The Management University of Africa

MUA

Sponsored by the Kenya Institute of Management

DIPLOMA UNIVERSITY EXAMINATIONS

SCHOOL OF MANAGEMENT AND LEADERSHIP

DIPLOMA IN INTERNATIONAL RELATIONS AND DIPLOMACY

DIR 103: INTERNATIONAL SECURITY AND STRATEGY

DATE: 2ND DECEMBER 2024

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:

Title: Cybersecurity Threats in the Digital Age: A Comprehensive Case Study

In the modern world, our lives are deeply intertwined with the digital landscape. This transformation has brought about remarkable advancements in communication, commerce, and governance. However, it has also given rise to a wave of cybersecurity threats that pose profound challenges to global security. In this comprehensive case study, we will delve into three significant incidents, shedding light on the evolving nature of these threats and their far-reaching implications.

Incident 1: State-Sponsored Cyber Espionage

In recent times, a troubling trend has emerged on the international stage—state-sponsored cyber espionage. Various governments have pointed fingers at one another, alleging involvement in this covert activity. At the heart of these allegations are Advanced Persistent Threat (APT) groups, believed to be connected to these governments. These groups have masterminded intricate attacks, targeting critical infrastructure, government agencies, and private-sector organizations with the aim of pilfering sensitive information and securing strategic advantages.

The motivations behind these state-sponsored cyber espionage campaigns are often rooted in geopolitics. Nations seek to gain a competitive edge in global affairs, acquire invaluable intelligence, and protect their national interests. The tactics employed by APT groups are equally sophisticated, including spear-phishing, zero-day exploits, and supply chain attacks, all executed with a high degree of stealth. The repercussions are profound, encompassing economic losses, compromised national security, and strained diplomatic relations. Attribution remains a challenge, adding complexity to the situation.

Incident 2: Ransomware Attack on Healthcare Systems

The healthcare sector, owing to its critical nature and vulnerabilities, has emerged as a prime target for cybercriminals. A major ransomware attack transcended borders, wreaking havoc on healthcare systems across multiple nations. Hospitals and medical facilities found themselves locked out of patient records, leading to delayed treatments and grave patient safety concerns. The attackers demanded a substantial

ransom in cryptocurrency for the release of the encrypted data. This attack had a catastrophic impact on patient care, causing delays in treatments and surgeries, and compromising the privacy of patient data. Ransomware attacks have evolved into financially motivated endeavors, characterized by exorbitant ransom demands and formidable encryption techniques. Beyond the immediate healthcare fallout, these attacks can have broader economic ramifications, as healthcare providers grapple with financial losses and damage to their reputations.

Incident 3: Cyber-Enabled Election Interference

In the realm of cyber threats, election interference has taken on a new, insidious form. During a recent election cycle, foreign actors leveraged social media platforms and disinformation campaigns to influence public opinion and undermine the electoral process across several nations. The objective was to sow discord and cast doubt on the legitimacy of the elections. Foreign actors exploited the anonymity and reach of the internet to disseminate false information, exploit societal divisions, and manipulate public sentiment. This form of cyber-enabled election interference challenges the very foundations of democratic governance by eroding trust in electoral processes and institutions. Attributing such interference is a complex endeavor, and coordinating an international response remains a formidable task.

Addressing these challenges necessitates a multifaceted approach, encompassing technological defenses, international collaboration, and a deeper understanding of the motives and tactics employed by cyber threat actors.

Required:

a) Analyze the major cybersecurity threats outlined in the case study and explain their potential impact on international security. **(10 Marks)**

b) Discuss the strategies that governments and international organizations can adopt to mitigate the risks posed by these cybersecurity threats. **(10 Marks)**

c) Assess the role of private cybersecurity firms and their collaboration with governments in addressing these threats. Highlight the challenges and benefits of such partnerships. **(10 Marks)**

QUESTION TWO

a) Compare and contrast the individual-level and domestic-level theories of war. **(7 Marks)**

b) Explain the concept of the "security dilemma" and its relevance to contemporary international relations. **(3 Marks)**

QUESTION THREE

a) Define "coercion" and "deterrence" in the context of international security. **(4 Marks)**

b) Analyze the challenges and limitations associated with the use of military force as a means of coercion in international conflicts. **(6 Marks)**

QUESTION FOUR

a) Discuss the four features of "collective security" in international relations. **(4 Marks)**

b) Discuss the key principles and functions of international alliances in maintaining global peace and security. **(6 Marks)**

QUESTION FIVE

a) Discuss how nuclear deterrence during the Cold War shaped international relations and security policies during that period? **(5 Marks)**

b) Evaluate the challenges posed by civil violence and its implications for human security in the contemporary world. **(5 Marks)**

QUESTION SIX

a) Analyze how China's role as a great power challenger in the 21st century impacts international security dynamics. **(5 Marks)**

b) Discuss how the global community can address the unconventional security threat of climate change effectively? **(5 Marks)**