JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF INFORMATION SYSTEMS & TECHNOLOGY

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY & FORENSIC

4TH YEAR 1ST SEMESTER 2015/2016 ACADEMIC YEAR

MAIN CAMPUS

COURSE CODE: IIT 3421

COURSE TITLE: INFORMATION WARFARE

EXAM VENUE: **STREAM: COMPUTER SECURITY & FORENSICS**

DATE: **EXAM SESSION:**

TIME:

INSTRUCTIONS

1. **Answer Question 1 (Compulsory) and ANY other TWO questions**
2. **Candidates are advised not to write on the question paper**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room**

QUESTION 1 [30 MARKS]

a) Define the following terms
   i) Information Warfare **(2 marks)**
   ii) Cyber-crime **(2 marks)**
   iii) Cyber Espionage **(2 marks)**
   iv) Cyber-terrorism **(2 marks)**
   v) Critical infrastructure **(2 marks)**

b) Briefly discuss the motives/drives behind cyber threats/attack. **(7 marks)**

c) Identify the steps an attack would follow in conducting a cyber attack **(5 marks)**

d) The Kenya national infrastructure is critical to day to day activities. Without it there may be no air transport, financial transactions would cripple, emergency services would cease to function and many other things may happen. Identify eight things that is considered critical infrastructure in Kenya with brief description of its importance. **(8 marks)**

QUESTION 2 [20 MARKS]

Within popular culture, cyber warfare is sensationalized. On television, with the tap of a button and a few swift keystrokes, cyber warriors can override the lockdown procedures of a military base, or turn off a country's power grid. In the real world, however, cyber warfare requires considerably more effort and organization. The manpower and time required to make a large-scale virus serve as a limiting factor in cyber attacks. Use the following case studies to discuss the type of Cyberwar involved, strategies and tactics that were used.

i) South Ossetia War - Georgia
ii) US power grid hack
iii) Stuxnet
iv) Operation Tunisia

QUESTION 3 [20 MARKS]

a) Briefly discuss the common strategies used by attackers in information warfare. **(10 marks)**

b) Identify reasons why it's difficult to implement proper defense in information warfare? Suggest possible solutions **(10 marks)**

QUESTION 4 [20 MARKS]

In the article "Information Warfare and Deception", Hutchinson examines information warfare and the increasingly dominant role of deception. Discuss the significance of deception in contemporary information warfare. **(20 marks)**

QUESTION 5 [20 MARKS]

A reasonable approach to the current shortage of trained and experienced Cyber Operations Specialists is to use simulations to foster training, assessment and tool development though a standardized approach. Discuss how games and simulations can be used for training of cyber operations specialist. In your discussion, include the simulation definition language, objects, attributes and constraints. (**20 marks)**