Cyber Kill Chain

In order for network defenders to defeat cyber adversaries – to compress the "Cyber Kill Chain" – they have to: Find, Fix, Track, Target, Engage and Assess. Find them in their networks. Fix them in place. Track their behavior. Target them with the right prevention control. Engage them with that control. Assess the control's effects. The military uses the acronym F2T2EA as shorthand for this concept.[4] Lockheed Martin describes it as a linked chain because the network defender has to accomplish every step in the F2T2EA system, or it completely falls apart. In order to do that, network defenders have to understand exactly how cyber adversaries move through their victims' networks. It turns out, according to the Lockheed Martin research team, regardless of which hacker tools the cyber adversaries use or what motivates them to attack their victims in the first place, the hackers have to successfully complete the same seven tasks to accomplish their mission.

The Lockheed Martin Cyber Kill Chain®:[4]

1. Recon their target for potential weaknesses.
2. Build a tool that will leverage those newly found weaknesses.
3. Deliver that tool to some endpoint on the target's network.
4. Use that now delivered tool to compromise the endpoint and establish a beachhead for future operations.
5. Install a back door on the beachhead that will allow the cyber adversaries to return whenever they like to maintain persistence within the victim's network.
6. Establish a command and control channel that will allow the adversaries to fully control the beachhead and deliver more tools that will help complete the mission.
7. Finally, after all of that work, the cyber adversaries are ready to take the actions to complete their mission. Since they are inside the victim's network now, they can search for the information they came to steal, collect it, and exfiltrate it using the already established command and control channel.