UNIVERSITY OF JOHANNESBURG

FACULTY OF SCIENCE

ACADEMY OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

MODULE:	IT08X32 CRITICAL INFORMATION INFRASTRUCTURE PROTECTION
CAMPUS:	APK
ASSESSMENT:	EXAM SSA

MEMORANDUM

DATE: 30/11/2021 **TIME:** 15:00

ASSESSOR:	MR SP SITHUNGU
MODERATOR:	PROF BL TAIT (UNISA)
DURATION:	120 MINUTES
MARKS:	100
NUMBER OF PAGES:	4

PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY:

1. Write clearly and legibly.
2. Answer all the questions.
3. When done, save your work as a PDF and upload it to https://eve.uj.ac.za/ → Practicals → Exam SSA .
4. Remember to download, complete and upload your **Honesty Declaration** to https://eve.uj.ac.za/ → Practicals → HD Exam SSA.
5. Download time: 15 minutes.
6. Upload time: 15 minutes.

QUESTION 1

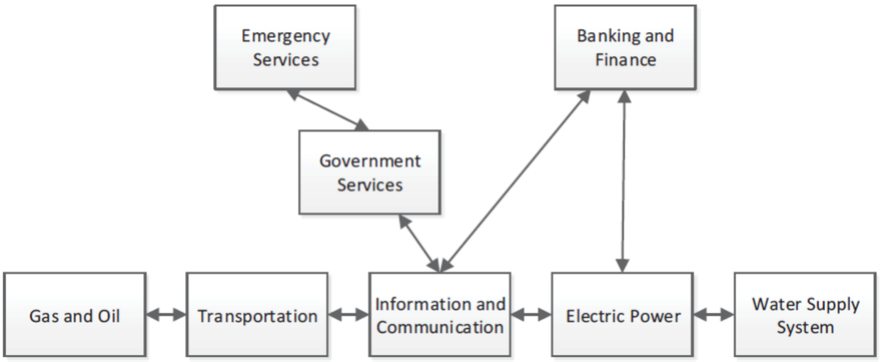
1. The **Utopian Space Exploration Agency (USEA)** has finally made a breakthrough by discovering a planet that supports life (which they have given the name Utopia 2.0). Due to Utopia nearing its capacity to provide water for its inhabitants, USEA is treating the mission of occupying Utopia 2.0 as a top priority. The first step is to determine the most basic infrastructure sectors that must be built.

1.1 As one of Utopia's Critical Information Infrastructure Protection (CIIP) experts, you must determine which are the **most important** Critical Infrastructure (CI) sectors (**name 5**) to be built first. **Justify** the **importance** of each sector. (10)

- Any 5 CI sectors are acceptable as long as they fit the above context (1 mark for each sector and 1 mark for each valid justification.)

1.2 Due to the complex interactions and dependencies between components of CI systems, use the **Interpretive Structural Modelling (ISM)** methodology to show the dependencies you think will exist **between the CI sectors** you named in **Question 1.1**. (5)

- The student should use the following diagram to show dependencies as they see fit (1 mark for each dependency.)



Interpretive Structural Modelling (Han et al., 2009)

1.3 Justify the dependencies you showed in **Question 1.2**. (5)

- Any valid justification is acceptable (1 mark for each justification).

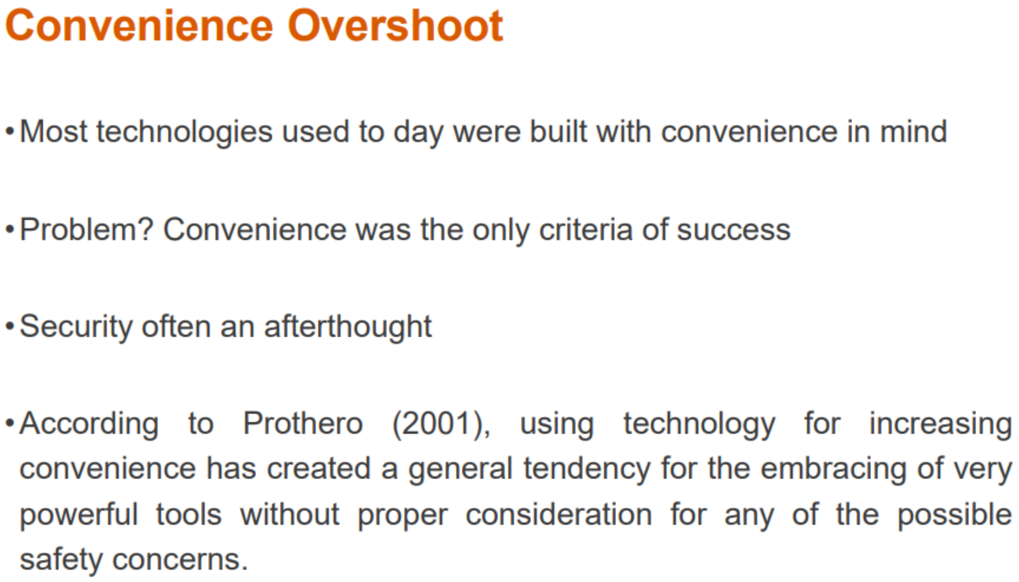
[20]

QUESTION 2

2. Now that you have helped USEA identify they most important CI sectors, USEA wants to apply as much automation as possible to the functioning of their CI systems. This would mean that there would be information systems facilitating the operation of the CIs – making them CIIs – and that would result in the Internet being the communication medium.

2.1 As a CIIP expert, **discuss (in extensive detail)** why USEA must build their CIIs with security in mind. In your discussion be sure to include the following:

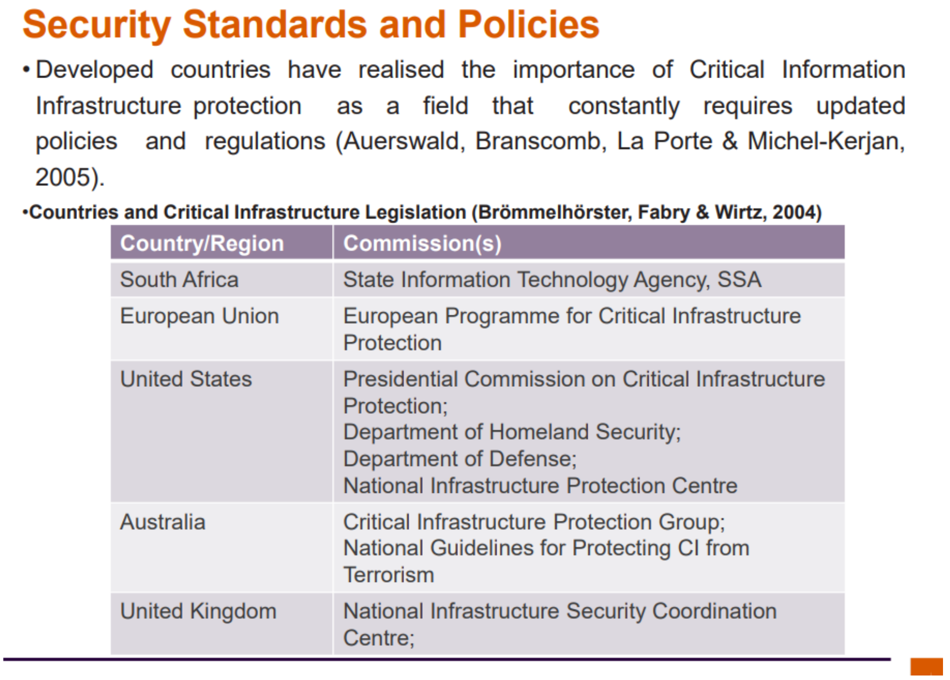
- CIIP.
- Convenience Overshoot and why building CII with a security-oriented approach can prevent it.
- The importance of Security Standards and Policies. (20)
- The student should comprehensively discuss CIIP (1 mark per fact).



Convenience Overshoot

- Most technologies used to day were built with convenience in mind
- Problem? Convenience was the only criteria of success
- Security often an afterthought
- According to Prothero (2001), using technology for increasing convenience has created a general tendency for the embracing of very powerful tools without proper consideration for any of the possible safety concerns.

- 1 mark per fact.



Security Standards and Policies

- Developed countries have realised the importance of Critical Information Infrastructure protection as a field that constantly requires updated policies and regulations (Auerswald, Branscomb, La Porte & Michel-Kerjan, 2005).
- **Countries and Critical Infrastructure Legislation (Brömmelhörster, Fabry & Wirtz, 2004)**

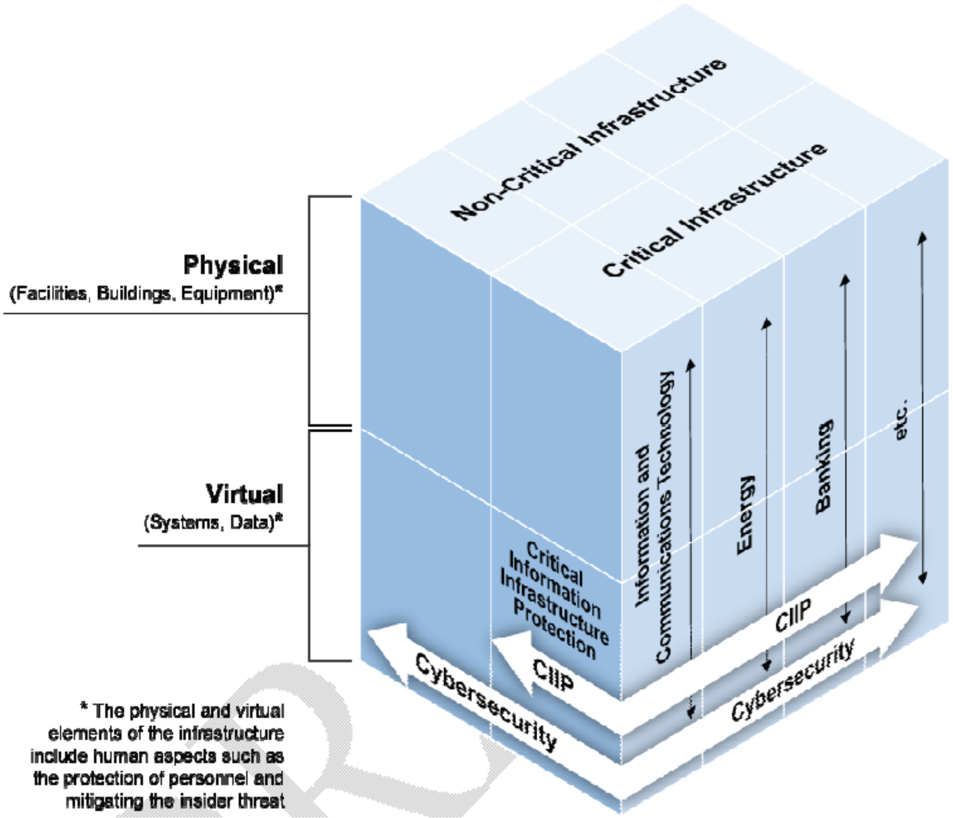
Country/Region	Commission(s)
South Africa	State Information Technology Agency, SSA
European Union	European Programme for Critical Infrastructure Protection

United States	Presidential Commission on Critical Infrastructure Protection;
	Department of Homeland Security;
	Department of Defense;
	National Infrastructure Protection Centre

Australia	Critical Infrastructure Protection Group; National Guidelines for Protecting CI from Terrorism
United Kingdom	National Infrastructure Security Coordination Centre;

- 1 mark per fact.

2.2 **Explain** how USEA's cybersecurity division can **include** CIIP-oriented policies **as part of its broader legislation** using the diagram below. (5)


Non-Critical Infrastructure
Critical Infrastructure
Physical
(Facilities, Buildings, Equipment)*
Virtual
(Systems, Data)*
Information and Communications Technology
Energy
Banking
etc.
Critical Information Infrastructure Protection
CIIP
Cybersecurity
CIIP
Cybersecurity
* The physical and virtual elements of the infrastructure include human aspects such as the protection of personnel and mitigating the insider threat

- Any valid explanation of the diagram is acceptable (1 mark per fact.)

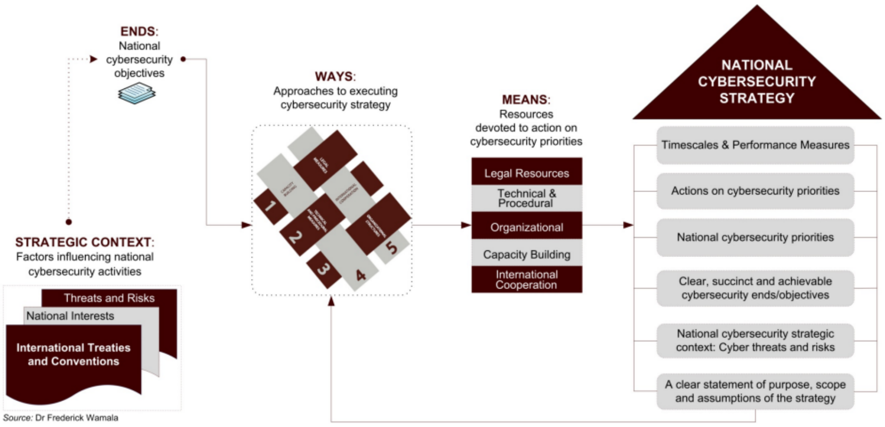
[25]

QUESTION 3

3. Utopia 2.0 needs to be aware of the importance of a good CIIP model. **Discuss** how USEA's cybersecurity division can apply the International Telecommunication Union's (ITU) **CIIP/Cybersecurity Strategy Model** to achieve effective CIIP.

(Please zoom in the diagram.) **[20]**

CIIP/Cybersecurity Strategy Model

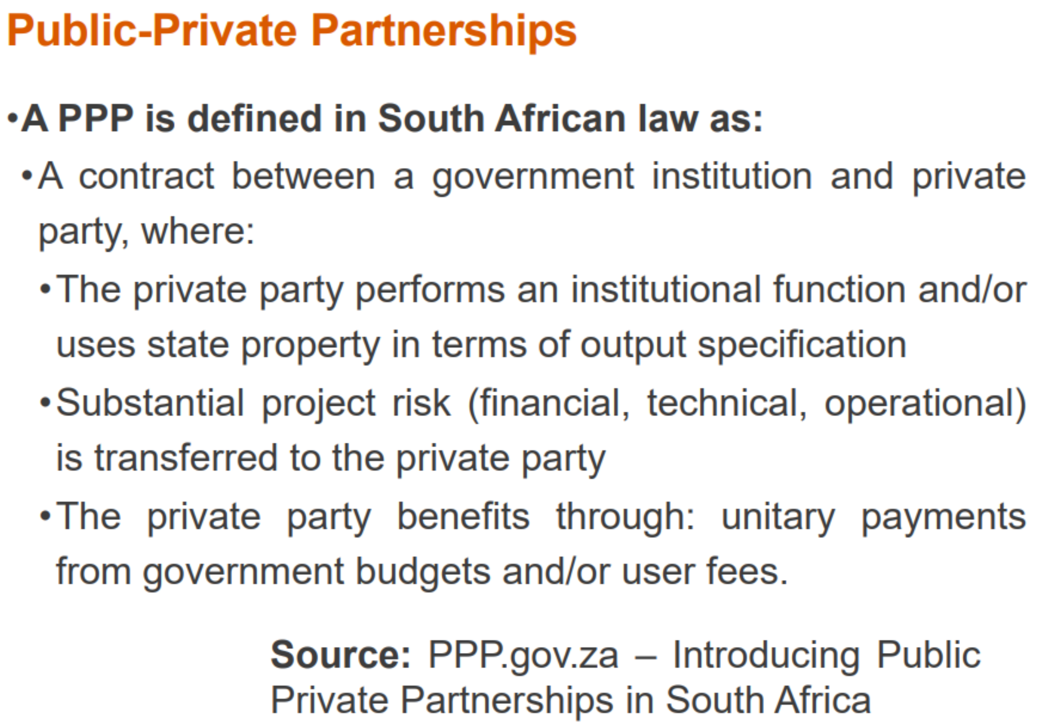

ENDS:
National cybersecurity objectives
WAYS:
Approaches to executing cybersecurity strategy
1
2
3
4
5
MEANS:
Resources devoted to action on cybersecurity priorities
Legal Resources
Technical & Procedural
Organizational
Capacity Building
International Cooperation
NATIONAL CYBERSECURITY STRATEGY
Timescales & Performance Measures
Actions on cybersecurity priorities
National cybersecurity priorities
Clear, succinct and achievable cybersecurity ends/objectives
National cybersecurity strategic context: Cyber threats and risks
A clear statement of purpose, scope and assumptions of the strategy
STRATEGIC CONTEXT:
Factors influencing national cybersecurity activities
Threats and Risks
National Interests
International Treaties and Conventions

Source: Dr Frederick Wamala

URL: http://www.itu.int/ITU-D/cyb/cybersecurity/strategies.html

QUESTION 4

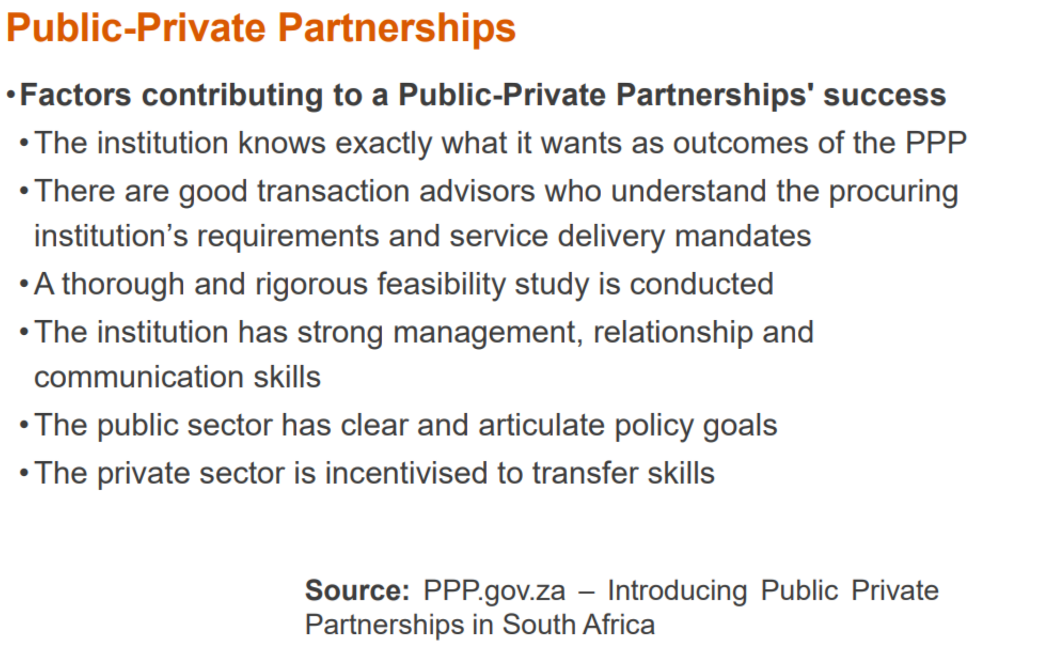
4. **Discuss** how USEA's cybersecurity division can create meaningful Public-Private Partnerships (PPPs) in the context of CIIP. Be sure to include the following in your discussion:
   - A definition of a PPP according to South African law.
   - Factors that could contribute to Utopia 2.0's success in PPPs.
   - Challenges USEA's cybersecurity division should consider regarding PPPs. **[15]**



Public-Private Partnerships

- **A PPP is defined in South African law as:**
  - A contract between a government institution and private party, where:
    - The private party performs an institutional function and/or uses state property in terms of output specification
    - Substantial project risk (financial, technical, operational) is transferred to the private party
    - The private party benefits through: unitary payments from government budgets and/or user fees.

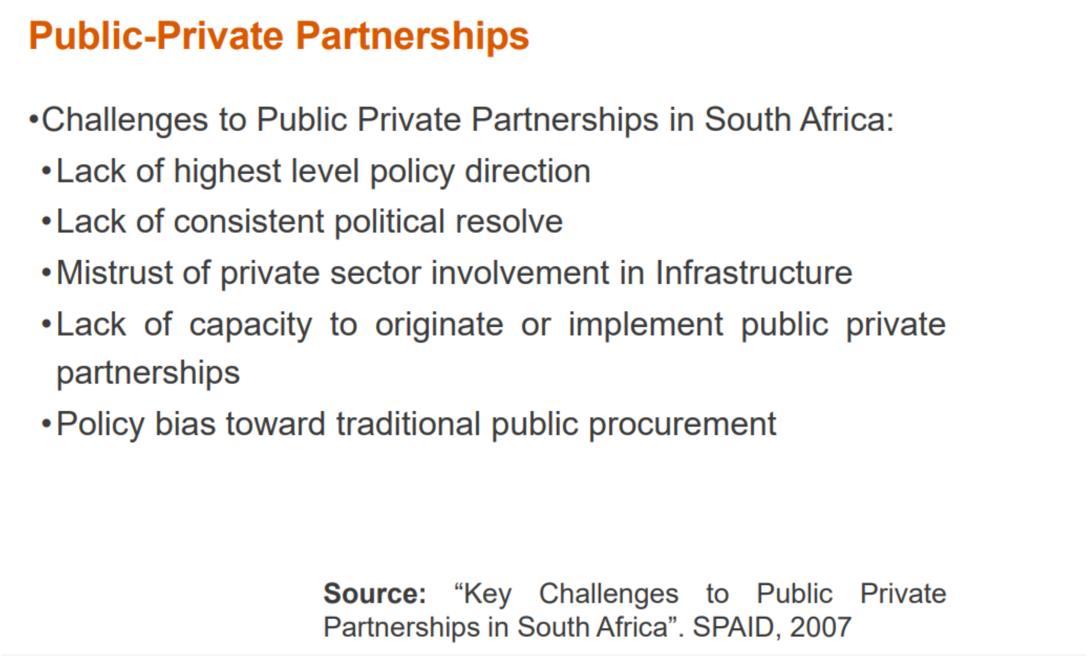
Source: PPP.gov.za – Introducing Public Private Partnerships in South Africa



Public-Private Partnerships

- **Factors contributing to a Public-Private Partnerships' success**
  - The institution knows exactly what it wants as outcomes of the PPP
  - There are good transaction advisors who understand the procuring institution's requirements and service delivery mandates
  - A thorough and rigorous feasibility study is conducted
  - The institution has strong management, relationship and communication skills
  - The public sector has clear and articulate policy goals
  - The private sector is incentivised to transfer skills

Source: PPP.gov.za – Introducing Public Private Partnerships in South Africa



Public-Private Partnerships

- Challenges to Public Private Partnerships in South Africa:
  - Lack of highest level policy direction
  - Lack of consistent political resolve
  - Mistrust of private sector involvement in Infrastructure
  - Lack of capacity to originate or implement public private partnerships
  - Policy bias toward traditional public procurement

Source: "Key Challenges to Public Private Partnerships in South Africa". SPAID, 2007

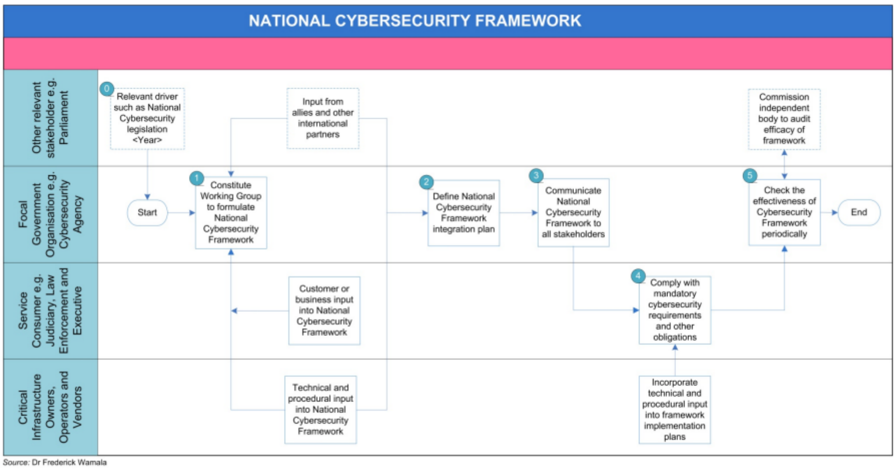
QUESTION 5

5.

5.1 USEA's cybersecurity division feels that it is now ready to focus on developing a CIIP policy framework. As an expert in the field, you have informed the division that it is wise to first develop a cybersecurity policy framework because it can be used as a reference when creating a CIIP-specific policy framework. Discuss the steps the division needs to follow to develop a global cybersecurity policy framework for Utopia 2.0 (you may refer to the national cybersecurity framework flowchart). (10)

(Please zoom in the diagram.)

Cybersecurity Framework Flowchart

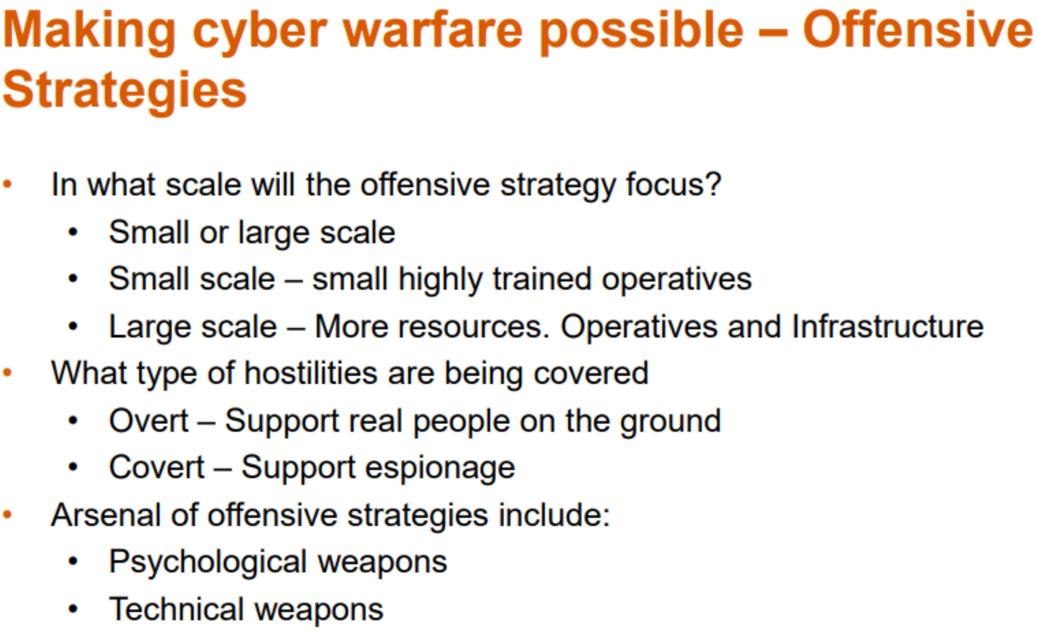

NATIONAL CYBERSECURITY FRAMEWORK
Other relevant stakeholder e.g. Parliament
Focal Government Organisation e.g. Cybersecurity Agency
Service Consumer e.g. Judiciary, Law Enforcement and Executive
Critical Infrastructure Owners, Operators and Vendors
0
Relevant driver such as National Cybersecurity legislation <Year>
Input from allies and other international partners
Commission independent body to audit efficacy of framework
Start
1
Constitute Working Group to formulate National Cybersecurity Framework
2
Define National Cybersecurity Framework integration plan
3
Communicate National Cybersecurity Framework to all stakeholders
5
Check the effectiveness of Cybersecurity Framework periodically
End
Customer or business input into National Cybersecurity Framework
4
Comply with mandatory cybersecurity requirements and other obligations
Technical and procedural input into National Cybersecurity Framework
Incorporate technical and procedural input into framework implementation plans

Source: Dr Frederick Wamala

Source: Pages 52-55, **"ITU National Cybersecurity Strategy Guide"**

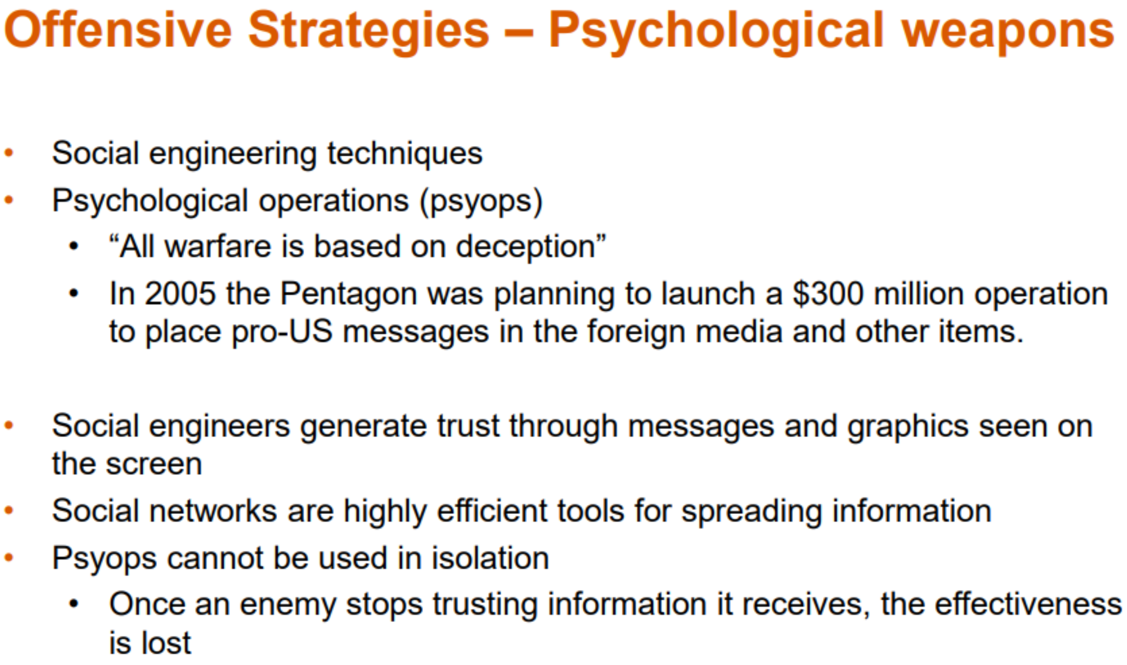
5.2 Finally, you need to make USEA aware of the possibility of interplanetary cyberwarfare from extraterrestrial enemy civilisations. Explain how USEA's cybersecurity division can be ready for such an event by discussing the following:

- Preparation
- Offensive Strategies
- Defensive Strategies (10)



Making cyber warfare possible – Offensive Strategies

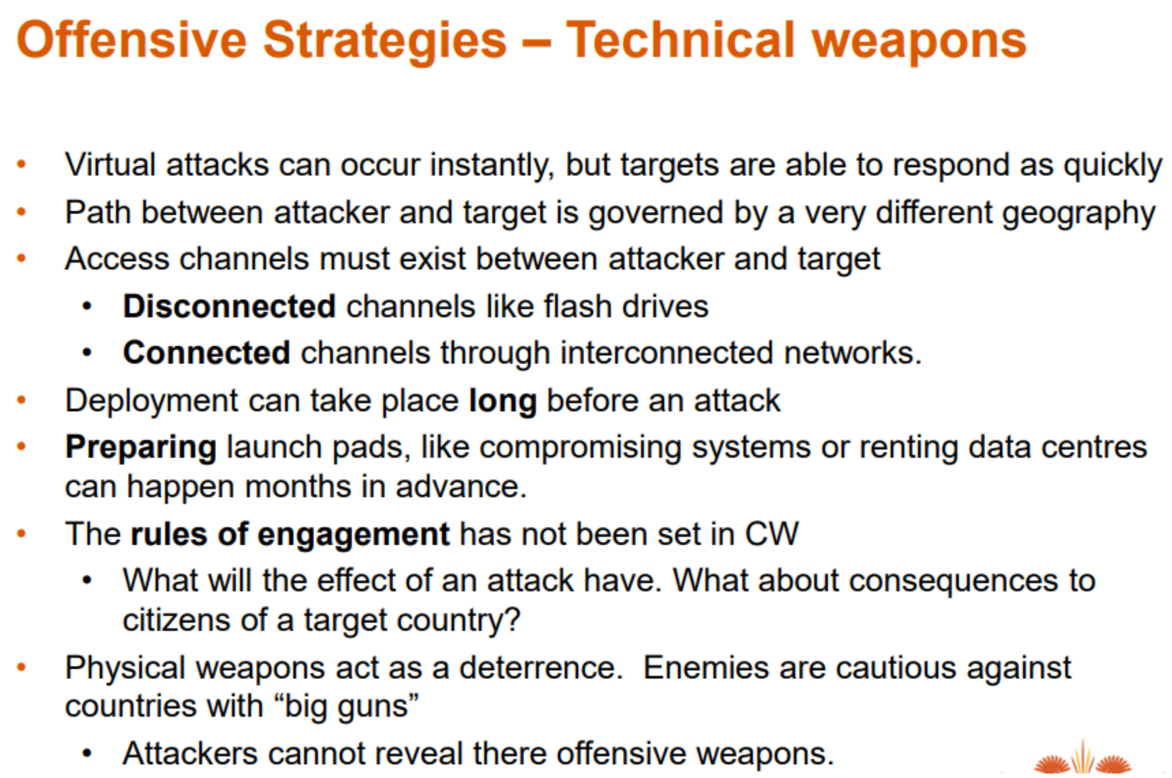
- In what scale will the offensive strategy focus?
  - Small or large scale
  - Small scale – small highly trained operatives
  - Large scale – More resources. Operatives and Infrastructure
- What type of hostilities are being covered
  - Overt – Support real people on the ground
  - Covert – Support espionage
- Arsenal of offensive strategies include:
  - Psychological weapons
  - Technical weapons



Offensive Strategies – Psychological weapons

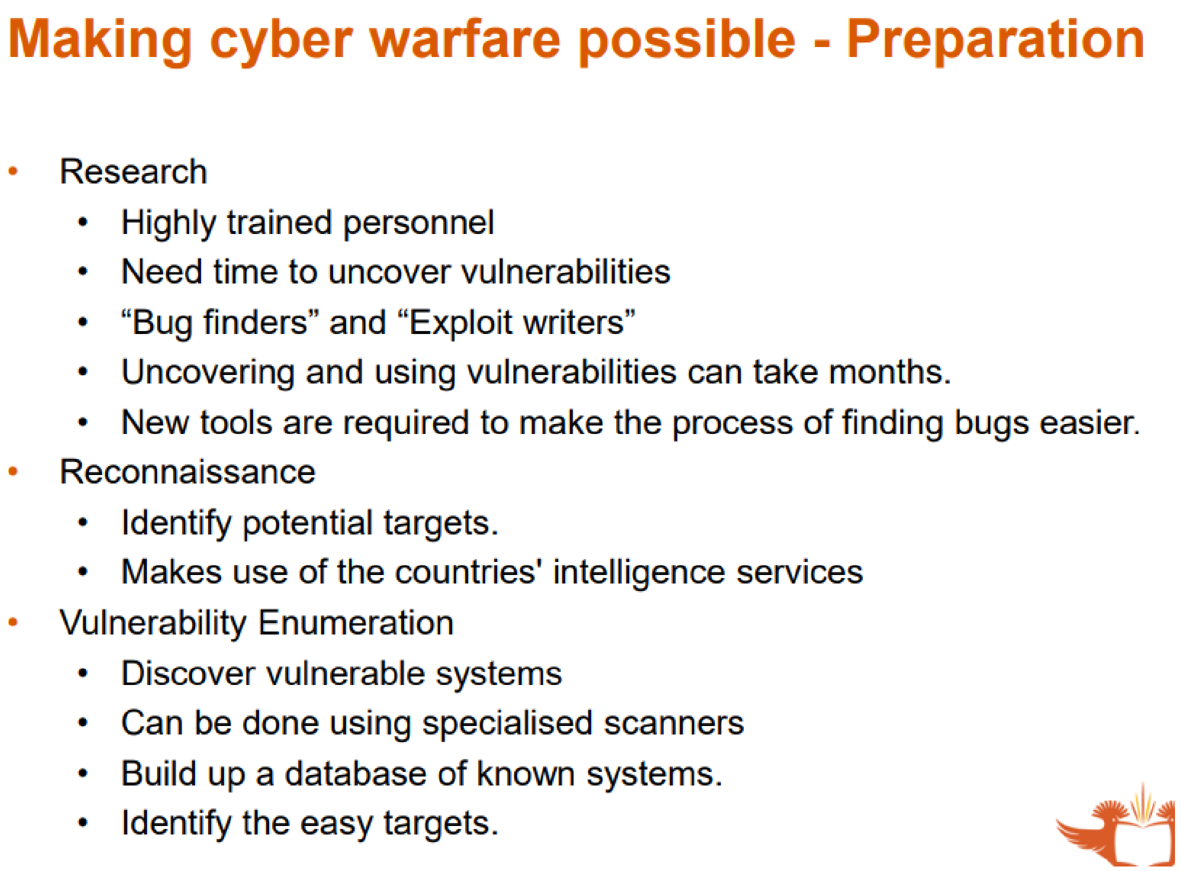
- Social engineering techniques
- Psychological operations (psyops)
  - "All warfare is based on deception"
  - In 2005 the Pentagon was planning to launch a $300 million operation to place pro-US messages in the foreign media and other items.

- Social engineers generate trust through messages and graphics seen on the screen
- Social networks are highly efficient tools for spreading information
- Psyops cannot be used in isolation
  - Once an enemy stops trusting information it receives, the effectiveness is lost



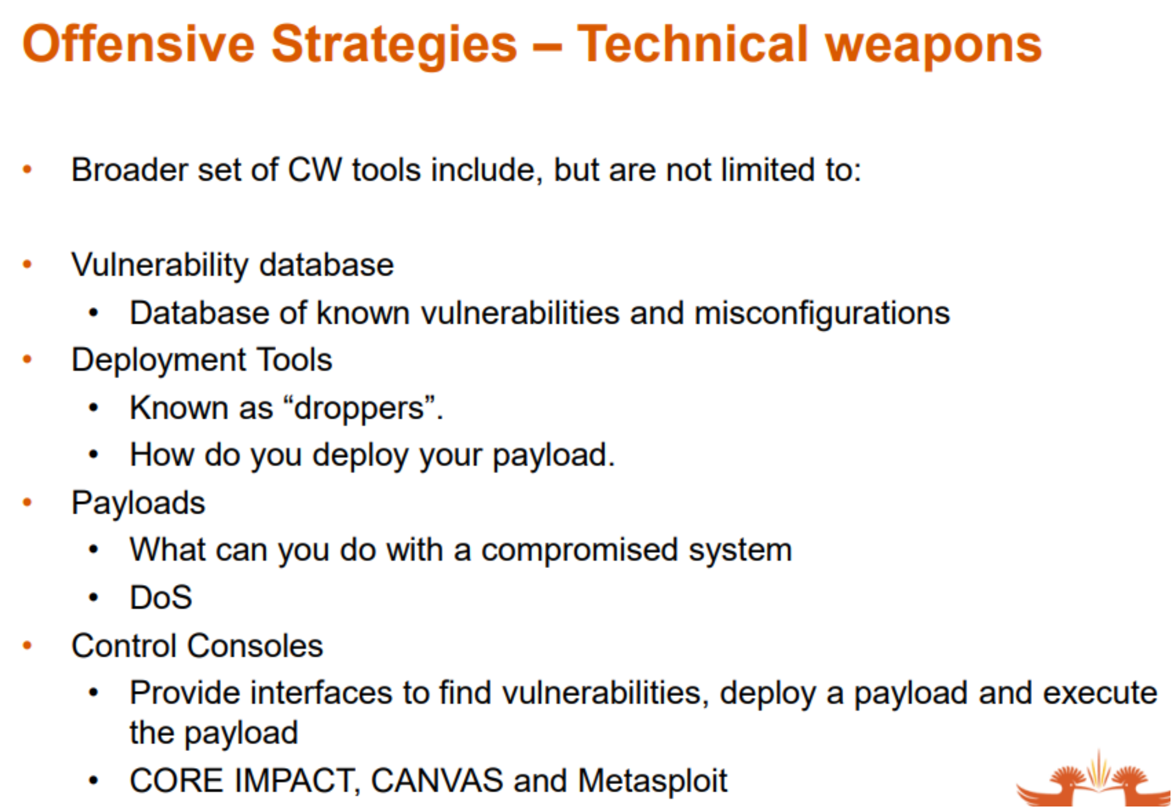
Offensive Strategies – Technical weapons

- Virtual attacks can occur instantly, but targets are able to respond as quickly
- Path between attacker and target is governed by a very different geography
- Access channels must exist between attacker and target
  - **Disconnected** channels like flash drives
  - **Connected** channels through interconnected networks.
- Deployment can take place **long** before an attack
- **Preparing** launch pads, like compromising systems or renting data centres can happen months in advance.
- The **rules of engagement** has not been set in CW
  - What will the effect of an attack have. What about consequences to citizens of a target country?
- Physical weapons act as a deterrence. Enemies are cautious against countries with “big guns”
  - Attackers cannot reveal there offensive weapons.



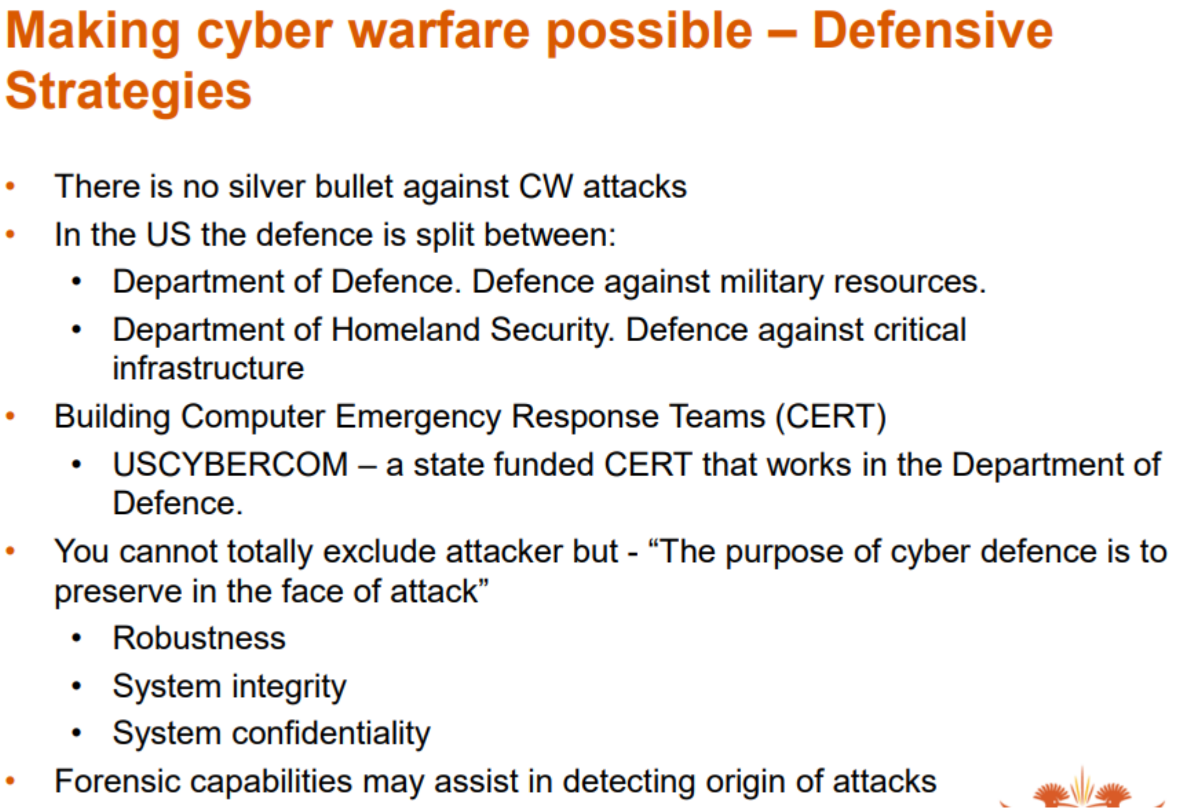
Making cyber warfare possible - Preparation

- Research
  - Highly trained personnel
  - Need time to uncover vulnerabilities
  - “Bug finders” and “Exploit writers”
  - Uncovering and using vulnerabilities can take months.
  - New tools are required to make the process of finding bugs easier.
- Reconnaissance
  - Identify potential targets.
  - Makes use of the countries' intelligence services
- Vulnerability Enumeration
  - Discover vulnerable systems
  - Can be done using specialised scanners
  - Build up a database of known systems.
  - Identify the easy targets.



Offensive Strategies – Technical weapons

- Broader set of CW tools include, but are not limited to:
- Vulnerability database
  - Database of known vulnerabilities and misconfigurations
- Deployment Tools
  - Known as "droppers".
  - How do you deploy your payload.
- Payloads
  - What can you do with a compromised system
  - DoS
- Control Consoles
  - Provide interfaces to find vulnerabilities, deploy a payload and execute the payload
  - CORE IMPACT, CANVAS and Metasploit



Making cyber warfare possible – Defensive Strategies

- There is no silver bullet against CW attacks
- In the US the defence is split between:
  - Department of Defence. Defence against military resources.
  - Department of Homeland Security. Defence against critical infrastructure
- Building Computer Emergency Response Teams (CERT)
  - USCYBERCOM – a state funded CERT that works in the Department of Defence.
- You cannot totally exclude attacker but - "The purpose of cyber defence is to preserve in the face of attack"
  - Robustness
  - System integrity
  - System confidentiality
- Forensic capabilities may assist in detecting origin of attacks

[20]

TOTAL: 100