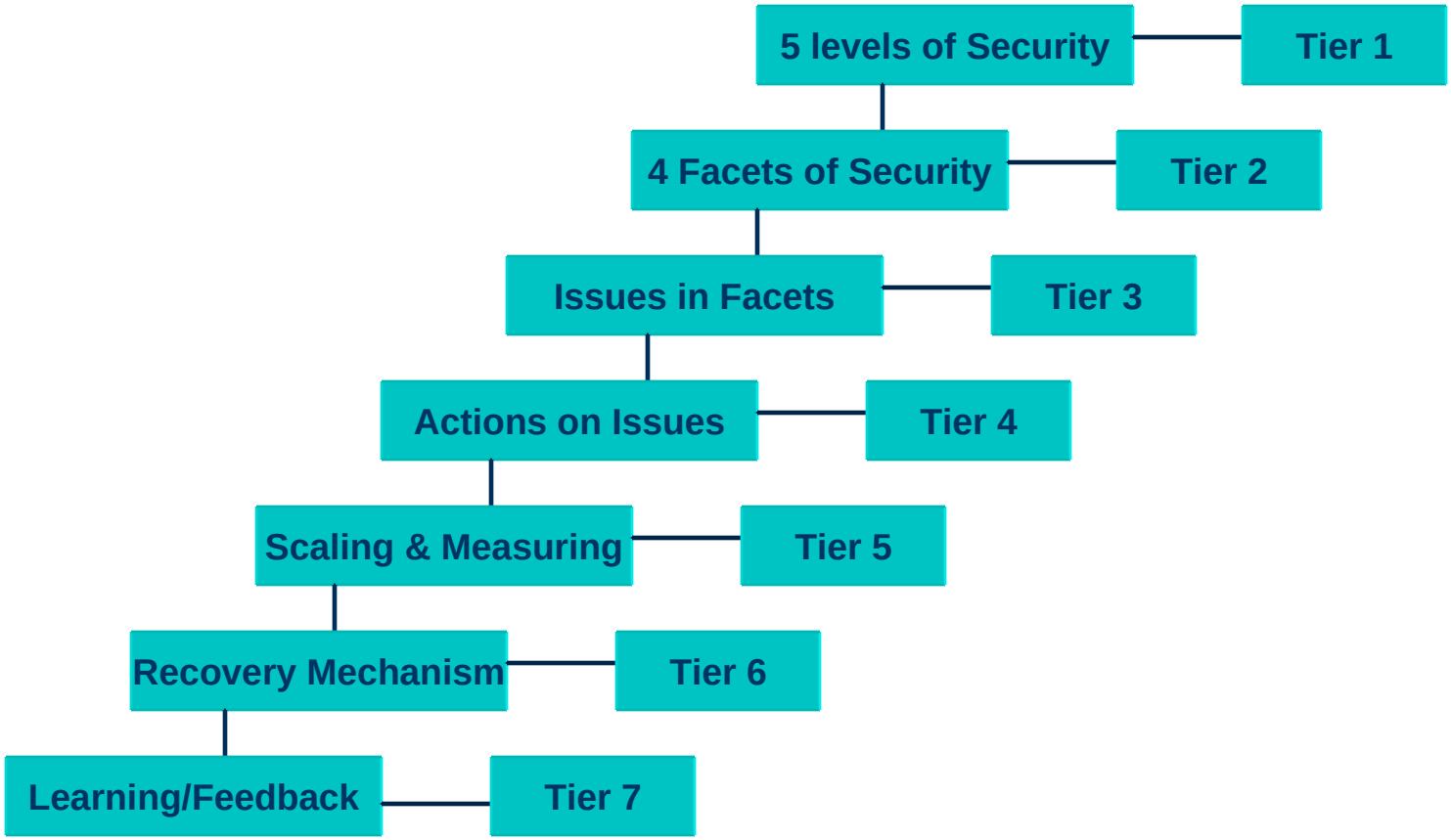
FRAMEWORK
for
NATIONAL NETWORK & CYBER SECURITY

23 September 2009

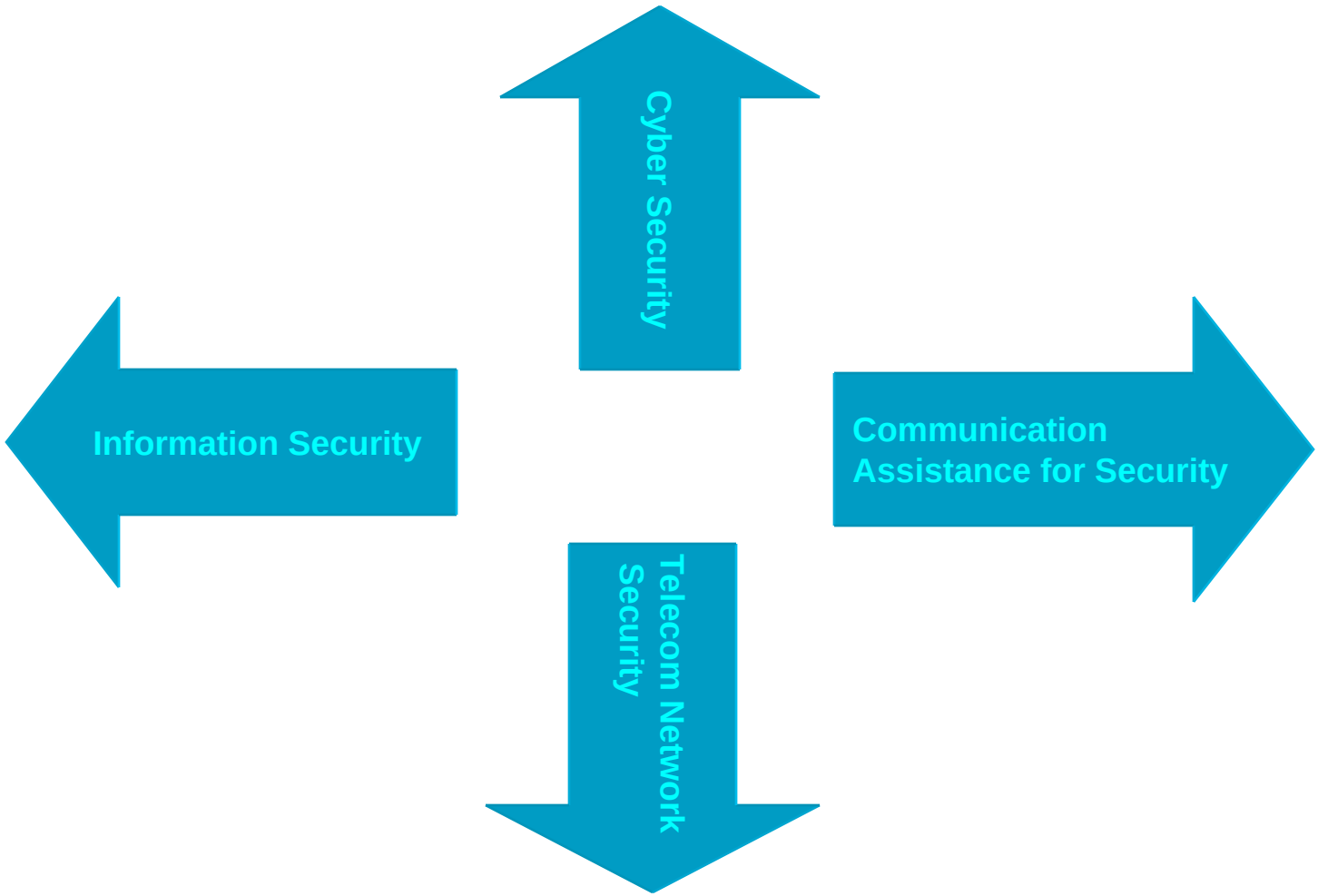
Ram Narain
DDG (Security), DOT
Email: ramnarain@hotmail.com

7 Tier Approach to Network & Cyber Security

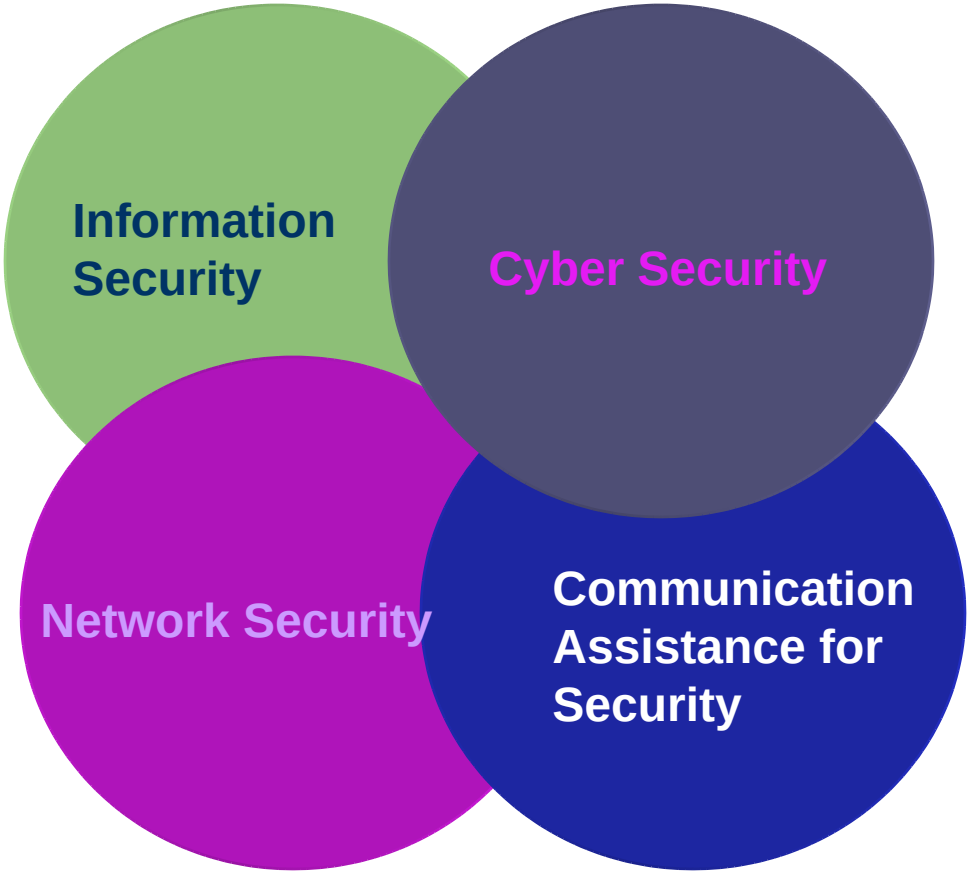


Five Levels of Security

4 Facets of Security



Overlapping in Facets of Security



Security Issues Matrix

Information Security	Cyber Security	Telecom Network Security	Communication Assistance for Security
• Standardization • Confidentiality • Integrity • Availability • Non-repudiation • Access Control and Authentication	• De capacitating (DoS, DDoS) • Website Compromise • Network Scanning • Probing • Phishing • Span • Virus • Steeling of info (Trojan etc.)	• Communication Monitoring • Data Access -RA • Network De-capacitating • Maintenance capability • Trapdoors, Trojans etc	• Interception • Monitoring • Analysis • Speech Recognition • Social Network analysis • Trace ability of users

Action Table for Information Security

Issues	Action
Standardization	• Standard Formulation • Awareness of Standard • Use of standards • Enactment of Regulations • Organization & Structure
Confidential	• Security of Media • Encryption policy • Protocol Standardization
Integrity	• Digital Signature • Distortionless Communication • Intrusion detection • Addressing
Availability	• Reliability of Media • Media capacity • Protection
Access Control and Authentication	• Physical Access • Password Management

Action Table for Cyber Security

Issues	Action
• Decapacitating (DoS, DDoS, Botnets) • Website Hacking • Network Scanning • Probing • Phishing • Spams • Virus • Steeling of info (Trojan etc.)	• Installing Honeypots • Intrusion Detections System (IDS) • Firewall • Antivirus • Hardening of Operating System software • Port Management • Use of Proxy servers • Use of Safe Software • Vulnerability Scan • Identity Tracing • National Regulations • International Co-operation • Monitoring & Tracking • Organization and Structure • Incident Reporting System • Addressing BGP, DNS vulnerabilities

Action Table for Network Security

Issues	Action
• Communication Monitoring • Data Access -RA • Network De-capacitating • Maintenance capability • Trapdoors, Trojans etc	• Equipment Testing • Equipment Purchase Procedure & Conditions • RA Access Precautions • Installing Sensors • Maintenance Skills Development • Enacting Laws • Solution implementation • Algorithm designs • Regulation Operations • Involvement of SPs • Organization & Structure

Action Table for Communication Assistance for Security

Issues	Action
• Interception & Monitoring • Speech Recognition • Analysis • Trace ability of users	• Legal framework • Technical capability • Structure • Availability of Tools & Technology • Development of Analytical Tools • Users Verification Process • CLI Restriction • Identity Management • Encryption Policy • Decryption Capability

Scaling & Measuring

- **What can’t be quantified, can’t be measured**
- **What can’t be measured, can’t be monitored**
- **What can’t be monitored, can’t be controlled & improved**

Scaling & Measuring – Information Security

Issues	Action	Scale	Score
Standardization	• Standard Formulation	4	3
	• Awareness Standard	4	3
	• Use of standard equipment	4	2
	• Enactment of Regulations	4	2
	• Organization & Structure	4	1
Confidential	• Security of Media	5	4
	• Encryption policy	8	6
	• Protocol Standardization	7	4
Integrity	• Digital Signature	4	3
	• Distortion less Communication	4	2
	• Intrusion detection	6	4
	• Addressing	6	3
Availability	• Reliability of Media	7	5
	• Media capacity	7	4
	• Protection of data	6	3
Access Control and Authentication	• Physical Access	8	6
	• Password management	12	7
	Total	**100**	**62**

Scaling & Measuring – Cyber Security

Action	Issues	Scale	Score
• Installing Honeypots • Intrusion Detections System (IDS) • Firewall • Antivirus • Hardening of Operating System software • Port Management • Proxy servers • Use of Safe Software • National Regulations • International Co-operation • Monitoring & Trading • Organization and Structure	• Decapacitating (DOS, DOSS, Botnets) • Website Compromise • Network Scanning • Probing • Phishing • Spams • Virus • Steeling of info (Trojan etc.)	20 10 15 10 10 10 10 15	8 5 6 5 4 7 8 5
	Total	100	48

Scaling & Measuring – Network Security

Action	Issues	Scale	Score
• Equipment Testing • Equipment Purchase Procedure & Conditions • RA Access Precautions • Installing Sensors • Maintenance Skills Development • Enacting Laws • Solution implementation • Algorithm designs • Blocking of sites • International Regulation & Co-Operations • Organization & Structure	• Communication Monitoring • Data Access -RA • Network De-capacitating • Maintenance capability • Trapdoors, Trojans etc	20 20 40 20 20	10 12 15 5 12
	Total	100	54

Scaling & Measuring – CAFS

Action	Issues	Scale	Score
• Legal framework • Technical capability • Structure • Availability of Tools & Technology • Development of Analytical Tools • Subscriber Verification • CLI Restriction • Identity Management	• Interception & Monitoring • Speech Recognition • Analysis • Trace ability of users	30 20 25 25	20 4 12 20
	Total	100	56

Grading

Score	Grade
>80	Excellent
70-80	Very Good
60-70	Good
50-60	Average
<50	Poor

Composite Score
&
Grade

- Composite Maximum Score: Total Max Score/4
  =400/4= 100
- Total Score: 220/4= 54
- Grade: Average

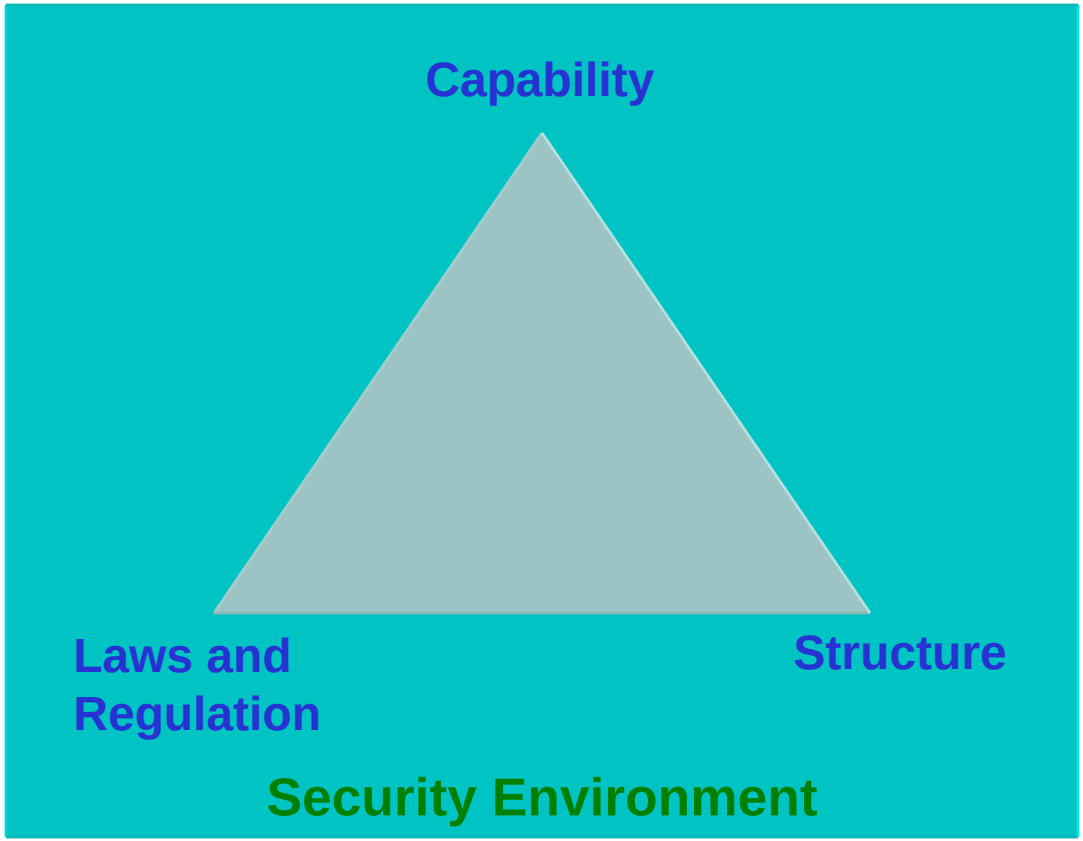
Recovery Mechanism

- Don’t loose heart
- Activate Command & Control System
- Determine the Level of Problem
- Assess Damage
- Check for any Skill Gap
- Equipment and tool Availability and their working Condition
- Network Awareness
- Documentation of Network – A short pencil is better than long memory
- Accessibility of Documentation

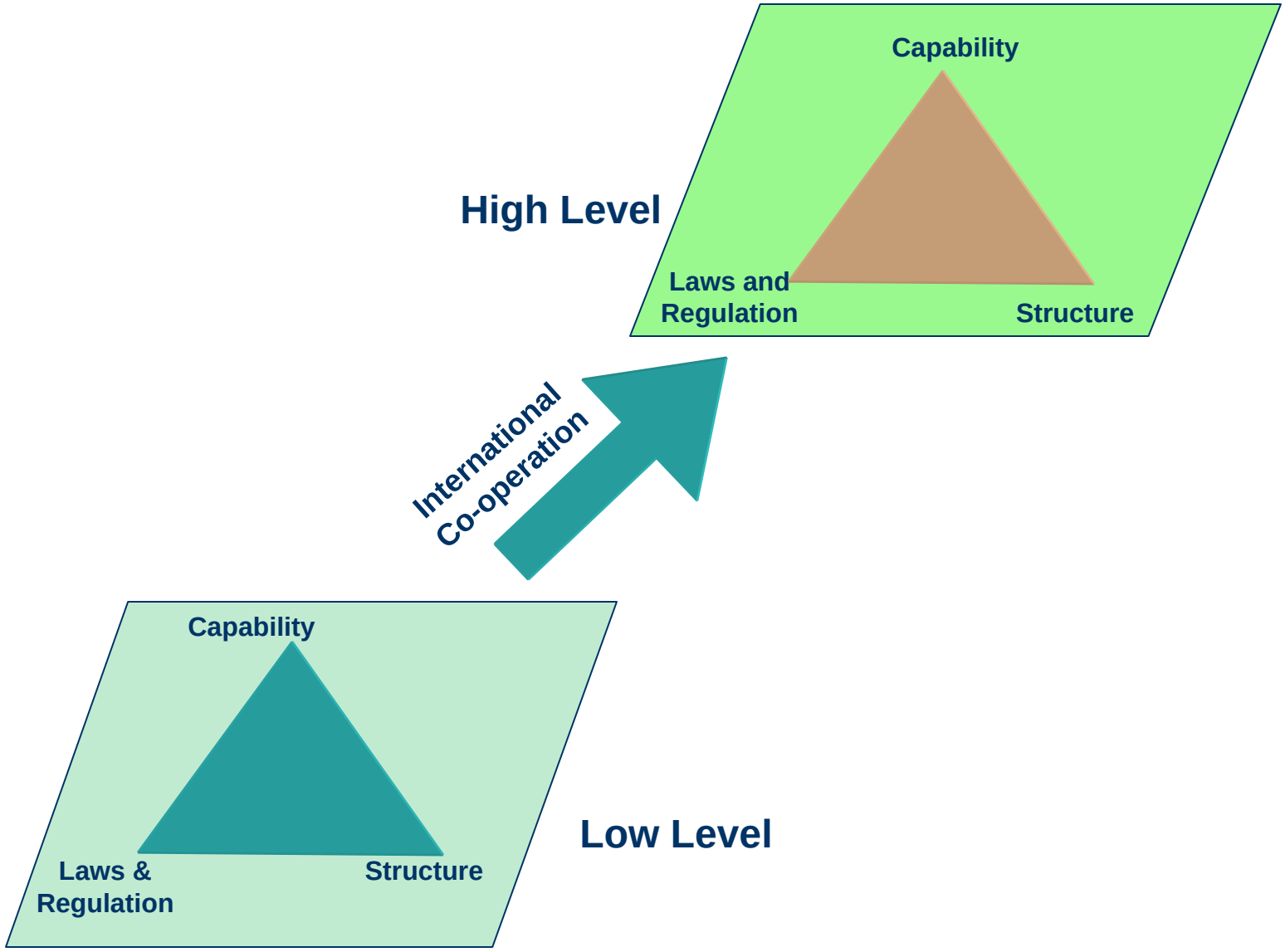
Feedback/Learning

- From every Success and Failure there are lessons
- Failure is not when you fall; failure is when you don’t get up
- Feedback is the food of Champions

National Security Environment



Enhancing Security Environment



Cyber Security

S – Structure

E – Experience

C – Capability

U – Undertaking

R – Regulation

I - International

T – Technology

Y - Youth

Cyber City

Cyber Security

THANKS