Phases of Cyber Operation

Phase of Operation	Defined
Target Identification	is where it all starts, in order to execute an attack or defense, the target must be noted first. This is important because once the target is established, the rest of the stamps now know who or what they are preparing for. Consider this the step where you look at the map and there is a big red X on who the preparation is intended for.
Reconnaissance	The reconnaissance step is similar to studying before the test. This is a vital part of an operation because there is information that is necessary to know before the rest of the operation can continue. This step includes research and intelligence gathering of a network, data security, or relevant applications/coding within the adversaries. We must know what we are working with before any execution can be started.
Gaining Access	Gaining access is step one of the intrusion phase. There has been a delivery method chosen and a door within a network selected. A user or vulnerability has been found and exploitation has started. This stage ends with the success of gaining access to a company's adversary and now we will use this access as a platform to execute an attack. This step is the riskiest and often where everything can be halted. Once in, there must be a strategy for how we will moreover.
Hiding Presence	Shortly after the gaining access phase, we must start hiding our presence. This is a crucial step that must be taken because, during the gaining access phase, it was definitely possible that we set off some red flags within a security system. If anything was edited or evidence of our breach is left behind, it is critical that we cut the loose

	strings left behind so we can best conceal our presence. If this is not done properly, we can definitely be found within an environment we are not a part of and the security system may change soon after that.
Establishing Presence	Once we are in a system and we've gathered the information we were after, it is important that we establish our presence. This can be done through public announcements such as social media, or contact the company directly and let them know. Another strategy is to trigger their security system, and when they try to access a vital part of their network, they will realize that they no longer have control. This is how we move towards our established goal and receive what we are after in the first place.
Execution	The execution phase is everything we prepared for prior. This is the stage where we finally abuse the vulnerability that was found that will now help us gain access to vital information. This is where damage will be done and assets will be lost if on the wrong side of an attack. Our presence will most likely be seen and what we've gone in to obtain has been taken. This is the stage where all the prior setup has been done for.
Assessment	The post-assessment is an important step that wraps up the competition of a successful cyber operation. This is where we go over the initial goals and strategies that we originally came up with. If something occurred that we are not expecting, we discuss a strategy around that for next time. If your objective was not met or compared, we must find out why and how we can get around it. It is always important to ensure our strategies are improving, and that our innovations are moving in the correct direction.