

The logo for NPTel (National Program on Technology Enhanced Learning) is centered in the background. It features a stylized flower or star shape with eight petals, composed of concentric lines, enclosed within a circular border made of small rectangular segments. Below the flower, the word "NPTel" is written in a bold, sans-serif font, with "NPT" in a darker shade and "el" in a lighter shade.

Malicious Software

DR. NEMINATH HUBBALLI

Overview

- ❑ Malware
- ❑ Implications
- ❑ Flooding based DDoS Attacks
- ❑ Botnets



What is Malicious Software ?

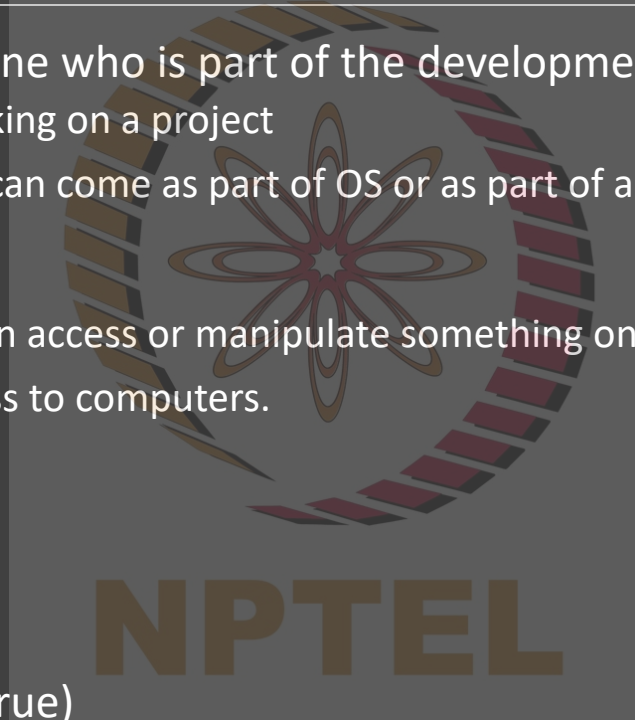
- ❑ A software which can cause harm to a computing system or network and has some intentionally inserted code.
- ❑ Malicious Software - > Malware
- ❑ Virus: Which replicates itself into other program. When executed the malicious code runs.
- ❑ Worm: Can execute on its own.
- ❑ Keyloggers: Grab the keystrokes.
- ❑ Spyware: Collect information from one computer and transmits to another computer illegally.
- ❑ Ransomware: Lock files on the computer.

Insider Attack

- ❑ Generated by someone who is part of the development team
 - ❑ Ex: Programmer working on a project
 - ❑ Embedded malware can come as part of OS or as part of application installed later.
- ❑ Backdoor
 - ❑ Hidden feature to gain access or manipulate something on the target system.
 - ❑ Provide remote access to computers.
 - ❑ Legitimate use
 - ❑ Illegitimate use

❑ Logic Bomb

```
if (trigger-condition==true)
{ action }
```



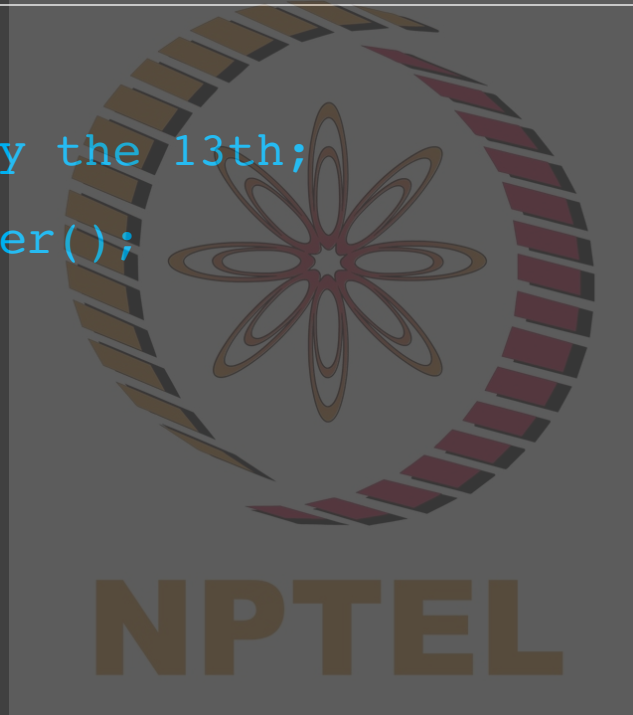
Insider Attack

legitimate code

```
if day is Friday the 13th;
```

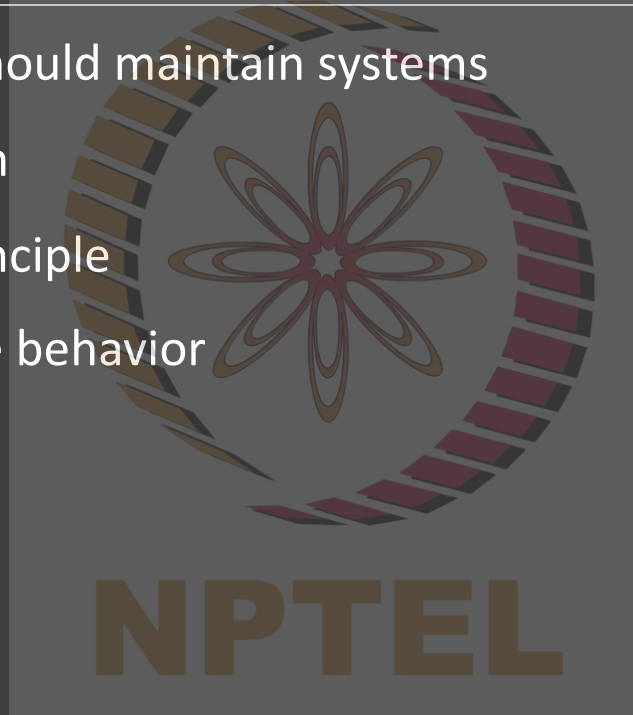
```
    crash_computer();
```

legitimate code



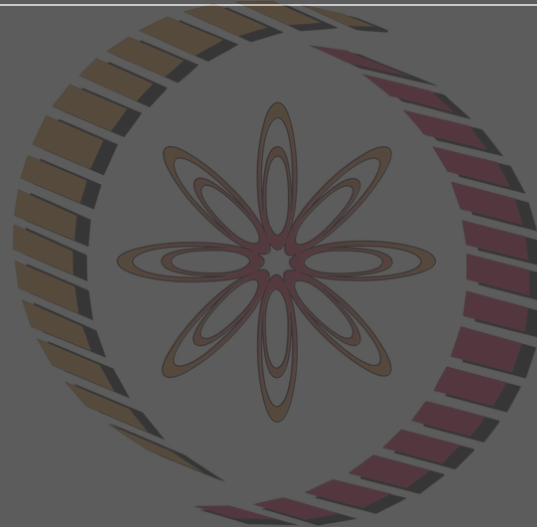
Insider Attack: Defense

- ❑ Multiple people should maintain systems
- ❑ Code walk-through
- ❑ Least privilege principle
- ❑ Monitor employee behavior



Virus

- ❑ Dormant Phase
- ❑ Propagation Phase
- ❑ Triggering Phase
- ❑ Action Phase



NPTEL

Virus: Defense

- ❑ Detection – Antivirus

- ❑ Evasion

 - ❑ Encryption

 - ❑ Polymorphic Virus

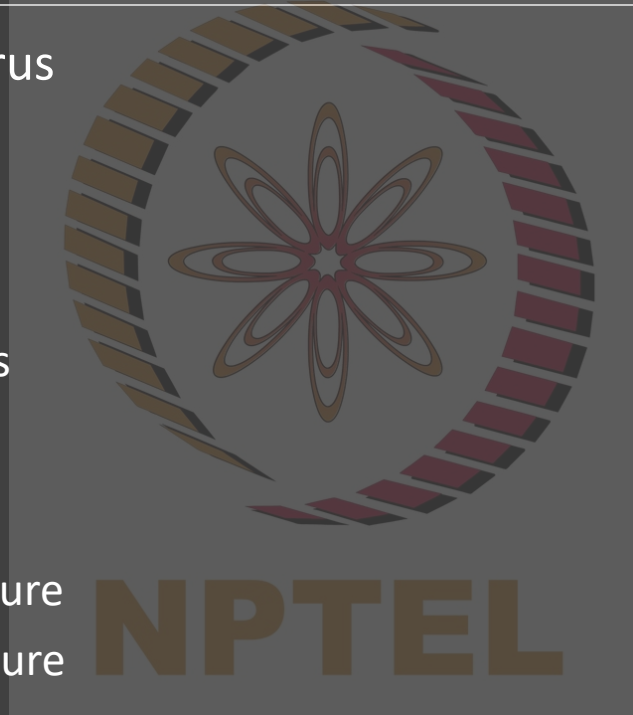
 - ❑ Metamorphic Virus

- ❑ Signatures

 - ❑ In order signature

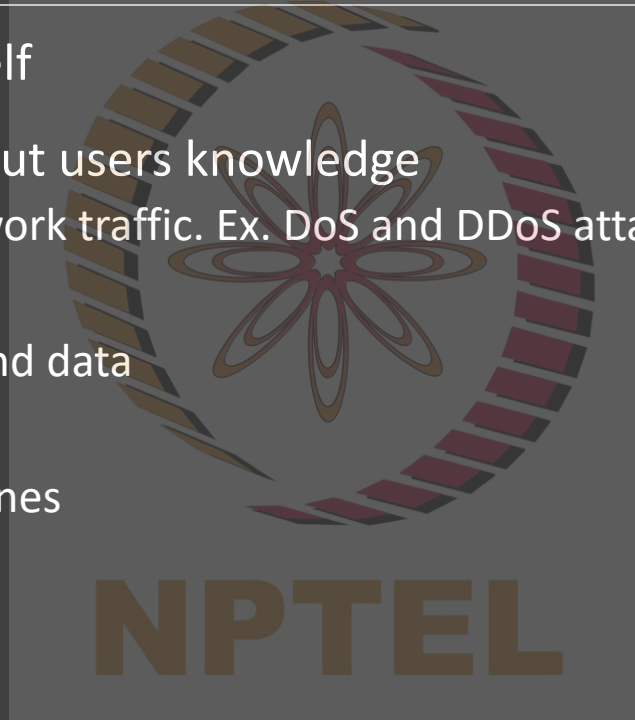
 - ❑ Conjunction signature

 - ❑ Probabilistic signature

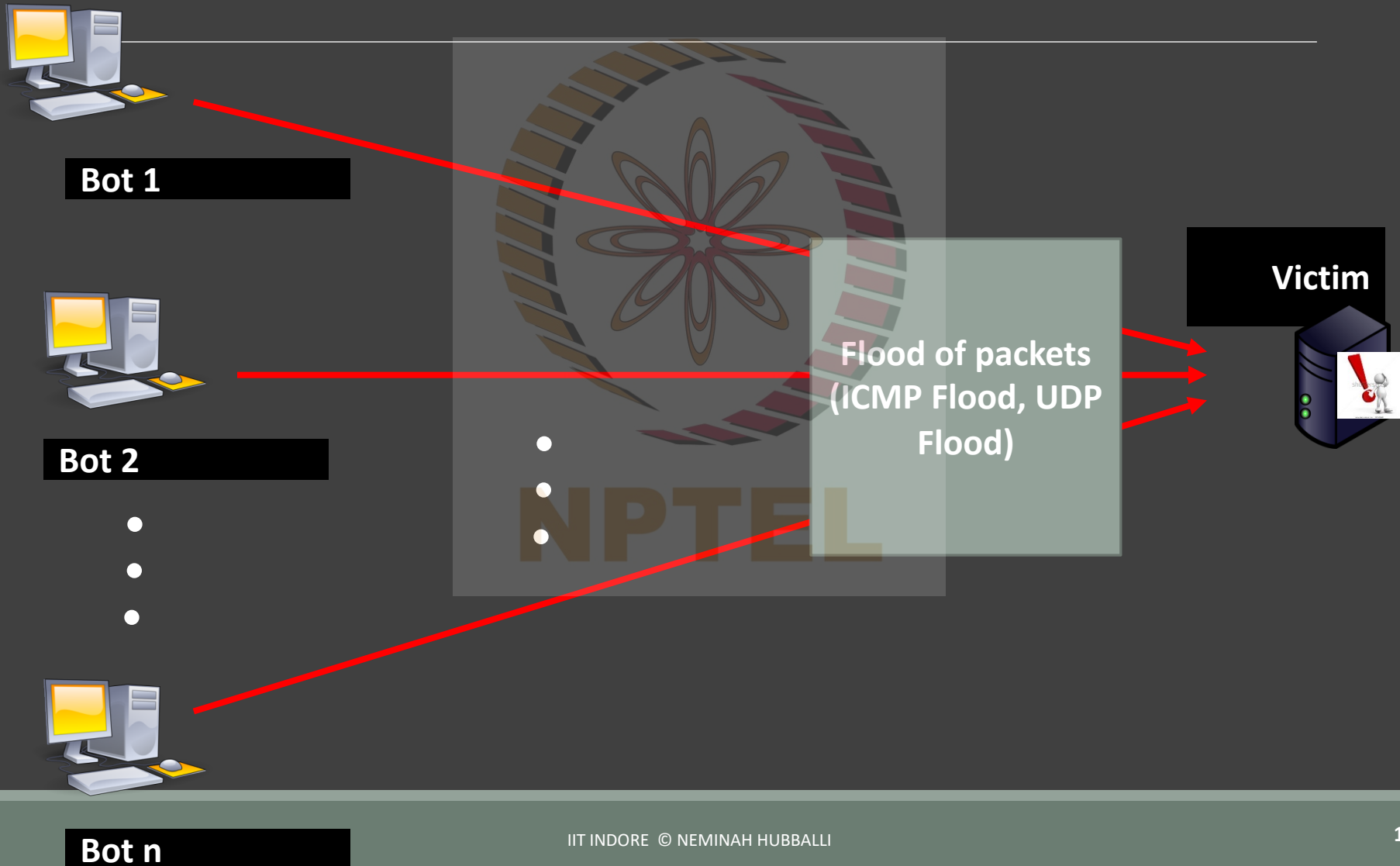


What they Can Do ?

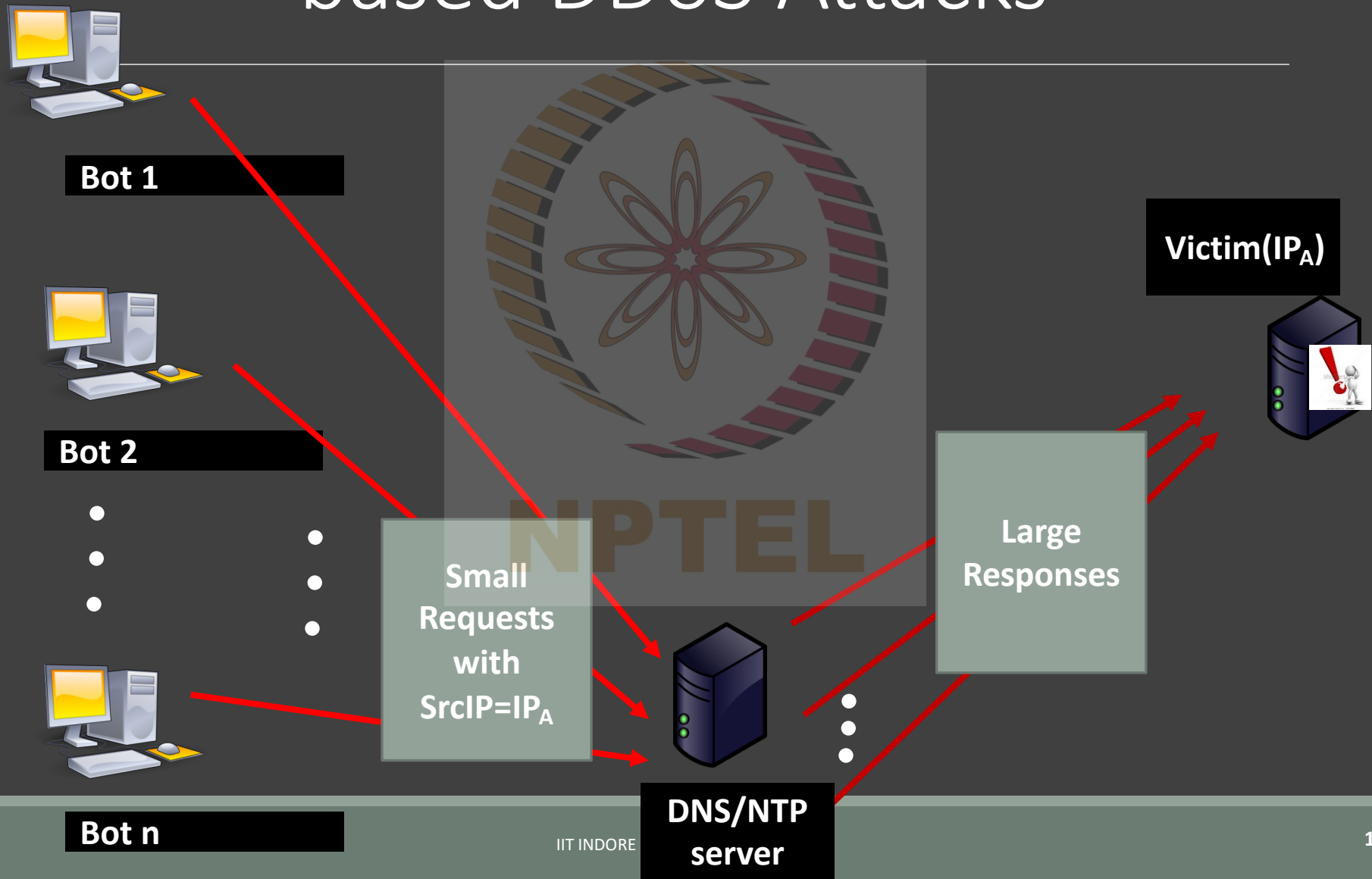
- ❑ Send copies of itself
- ❑ Take actions without users knowledge
 - ❑ Can generate network traffic. Ex. DoS and DDoS attacks
 - ❑ Harvest passwords
 - ❑ Encrypt the files and data
 - ❑ Delete files
 - ❑ Infect other machines



Flooding-based DDoS Attacks



Reflection- and Amplification-based DDoS Attacks



Botnet

- ❑ Bot: A program performing automated task
 - ❑ A bot itself is not bad
- ❑ A botnet is a collection of computers, which are connected and work under the instruction of a master in order to accomplish something
 - ❑ Typically botnets are used for committing computer crimes
- ❑ A botnet is controlled by a person or a group of people
- ❑ Usually has monetary interests
 - ❑ Advertisement companies
 - ❑ Spam mailing companies: outsource the work to bots

Botnet Components

❑ Command and Control Infrastructure

❑ Centralized

- ❑ Client server model

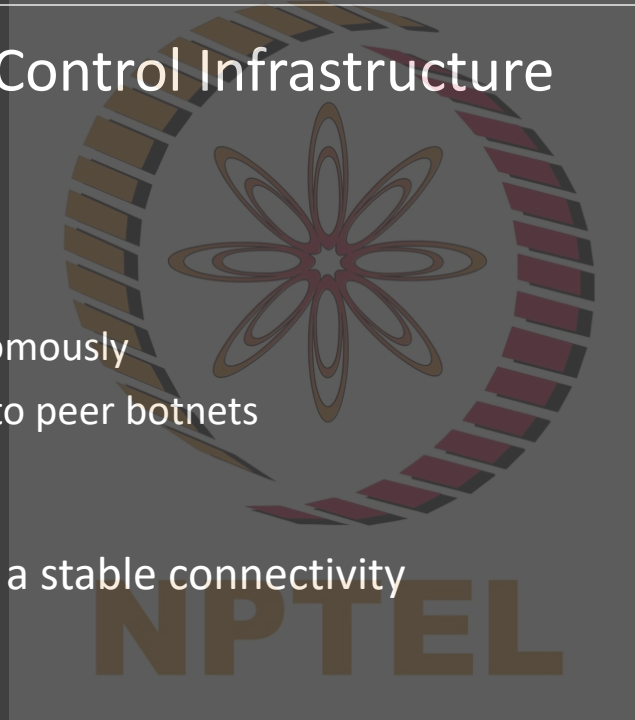
❑ Distributed

- ❑ Works more autonomously
- ❑ Also called as peer to peer botnets

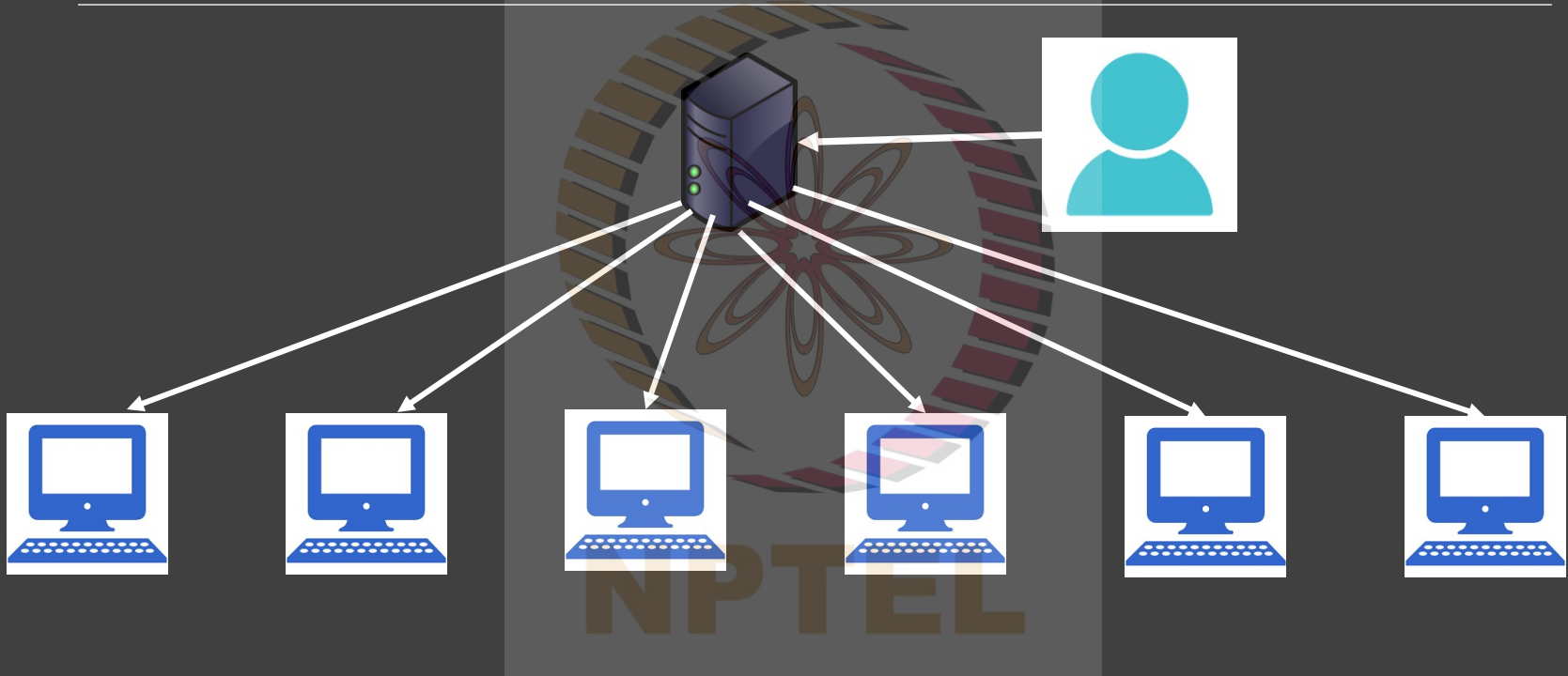
❑ Crucial

- ❑ Have to maintain a stable connectivity
- ❑ Robust
- ❑ Reaction time

❑ Communication protocol



Centralized Control



Decentralized Control

