The Management University of Africa

Sponsored by the Kenya Institute of Management

CERTIFICATE UNIVERSITY EXAMINATIONS

SCHOOL OF MANAGEMENT AND LEADERSHIP

CERTIFICATE IN INTERNATIONAL RELATIONS AND DIPLOMACY

CIR 104 : POLITICAL SCIENCE AND INTERNATIONAL SECURITY

DATE: 3RD APRIL 2025

DURATION: 2 HOURS

MAXIMUM MARKS: 70

INSTRUCTIONS:

1. Write your registration number on the answer booklet.
2. **DO NOT** write on this question paper.
3. This paper contains **SIX (6)** questions.
4. Question ONE is compulsory.
5. Answer any other **FOUR** questions.
6. Question ONE carries **30 MARKS** and the rest carry **10 MARKS** each.
7. **Write all your answers in the Examination answer booklet provided.**

QUESTION ONE

Read the Case Study below carefully and answer the questions that follow:

Case Study: The Rise of Cyber Warfare

In recent years, the world has witnessed a significant escalation in cyber warfare activities, marking a paradigm shift in the nature of modern conflicts. Cyber warfare refers to the use of digital technologies, such as computer networks, to launch attacks on the infrastructure, communication systems, and data of adversaries. These attacks are often carried out by state-sponsored actors, criminal organizations, and hacktivist groups, posing unprecedented challenges to international security and stability.

Cyber-attacks come in various forms, ranging from sophisticated infiltration of government networks to disruptive malware targeting critical infrastructure, such as power grids, financial systems, and transportation networks. One of the most notable examples is the Stuxnet virus, believed to be developed jointly by the United States and Israel, which targeted Iran's nuclear facilities, causing significant damage to its uranium enrichment program.

The implications of cyber warfare for international security are profound and multifaceted. Firstly, the borderless nature of cyberspace blurs the lines between traditional notions of warfare and peacetime activities, complicating the application of international laws and norms governing armed conflicts. Moreover, the anonymity and deniability afforded by cyber operations make it difficult to attribute attacks to specific actors, leading to ambiguity and uncertainty in response strategies.

Attribution challenges, compounded by the lack of universally accepted rules of engagement in cyberspace, undermine traditional deterrence mechanisms and increase the risk of escalation. Unlike conventional warfare, where the use of force is overt and attributable, cyber-attacks can be launched clandestinely, making it challenging for states to retaliate without risking unintended consequences or triggering a broader conflict.

In light of these challenges, policymakers and international actors face the daunting task of developing effective strategies to mitigate the risks posed by cyber warfare.

This includes bolstering cybersecurity capabilities, enhancing international cooperation and information sharing, and promoting norms of responsible state behavior in cyberspace. Additionally, efforts to establish clear rules of engagement and mechanisms for attribution are crucial to enhancing deterrence and reducing the likelihood of conflict escalation.

Despite the complexities and uncertainties surrounding cyber warfare, it is clear that it has emerged as a defining feature of contemporary geopolitics, reshaping the landscape of international security in profound and unprecedented ways. As societies become increasingly dependent on digital technologies for critical functions, the need for robust cybersecurity measures and effective governance mechanisms has never been more urgent. Failure to address these challenges risks undermining global stability and leaving nations vulnerable to the disruptive effects of cyber-attacks.

Required:

a) According to the case study, attributing cyber-attacks to specific actors difficult. Discuss the consequences of these attribution challenges for international security? **(10 marks)**

b) In reference to the case study, discuss implications of cyber warfare for international security. **(10 marks)**

c) Discuss strategies that policymakers can implement to mitigate the risks posed by cyber warfare. **(10 marks)**

QUESTION TWO

(a) Explain the concept of democracy in political science. **(5 marks)**

(b) Discuss the role of political parties in shaping democratic processes. **(5 marks)**

QUESTION THREE

(a) Describe the characteristics of interest groups and their impact on political decision-making. **(5 marks)**

(b) Explain the role of social movements in driving political change. **(5 marks)**

QUESTION FOUR

(a) Compare and contrast coalition and single-party governments. **(5 marks)**

(b) Discuss the significance of economic performance and equality in governance. **(5 marks)**

QUESTION FIVE

(a) Analyze the theoretical foundations of security studies. **(5 marks)**

(b) Explain the concept of coercion in the context of international security. **(5 marks)**

QUESTION SIX

(a) Discuss the role of peacekeeping in contemporary security issues. **(5 marks)**

(b) Evaluate the effectiveness of diplomacy and sanctions in resolving conflicts. **(5 marks)**