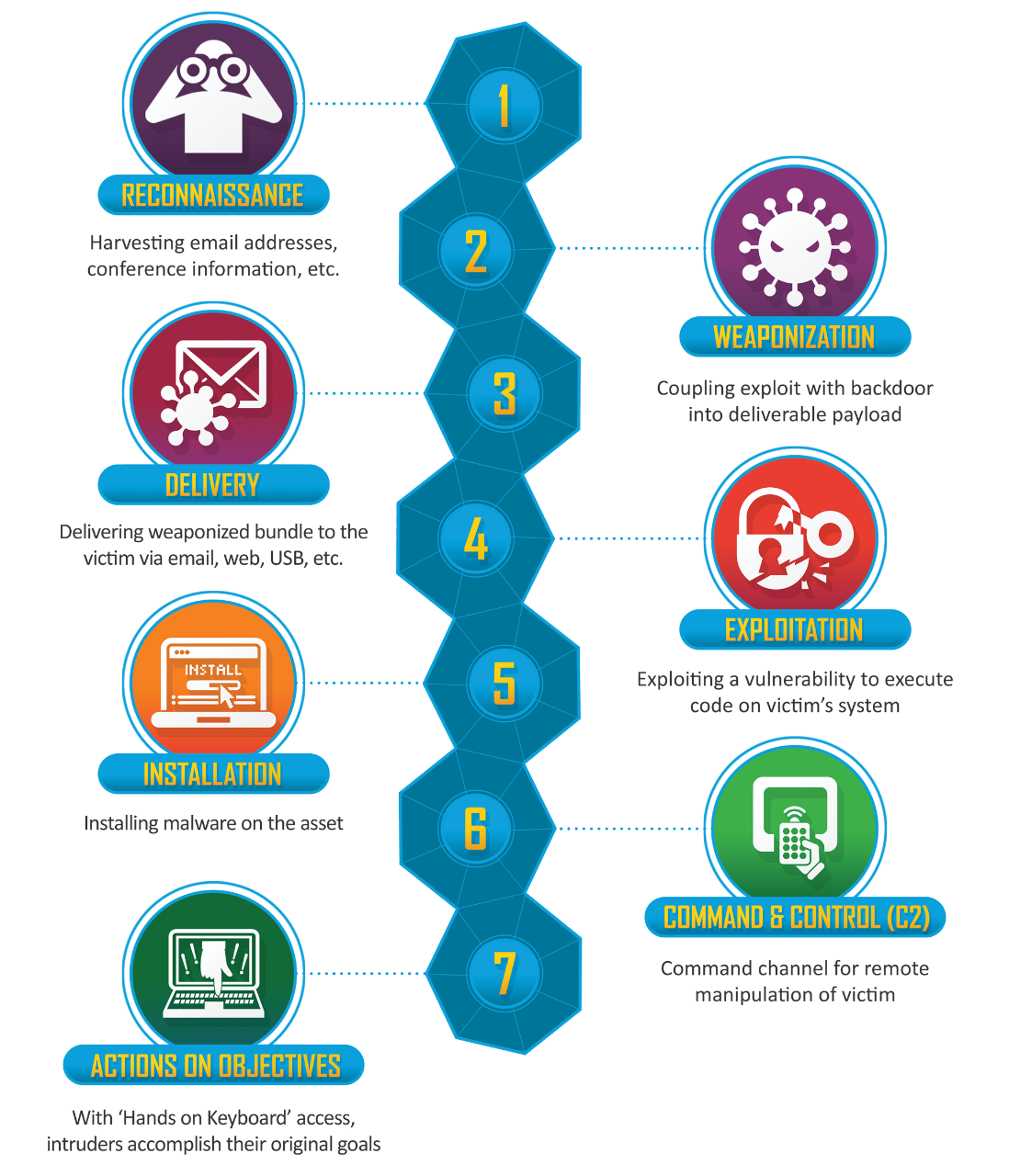
**Cyber Kill Chain**

****

The Cyber Kill Chain is a methodology for identifying and defending against cyber-attacks. It was developed by Lockheed Martin and consists of seven stages:

1. Reconnaissance: The attacker gathers information about the target and its defenses.
2. Weaponization: The attacker prepares and delivers the payload (malware or other means of compromise).
3. Delivery: The payload is delivered to the target.
4. Exploitation: The payload is activated and the attacker gains access to the target system.
5. Installation: The attacker establishes a foothold within the target system and prepares for further actions.
6. Command and control: The attacker establish a communication channel with the target system and begins to control it.
7. Actions on objectives: The attacker achieves their objectives, such as exfiltrating data or disrupting operations.

The Cyber Kill Chain is used as a framework for understanding and defending against cyber-attacks. By identifying the stage of an attack, organizations can take appropriate actions to prevent it from succeeding or minimize the damage it causes.

****

In summary, the cyber kill chain model is a valuable tool for understanding and preventing cyber-attacks. It helps organizations to detect and disrupt attacks at different stages and to understand how an attack is likely to progress. However, it is important to remember that different attackers may have different goals, resources, and methods, so the model should be used as a guide rather than a rigid framework.