Postgraduate Certificate in Military Intelligence Studies

Information Operations

Information Operations (IO) involve the integrated use of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception, and operations security (OPSEC), in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making.

Electronic Warfare (EW) is a military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and to ensure friendly use of the electromagnetic spectrum.

Computer Network Operations (CNO) are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Psychological Operations (PSYOP), also known as Military Information Support Operations (MISO), are operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

Military Deception is actions executed to deliberately mislead adversary decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

Operations Security (OPSEC) is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to identify those actions that can be observed by adversary intelligence systems, determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries, and then executing selected measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Command and Control Warfare (C2W) is the integrated use of operations security, military deception, PSYOP, EW, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions.

Cyberspace Operations are operations in or through cyberspace to manipulate, deny, disrupt, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Information Assurance (IA) encompasses measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information Environment consists of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Information Operations Planning is the systematic process of determining the information requirements of a mission and then assessing and developing the necessary information strategies, plans, or activities to meet those requirements.

Target Audience Analysis is the process of identifying and examining the characteristics, motivations, and preferences of the group(s) of individuals or organizations that influence or are influenced by the actions of a particular entity.

Counter-Messaging refers to the proactive effort by a military or government entity to disrupt, discredit, or counter adversarial messaging or propaganda.

Information Warfare refers to actions taken to achieve information superiority by affecting an adversary's information, information-based processes, information systems, and computer-based networks while defending one's own.

Strategic Communications is the coordinated and synchronized application of national informational instruments to influence target audiences abroad in support of national objectives.

Disinformation is false information spread deliberately to deceive or mislead.

Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Social Engineering is the psychological manipulation of individuals to divulge confidential information or perform actions that compromise security.

Denial-of-Service (DoS) Attack is an attempt to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests.

Phishing is a type of cyber attack in which attackers disguise themselves as a trustworthy entity in an electronic communication to obtain sensitive information, such as usernames, passwords, and credit card details.

Open Source Intelligence (OSINT) is intelligence collected from publicly available sources, such as newspapers, the internet, and social media.

Signals Intelligence (SIGINT) is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems.

Human Intelligence (HUMINT) is intelligence collected through interpersonal contact with human sources.

Geospatial Intelligence (GEOINT) is intelligence derived from the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth.

Cyber Threat Intelligence (CTI) is information that provides context and insights into potential cyber threats to an organization.

Command and Control (C2) is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Geopolitical Analysis is the study of the effects of geography, economics, and politics on international relations and the behavior of states.

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.

Propaganda is information, especially of a biased or misleading nature, used to promote or publicize a particular political cause or point of view.

Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Information Operations Cell (IOC) is an organization within a military unit or agency that plans, coordinates, and executes information operations.

Information Dominance is the capability to control, exploit, and defend information to achieve an advantage across the full range of military operations.

Strategic Influence is the ability to affect the perceptions, attitudes, beliefs, and behaviors of target audiences in ways that support the achievement of strategic objectives.

Operational Security (OPSEC) Plan is a systematic process used to identify, control, and protect generally unclassified information that is determined to be critical to the national security.

Information Operations Integration is the process of synchronizing and coordinating all information-related capabilities and activities to achieve unity of effort.

Information Operations Assessment is the evaluation of the effectiveness and impact of information-related activities and capabilities on the achievement of objectives.

Information Operations Support Plan is a plan that describes how information operations will support the overall campaign or operation.

Deception Plan is a plan that outlines the intended deception operations and objectives to mislead the adversary.

Information Operations Targeting is the process of selecting and prioritizing targets for information-related

activities.

Information Operations Execution is the implementation of information-related activities and capabilities to achieve desired effects.

Information Operations Evaluation is the assessment of the success of information-related activities in achieving their intended effects.

Information Operations Training is the education and preparation of personnel to conduct information-related activities effectively.

Information Operations Doctrine is the established principles, tactics, techniques, and procedures for conducting information-related activities.

Information Operations Capabilities are the resources and tools available to a military or government entity to conduct information-related activities.

Information Operations Challenges are the obstacles and difficulties faced in planning, executing, and assessing information-related activities.

Information Operations Opportunities are the favorable conditions and possibilities that can be exploited to achieve information-related objectives.

Information Operations Best Practices are the proven methods and approaches that have been successful in conducting information-related activities.

Information Operations Lessons Learned are the insights and conclusions drawn from past information-related activities to improve future operations.

Information Operations Risks are the potential negative outcomes or consequences of information-related activities.

Information Operations Technologies are the tools and systems used to conduct information-related activities, such as cyber tools, communication devices, and information systems.

Information Operations Planning Cycle is the iterative process of planning, executing, and assessing information-related activities to achieve desired effects.

Information Operations Legal Considerations are the laws, regulations, and policies that govern the conduct of information-related activities, such as privacy laws and rules of engagement.

Information Operations Ethical Considerations are the moral principles and values that guide the conduct of information-related activities, such as respect for human rights and the protection of civilians.

Information Operations Strategic Objectives are the overarching goals and aims of information-related activities, aligned with national or organizational priorities.

Information Operations Tactical Objectives are the specific, measurable goals and targets of information-related activities, aimed at achieving strategic objectives.

Information Operations Target Audience Analysis is the process of identifying and understanding the characteristics, motivations, and preferences of target audiences to tailor information-related activities effectively.

Information Operations Influence Operations are activities designed to shape perceptions, attitudes, and behaviors of target audiences to achieve desired outcomes.

Information Operations Support to Kinetic Operations is the integration of information-related activities with traditional military operations to enhance overall effectiveness and achieve mission success.

Information Operations Multi-Domain Integration is the coordination and synchronization of information-related activities across multiple domains, such as land, sea, air, space, and cyberspace.

Information Operations Cyber Defense is the protection of information and information systems from cyber threats, such as malware, phishing, and denial-of-service attacks.

Information Operations Cyber Offense is the use of cyber tools and capabilities to disrupt, degrade, or destroy adversary information systems and networks.

Information Operations Social Media Engagement is the use of social media platforms to disseminate information, shape narratives, and engage with target audiences.

Information Operations Counter-Disinformation is the effort to identify, expose, and counter false or misleading information spread by adversaries or hostile actors.

Information Operations Psychological Warfare is the use of psychological tactics and techniques to influence the perceptions, beliefs, and behaviors of adversaries or target audiences.

Information Operations Strategic Communication is the deliberate use of communication tools and channels to convey messages that support national or organizational objectives.

Information Operations Crisis Response is the rapid deployment of information-related activities to address emergencies, disasters, or critical incidents.

Information Operations Partner Engagement is the collaboration with allied or partner nations to achieve common information-related objectives.

Information Operations Counterterrorism is the use of information-related activities to disrupt, defeat, or deter terrorist organizations and operations.

Information Operations Counterintelligence is the effort to detect, neutralize, and exploit adversary intelligence activities that threaten national security.

Information Operations Hybrid Warfare is the combination of conventional military operations with

information-related activities to achieve strategic advantage.

Information Operations Influence Campaign is a coordinated series of information-related activities designed to shape perceptions, attitudes, and behaviors over time.

Information Operations Target Development is the process of identifying, analyzing, and selecting targets for information-related activities based on their relevance and impact.

Information Operations Data Analytics is the use of statistical analysis and algorithms to extract insights and patterns from large datasets for decision-making.

Information Operations Cyber Resilience is the ability to withstand, recover from, and adapt to cyber threats and disruptions to maintain operational effectiveness.

Information Operations Cultural Awareness is the understanding and appreciation of cultural differences and sensitivities when conducting information-related activities in diverse environments.

Information Operations Geographic Context is the consideration of geographical factors and terrain features in planning and executing information-related activities.

Information Operations Network Exploitation is the use of technical means to gain unauthorized access to adversary computer networks to collect intelligence or disrupt operations.

Information Operations Network Defense is the protection of friendly computer networks from cyber threats and vulnerabilities to ensure operational security.

Information Operations Intelligence Fusion is the integration of multiple sources of intelligence, such as SIGINT, HUMINT, and OSINT, to produce comprehensive and actionable insights.

Information Operations Rapid Response is the ability to deploy information-related activities quickly in response to emerging threats or opportunities.

Information Operations Strategic Partnerships are collaborative relationships with government agencies, non-governmental organizations, and private sector entities to achieve mutual information-related objectives.

Information Operations Risk Management is the process of identifying, assessing, and mitigating risks associated with information-related activities to ensure mission success.

Information Operations Resilience Planning is the development of strategies and measures to maintain operational continuity in the face of disruptions or attacks on information systems.

Information Operations Training and Education is the provision of knowledge, skills, and resources to personnel to enable them to conduct information-related activities effectively.

Information Operations Technology Integration is the incorporation of advanced technologies, such as artificial intelligence and machine learning, into information-related capabilities.

Information Operations Legal Compliance is the adherence to laws, regulations, and international norms governing the conduct of information-related activities to avoid legal repercussions.

Information Operations Ethical Standards are the principles and guidelines that guide the behavior and decision-making of personnel engaged in information-related activities.

Information Operations Strategic Communication Plan is a comprehensive strategy for crafting and disseminating messages to target audiences to achieve desired outcomes.

Information Operations Crisis Management is the coordination of information-related activities during emergencies or critical incidents to maintain situational awareness and respond effectively.

Information Operations Threat Assessment is the evaluation of potential risks and vulnerabilities in information systems and networks to prevent or mitigate cyber threats.

Information Operations Incident Response is the immediate actions taken to contain and mitigate the impact of cyber incidents on information systems and networks.

Information Operations Continuous Monitoring is the ongoing surveillance and evaluation of information systems and networks to detect and respond to security threats in real-time.

Information Operations Intelligence Sharing is the exchange of information and intelligence with partner agencies and organizations to enhance situational awareness and collaborative efforts.

Information Operations Resource Allocation is the allocation of personnel, funding, and assets to support information-related activities and achieve mission objectives.

Information Operations Performance Metrics are the quantitative and qualitative measures used to assess the effectiveness and impact of information-related activities.

Information Operations Reporting and Analysis is the collection, processing, and interpretation of data and information to generate insights and inform decision-making.

Information Operations Knowledge Management is the organization and dissemination of information, best practices, and lessons learned to enhance operational effectiveness.

Information Operations Strategic Planning is the development of long-term goals, objectives, and strategies to guide information-related activities and achieve desired outcomes.

Information Operations Operational Planning is the detailed planning and coordination of information-related activities to support military operations and campaigns.

Information Operations Tactical Execution is the implementation of information-related activities at the tactical level to achieve specific mission objectives.

Information Operations Intelligence Collection is the systematic gathering of information and intelligence to support decision-making and achieve operational goals.

Information Operations Cybersecurity Measures are the safeguards and protocols implemented to protect information systems and networks from cyber threats and vulnerabilities.

Information Operations Threat Intelligence Sharing is the exchange of intelligence on cyber threats and vulnerabilities to enhance situational awareness and improve defenses.

Information Operations Incident Response Plan is a documented procedure outlining the steps to be taken in response to a cyber incident to minimize damage and restore operations.

Information Operations Crisis Communication is the strategic dissemination of information during emergencies or crises to manage public perception and maintain trust.

Information Operations Situational Awareness is the understanding of the current operational environment and the factors that may impact mission success.

Information Operations Decision Support is the provision of timely and relevant information to decision-makers to facilitate informed choices and actions.

Information Operations Training and Exercises are simulations and drills conducted to enhance the skills and readiness of personnel in conducting information-related activities.

Information Operations Capability Development is the continuous improvement and enhancement of information-related capabilities to meet evolving threats and challenges.

Information Operations Innovation and Research is the exploration of new technologies, techniques, and approaches to advance information-related activities and capabilities.

Information Operations Collaboration and Partnerships are cooperative relationships with government agencies, industry partners, and international allies to leverage expertise and resources in information-related activities.

Information Operations Quality Assurance is the process of ensuring that information-related activities meet established standards and objectives to achieve desired outcomes.

Information Operations Compliance and Auditing is the assessment and verification of adherence to regulations, policies, and best practices in information-related activities.

Information Operations Crisis Response Coordination is the integration and synchronization of information-related activities during emergencies or crises to achieve a unified and effective response.

Information Operations Strategic Communication Campaign is a coordinated series of messages and activities designed to shape perceptions, attitudes, and behaviors over an extended period.

Information Operations Situational Assessment is the evaluation of the operational environment, threats, and opportunities to inform decision-making and planning.

Information Operations Risk Mitigation is the identification and implementation of measures to reduce or

eliminate potential risks to information systems and operations.

Information Operations Incident Handling is the process of responding to and resolving cyber incidents to minimize disruption and restore normal operations.

Information Operations Continuous Improvement is the ongoing effort to enhance processes, capabilities, and outcomes in information-related activities through feedback and evaluation.

Information Operations Resilience Testing is the assessment of the ability of information systems and networks to withstand and recover from cyber threats and disruptions.

Information Operations Lessons Identification is the recognition and documentation of insights and experiences gained from past activities to inform future decision-making.

Information Operations Capability Assessment is the evaluation of information-related capabilities to determine strengths, weaknesses, and areas for improvement.

Information Operations Technology Evaluation is the analysis and testing of new technologies and tools to assess their suitability and effectiveness in information-related activities.

Information Operations Policy Development is the creation and implementation of guidelines, procedures, and regulations to govern information-related activities.

Information Operations Organizational Structure is the design and arrangement of units, teams, and functions to support information-related activities effectively.

Information Operations Resource Management is the allocation and