Lesson 3.4
Cyber Threat Mitigation

Lesson Content

- Prevention
- Monitor - Analyse – Determine (MAD)
- Mitigation

Lesson Outcomes

- Describe methods to prevent Cyber-attacks
- Explain MAD process when planning tactical operations
- Explain cyber risks mitigation

Prevention Step 1

- Critical Information technology (IT) asset inventory, if compromised, impact operations
- Systems with stored sensitive information
- Security SOPs in place
- Controlled access IT equipment
- Control use of sensitive information

Prevention Step 2

- Use a strong password to protect IT systems
- Train personnel; be security conscious
- Be conscious of social engineering
- Do not attempt to change system settings
- Check and Report – attacks, fraudulent emails, links, hardware

Prevention Plus

- Conduct regular security audits and penetration testing
- Implement a defense-in-depth approach
- Develop an incident response plan / SOP
- Ensure regular updates and patch management

Do Not

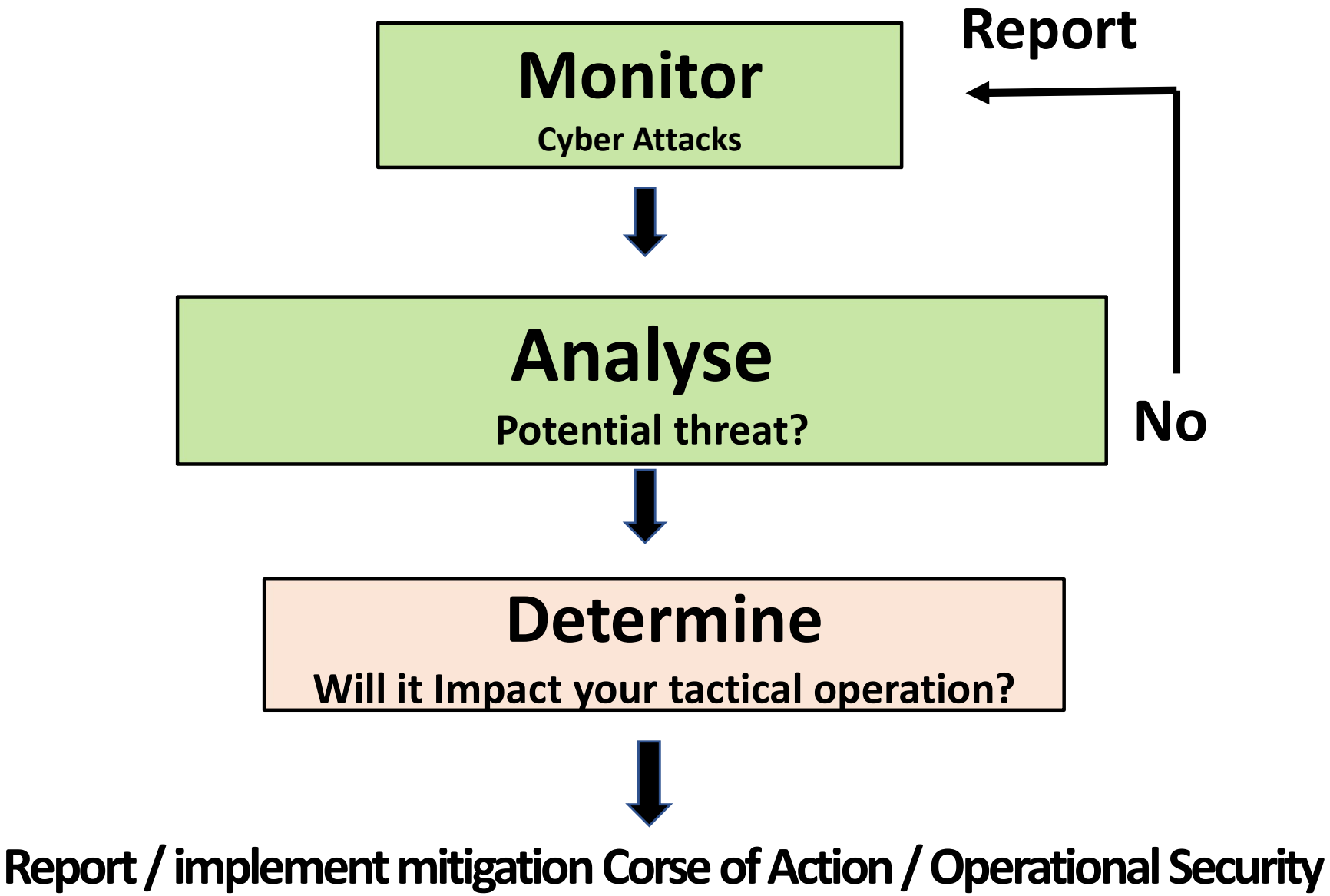
- Connect personal, unauthorized- CD, DVDs, USBs, computers, hardware into UN IT systems / networks
- Disclose operational information on social media
- Open suspicious emails / links

DO

Suspect an IT system is under a cyber-attack - **STOP** using the equipment and **do not turn off** - inform and report

Monitor-Analyse-Determine

"MAD"



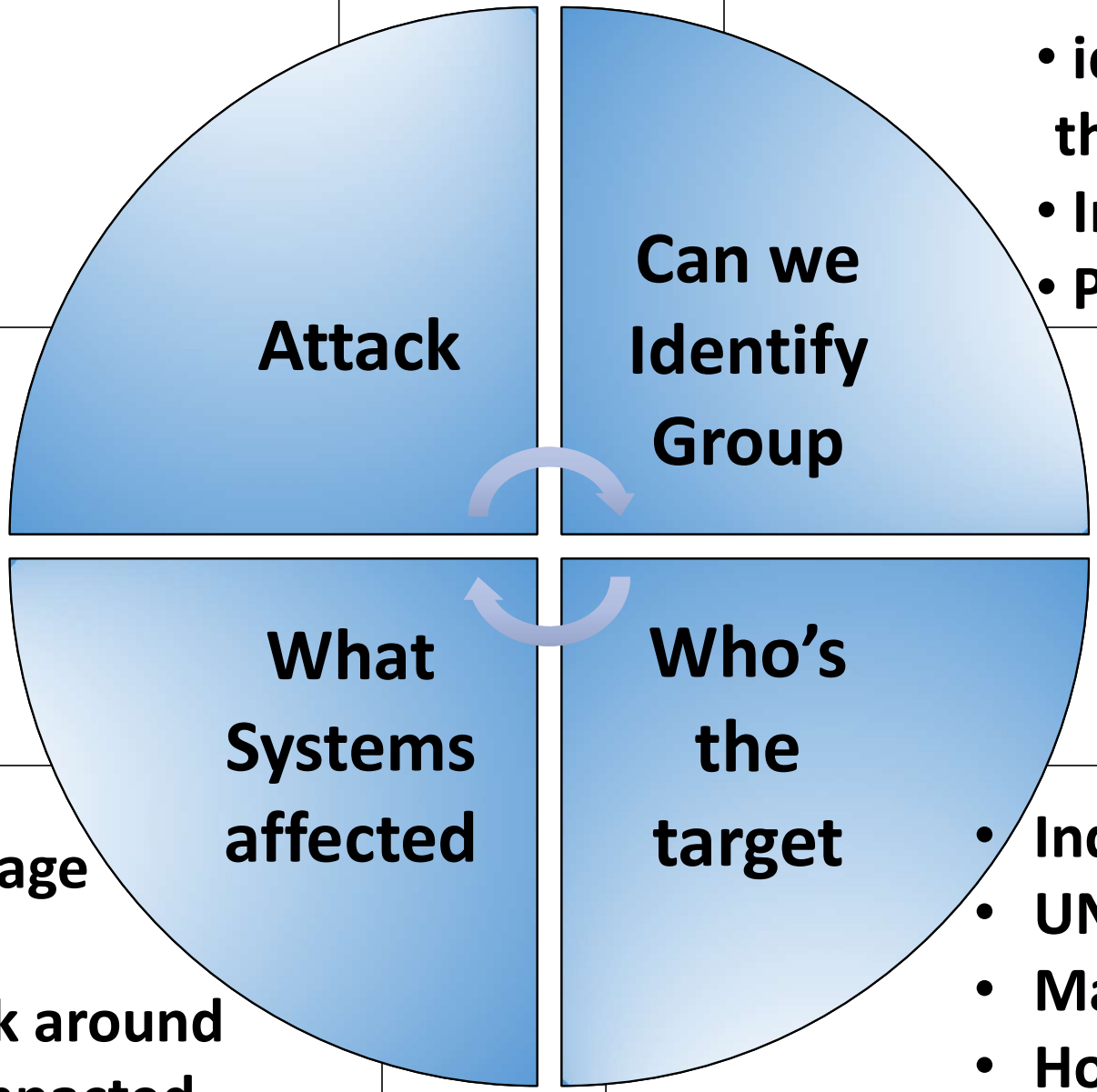
Monitor- Suggested techniques

- Train unit personnel to monitor and report
- Collaborate with subject matter experts
- Use Artificial Intelligence powered tools
- Specialised platforms and algorithms to monitor
- Engage stakeholders in a multi-pronged approach to help monitor IT and communication systems

Analyse

- Type
- Method

- identified threats
- Intent
- Purpose



- Extent of damage
- Can it be fixed
- Is there a work around
- Capabilities impacted

- Individuals
- UN Mission
- Mandate
- Host Government
- Our Unit

Determine / Risk Mitigation

- Focused on specific Impact to tactical operations
- Collateral damage from Cyber attack that may affect / impact unit operations
- Compromised operational information that groups can exploit
- Threat identified- FP plan to mitigate risks

Take Away

- Promote preventive measures, foster a FP conscious culture, prioritise training, awareness, and reporting mechanisms to reduce cyber-attacks
- Implement technical measures and best practices to enhance system resilience and safeguard critical assets and information
- Implement the MAD assessment methodology, prioritising monitoring, analysis, and impact evaluation on unit operations
- By focusing on cybersecurity and implementing force protection plans, units can mitigate both direct and indirect consequences of cyber-attacks on unit operations

Learning Activity- ”MAD” Methodology

- Break away in 3 small groups and discuss (30 minutes); using the MAD assessment methodology:

1. Group 1- Explain the components and processes that you would establish in your unit’s cyber-attack monitoring system
2. Group 2- Explain the components and processes that you would establish in your unit’s cyber-attack analysis
3. Group 3- Explain the components and processes that you would establish in your unit’s cyber-attack determine impact on operations

- All Groups- Give examples of possible secondary or collateral tactical threats against UN units associated with cyber attacks
- Group leaders report back to the plenary the group’s findings / discussion points

Questions