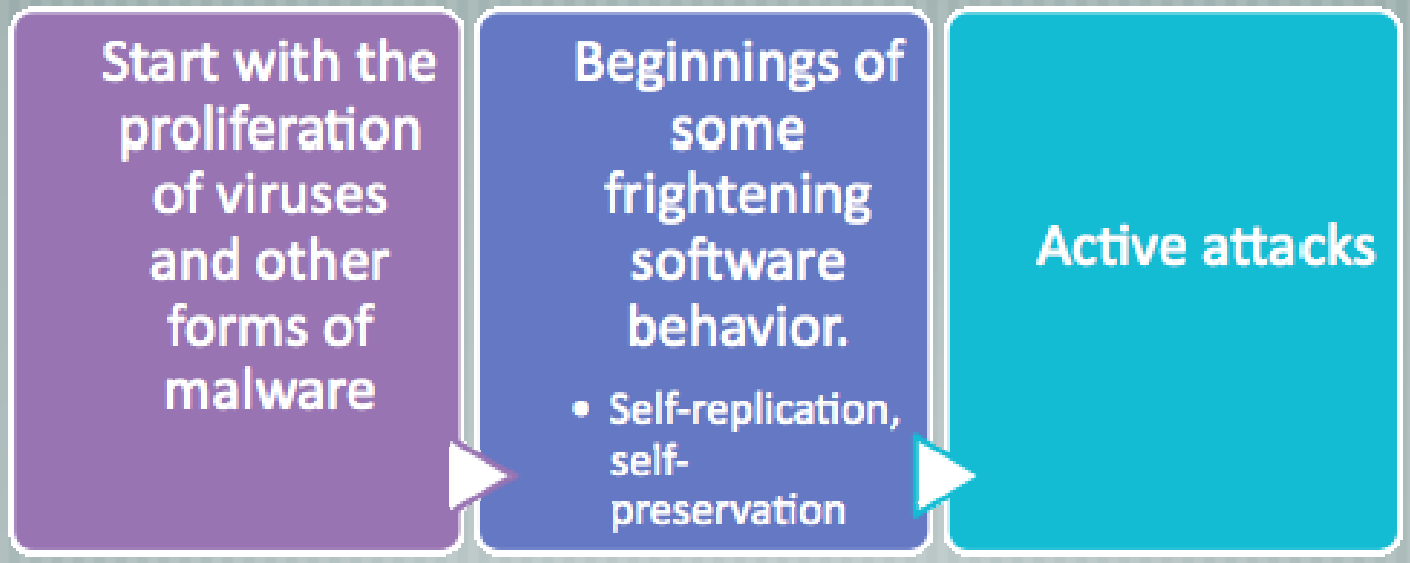
Battling the Threat of the Internet

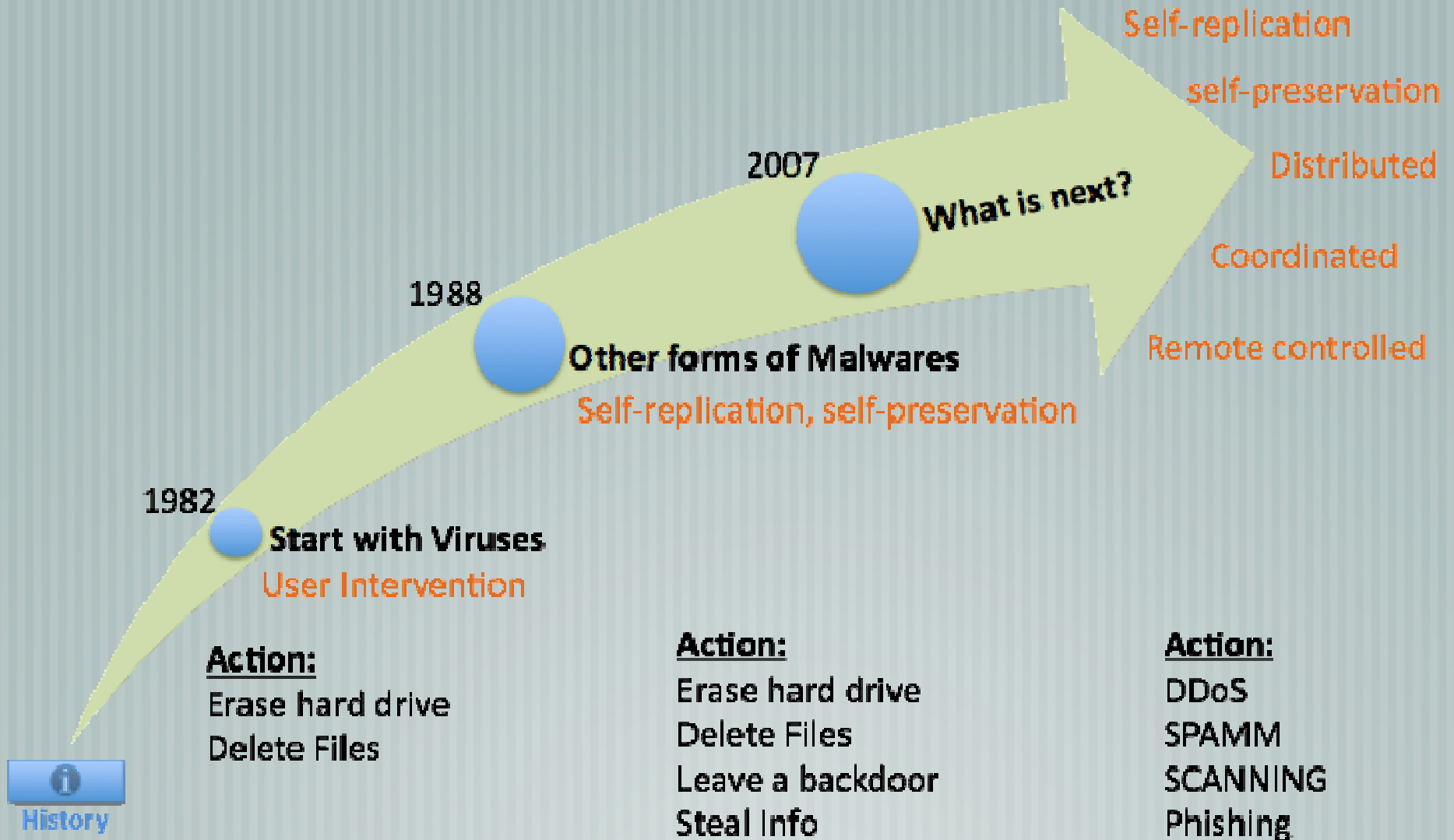
Dr. Ahmed M. Manasrah
National Advanced IPv6 Centre, Universiti Sains Malaysia,
11800 USM, Penang, Malaysia.

Introduction

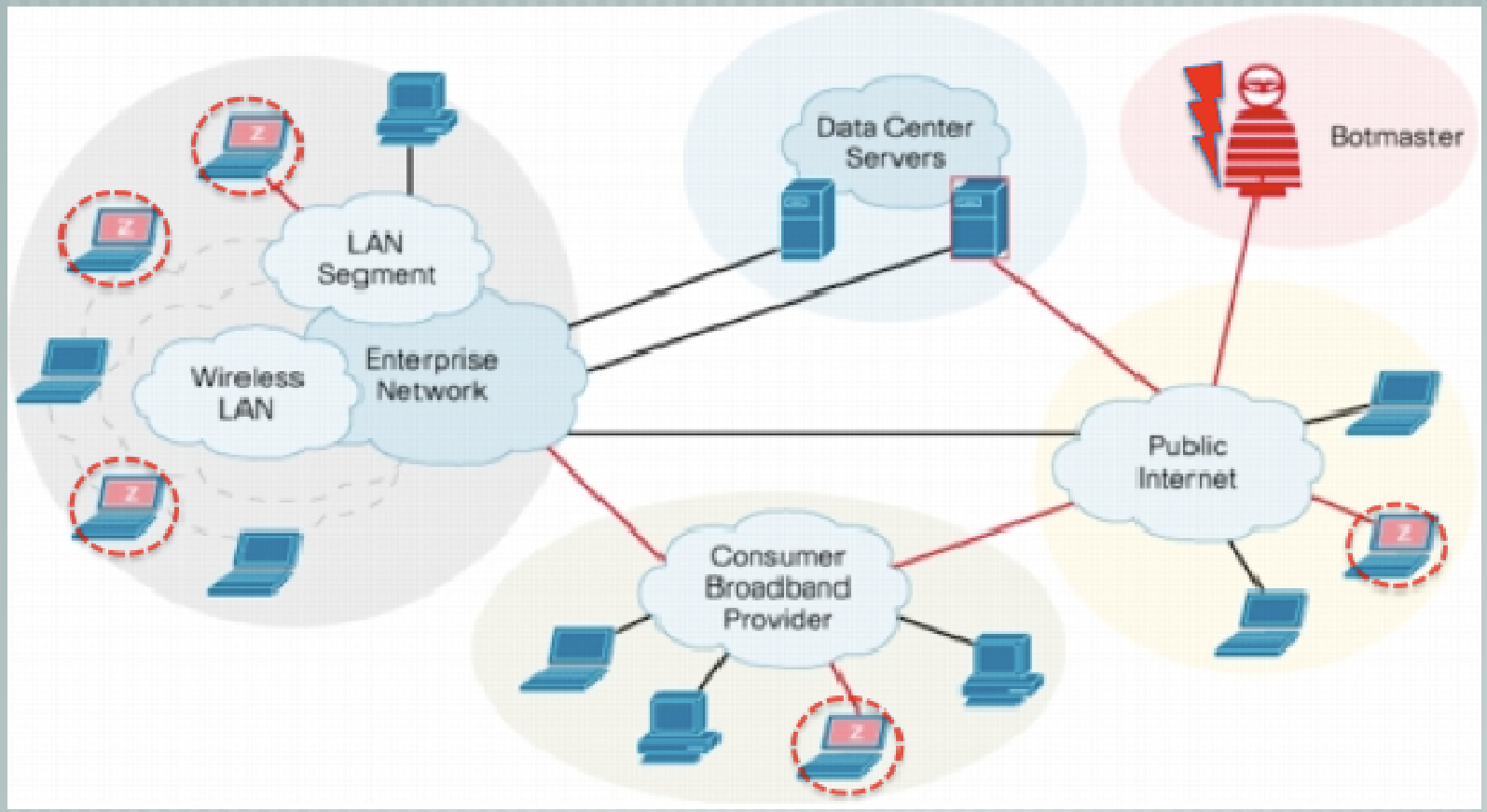
Is the emerging security threats tends to be a science fiction?



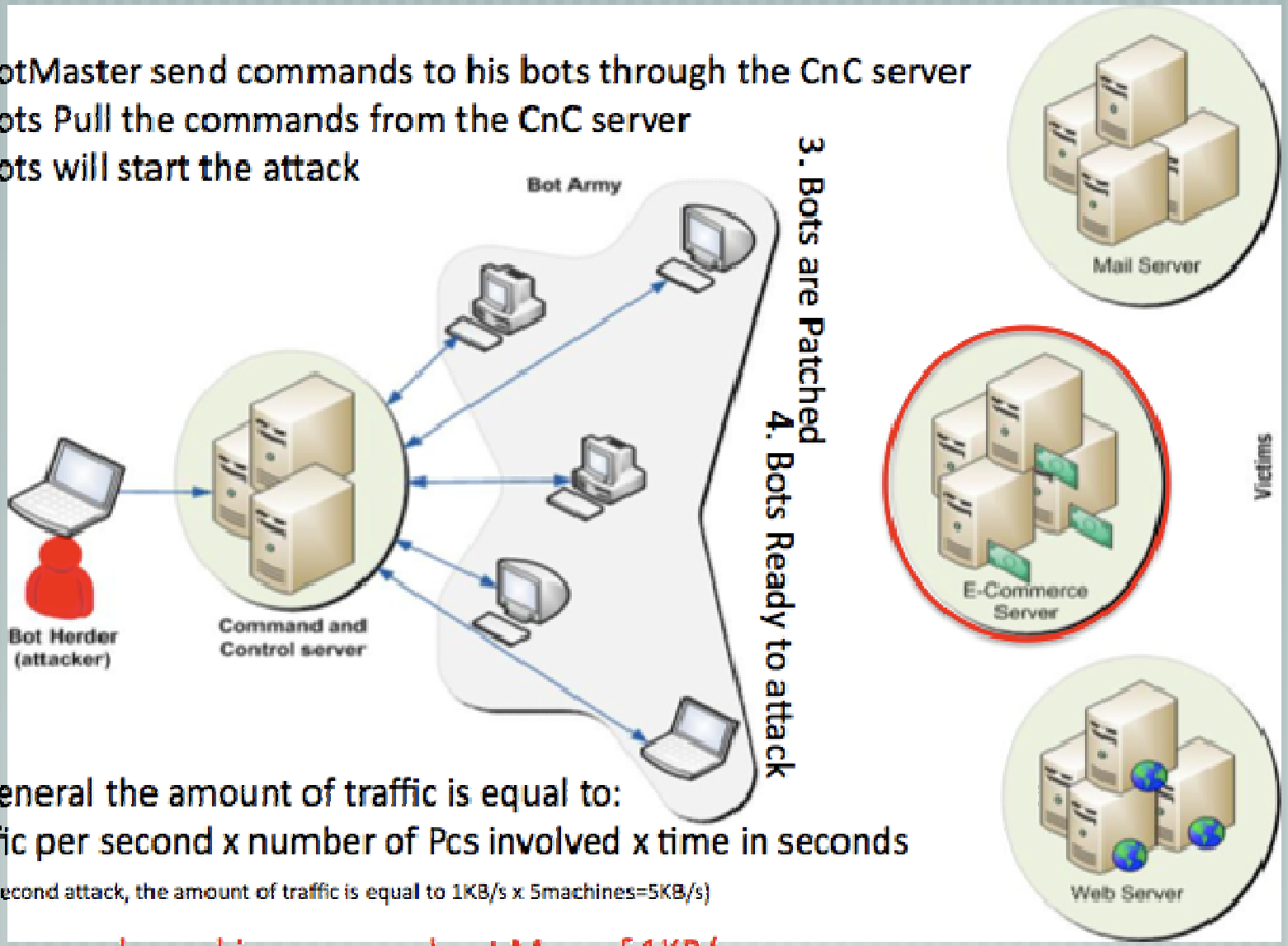
Starting to sound like a science fiction movie. Unfortunately, it's real.


Self-replication
self-preservation
Distributed
Coordinated
Remote controlled
2007
What is next?
1988
Other forms of Malwares
Self-replication, self-preservation
1982
Start with Viruses
User Intervention
Action:
Erase hard drive
Delete Files
Action:
Erase hard drive
Delete Files
Leave a backdoor
Steal Info
Action:
DDoS
SPAMM
SCANNING
Phishing
History

- **Botnet: refer to a collection of compromised computers (zombies) under a common command-and-control infrastructure.**



1. BotMaster send commands to his bots through the CnC server
2. Bots Pull the commands from the CnC server
5. Bots will start the attack



In General the amount of traffic is equal to:
Traffic per second x number of Pcs involved x time in seconds

(one second attack, the amount of traffic is equal to 1KB/s x 5machines=5KB/s)

* Assume each machine can send out Max. of 1KB/s (which is not the case)

Use of Botnets

Botnet Purposes

- ✓Attacks usually target servers belonging to government organizations.
- ✓The attacks can be used as provocation, with a cyber attack on one country being conducted from servers in another country and controlled from a third country. (USA attack)
- ✓Revenge (estonia Attack)

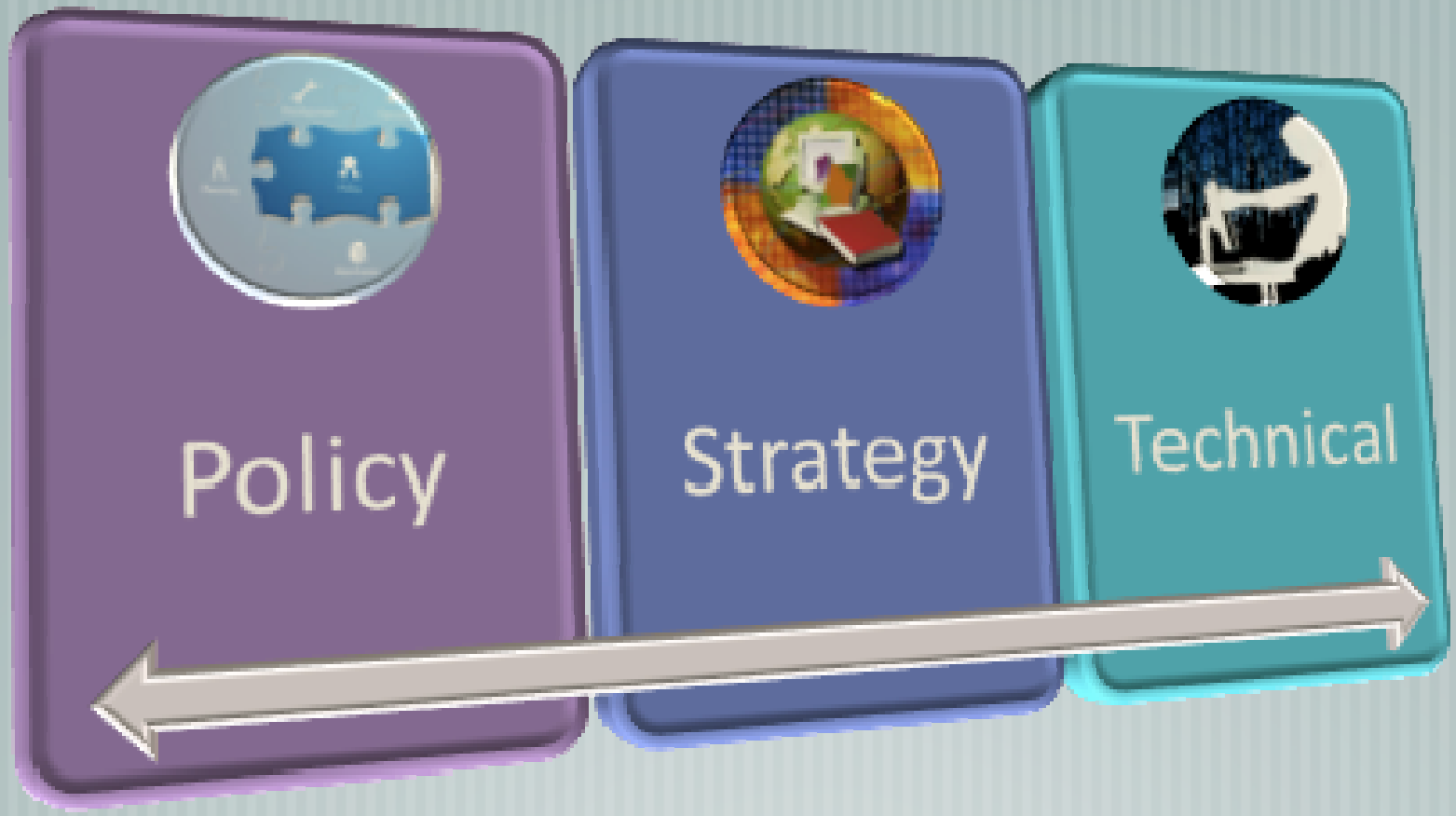
- ✓Theft of application serial numbers, login IDs, and financial information (credit card numbers).
- ✓Blackmail: DDoS, Distribute Denial-of-service attacks.
- ✓Creation or misuse of SMTP mail relays for spam (Spambot).
- ✓Click fraud.

- ✓ Fun
- ✓Challenge
- ✓ Exploring, Trying

What do we need?

- A Platform that brings together the social, law, cultural and communities together.
- To evaluate and study the various cultural factors that contributes towards the continuous infection series worldwide despite that fact that various security vendors and products are in use by different users.

Cyber-Security Platforms



Policy Platform

Cyber Security Policies

- The purpose of a Security Policy is to decide how an organization is going to protect itself.
- The policy will require two parts: a general policy & specific rules.
- The general policy sets the overall approach to Internet Security.
- The rules define what is and what is not allowed. The rules may be supplemented with procedures and other guidance.

Cyber Law

- Summarizes the legal issues related to the use of communicative, transactional, and distributive aspects of networked information devices and technology.
- It is less a distinct field of law in the way that property or contract is, as it is a domain covering many areas of law and regulation.
- Some leading topics include intellectual property, privacy, freedom of expression, and jurisdiction.

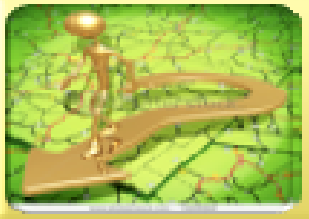
Strategy Platform

Awareness

- To build a strong foundation of cyber aware public

Human Resource Capacity Building

- To create a pool of skilled personnel in the cyber security area



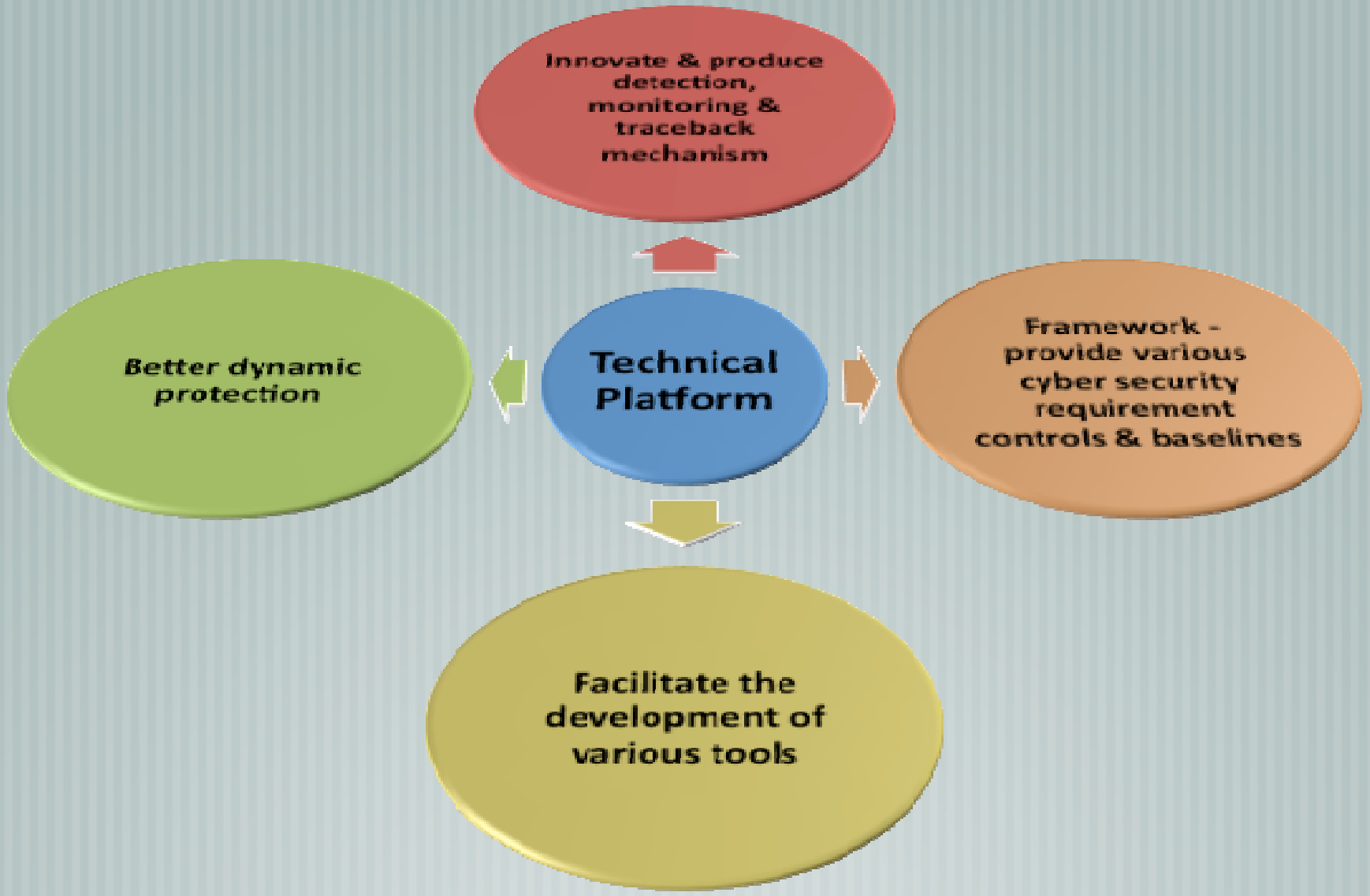
Roadmap

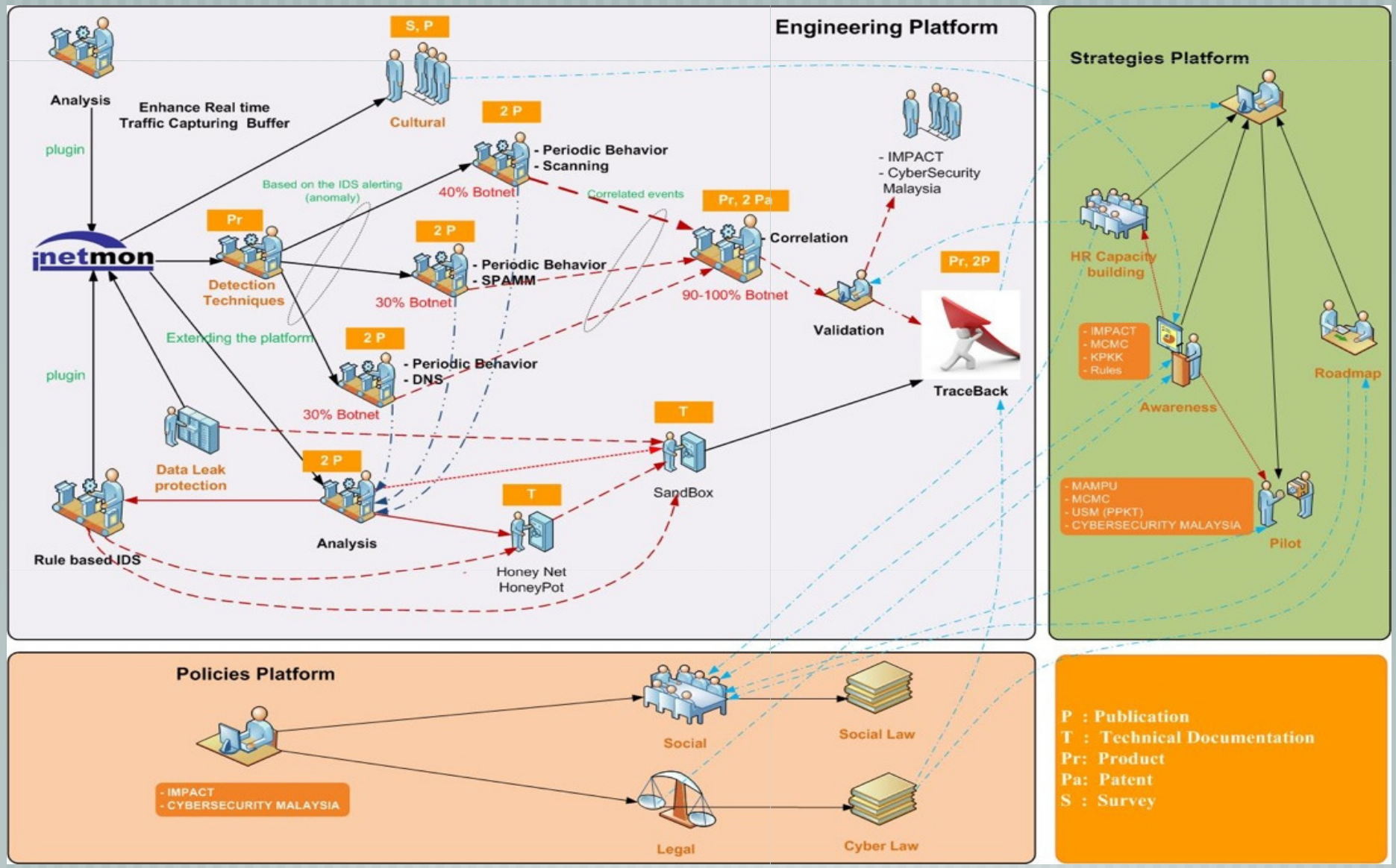
- Creation of a national guideline which identifies the areas to work on as well as the stakeholders roles and responsibilities

Pilot Project

- Pilot implementation of the Botnet Mitigation Toolkit

Technical Platform




Engineering Platform
Analysis
Enhance Real time
Traffic Capturing Buffer
plugin
S, P
Cultural
2 P
- Periodic Behavior
- Scanning
40% Botnet
Based on the IDS alerting
(anomaly)
Correlated events
Pr, 2 Pa
Correlation
- IMPACT
- CyberSecurity
Malaysia
Pr
inetmon
Detection
Techniques
2 P
- Periodic Behavior
- SPAMM
30% Botnet
90-100% Botnet
Pr, 2P
Validation
TraceBack
Extending the platform
plugin
2 P
- Periodic Behavior
- DNS
30% Botnet
T
SandBox
Data Leak
protection
2 P
Analysis
T
Honey Net
HoneyPot
Rule based IDS
Strategies Platform
HR Capacity
building
- IMPACT
- MCMC
- KPKK
- Rules
Awareness
Roadmap
- MAMPU
- MCMC
- USM (PPKT)
- CYBERSECURITY MALAYSIA
Pilot
Policies Platform
Social
Social Law
- IMPACT
- CYBERSECURITY MALAYSIA
Legal
Cyber Law
P : Publication
T : Technical Documentation
Pr: Product
Pa: Patent
S : Survey