Cyber Security -The New Frontier

SPEAKER : Mohammad Ismail
Ahmad Bakht

Presenter Introduction

Name: Mohammad Ismail
Title: Director/CEO
Company Name: SNSKIES

Industry Experience: + 20 Years

Work Experience: Internet Technologies, Internet Architecture, Internet and Telecom regulatory Policy work, Cyber Security policy and technology, Lawful Interception, Strategic and tactical LBS, IOT.

Speaker/Presenter for Multiple national and international events on internet and Cyber Technologies

CYBER SECURITY APAC 2016

Highlights

CYSEC APAC 2016 (EXPERT PANEL)

APAC Cyber Security Summit 2016

2 & 3 June 2016, DoubleTree by Hilton, Kuala Lumpur, Malaysia

Expert Speaker Panel

Christophe Durand
Head of Cyber Strategy
INTERPOL

Benoit Godart
Head of Outreach & Support
European Cybercrime Centre (EC3), EUROPOL

Drew Donovan (CPP, PSP)
Head, Protocol and Security Division
International Telecommunication Union

Brian Wilson
Deputy Director,
Global Maritime Operational Threat Response
US Department of Homeland Security

Tien Wei Chng
Head Brand Protection, Risk Management
Visa

Maria Milosavljevic
Chief Information Officer (CIO)
The Australian Transaction, Reports and Analysis Centre

Mohammad Ismail
Director/CEO
Snskies Private Limited

SoontornSirapaisan
Research Assistant
National Electronics and Computer Technology Center (NECTEC)

Ryuichi HIRANO
Counsellor,
National Center of Incident Readiness & Strategy for Cybersecurity, Government of Japan,
Cabinet Secretariat of Japan

Alan Seow
Board Member
Securing Smart Cities

CYBERSPACE OF PAKISTAN

PAKISTAN'S DIGITAL BORDERS

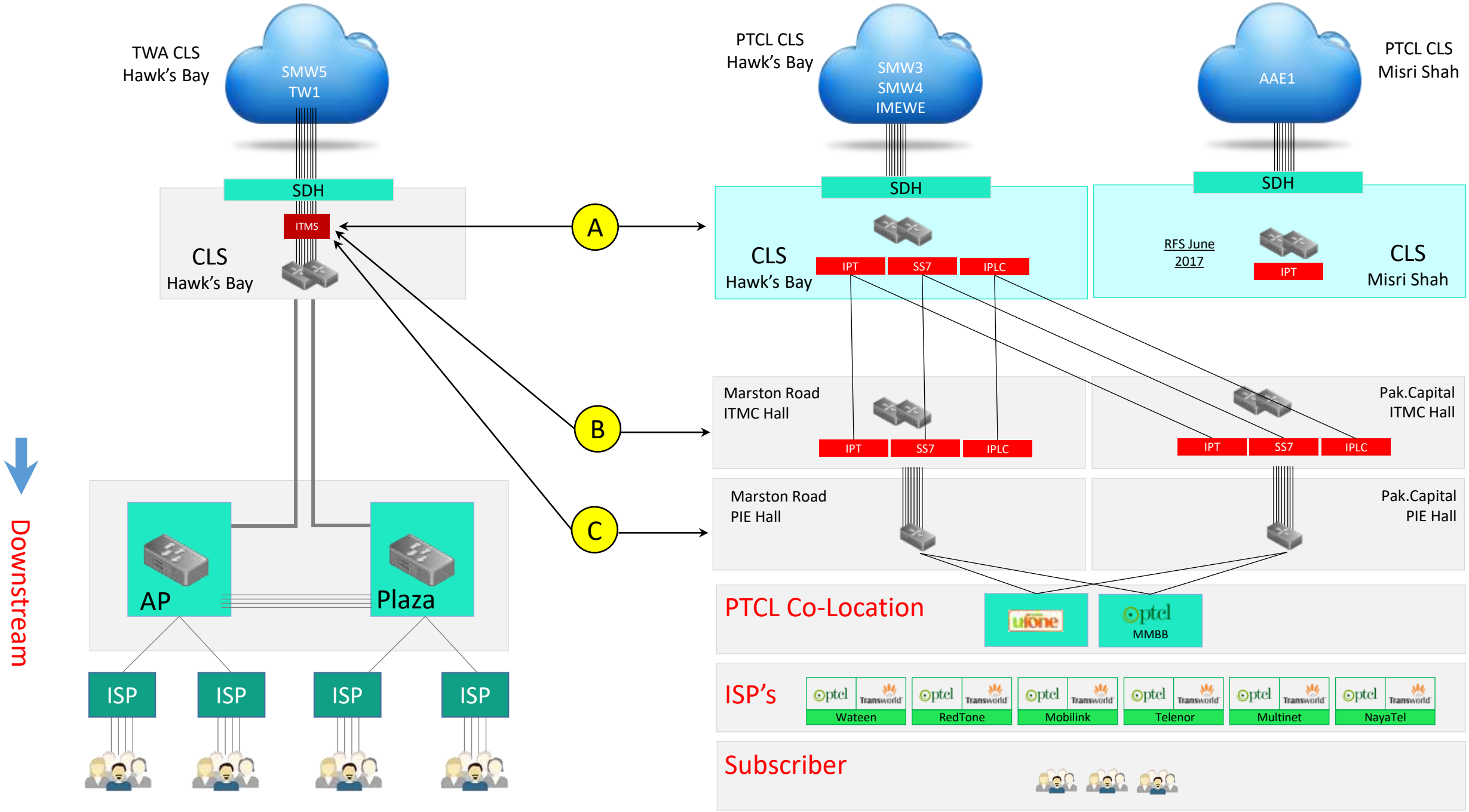
PTCL

- SEA ME WE-3
- SEA ME WE -4
- I ME WE
- AAE-1

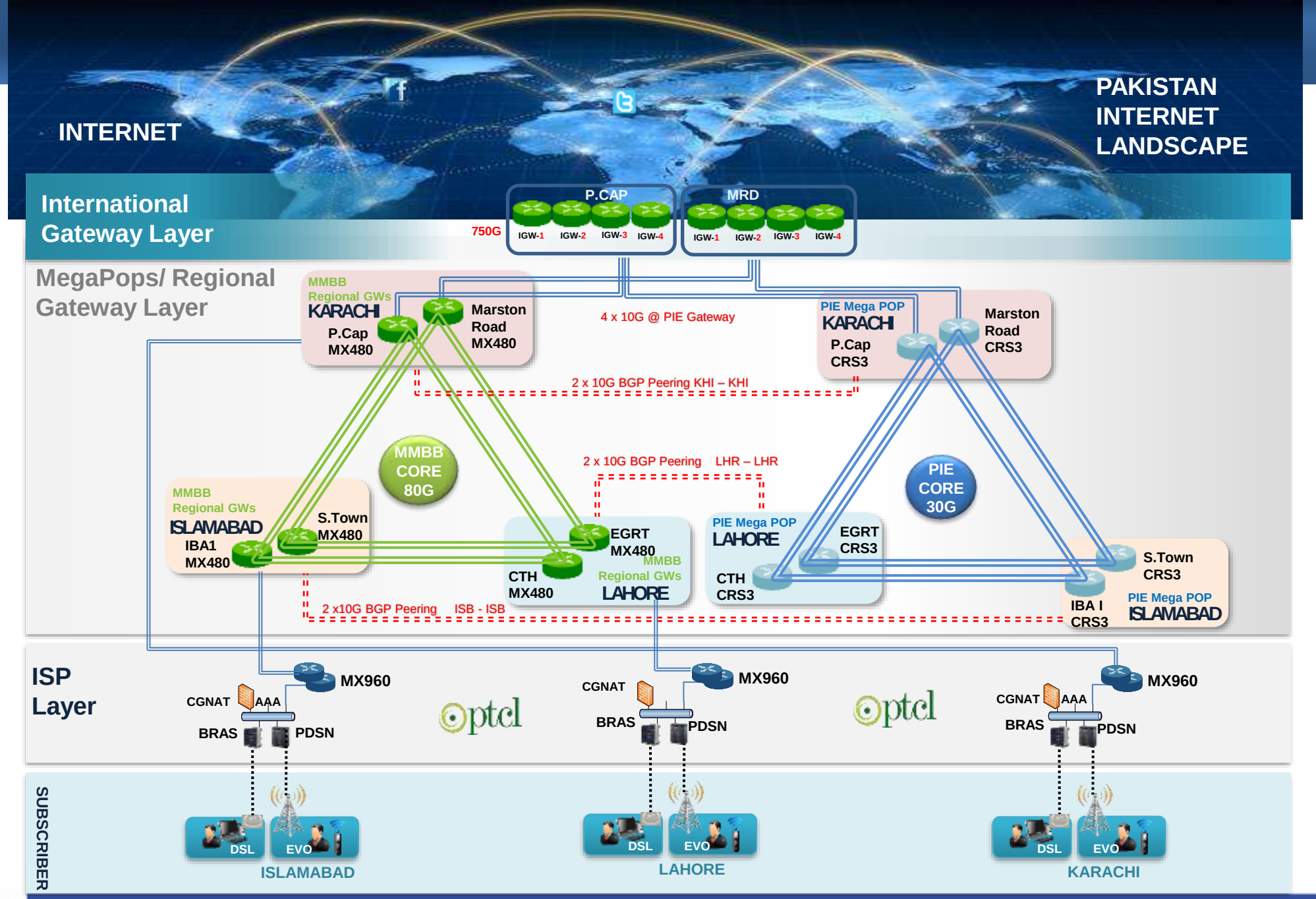
Transworld Associates

- TW-1
- SEA ME WE -5

Layer	Direction	Interface Type	2018		2019		2020		2021		2022	
			Traffic Gb	Capacity Gb	Traffic Gb	Capacity Gb	Traffic Gb	Capacity Gb	Traffic Gb	Capacity Gb	Traffic Gb	Capacity Gb
PTCL IGW	Upwards (internati onal)	10/100G	1,125	1,607	1,603	2,290	2,289	3,270	3,264	4,663	4,656	6,651
IGW TWA	Upwards(Internati onal)	10/100G	425	660	525		760				1200	
Total			1550		2128		3049		3664		5856	


TWA CLS
Hawk's Bay
SMW5
TW1
SDH
ITMS
CLS
Hawk's Bay
A
B
C
PTCL CLS
Hawk's Bay
SMW3
SMW4
IMEWE
SDH
CLS
Hawk's Bay
IPT
SS7
IPLC
PTCL CLS
Misri Shah
AAE1
SDH
RFS June
2017
IPT
CLS
Misri Shah
Marston Road
ITMC Hall
IPT
SS7
IPLC
Pak.Capital
ITMC Hall
IPT
SS7
IPLC
Marston Road
PIE Hall
Pak.Capital
PIE Hall
Downstream
AP
Plaza
ISP
ISP
ISP
ISP
PTCL Co-Location
ufone
optel
MMBB
ISP's
optel
Transworld
Wateen
RedTone
Mobilink
Telenor
Multinet
NayaTel
Subscriber

PAKISTAN INTERNET LANDSCAPE



PAKISTAN INTERNET LANDSCAPE

International Gateway Layer

750G

P.CAP: IGW-1 IGW-2 IGW-3 IGW-4

MRD: IGW-1 IGW-2 IGW-3 IGW-4

MegaPops/ Regional Gateway Layer

Converge two Mega cores into 1 single UNIFIED core

SNS RECOMMENDED DESIGN:

Incorporate NEW NODES in UNIFIED MSC

MMBB Regional GWs
KARACHI
P.Cap MX480
Marston Road MX480

PIE Mega POP
KARACHI
P.Cap CRS3
Marston Road CRS3

MMBB CORE

PIE CORE

MMBB Regional GWs
ISLAMABAD
IBA1 MX480
S.Town MX480

MMBB Regional GWs
LAHORE
CTH MX480
EGRT MX480

PIE Mega POP
LAHORE
CTH CSR3
EGRT CRS3

PIE Mega POP
ISLAMABAD
IBA I CSR3
S.Town CRS3

MX960 / Cisco

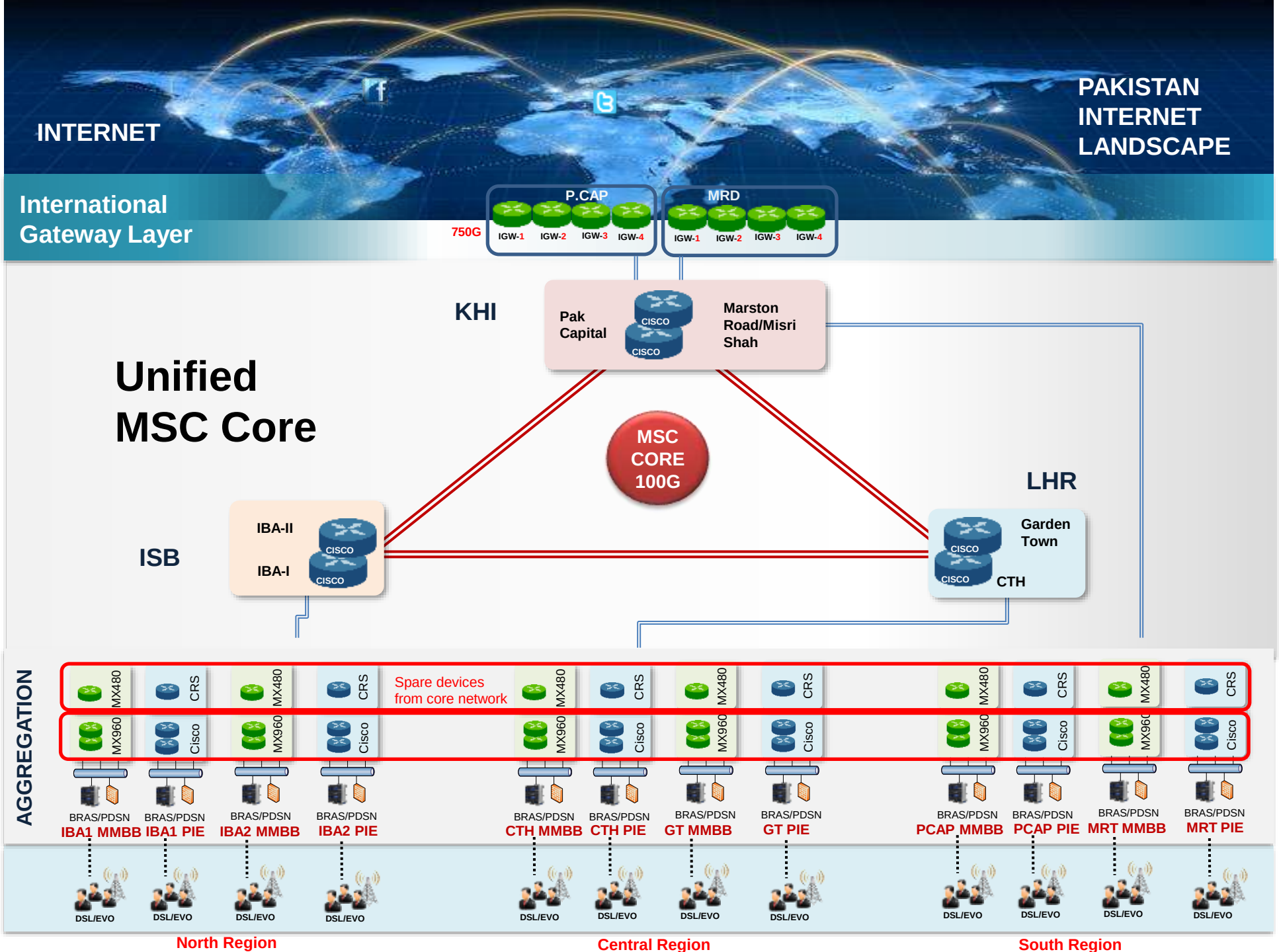
BRAS/PDSN IBA1 MMBB
BRAS/PDSN IBA1 PIE
BRAS/PDSN IBA2 MMBB
BRAS/PDSN IBA2 PIE
BRAS/PDSN CTH MMBB
BRAS/PDSN CTH PIE
BRAS/PDSN GT MMBB
BRAS/PDSN GT PIE
BRAS/PDSN PCAP MMBB
BRAS/PDSN PCAP PIE
BRAS/PDSN MRT MMBB
BRAS/PDSN MRT PIE

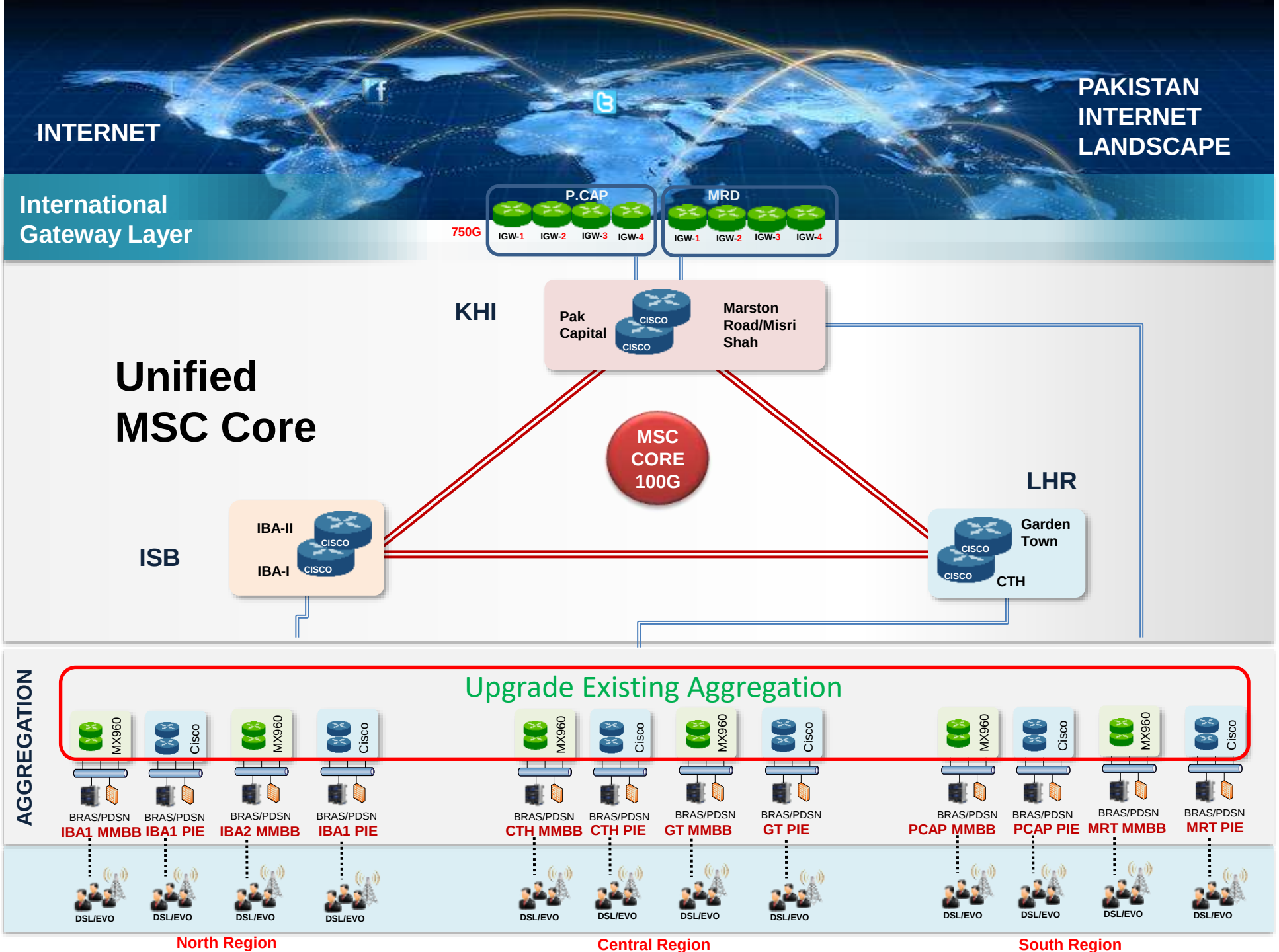
DSL/EVO

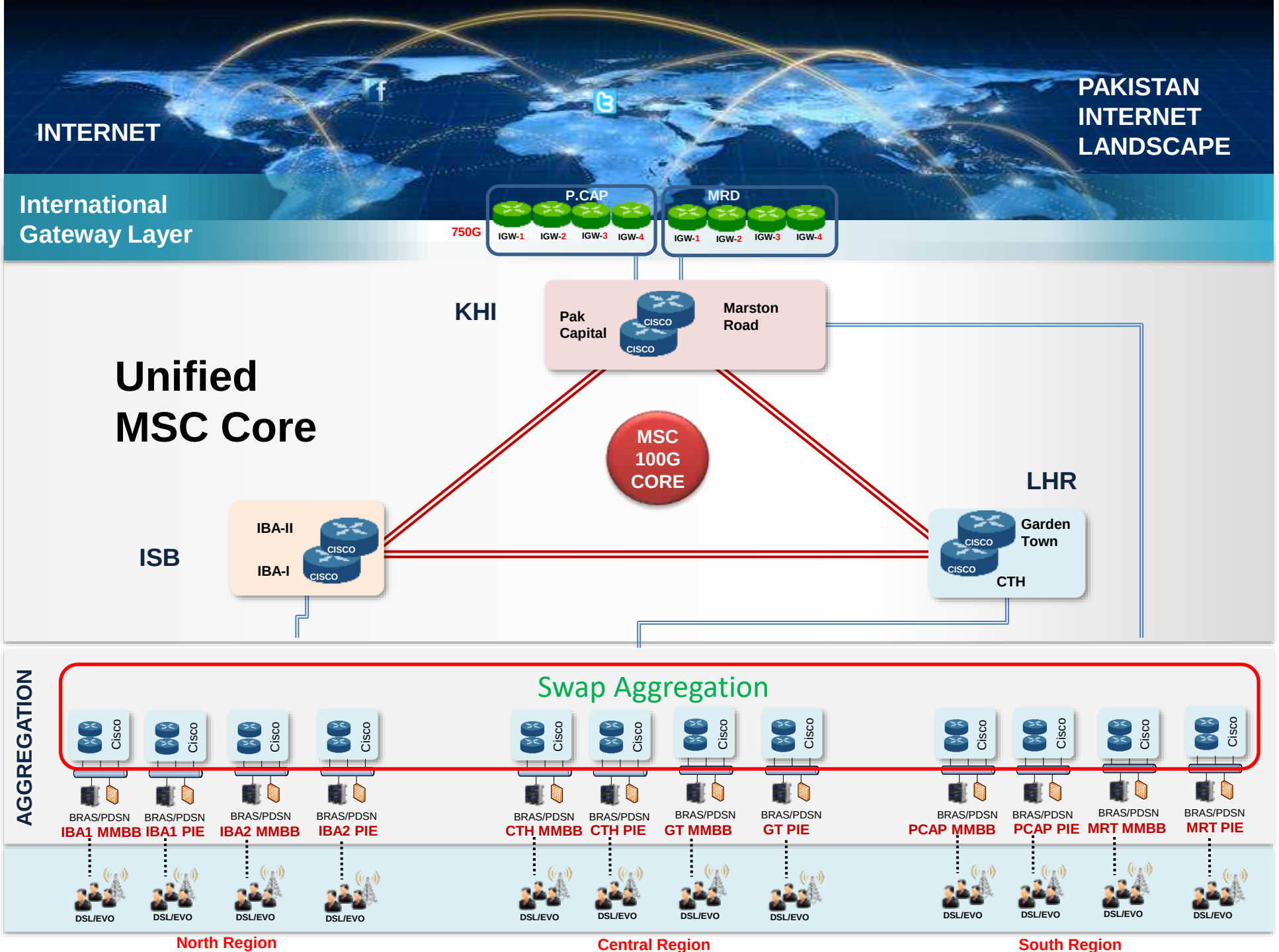
North Region

Central Region

South Region


INTERNET
PAKISTAN INTERNET LANDSCAPE
International Gateway Layer
750G
P.CAP
IGW-1
IGW-2
IGW-3
IGW-4
MRD
IGW-1
IGW-2
IGW-3
IGW-4
KHI
Pak Capital
CISCO
CISCO
Marston Road/Misri Shah
Unified MSC Core
MSC CORE 100G
LHR
Garden Town
CISCO
CISCO
CTH
ISB
IBA-II
IBA-I
CISCO
CISCO
AGGREGATION
MX480
CRS
MX480
CRS
Spare devices from core network
MX480
CRS
MX480
CRS
MX480
CRS
MX480
CRS
MX960
Cisco
MX960
Cisco
MX960
Cisco
MX960
Cisco
MX960
Cisco
MX960
Cisco
MX960
Cisco
BRAS/PDSN
IBA1 MMBB
BRAS/PDSN
IBA1 PIE
BRAS/PDSN
IBA2 MMBB
BRAS/PDSN
IBA2 PIE
BRAS/PDSN
CTH MMBB
BRAS/PDSN
CTH PIE
BRAS/PDSN
GT MMBB
BRAS/PDSN
GT PIE
BRAS/PDSN
PCAP MMBB
BRAS/PDSN
PCAP PIE
BRAS/PDSN
MRT MMBB
BRAS/PDSN
MRT PIE
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
North Region
Central Region
South Region


INTERNET
PAKISTAN
INTERNET
LANDSCAPE
International
Gateway Layer
750G
P.CAP
IGW-1
IGW-2
IGW-3
IGW-4
MRD
IGW-1
IGW-2
IGW-3
IGW-4
KHI
Pak
Capital
CISCO
CISCO
Marston
Road/Misri
Shah
Unified
MSC Core
MSC
CORE
100G
LHR
ISB
IBA-II
IBA-I
CISCO
CISCO
Garden
Town
CISCO
CISCO
CTH
AGGREGATION
Upgrade Existing Aggregation
MX960
Cisco
MX960
Cisco
MX960
Cisco
MX960
Cisco
MX960
Cisco
MX960
Cisco
BRAS/PDSN
IBA1 MMBB
BRAS/PDSN
IBA1 PIE
BRAS/PDSN
IBA2 MMBB
BRAS/PDSN
IBA1 PIE
BRAS/PDSN
CTH MMBB
BRAS/PDSN
CTH PIE
BRAS/PDSN
GT MMBB
BRAS/PDSN
GT PIE
BRAS/PDSN
PCAP MMBB
BRAS/PDSN
PCAP PIE
BRAS/PDSN
MRT MMBB
BRAS/PDSN
MRT PIE
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
DSL/EVO
North Region
Central Region
South Region


INTERNET
PAKISTAN INTERNET LANDSCAPE
International Gateway Layer
750G
P.CAP
IGW-1
IGW-2
IGW-3
IGW-4
MRD
IGW-1
IGW-2
IGW-3
IGW-4
KHI
Pak Capital
CISCO
CISCO
Marston Road
Unified MSC Core
MSC 100G CORE
LHR
Garden Town
CISCO
CISCO
CTH
ISB
IBA-II
IBA-I
CISCO
CISCO
AGGREGATION
Swap Aggregation
Cisco
BRAS/PDSN
IBA1 MMBB
IBA1 PIE
IBA2 MMBB
IBA2 PIE
CTH MMBB
CTH PIE
GT MMBB
GT PIE
PCAP MMBB
PCAP PIE
MRT MMBB
MRT PIE
DSL/EVO
North Region
Central Region
South Region

THREAT LANDSCAPE

CYBER SECURITY – AN OVERVIEW

- ICT has become an integral part of our life for productivity, growth and innovation.
- How we protect our privacy & freedom and maintain an open and innovative cyberspace will determine how effective our society functions.

Challenge:

The complexity of evolving trends:

Social media, Mobile, Cloud computing, Advanced Persistent Attacks.

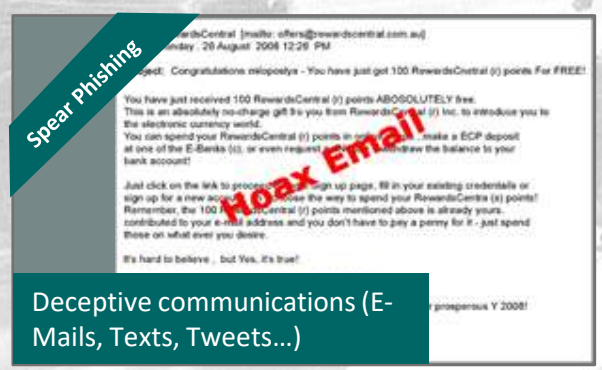
Cyber crime costs global economy $445 billion a year.

CYBER SECURITY - ATTACK STRATEGIES

blocking user access to multiple websites!

Border Gateway Protocol (BGP) Hijacking

Domain Name System (DNS) Hijacking



Deceptive communications (E-Mails, Texts, Tweets…)

Malicious software to disrupt computers

Mobile Devices & Applications attacks

Entice users to click on Malicious Links

Cyber protests that are socially or politically motivated

Theft of Intellectual Property or Data

CYBER SECURITY - THREAT LANDSCAPE

DATA THEFT

CYBER CRIME

INFO ON SENSITIVE LOCATIONS

MILITARY ESPIONAGE

INDUSTRY ESPIONAGE

THEFT OF TRADE SECRETS

ECONOMIC ESPIONAGE

TRADE MONOPOLY

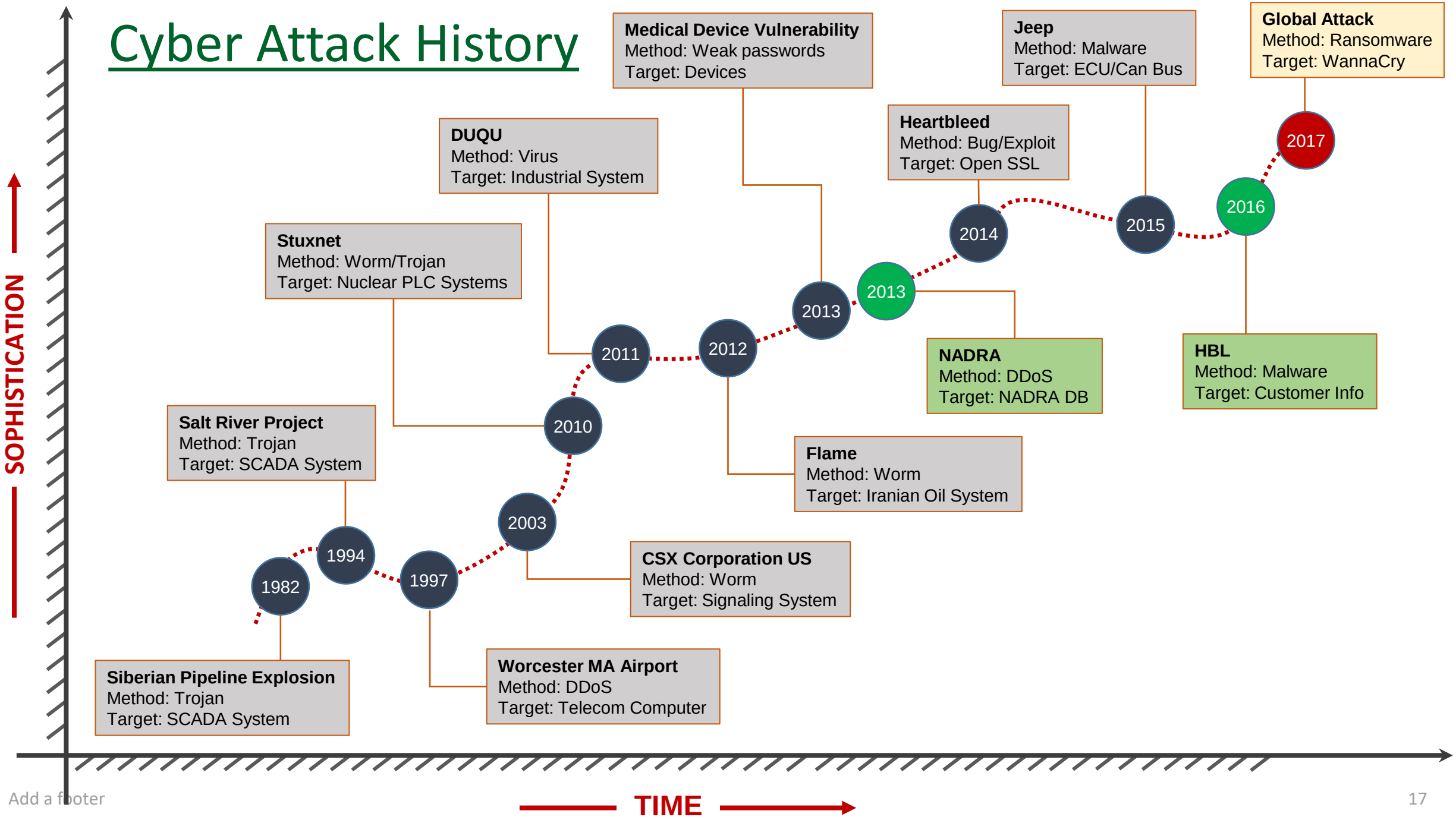
OFFICIAL WEBSITES DEFAMING

NATIONAL SECURITY

CYBER WARFARE

HACKING FOR POLITICAL MOTIVES

Cyber Attack History



What has changed?

The attacker has changed

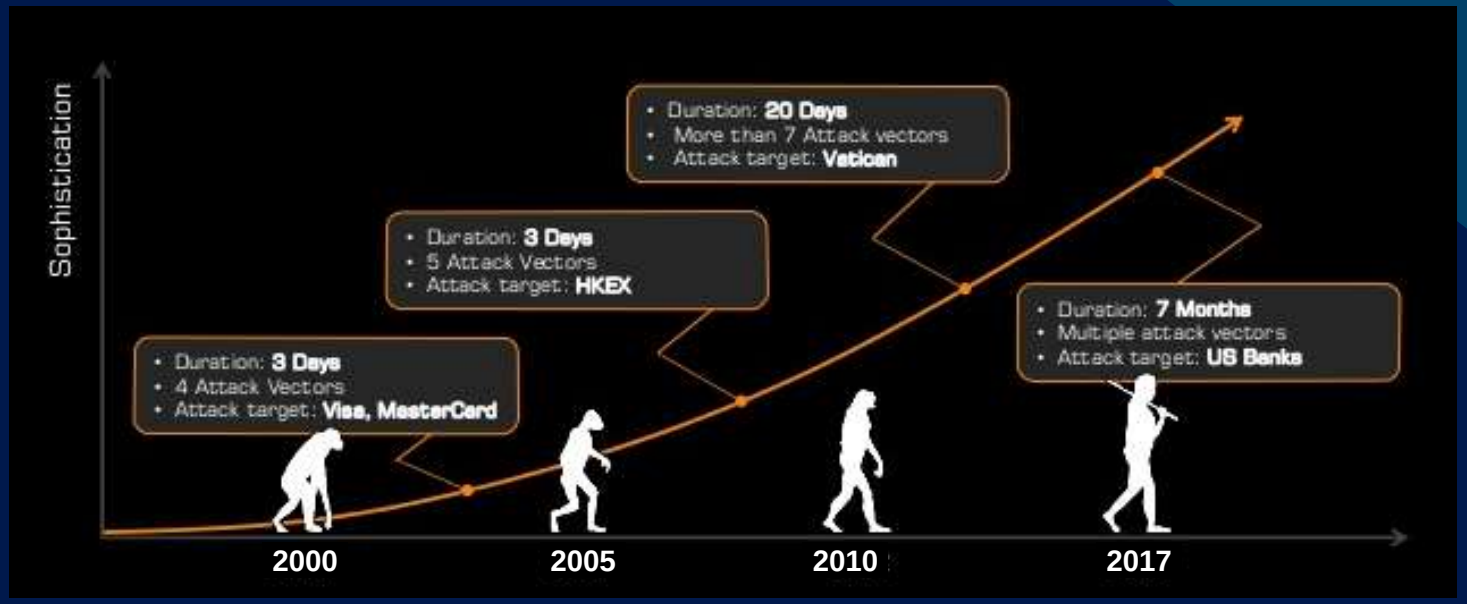
- Nation-states
- Criminal Organizations
- Political Groups

Attack Strategy Evolved

- Pateint-multisteps process
- Compromise user, then expand

Attack techniques evolved

- New ways of delivering malware
- Hiding malware communications
- Signature avoidance



How a cyber attack is manipulated

1 - INVESTIGATION
Harvesting email addresses, conference information, etc.

2 - WEAPONIZATION
Coupling exploit with backdoor into a deliverable payload.

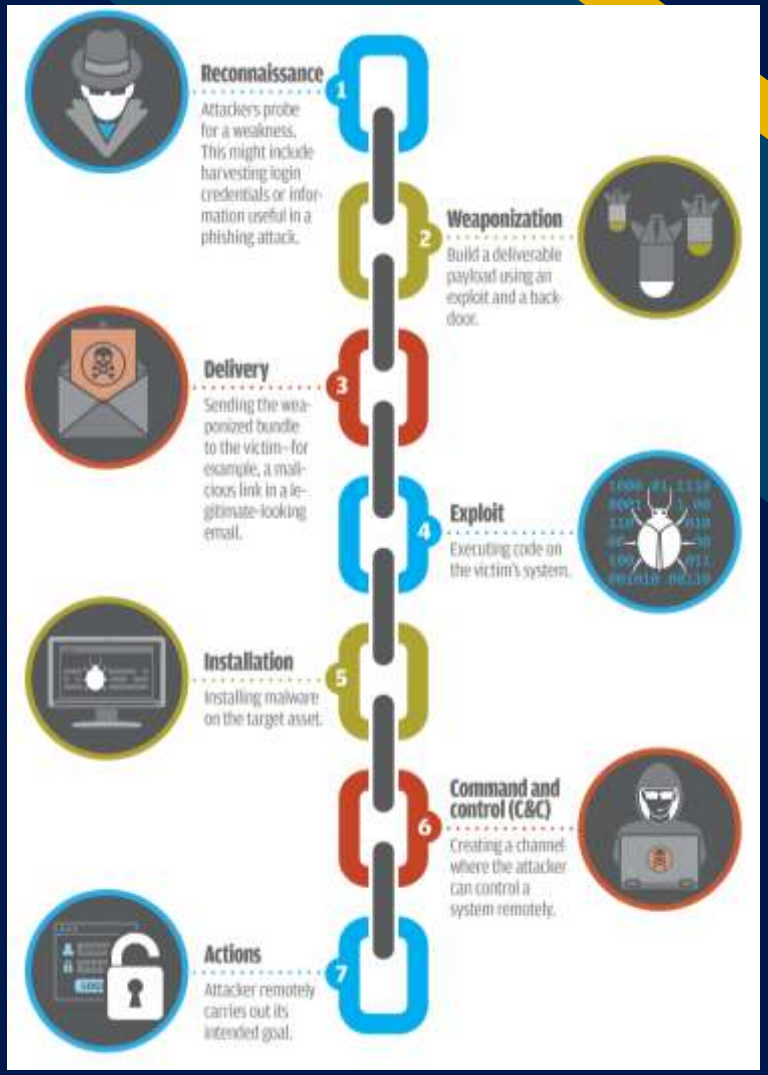
3 - DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 - EXPLOITATION
Exploiting a vulnerability to execute code on victim's system.

5 - INSTALLATION
Installing malware on the asset.

6 - COMMAND & CONTROL
Command channel for remote manipulation of victim.

7 - ACTION ON OBJECTIVES
With 'Hands-on-keyboard' access intruders accomplish their prime goal.



Cyber Attacks – Whats up next?

Information warfare - Spying

- Fileless Malware

Cyber warfare – The Fifth Element

- Drone Jacking
- Satellite Control

Ransomware

- Driverless Cars Highly dependent on remote access networking.

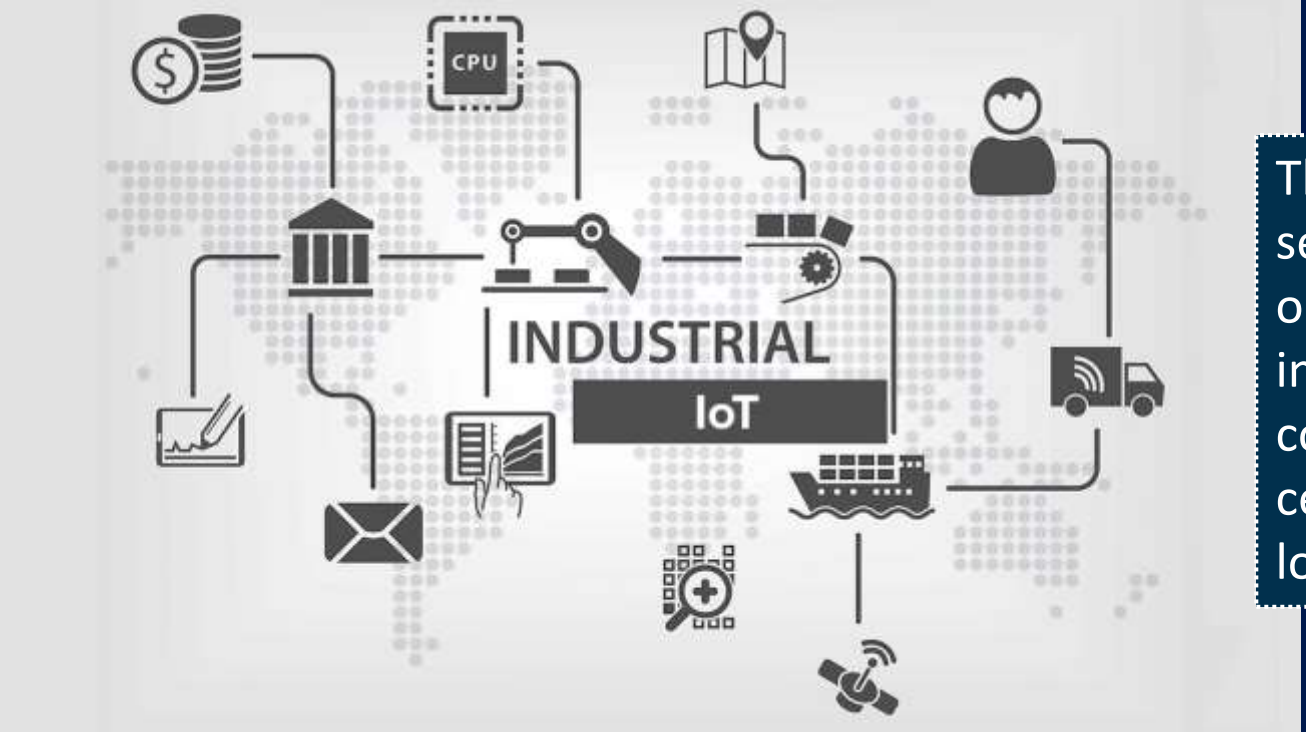
In terms of cyber attack, cyber crimes including:

- Malware
- POS Malware
- Account Hijacking
- DDoS
- DNS Hijacking
- Email Harvesting
- Defacement
- Malvertising

always tend to top the list.

Industrial IOT (IIOT)

The Industrial Internet of Things (IIoT), is the integration of complex machinery with networked sensors & softwares.



The sensors talk to the servers over electrical & optical signals, & all interconnected machines communicate back to a centralized control system located in a datacenter.

According to Industrial Internet Consortium (IIC), only 25% of organization have a clear IIoT security strategy, Leaders are struggling most with data security (51%) and privacy (39%). Overcoming these barriers is essential to the success of the IIoT.

Pak Cyber Law

Prevention of Electronic Crime Act

Salient features of the new bill:


Pakistan's first-ever Cyber Security Centre launched

+MGN

Islamabad: Pakistan government's Cyber Security Centre has been inaugurated at Air University in Islamabad to deal with cyber security challenges in the digital age.

1. Unauthorized access to critical infrastructure information system or data
   - Punishment: Up to three years imprisonment, Rs1 million fine or both
2. Interference with critical infrastructure information system with dishonest intention
   - Punishment: Up to seven years, Rs10 million fine or both
3. Glorification of an offence relating to terrorism
   - Punishment: Up to seven years, Rs10 million fine or both
4. Producing, making, generating, adapting, exporting, supplying, offering to supply or importing a device for use in an offence
   - Punishment: Up to six months imprisonment, Rs50 thousand or both
5. Obtaining, selling, possessing, transmitting or using another person's identity information without authorization
   - Punishment: Up to three years imprisonment, Rs5 million fine or both

Types of Malware

TROJANS 76%

INFECTED BY PRETENDING TO BE A REAL PROGRAM

11% WORMS

INFECTED BY SPREADING ACROSS COMPUTER NEWTORKS

VIRUSES 09%

INFECTED BY REPLICATING ITSELF AND SPREADING

Individual Level Protection

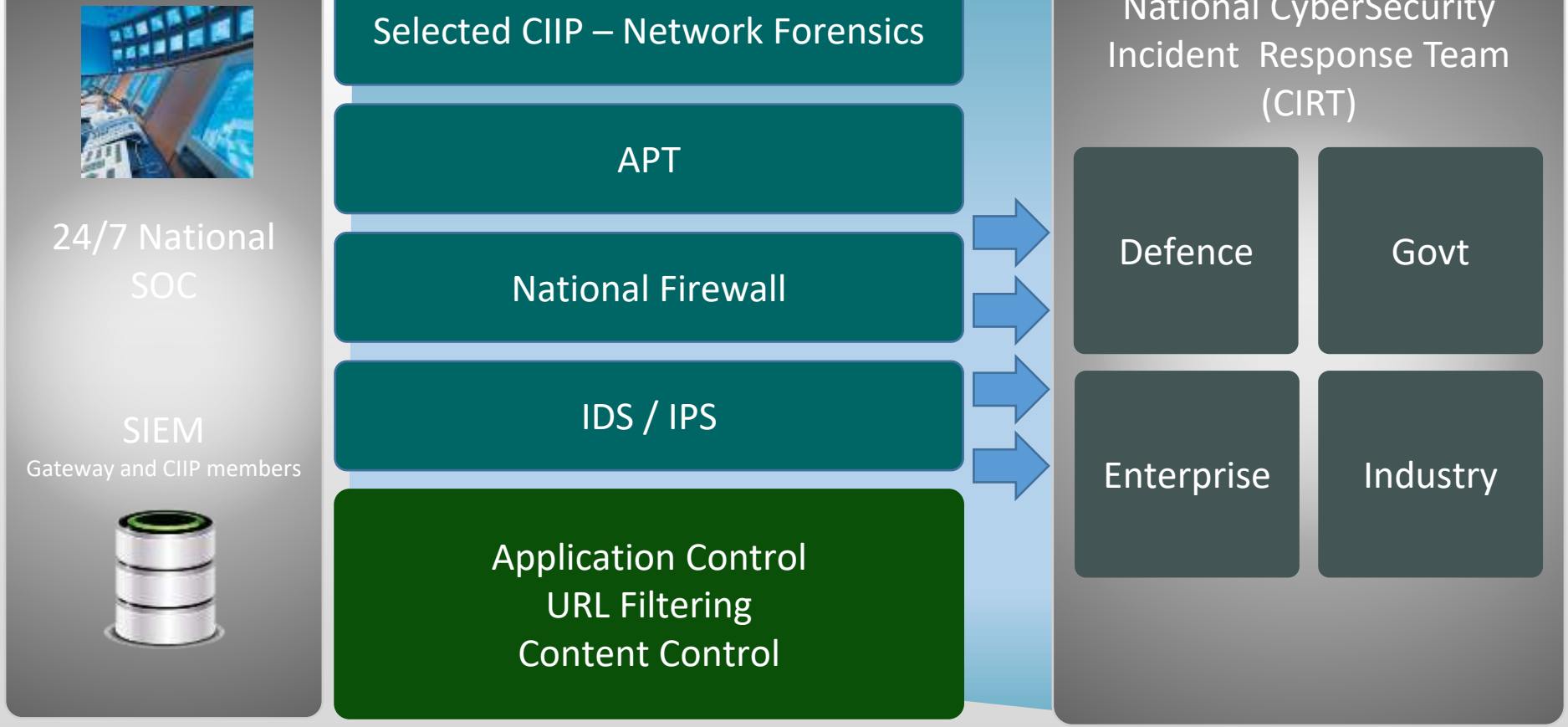
A Malware may be designed to damage your phone or computer, remotely control your device, steal your personal data & valuable info like password, credit card no. etc.

National Level Protection

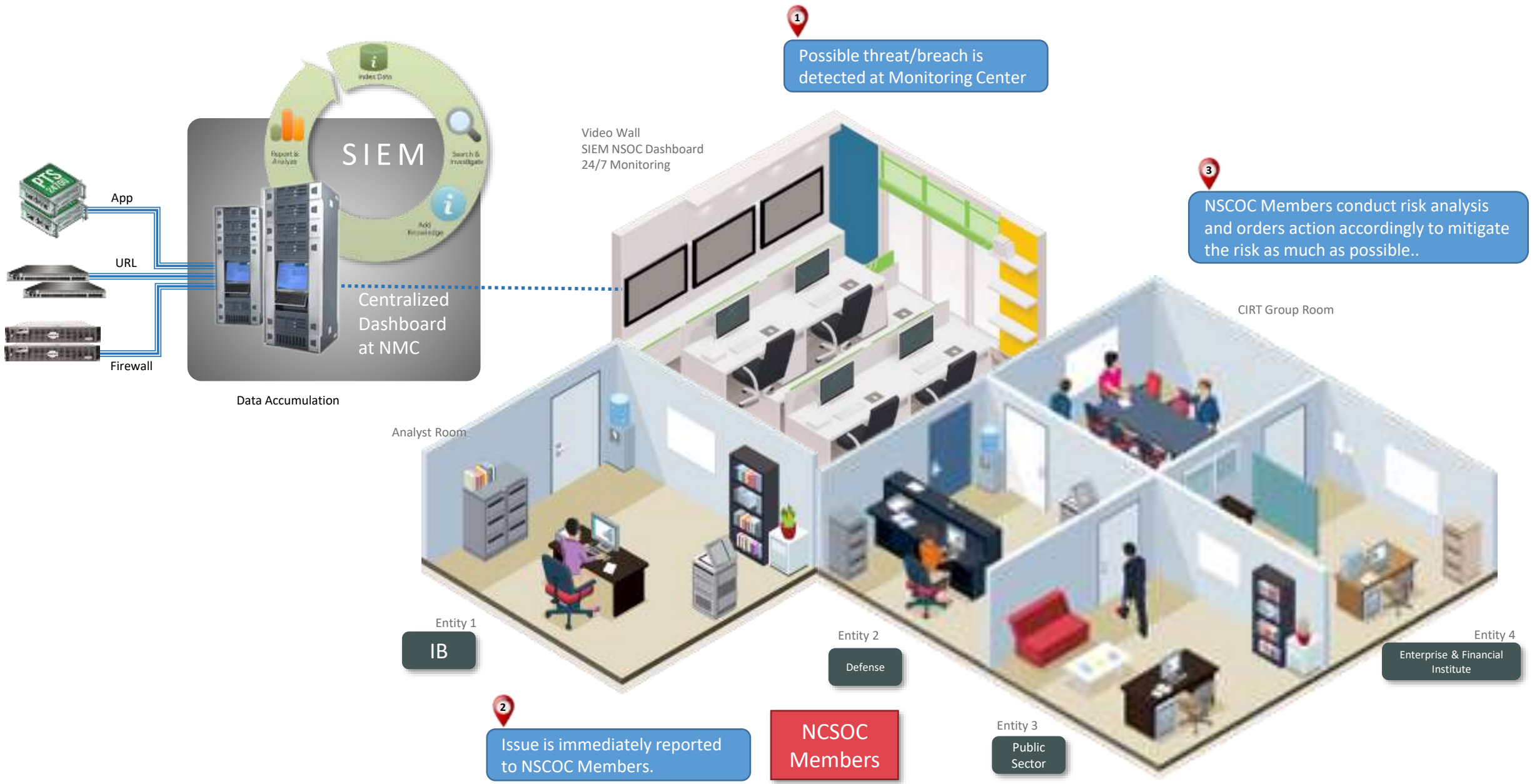
Cyber Security Strategy

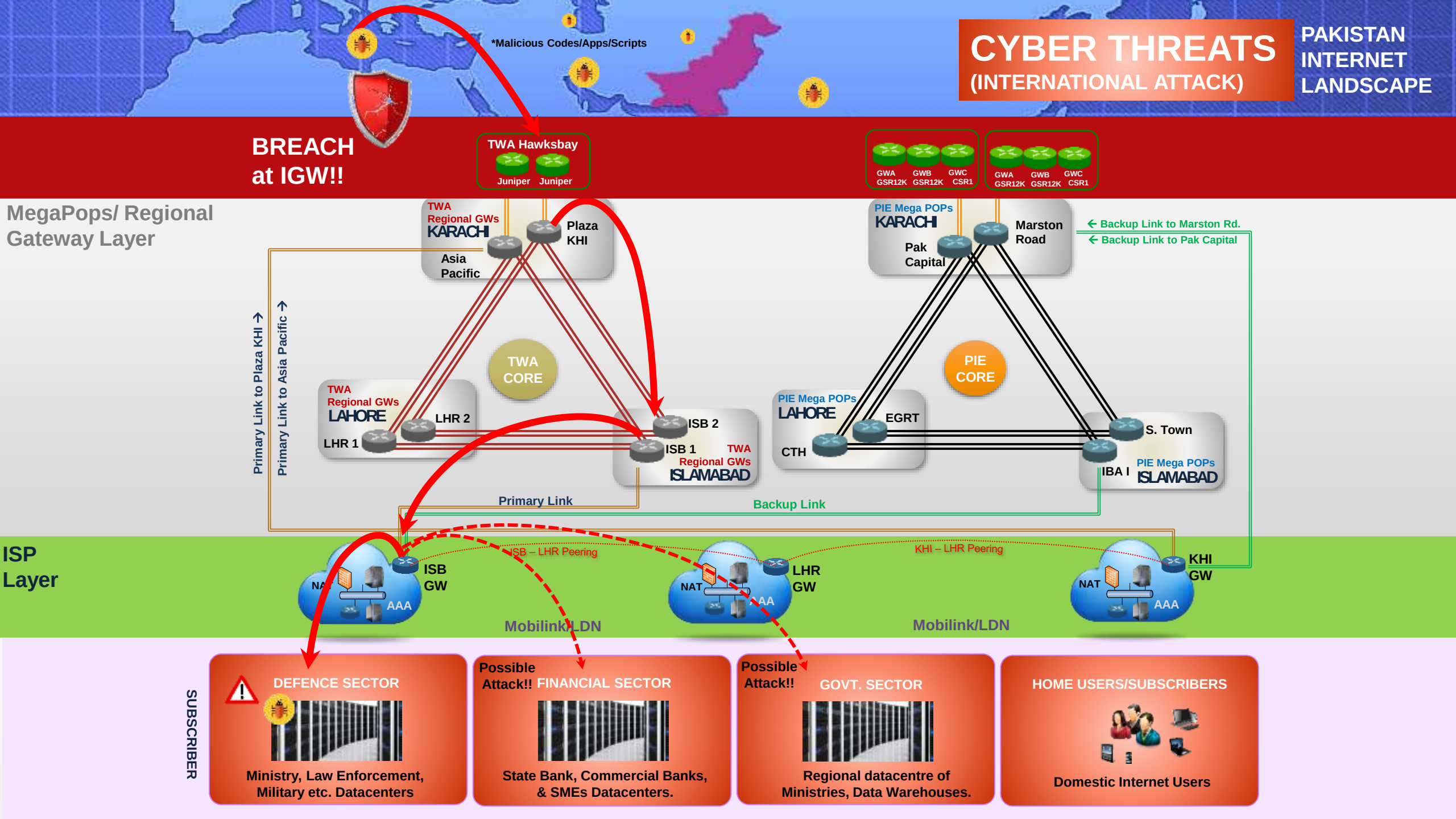
- Security Policy, Compliance & Assurance – Legal Framework
  - National IT Security Policy
  - Data protection & Crimes Bill
  - ISMS Best Practice, ISO 27001
  - Security Assurance Framework
- Security Incident – Early Warning & Response System
  - CERT – National Cyber Alert System
  - Knowledge sharing with international CERTS
- Capacity Building
  - Skill & Competence Development
  - Training of LEAs & Judicial Officials in collection & analysis of digital evidence
  - Training in area of implementing information security in collaboration with specialized organization
- Setting Up Digital Forensics Center
  - Domain Specific Trainings - Cyber Forensics
- Research & Development
  - National CERT
  - National SOC

CYBER SECURITY PARADIGM



Cyber Security Solution for NCSOC




*Malicious Codes/Apps/Scripts
CYBER THREATS
(INTERNATIONAL ATTACK)
PAKISTAN INTERNET LANDSCAPE
BREACH at IGW!!
TWA Hawksbay
Juniper
Juniper
GWA GSR12K
GWB GSR12K
GWC CSR1
GWA GSR12K
GWB GSR12K
GWC CSR1
MegaPops/ Regional Gateway Layer
TWA Regional GWs KARACHI
Plaza KHI
Asia Pacific
PIE Mega POPs KARACHI
Pak Capital
Marston Road
Backup Link to Marston Rd.
Backup Link to Pak Capital
Primary Link to Plaza KHI
Primary Link to Asia Pacific
TWA CORE
PIE CORE
TWA Regional GWs LAHORE
LHR 2
LHR 1
ISB 2
ISB 1
TWA Regional GWs ISLAMABAD
PIE Mega POPs LAHORE
EGRT
CTH
S. Town
IBA I
PIE Mega POPs ISLAMABAD
Primary Link
Backup Link
ISP Layer
ISB – LHR Peering
KHI – LHR Peering
NAT
AAA
ISB GW
LHR GW
KHI GW
Mobilink/LDN
Mobilink/LDN
SUBSCRIBER
DEFENCE SECTOR
Ministry, Law Enforcement, Military etc. Datacenters
Possible Attack!!
FINANCIAL SECTOR
State Bank, Commercial Banks, & SMEs Datacenters.
Possible Attack!!
GOVT. SECTOR
Regional datacentre of Ministries, Data Warehouses.
HOME USERS/SUBSCRIBERS
Domestic Internet Users

SNSKIES