMATION TECHNOLOGY]

Perform Backup

DL: Trivial **RES:** 2

SV: 5 **DV:** 8 **FV**: 1 **ST**: V* **HT**: 1*

Services: None

Gear: Backup software | Storage media (Backup Tape Drive & Backup Tape Cartridge or Portable Hard Drive)

An attempt to perform a backup of files on a computer. Players should specify the computer that is being backed up and whether all files (including OS and software files) or only certain files are backed up. *Varies depending on the size of files being backed up.

Check for Needed Updates

DL: Trivial **RES:** 1

SV: N **DV:** 7 **FV**: 1 **ST**: V* **HT**: V*

Services: None

Gear: Update software (OS Update Software, Application Update Software, Firmware Update Software, or Anti-Malware **Update** Software)

An attempt to identify whether updates are needed for an operating system or installed software. Players should specify what software they are attempting to check for updates for and on what computer or device. *Varies depending on the amount of software that updates are sought for and the level of configuration required. HT for configuration will typically be approximately 3 pieces of software per HT unit.

Install Software Updates

DL: Trivial **RES:** 1

SV: N **DV:** 8 **FV**: 4 **ST**: V* **HT**: 1

Services: None

Gear: Update software (OS Update Software or Application Update Software)

An attempt to install needed updates to an operating system or piece of application software. Requires players to have performed the check for needed updates and identified that updates need to be installed. *Varies depending on the amount of software that updates are sought for and the level of configuration required.

Install Firmware Updates

DL: Trivial **RES:** 1

SV: N **DV:** 8 **FV**: 4 **ST**: 3 **HT**: 1

Services: None

Gear: Firmware Update Software

An attempt to install needed updates to a device's firmware. Requires a restart of the device.

Update Anti-Malware Definitions

DL: Trivial **RES:** 1

SV: N **DV:** 9 **FV**: 5 **ST**: 1 **HT**: 1

Services: None

Gear: Anti-Malware Update Software

An attempt to install new malware definitions for use by anti-malware software.

Train Intrusion Detection System

DL: Trivial **RES:** 2

SV: 7 **DV:** 12 **FV**: 6 **ST**: 2 **HT**: 3

Services: None

Gear: Intrusion Detection Software | IDS Management Software

An attempt to improve the performance of an intrusion detection system at detecting attacks by training it on normal network behavior. User should identify an IDS to train. Improves IDS performance (+1 per run, maximum of +3). Training during an attack may reduce IDS performance, if attack traffic is going through the area of the network observed by the targeted IDS (-1 per run, maximum of -2).

Train Firewall

DL: Moderate **RES:** 3

SV: 8 **DV:** 13 **FV**: 6 **ST**: 3 **HT**: 3

Services: None

Gear: Firewall Management Software

An attempt to improve the performance of a firewall at detecting attacks by training it on normal network behavior. User should identify a firewall to train. Improves firewall performance (+1 per run, maximum of +3). Training during an attack may reduce firewall performance, if attack traffic is going through the targeted firewall (-1 per run, maximum of -2).

Identify & Remove Unused Logins

DL: Simple **RES:** 1

SV: N **DV:** 10 **FV**: 6 **ST**: V* **HT**: 4

Services: None

Gear: Log Analysis Software | Laptop

An attempt to use software to find logins that have not been recently used and remove them to prevent their exploitation. Improves performance against attacker techniques that exploit logins. Can be targeted at an individual system to check it for unused logins or at an authentication server to check it. *Varies based on the number of logins present in the system, at IM discretion.

Implement Secure Password Policy

DL: Moderate **RES:** 1

SV: 5 **DV:** 10 **FV**: 8 **ST**: 2 **HT**: 3

Services: None

Gear: Basic Laptop

An attempt to configure a computer or authentication server to require users to have more robust passwords. Improves performance against techniques that exploit logins. May create issues during operations phases.

Implement Multi-Factor Authentication

DL: Moderate **RES:** 1

SV: N **DV:** 9 **FV**: 6 **ST**: 1 **HT**: 2

Services: None

Gear: MFA Software

An attempt to configure a computer or authentication server to require users to use multi-factor authentication mechanisms. Improves performance against techniques that exploit logins. May create issues during operations phases.

Implement Physical Security

DL: Difficult **RES:** V*

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Varies

An attempt to enhance the physical security of a building, room or piece of equipment. Improves performance against attack techniques that seek to exploit physical security vulnerabilities. The player should tell the IM what they wish to do. The IM will determine appropriate SC/DV/FV values, based upon this, whether gear is required and how much HT is required. *Varies based upon action taken.

Establish Consultant Relationship

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: None

An attempt to establish a relationship with a consultant to assist in response and recovery actions. Enhances performance in the area of the consultant relationship and reduces the time required to engage a consultant during the operations and/or attack and response phases. The player should tell the IM what type of consultant relationship that they wish to try to establish. The IM will determine appropriate SC/DV/FV values, based upon this, and how much HT is required. *Varies based upon the type of relationship that is attempted to be created.

Establish Law Enforcement Relationship

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: None

An attempt to establish a relationship with a member of law enforcement to assist in response and recovery actions. Enhances performance against attacks where law enforcement assistance would be beneficial and reduces the time required to engage the particular law enforcement agency during the operations and/or attack and response phases. The player should tell the IM what type of law enforcement relationship that they wish to try to establish. The IM will determine appropriate SC/DV/FV values, based upon this, and how much HT is required. *Varies based upon the type of relationship that is attempted to be created.

Establish Emergency Response Plan

DL: Difficult **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Word Processing Software or Notepad

An attempt to develop a response plan for a particular type of emergency. Enhances the speed and performance of response and recovery actions for the particular type of emergency targeted. The player should tell the IM what type of emergency that they wish to develop a response plan for. The IM will determine appropriate SC/DV/FV values, based upon this, and how much HT is required. *Varies based upon the type of response plan that is attempted to be created.

[ELECTRONIC]

Set Up RF Interference Shield

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Computer | Screwdriver Kit

An attempt to setup a shielding device to protect a piece of hardware from radio frequency interference.

Electromagnetic Shield Setup

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Computer | Screwdriver Kit

An attempt to set up a shielding device that will block electromagnetic signals from other devices.

Set Up Hardware Defense

DL: Difficult **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Hardware Toolkit

An attempt to secure the hardware by making it more difficulty to physically access and alter.

Set Up Spare Hardware

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Hardware to set up

An attempt to setup a redundant piece of hardware to serve as a backup in case the primary unit is disabled, damaged or tampered with.

| Vulnerability Identification

Vulnerability identification techniques are designed to identify security deficiencies with a network to facilitate their remediation before they can be exploited by an attacker. These techniques can be used during the preparation phase to detect potential issues to resolve. They can also be used during the operations and attack and response phases to identify pre-existing and newly created vulnerabilities.

When used during the preparation phase, skill roles are typically not required (as the phase is timeless and a failed technique is presumed to be reattempted successfully). IMs may still require skill checks for unusual uses of techniques or particularly difficult circumstances (potentially with a modifier). Success, difficulty and failure values are included for these techniques principally for when they are used during the operations and attack and response phases.

[INFORMATION TECHNOLOGY]

IP Range Scan

DL: Trivial **RES:** 1

SC: N **DV:** 7 **FV**: 5 **ST**: 1 **HT**: 1

Services: None

Gear: Computer connected to the network to be scanned

An attempt to scan a range of IP addresses to identify addresses assigned to an active device within the range. Supplies IP addresses that can be used to identify unexpected computers or by the port scan technique.

Port Scan

DL: Trivial **RES:** 1

SC: N **DV:** 8 **FV**: 5 **ST**: V* **HT**: 1

Services: None

Gear: Device connected to the network to be scanned

An attempt to scan an IP address or range of IP addresses to determine what ports are open and, thus, predict what services are running on the computer. *Varies based on the number of IP addresses scanned. Approximately 15 addresses can be scanned per unit of ST.

Vulnerability Assessment Tool Scan

DL: Simple **RES:** 2

SC: N **DV:** 10 **FV**: 6 **ST**: V* **HT**: 2

Services: None

Gear: Device connected to the network to be scanned | Vulnerability Assessment Software

An attempt to scan an IP address or range of IP addresses to determine what services are running on the computer and identify vulnerabilities. Provides players with a list (possibly not complete) of vulnerabilities to address. Approximately 5 addresses can be scanned per unit of ST.

Log Analysis

DL: Moderate **RES:** 1

SC: N **DV:** 12 **FV**: 6 **ST**: V* **HT**: 1

Services: None

Gear: Log Analysis Software | Logs to Review

An attempt to analyze log files to identify symptoms that may indicate that an attack is ongoing or has occurred. The player should tell the IM what log or logs on what system they wish to analyze. The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much ST is required. *Varies based upon the number and type of logs to be analyzed.

[ELECTRONIC]

Air Gapped System Scan

DL: Moderate **RES:** 1

SV: V* **DV:** 10 **FV**: 5 **ST**: 1 **HT**: 2

Services: None

Gear: Laptop

An attempt to determine if a system is air gapped.

Secure Hardware Scan

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Hardware Toolkit

An attempt to physically check a piece of hardware to determine whether the device has any easy access points that would facilitate tampering with it.

| Network Reconfiguration

Network reconfiguration techniques are designed to make changes to the IT network. These can be used to remediate security deficiencies that have been identified, to provide functionality required by system users (during the operations phase) and/or to remediate issues created by attackers.

These techniques can be used during the preparation phase to resolve configuration issues. They can also be used during the operations and attack and response phases to remediate pre-existing and newly created vulnerabilities.

When used during the preparation phase, skills roles are typically not required (as the phase is timeless and a failed technique is presumed to be reattempted successfully). IMs may still require skill checks for unusual uses of techniques or particularly difficult circumstances (potentially with a modifier). Success, difficulty and failure values are included for these techniques principally for when they are used during the operations and attack and response phases.

[INFORMATION TECHNOLOGY]

Reconfigure Firewall

DL: Moderate **RES:** 1

SC: V* **DV:** V* **FV**: V* **ST**: 1 **HT**: V*

Services: None

Gear: Laptop | Ethernet Cable or Serial Cable

An attempt to make configuration changes to a firewall device. May improve or harm performance, based on the change attempted and its success. The player should describe the nature of the change that they would like to make to the IM (including any new or altered firewall rules, if rules are being changed). The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. *Varies based upon the type of change attempted.

Reconfigure Router

DL: Moderate **RES:** 1

SC: V* **DV:** V* **FV**: V* **ST**: 1 **HT**: V*

Services: None

Gear: Laptop | Ethernet Cable or Serial Cable

An attempt to make configuration changes to a router device. May improve or harm performance, based on the change attempted and its success. The player should describe the nature of the change that they would like to make to the IM (including any new or altered routing rules, if rules are being changed). The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. *Varies based upon the type of change attempted.

Reconfigure Switch

DL: Moderate **RES:** 1

SC: V* **DV:** V* **FV**: V* **ST**: 1 **HT**: V*

Services: None

Gear: Laptop | Ethernet Cable or Serial Cable

An attempt to make configuration changes to a switch device. May improve or harm performance, based on the change attempted and its success. The player should describe the nature of the change that they would like to make to the IM (including any vLAN configuration changes or ports to enable, disable or connect to particular vLANs, if applicable). The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. *Varies based upon the type of change attempted.

Reconfigure Cabling

DL: Simple **RES:** N

SC: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Cables Required for Configuration

An attempt to make network cabling changes which go beyond simply disconnecting the network cabling (the physical disconnection technique is used for simple disconnections). The player should describe the nature of the change that they would like to make to the IM. The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. *Varies based upon the type of change attempted.

Reconfigure Computer

DL: Simple **RES:** 1

SC: V* **DV:** V* **FV**: V* **ST**: 1 **HT**: V*

Services: None

Gear: Varies*

An attempt to make a configuration change to a computer (laptop, desktop or server). May improve or harm performance, based on the change attempted and its success. The player should describe the nature of the change that they would like to make to the IM. The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. *Varies based upon the type of change attempted.

Reconfigure IoT Device

DL: Simple **RES:** 1

SC: V* **DV:** V* **FV**: V* **ST**: 1 **HT**: V*

Services: None

Gear: Varies*

An attempt to make a configuration change to a internet of things (IoT) device. May improve or harm performance, based on the change attempted and its success. The player should describe the nature of the change that they would like to make to the IM. The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. *Varies based upon the type of change attempted.

Reconfigure Wireless Access Point

DL: Simple **RES:** 1

SC: V* **DV:** V* **FV**: V* **ST**: 1 **HT**: V*

Services: None

Gear: Varies*

An attempt to make configuration changes to a wireless access point device. May improve or harm performance, based on the change attempted and its success. The player should describe the nature of the change that they would like to make to the IM (including any wireless network, vLAN or other configuration changes, if applicable). The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. *Varies based upon the type of change attempted.

[ELECTRONIC]

Hardware Reconfiguration

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Computer Toolkit or Hardware Toolkit

An attempt to change the configuration of a hardware device, which may increase or decrease its security and/or performance.

Air Gap System

DL: Difficult **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: V* **HT**: V*

Services: None

Gear: Varies*

An attempt to create an 'air gap' between a system and others by removing network connectivity from the system.

[BOTH]

Disable Device

DL: Simple **RES:** 1

SC: V* **DV:** V* **FV**: V* **ST**: 1 **HT**: V*

Services: None

Gear: Typically None*

An attempt to disable a device, typically through the use of a normal shutdown process. The player should identify the device that they wish to disable to the IM along with any special instructions for how they would like to disable it. The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. This technique is not used for simply removing power from the device (which can be performed using the physical disconnection technique). *Varies based upon the type of change attempted and the state of the device.

|Attack Detection

The attack detection techniques are used to identify red team activities. They can help the players to identify when the scenario has moved from the operations phase into the attack and response phase. They can also be used to identify the type and target of attacks.

Because a scenario may include multiple attacks, and because it may move back and forth between the operations phase and the attack and defense phase, the attack detection techniques can be used during both the operations and attack and defense phases. These techniques are not designed to be used during the preparation phase.

[INFORMATION TECHNOLOGY]

Intrusion Detection

DL: Simple **RES:** 2

SC: N **DV:** 10 **FV**: 6 **ST**: 1 **HT**: 1

Services: None

Gear: Intrusion Detection Software

An attempt to determine whether an attack against a network or computing system is ongoing. Intrusion detection can be performed manually or automated using an intrusion detection system. If it is automated, ST is required but no HT is required. If successful and an attack is ongoing, will identify the attack as ongoing and provide details about its origin point and target (which are visible from the vantage point of the intrusion detection system or software). If multiple attacks are ongoing, roll a d6 to determine how many may be attempted to be detected and roll a skill check for each attempt. Skill checks may have a modifier applied based on the level of stealth of the attack that is attempting to be detected.

Real-time Malware Scanning

DL: Simple **RES:** 2

SC: 6 **DV:** 8 **FV**: 5 **ST**: 1 **HT**: 0

Services: None

Gear: Anti-Malware Software | Computer

An attempt to determine whether a file that is being accessed or run is infected by malware. Triggered automatically on systems where real-time anti-malware is present. May have a modifier applied to SC/DV/FV values based on the level of stealth of the malware.

Malware Scan

DL: Simple **RES:** 2

SC: 5 **DV:** 10 **FV**: 6 **ST**: 1 **HT**: 2

Services: None

Gear: Anti- Malware Software | Computer

A manual attempt to determine whether files that are on a given computer are infected by malware. May have a modifier applied to SC/DV/FV values based on the level of stealth of the malware.

Functional Testing

DL: Trivial **RES:** 3

SC: 7 **DV:** 12 **FV**: 5 **ST**: 1 **HT**: 3

Services: None

Gear: Laptop | Functional Testing Software

An attempt to determine whether a piece of software is functioning in accordance with its specifications or in a manner that is similar to how it performed previously. Can be used to detect changes that indicate an attack. To compare to the previous performance, a baseline test must be successfully conducted. If the baseline test is conducted after a change made by a successful attack, that attack's change will not be detected by future comparisons to it. The player should advise the IM as to the general nature of the test that they would like to conduct and what software, on what device, and what functionality of the software is targeted.

Traffic Analysis

DL: Trivial **RES:** 1

SC: 4 **DV:** 9 **FV**: 2 **ST**: 1 **HT**: 1

Services: None

Gear: Laptop | Network Cable

An attempt to determine whether network traffic indicates the presence of an attack. Can be used to perform analysis based on attack signatures or by comparing network traffic to assess whether it is similar to previous network traffic. Can be used to detect changes that indicate an attack. To compare to the previous performance, a baseline test must be successfully conducted. If the baseline analysis is conducted during an attack, that attack and other similar attacks won't be detected as different and non-attack periods may indicate false positives. The player should indicate what area of the network that traffic analysis is being performed on.

Rogue Wi-Fi Access Point Scanning

DL: Trivial **RES:** 1

SC: N **DV:** 10 **FV**: 7 **ST**: 1 **HT**: 1

Services: None

Gear: Laptop | Wi-Fi Antenna

An attempt to detect the presence of an unauthorized Wi-Fi access point. The player should tell the IM what physical area is being scanned for unauthorized Wi-Fi access points.

[ELECTRONIC]

Electromagnetic Attack Detection

DL: Difficult **RES:** 1

SV: N **DV:** 10 **FV**: 8 **ST**: N **HT**: 3

Services: None

Gear: Electromagnetic Sensor

An attempt to conduct a scan to determine whether there are indications of a current or past electromagnetic attack against a device.

RF Interference Attack Detection

DL: Difficult **RES:** N

SV: N **DV:** 12 **FV**: 8 **ST**: N **HT**: 3

Services: None

Gear: Laptop

An attempt to conduct a scan to determine whether there are indications of a current or past radio frequency interference attack against a device.

Hardware Tampering Inspection

DL: Moderate **RES:** N

SV: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: Hardware Toolkit

An attempt to inspect a device to determine whether it has been tampered with.

|Clean Up

Clean up techniques are designed to be used to remediate the actions and activities of attackers specifically related to removing persistence mechanisms and attack tools. Notably, some attacker actions, which result in network changes, may be remediated using the network reconfiguration techniques.

Unless a scenario were to start with a previously compromised network, there would be no reason to use these techniques during the preparation phase. If this was to be the case, and the techniques were used during the preparation phase, skill roles are typically not required (as the phase is timeless and a failed technique is presumed to be reattempted successfully). IMs may still require skill checks for unusual uses of techniques or particularly difficult circumstances (potentially with a modifier).

Normally, these techniques will be used during the operations and attack and response phases to remediate attacks conducted during the attack and response phase. Success, difficulty and failure values are included for these techniques principally for when they are used during these two phases.

[INFORMATION TECHNOLOGY]

Remove Malware

DL: Simple **RES:** 1

SC: N **DV:** 9 **FV**: 5 **ST**: 1 **HT**: 2

Services: None

Gear: Anti-Virus Software or Anti-Malware Software

An attempt to remove malware from software or the operating system of an infected computer. To be effective, this technique should only be used after malware has been detected on a given computer.

Remove BIOS Malware

DL: Moderate **RES:** 1

SC: N **DV:** 11 **FV**: 6 **ST**: 2 **HT**: 2

Services: None

Gear: Firmware Update Software

An attempt to remove malware from the BIOS of an infected computer. To be effective, this technique should only be used after malware has been detected on a given computer.

Remove Rootkit

DL: Moderate **RES:** 1

SC: N **DV:** 12 **FV**: 6 **ST**: 1 **HT**: 2

Services: None

Gear: Rootkit Removal Software

An attempt to remove a rootkit from an infected computer. To be effective, this technique should only be used after a rootkit has been detected on a given computer.

Restage Computer

DL: Trivial **RES:** 2

SC: N **DV:** 9 **FV**: 6 **ST**: 2 **HT**: 3

Services: None

Gear: Computer to Restage

An attempt to reinstall the operating system and application software on a computer that is infected or has had its software damaged. Failure may result in the restaged computer still being infected.

Reset Credentials

DL: Trivial **RES:** 1

SC: N **DV:** 7 **FV**: 4 **ST**: 1 **HT**: 1

Services: None

Gear: Laptop

An attempt to reset credentials on a computer where administrative access is not available to the blue team. Requires a restart.

Restore Backup

DL: Trivial **RES:** N

SC: N **DV:** 9 **FV**: 5 **ST**: 2* **HT**: 2

Services: None

Gear: Backup Software | Backup of computer on media

An attempt to restore a computer from a backup of its configuration. Note that if the backup was taken after the attack against the computer had been successful, the restored computer may still be infected. *Could vary based on backup size

[ELECTRONIC]

Remove Tampered With Hardware

DL: Moderate **RES:** N

SV: N **DV:** 10 **FV**: 5 **ST**: 0 **HT**: 2

Services: None

Gear: Hardware Toolkit

An attempt to remove hardware that has been tampered with from an operational environment. May impact the functionality of the operational environment.

Replace Tampered With Hardware

DL: Moderate **RES:** N

SV: 12 **DV:** 11 **FV**: 5 **ST**: 0 **HT**: 2

Services: None

Gear: Hardware Toolkit | Replacement Hardware

An attempt to replace hardware that has been tampered with within an operational environment. May have a temporary impact on the functionality of the operational environment. If successful, no long-term impact to the operational environment will occur.

Correct Physical Discrepancies

DL: Difficult **RES:** N

SV: 10 **DV:** 13 **FV**: 6 **ST**: 0 **HT**: 3

Services: None

Gear: Hardware Toolkit

An attempt to remove an identified physical discrepancy in a piece of hardware by returning it to its original physical state.

|Communications

Communications techniques are used to interact with other parties that may have a role in response and recovery activities. These techniques will typically be used during the attack and response phase or during an operations phase following an attack and response phase.

Stakeholder Notification

DL: Trivial **RES:** N

SC: 7 **DV:** 11 **FV**: 4 **ST**: N **HT**: 3

Services: None

Gear: None

An attempt to notify organizational stakeholders, such as senior managers and board members regarding a cyberattack. Can be used to seek organizational assistance.

Media Notification

DL: Trivial **RES:** N

SC: 6 **DV:** 10 **FV**: 4 **ST**: N **HT**: 3

Services: None

Gear: None

An attempt to notify the media regarding a cyberattack. Can be used to mitigate the impact to victims and others that may be impacted.

Breach Victim Notification

DL: Moderate **RES:** N

SC: 7 **DV:** 12 **FV**: 6 **ST**: N **HT**: 4

Services: None

Gear: None

An attempt to directly notify victims of a data breach regarding a cyberattack. Can be used to mitigate the impact to victims and others that may be impacted.

Government Notification

DL: Trivial **RES:** N

SC: 9 **DV:** 13 **FV**: 7 **ST**: N **HT**: 3

Services: None

Gear: None

An attempt to notify government entities regarding a cyberattack. Can be used to mitigate the impact to victims and others that may be impacted.

|Organizational Response

Organizational response techniques are used to conduct the non-IT side of attack response and recovery. Because of this, these techniques will typically be used during the attack and response phase or during an operations phase following an attack and response phase.

Engage Law Enforcement

DL: Difficult **RES:** N

SC: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: None

An attempt to enlist the support of law enforcement in responding to a cyberattack. The player should identify what type of law enforcement agency they would like to engage, to the IM. The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. A modifier should be applied if a relationship with law enforcement has been previously established. *Varies based upon the type of engagement attempted.

Initiate Emergency Response Plan

DL: Moderate **RES:** N

SC: V* **DV:** V* **FV**: V* **ST**: 0 **HT**: V*

Services: None

Gear: None

An attempt to perform the steps identified in an emergency response plan in responding to a cyberattack. In many cases, other techniques will also need to be used. However, these can be aided through the initiation of an emergency response plan. HT may be reduced through the use of the plan and modifiers may be applied to the skill checks performed. The IM will determine appropriate SC/DV/FV values for this technique and determine how much HT is required. An emergency response plan must be developed before it can be initiated. *Varies based upon the type of plant attempted.

Engage Consultant

DL: Moderate **RES:** N

SC: N **DV:** 12 **FV**: 5 **ST**: N **HT**: 3

Services: None

Gear: None

An attempt to enlist the support of a consultant in responding to a cyberattack. The player should identify what type of consultant that they would like to engage, to the IM. The IM will determine appropriate SC/DV/FV values, based upon this, and determine how much HT is required. A modifier should be applied if a relationship with a consultant has been previously established. *Varies based upon the type of engagement attempted.

| Other Techniques

A limited number of techniques do not fall squarely into one of the previously listed categories. These techniques are included in this section.

Offensive Action

DL: Moderate **RES:** N

SC: V* **DV:** V* **FV**: V* **ST**: V* **HT**: V*

Services: None

Gear: Varies

An attempt to take an offensive (red team) action. The player should describe the action and the target. The IM will determine appropriate SC/DV/FV values, based upon this, and how much HT is required. *Varies based upon the type of action that the player attempts to take.

Physical Disconnection

DL: Simple **RES:** N

SC: N **DV:** N **FV**: N **ST**: N **HT**: 1

Services: None

Gear: None

An attempt to physically disconnect a device from a network connection or power connection.

[VII. Red Team Actions]

This chapter presents techniques that the IM can use on behalf of the red team attackers in a scenario. These techniques are abstracted to facilitate their ease of use by the IM.

At the start of each round, the IM can take one or more red team actions, using the points in the attack points pool. The cost of the red team actions taken is subtracted from the attack points pool.

Attack & Compromise Network Device

Cost: 4

An attempt to attack and compromise a network (IoT or networking equipment) device. Requires the IM to identify a plausible attack pathway and approach. Provides administrative access to the device.

Attack & Compromise Computer

Cost: 4

An attempt to attack and compromise a computer (laptop, desktop or server). Requires the IM to identify a plausible attack pathway and approach. Provides administrative access to the device.

Collect & Exfiltrate Data

Cost: 3

An attempt to collect and remove data from a computer, IoT or networking device or from an application which has been compromised. Requires the IM to identify what data will be collected and a plausible exfiltration path. May take multiple turns, depending on the amount of data being transferred.

Disable Device

Cost: 2

An attempt to remotely disable a computer, IoT or networking device which has been compromised.

Deny Service

Cost: 2

An attempt to disable or impair the operations of a computer, IoT or networking device which has been compromised or where a networking device required to provide access to this device has been compromised. This technique can also be used for network traffic overload-based denial of service attacks. If not being used on a compromised computer or device, it requires the IM to identify a plausible attack pathway and approach.

Corrupt Network

Cost: 3

An attempt to change network settings on a networking device to interfere with the operations of the network. Requires a successful prior attack and compromise of the device. The IM must identify the changes to be made and their impact and ensure that they are appropriate for the device targeted.

Install Malware

Cost: 4

An attempt to install malware on a compromised device.

Install Ransomware

Cost: 4

An attempt to install ransomware on a compromised device.

Attack & Compromise Application

Cost: 6

An attempt to directly attack and compromise an application without compromising the computer or device that it is running on. Requires the IM to identify a plausible attack pathway and approach. Provides administrative access to the application.

Social Engineering

Cost: V*

An attempt to use a social engineering technique to have an action performed for the red team or to provide an attack pathway where no one exists. This technique cannot be used against the players' characters (any social engineering targeting players' characters should be conducted through gameplay). Requires the IM to identify a plausible approach. *Varies based on what is being attempted.

[IX. GEAR]

Gear is needed for red team and blue team members alike. It includes the software that is used for scanning for attacks and protecting networks and the hardware that is used for supporting network operations. Gear also includes the computers used for attacking and defending and storage devices for both software and physical items.

| GEAR DESCRIPTION

An example of how gear is described is provided below. Following this, the elements of gear description are listed and described.

Basic Laptop Computer (Name)

W: 1(Weight) **PS**: 0 (Physical Storage)

ES: 4 (Electronic Storage) **Type:** M

A lightweight laptop with limited computational capabilities that is designed to be easily carried. (Description)

[GEAR DEFINITION ELEMENTS]

Name: Gear name

W : Weight: The weight of the item

PS : Physical Storage: An indication of the physical storage capability (in weight) of a container item.

ES : Electronic Storage: An indication of the data storage capability (in GB) provided by or required. When listed for an electronic storage container, it indicates the amount of storage provided. When listed for software, it indicates the amount of storage required.

Type: Indicates the type of item, including its size and other characteristics.

Description: The description of the item, including any applicable restrictions on its use.

| SOFTWARE

This section includes software that can be used to prepare and protect networks and respond to attacks against network devices.

Backup Software

ES: 1

Software used for making and restoring backups of computing devices. Basic backup software requires the local connection of a backup tape drive or portable hard drive with sufficient space.

Network Backup Software

ES: 1

Software used for making and restoring backups of computing devices. Network backup software can use a locally connected backup tape drive or portable hard drive. It can also make a backup of a device to another computer or to a backup tape drive or portable hard drive connected to another computer. Sufficient space must be available on the target computer, drive or tape cartridge.

Network Scanning Software

ES: 1

Software used for scanning networks for operational IP addresses and open ports.

Intrusion Detection Software

ES: 2

Software used for detecting network intrusions.

Network Management Software

ES: 1

Software used for making changes to network devices. Can be used to make similar changes to multiple devices concurrently.

OS Installation Media

ES: 2

A DVD or USB stick (IM option) containing the files required to install or reinstall an operating system.

OS Staging Software

ES: 1

Software used to automate the installation of an operating system with similar configuration on multiple computers.

Anti-Malware Software

ES: 1

Software used for detecting and removing malware. Can be installed on a computer or used from a portable device to scan for malware on it.

Anti-Virus Software

ES: 1

Software used for detecting and removing viruses. Can be installed on a computer or used from a portable device to scan for malware on it.

Wi-Fi Management Software

ES: 1

Software that is used to change the configuration of Wi-Fi access points.

Rootkit Removal Software

ES: 2

Software that is used to remove a rootkit from an infected computing device.

BIOS Malware Removal Software

ES: 1

Software that is used to remove BIOS malware from an infected computing device.

OS Recovery Software

ES: 2

Software that can be used to attempt to repair an operating system that is damaged or has become infected or corrupted.

Firmware Update Software

ES: 1

Software that is used to identify if firmware updates are needed and to update device firmware on a computing device.

OS Update Software

ES: 1

Software that is used to identify if OS updates are needed and to update the OS on a computing device.

Application Update Software

ES: 2

Software that is used to identify if updates are needed to one or more applications and to update the application software on a computing device.

Anti-Malware Update Software

ES: 1

Software that is used to determine whether anti-malware software and definition updates are needed and to update anti-malware software and the malware definitions that it uses on a computing device.

IDS Management Software

ES: 1

Software that is used to configure and manage intrusion detection software and devices.

Firewall Management Software

ES: 1

Software that is used to configure and manage firewalls.

Security Management Software

ES: 1

Software that is used to configure and manage security settings on computers and network devices.

Word Processing Software

ES: 1

Software that is used to create, edit and view documents on a computing device.

Log Analysis Software

ES: 3

Software that is used to analyze log files to detect anomalies that may be configuration errors, network intrusions or other issues.

MFA Software

ES: 2

Software that is used to support multi-factor authentication.

Vulnerability Assessment Software

ES: 2

Software that is used to scan a network and the computers attached to it for vulnerabilities. Reports on the specific devices and vulnerabilities detected.

Functional Testing Software

ES: 3

Software that is used to perform functional testing. It can be used to identify bugs in software under development. It can also be used to determine whether an installed application is functioning properly or if it has been tampered with.

| Computing Devices

Computing devices are used to run software. This section lists computing devices that can be readily carried by characters. Characters can also run software on computers found within a physical environment. These are described in Chapter V.

Basic Laptop Computer

W: 1 **PS**: 0 **ES**: 4 **Type:** M

A lightweight laptop with limited computational capabilities that is designed to be easily carried.

Advanced Laptop Computer

W: 2.5 **PS**: 0 **ES**: 10 **Type:** M

A lightweight laptop with limited computational capabilities that is designed to be easily carried.

Backup Tape Drive

W: 6 **PS**: N **ES**: N **Type:** M

A device that backup tape cartridges can be placed into in order to be written to or read from.

| Tools & Other Items

This section describes handheld tools and other physical items that can be used by characters.

Computer Tool Kit

W: 1 **PS**: 0 **ES**: 0 **Type:** S

A small tool kit used for assembling and disassembling computers.

Screwdriver Kit

W: 1 **PS**: 0 **ES**: 0 **Type:** S

A small collection of screwdrivers in a small containing pouch.

Mobile Phone

W: 1 **PS**: 0 **ES**: 0 **Type:** S

A mobile phone with built in camera for taking pictures, internet access and the ability to make calls.

Notepad

W: 0.5 **PS**: 0 **ES**: 0 **Type:** S

A small tablet of paper that is easily carried. Includes a pen for writing on it.

MFA Token

W: 0.5 **PS**: 0 **ES**: 0 **Type:** S

A token for authenticating with multi-factor analysis systems.

Other Items

W: V* **PS**: V* **ES**: V* **Type:** V*

Other physical items can be specified by the IM. The IM should define relevant weight, size and other attributes for the items as needed. *Varies based on item.

| Storage

Storage items are a particular type of gear that is used to hold other gear. Storage items can contain either physical or electronic items. A few example types of storage items (e.g., backpacks and USB sticks) are included. Note that when a storage item is placed within another storage item the storage capacity is constrained by all nested items. The overall storage within any item (including items directly within it and items within other storage items inside it) cannot exceed its capacity.

Small Backpack

W: 1 **PS**: 8 **ES**: 0 **Type:** M

A lightweight backpack with limited storage capabilities that is designed to be easily carried. Only one backpack can be used. Backpack does not occupy hand or pocket. Can only hold type M, S and VS items.

Large Backpack

W: 3.5 **PS**: 15 **ES**: 0 **Type:** M

A larger backpack with more storage space that is designed to be easily carried. Only one backpack can be used. Backpack does not occupy hand or pocket. Can only hold type M, S and VS items.

USB Drive

W: 0.25 **PS**: 0 **ES**: 4 **Type:** VS

A drive that can be connected to a computer via USB that is used for data storage. Can be carried in pocket.

External Hard Drive

W: N **PS**: N **ES**: V* **Type:** N

A hard drive that can be connected to a computer using a USB cable. *Varies based upon device size. Multiple sizes may be used at IM discretion.

Backup Tape Cartridge

W: N **PS**: N **ES**: V* **Type:** N

A backup tape cartridge for use with a backup tape drive. *Varies based upon device size. Multiple sizes may be used at IM discretion.

[X. Further Expansion]

CRPG was designed for defensive-perspective cybersecurity wargaming. Wargaming in a physical environment can be conducted by augmenting it with a general-purpose system such as FATE or GURPS.

CYBERSECURITY RPG

• BLUE TEAM •

Character Worksheet

Name:

Role: Blue Team Member

Skills:

PRP: □

VI: □

NR: □

AD: □

CU: □

COM: □

OR: □

OTH: □ =∑(ALL)/ 7

Level (Select):

□ Beginner

□ Intermediate

□ Advanced

Gear:	Wgt:

Skills:	Lvl:

CYBERSECURITY RPG

• BLUE TEAM •

Character Worksheet

Name:

Role: Blue Team Member

Skills:

PRP: □

VI: □

NR: □

AD: □

CU: □

COM: □

OR: □

OTH: □ =∑(ALL)/ 7

Level (Select):

□ Beginner

□ Intermediate

□ Advanced

Gear: / Wgt:

Skills: / Lvl: