1. Study programme and study programme's design and development

On the programme's purpose and objectives comment

1. Programme's purpose and objectives (Initial Description)

In recent years, Security and Defence fields have attracted a lot of attention due to a globally volatile environment. Regional wars among neighbouring countries tend to affect not only the region in conflict but also inflict global recession in economy, uncontrolled rise in fuel prices and food insecurity. At the same time, security incidents such as terrorist attacks or regional social upheavals tend to lead to massive migration of citizens from one country to the neighbouring countries or even to another continent thus challenging the sense of security of the local population.

The Joint Master of Science Program in Security and Defence aims at preparing Armed and Security Forces officers, government executives involved in security and defence policy but also citizens aspiring to work in fields related to security and defence in a global, constantly evolving environment, full of geopolitical challenges. Upon completion of this program, the participants will have deepened their knowledge of current technological and asymmetric security and defence threats and developed the ability to manage challenges and crises in the contemporary international context.

1. Programme's purpose and objectives (Updated description)

In recent years, Security and Defence fields have attracted a lot of attention due to a globally volatile environment. Regional wars among neighbouring countries tend to affect not only the region in conflict but also inflict global recession in economy, uncontrolled rise in fuel prices and food insecurity. At the same time, security incidents such as terrorist attacks or other asymmetric threats, challenge the sense of security of the local populations.

The Joint Master of Science Program in Security and Defence, covers technological areas, techniques, and systems, related to the fields of Security and Defence. The aim is to introduce and to further expand on the usage of these techniques and systems in the modern technological security and defence arena. Through its courses, the programme covers cyber technologies and techniques, telecommunication systems and other security and defence related systems.

On the mapping of learning Outcomes to multiple modules

SEC101	Principles of Cyber Warfare
SEC102	CyberSecurity
SEC111	Telecommunication Systems for Security and Defence
SEC112	Information Security Management
SEC201	Open-Source Intelligence (OSINT)
SEC202	Research Methods
SEC211	Asymmetric Threats and Countermeasures
SEC212	Technoethics/Ethics for Emerging Military Technologies
SEC213	Space Applications for Security and Defence
SEC699	Preparatory Module (Thesis)
SEC701A	MSc Thesis A
SEC701B	MSc Thesis B

Subject Knowledge and Understanding

- Understand the basic principles of security and the contemporary security challenges, risks and threats
  - Relevant to: SEC101, SEC102, SEC111, SEC112, SEC211
- Recognize the offensive and defensive techniques used in a cyber war
  - **Relevant to: SEC101, SEC102, SEC112, SEC201**
- Demonstrate knowledge of modern weapons, especially smart ones
  – Relevant to: SEC101, SEC211, SEC213
- Recognize terms and concepts pertaining to different types of telecommunication systems, along with their embedded components and implementations
  - Relevant to: SEC111, SEC211, SEC213
- Demonstrate an understanding of the importance of cybersecurity governance and risk management
  - Relevant to: SEC112
- Show knowledge of laws, regulations, and policies as they relate to cybersecurity and data protection
  - Relevant to: SEC112
- Be aware of the tools and techniques that exist and can be applied in open-source intelligence gathering
  - Relevant to: SEC101, SEC201
- Demonstrate an understanding of the theoretical concepts of Space in Security and Defence
  -Relevant to: SEC213

Skills

- Define applications of security and defence in current operations
  - Relevant to: SEC101, SEC102, SEC111, SEC112, SEC201, SEC211, SEC212, SEC213
- Perform security risk analysis and assessments and develop contingency plans
  - Relevant to: SEC112
- Analyse basic tactics used in cyber-attacks
  - Relevant to: SEC101, SEC102, SEC112
- Analyse requirements associated with the design, implementation, and deployment of various types of telecommunication systems, especially for security and defence applications
  - Relevant to: SEC111, SEC211, SEC213
- Identify the most appropriate sources of information on the Internet for a specific subject under investigation
  - Relevant to: SEC201, SEC112
- Specify Electronic Warfare concepts and techniques
  - Relevant to: SEC211
- Comprehend low observable principles and anti-stealth approaches
  - Relevant to: SEC211
- Evaluate the potential impact of new space technologies on security and defence
  - **Relevant to: SEC213**

Abilities

- Ability to understand technology, management, and leadership issues related to cybersecurity governance
  - Relevant to: SEC101, SEC112
- Assess the security policy of your organization
  - Relevant to: SEC102, SEC112
- Assess the vulnerabilities of ICT infrastructures using Risk Assessment tools
  - Relevant to: SEC112
- Apply common security policies to protect critical infrastructures and high-value assets.
  - Relevant to: SEC112, SEC211
- Propose techniques and solutions against threats and security problems in telecommunication systems
  - Relevant to: SEC111
- Apply common techniques in collecting data from social media, online communities and blogs
  - Relevant to: SEC201
- Perform a basic assessment of a weapon system in terms of target detection, passive stealth capability and electronic warfare
  - Relevant to: SEC211
- Assess the feasibility and potential impact of space-based solutions for security and defence
  - Relevant to: SEC213