Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85579Neubiberg

Modulhandbuch des Studiengangs

Intelligence and Security Studies
(Master of Science)

an der
Universität der Bundeswehr München

(Version 2025)

Stand: 04. November 2025

Prolog

§ 22 - Mastergrad
Aufgrund der bestandenen Masterprüfung wird der akademische Grad "Master of Arts", abgekürzt **"M.A."** verliehen, wenn die Pflichtmodule der Vertiefungsrichtungen **"Nachrichtendienste und öffentliche Sicherheit", "Terrorismusbekämpfung", "Regionale Sicherheit" oder "Intelligence Cooperation"** absolviert wurden, bzw. der akademisch Grad "Master of Science", abgekürzt **"M.Sc."**, wenn die Pflichtmodule der Vertiefungsrichtung **"Cyber Defence"** absolviert wurden. Es wird eine gemeinsame Urkunde vergeben, die die Siegel beider Hochschulen (UniBw M und HS Bund) trägt.

Inhaltsverzeichnis

Modulname	Modulnummer
Cyber Defence I	5537

Konto	Pflichtmodule der Vertiefungsrichtung "Cyber Defence" - MISS 2025 M.Sc

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Pflicht	5

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
250	100	150	10

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10106	VÜ	Sicherheitsmanagement	Pflicht	3
10107	VÜ	Sichere vernetzte Anwendungen	Pflicht	3
5537-V2	VÜ	Sichere Netze und Protokolle	Pflicht	4
Summe (Pflicht und Wahlpflicht)				10

Empfohlene Voraussetzungen
Vorkenntnisse aus dem Modul 3479 erforderlich.

Qualifikationsziele
Das Modul vermittelt Kompetenzen zur Analyse, Bewertung und Absicherung von IT-Infrastrukturen und deren Bestandteilen auf den drei komplementären Ebenen 1. einzelner Systeme und darauf betriebener Anwendungen 2. von Rechnernetzen mit verschiedenen Übertragungsmedien und- protokollen 3. organisationsweit und z.B. im Rahmen von Supply Chains organisationsübergreifender Verbünde. Studierende kennen grundlegende und praktisch häufig anzutreffende Designfehler, Arten weit verbreiteter Sicherheitslücken und typische Implementierungsfehler sowie Betriebsdefizite. Sie können Sicherheitslücken u.a. auf Quelltextebene erkennen, beherrschen wichtige Härtungsmaßnahmen und können Verfahren wie Penetration-Tests in der Praxis gezielt einsetzen. Des Weiteren erlangen die Studierenden die Kompetenz, den Themenkomplex Informationssicherheit in seiner Breite strukturiert und nach technischen und organisatorischen Aspekten differenziert anzugehen und je nach Einsatzszenario systematisch Schwerpunkte im operativen Sicherheitsmanagement zu setzen. Studierende werden in die Lage versetzt, in realistischen Anwendungsbeispielen den Erfüllungsgrad von Anforderungen durchinternationale Normen und Zertifizierungskriterien zu beurteilen und Maßnahmen zu planen, um identifizierte Defizite zu beseitigen.

Inhalt

Die Vorlesung "Sichere Netze und Protokolle" vermittelt Wissen über verschiedene Methoden zur sicheren Datenübertragung in modernen Kommunikationsnetzen. Dafür werden zunächst der Aufbau von Daten- und Rechnernetzen sowie die klassischen Internet- Protokolle (z.B. IPv4 und IPv6, TCP und UDP, WLAN) vorgestellt und analysiert. Darauf aufbauend werden anhand der Schichten des ISO/OSI-Referenzmodells Protokolle und Dienste zum sicheren Datenaustausch im Internet und drahtlosen Netzwerken betrachtet, z.B. IPSec, TLS, WEP/WPA, S/MIME. Dabei werden die vorgestellten Protokolle und Dienste auf ihre Sicherheit analysiert. Es werden neben deren bekannten Schwächen und daraus resultierenden Angriffsvektoren die Gegenmaßnahmen diskutiert.

Die Vorlesung Sichere vernetzte Anwendungen betrachtet Methoden, Konzepte und Werkzeuge zur Absicherung von verteilten Systemen über deren gesamten Lebenszyklus. Anhand von Webanwendungen und anderen serverbasierten Netzdiensten werden zunächst Angreifer-, Bedrohungs- und Trustmodelle sowie typische Design-, Implementierungs- und Konfigurationsfehler und deren Zustandekommen analysiert. Auf Basis dieser Grundlagen wird ein systematisches Vorgehen bei der Entwicklung möglichst sicherer vernetzter Anwendungen erarbeitet. Nach einem Überblick über die Besonderheiten der auf IT-Sicherheitsaspekte angepassten Entwicklungsprozesse werden ausgewählte Methoden und Werkzeuge, u.a. zur statischen bzw. dynamischen Code-Analyse und für Penetration Tests, und ihr Einsatz in den einzelnen Phasen des Softwarelebenszyklus mit den Schwerpunkten Implementierung und operativer Einsatz vertieft. Eine Diskussion typischer sicherheitsrelevanter Aufgaben im IT-Betrieb und möglicher Disclosure-Verfahren zum Umgang mit identifizierten Sicherheitslücken rundet die Lehrveranstaltung ab.

Die Vorlesung Sicherheitsmanagement führt in die organisatorischen und technischen Aspekte des Umgangs mit dem Thema Informationssicherheit in komplexen, standortübergreifenden Umgebungen ein. Auf Basis der internationalen Normenreihe ISO/IEC 27000, die u.a. im Rahmen des IT-Sicherheitsgesetzes auch national stark an Bedeutung gewinnt, werden die Bestandteile so genannter Informationssicherheits-Managementsysteme (ISMS) analysiert und Varianten ihrer Umsetzung mit den damit verbundenen Stärken und Risiken diskutiert. Neben der Integration vorhandener technischer Sicherheitsmaßnahmen in ein ISMS werden auch die Schnittstellen zu branchenspezifischen Vorgaben, beispielsweise zur Produktzertifizierung, zum professionellen IT-Service Management bei IT-Dienstleistern und zu gesetzlichen Auflagen betrachtet.

Literatur

• Sachar Paulus: Basiswissen Sichere Software, dpunkt-Verlag, 2011

• Ross Anderson: Security Engineering, Wiley-Verlag, 2. Auflage, 2008

• Michael Howard, David LeBlanc, John Viega: 24 Deadly Sins of Software Security, McGraw-Hill, 2009

• William Stallings: Data and Computer Communications, 9. Auflage, 2010, Pearson Education, ISBN 978-0-13-139205-2

• Kurose, James & Ross, Keith: „Computernetzwerke – Der Top-Down-Ansatz“, 5. Auflage, 2012, Pearson Studium, ISBN 978-3-86894-185-2

• Michael Brenner et al.: Praxisbuch ISO/IEC 27001, Hanser-Verlag, 3. Auflage, 2019

• Th. Harich, IT-Sicherheitsmanagement – Arbeitsplatz IT Security Manager, mitp Professional Verlag, 2012

Leistungsnachweis
Der Leistungsnachweis besteht aus einer schriftlichen Prüfung (120 Minuten), die mit mindestens der Note 4,0 bestanden sein muss.
Verwendbarkeit
Die in diesem Modul vermittelten Kenntnisse und Fertigkeiten sind eine wichtige Grundlage für berufliche Tätigkeiten im Umfeld der IT-Sicherheit und bereiten auf die Praxis vor. Grundlage der Verfassung der Masterarbeit.
Dauer und Häufigkeit
Das Modul dauert 3 Monate (April-Jun) und beginnt jeweils im Frühjahrstrimester des 2. Studienjahres.

Modulname	Modulnummer
Cyber Defence II	5538

Konto	Pflichtmodule der Vertiefungsrichtung "Cyber Defence" - MISS 2025 M.Sc

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Pflicht	5

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
250	100	150	10

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5538-V1	VÜ	Hardware- und Betriebssystemsicherheit	Pflicht	3
5538-V2	VÜ	Data Science and Analytics	Pflicht	3
5538-V3	P	Security Engineering	Pflicht	4
Summe (Pflicht und Wahlpflicht)				10

Empfohlene Voraussetzungen

Vorkenntnisse aus dem Modul 3479 erforderlich.

Qualifikationsziele

Die Studierenden erlernen in diesem Modul im Themengebiet DASA das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den dargestellten Bereichen. Sie haben praktische Erfahrungen im Betrieb von Systemen unter Berücksichtigung verschiedener Sicherheitsaspekte gesammelt. Die Studierenden sind in der Lage, Methoden zur Bewertung und Erhöhung der IT-Sicherheit in allen Lebenszyklusphasen der eingesetzten Hard- und Software anzuwenden.

Inhalt

In der Vorlesung Hardware- und Betriebssystemsicherheit erhalten Studierende einen vertieften Einblick in Fragestellungen der Systemsicherheit. Die Grundlage bildet ein Überblick über aktuelle Systemarchitekturen. Sie erhalten einen Einblick in die systemnahe Programmierung verschiedener abzusichernder Systeme wie PCs, Server, Netzkomponenten und Mobilgeräte und die damit verbundenen physischen Angriffswege und Härtungsmaßnahmen. Nach einem Überblick über aktuelle Techniken zur Erhöhung der Betriebssystemsicherheit werden klassische Sicherheitsprobleme von Betriebssystemen diskutiert. Ausgewählte Fallbeispiele zeigen die konkrete Umsetzung am Windows- und Unix-Kernel und dienen als Ausgangsbasis für die Vermittlung grundlegender Analyse- und Reverse-Engineering-Methoden zur Diskussion systemnaher Sicherheitslücken.

In der Vorlesung Data Science and Analytics werden die Studierenden mit den Grundlagen Data Science vertraut gemacht. Insbesondere soll die moderne Entscheidungsunterstützung im Bereich von Intelligence Analysis damit vorbereitet und unterstützt werden. In der Vorlesung wird die Entwicklung von quantitativen und

qualitativen Analysemodellen zur Erforschung des komplexen Systemverhaltens (im Bereich Intelligence Collection und Complex Operations) sowie die Erarbeitung von Entscheidungsgrundlagen auf der Grundlage von Systembewertungen und speziellen OR-Techniken ausführlich behandelt. Ein weiterer ergänzender Schwerpunkt der Vorlesung liegt im Bereich der Anwendung und Weiterentwicklung von speziellen System Dynamics Modellen und statistischen Netzwerkanalysen im Bereich der strategischen Planung und Szenarentwicklung im Kontext von Safety & Security.

Eine exemplarische Auswahl der Inhalte besteht aus:

• Einführung in Data Science

• Theoretische Einführung in die System- und Entscheidungstheorie

• (Systemklassifikation, Eigenschaften von Systemen, Prozessoptimierung)

• Analyseverfahren

• Modellbildung, Dynamische Systeme und Simulationen

• Szenartechniken, Zukunftsanalysen (RAHS), System Dynamics

• Soft OR/ Hard OR Analysen

• Ausblick: System Dynamics im Bereich MST (Modelling, Simulation, Training), Bestimmungsgrößen internationaler Sicherheit „Safety & Security“ durch OR

Schwerpunkt im Praktikum Security Engineering ist die selbständige Durchführung von praktischen Aufgaben zu aktuellen Fragestellungen der Absicherung von IT-Systemen. Zu Beginn werden unter Unix einfache netzwerkbasierte Angriffe auf den Ebenen 2 bis 4 sowie 7 des ISO/OSI-Referenzmodells vorgestellt und mit Hilfe von Scapy und Python 3 umgesetzt. Neben der Einrichtung und Nutzung zentraler Dienste wie Certificate Authorities für Public-Key-Infrastrukturen und LDAP-Servern zur Authentisierung und Autorisierung von Anwendern werden auch dedizierte Sicherheitskomponenten wie Intrusion Detection Systeme und Honeypots implementiert. Im Weiteren werden einfache Anwendungen und Betriebssystemkomponenten mit typischen Verfahren zur Softwareanalyse bzgl. Schwachstellen untersucht. Dazu werden gängige Werkzeuge und Verfahren, wie etwa recursive descent Analyse mit IDApro, praktisch eingesetzt. Neben der Codeanalyse von unbekannter Software mit Hilfe des Einsatzes von Virtualisierungstechniken und Disassembler werden zudem die Möglichkeiten der Forensischen Analyse von Betriebssoftware sowohl klassischer, als auch mobiler Endgeräte vorgestellt und anhand praktischer Beispiele durchgeführt. Abschließend werden Angriffe auf mobile Endgeräte unter Android durch den Einsatz von Metasploit durchgeführt.

Literatur

• Andrew S. Tanenbaum, Herbert Bos: Moderne Betriebssysteme. Pearson Studium, 2016, 4. Auflage

• Andrew S. Tanenbaum, Todd Austin: Rechnerarchitektur: Von der digitalen Logik zum Parallelrechner. Pearson Studium, 2014, 6. Auflage • David Patterson (Autor), John LeRoy Hennessy: Rechnerorganisation und Rechnerentwurf: Die Hardware/Software-Schnittstelle. De Gruyter Oldenbourg, 2016, Auflage 4.
Leistungsnachweis
Der Leistungsnachweis besteht aus einer mündlichen Prüfung (30 Minuten), die mit mindestens der Note 4,0 bestanden sein muss.
Verwendbarkeit
Die in diesem Modul vermittelten Kenntnisse und Fertigkeiten sind eine wichtige Grundlage für berufliche Tätigkeiten im Umfeld der IT-Sicherheit und bereiten auf die Praxis vor. Grundlage der Verfassung der Masterarbeit.
Dauer und Häufigkeit
Das Modul dauert 3 Monate (April-Jun) und beginnt jeweils im Frühjahrstrimester des 2. Studienjahres.

Modulname	Modulnummer
Digitalisierung	5526

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Juniorprof. Dr. rer. nat. Maximilian Moll	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
250	120	130	10

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5526-V1	VS	Digitalisierung	Pflicht	4
5526-V2	P	Praktikum zur Digitalisierung	Pflicht	4
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Es werden keine besonderen Vorkenntnisse vorausgesetzt.

Qualifikationsziele

Die Studierenden können den grundsätzlichen Aufbau einer technischen IT-Infrastruktur sowie deren Zusammenspiel erläutern. Dies gilt ebenso für einzelne Rechensysteme wie für daraus zusammengesetzte Kommunikationsnetze. Sie sind in der Lage, verschiedene Formen und Darstellungen von Information zu verstehen und ineinander zu überführen. Sie kennen die grundlegende Bedeutung von Codes, insbesondere von kryptographischen Codes für die IT-Sicherheit. Die Studierenden können einfache Probleme selbständig durch Programmierung lösen und dabei ggfs. fertige Fremdkomponenten einbinden. Sie verstehen wichtige Software-Eigenschaften wie Korrektheit und Effizienz und wissen, wie man diese praktisch untersucht.

Inhalt

Dieses Modul vermittelt insbesondere Studierenden mit geringen informationstechnischen Vorkenntnissen das erforderliche Grundlagenwissen für das Kernstudium. In einer Vorlesung mit seminaristischen Anteilen erhalten die Studierenden eine solide Grundlagenausbildung zu den Verfahren, Einrichtungen und Systemen der Informations- und Kommunikationstechnik sowie einen breiten Überblick über deren Anwendungen. Sie lernen, wie Daten und Nachrichten dargestellt, codiert, verarbeitet, übertragen und gespeichert werden; sie verstehen den Aufbau und die Funktionsweise der technischen Systeme, welche diese Prozesse ermöglichen, unterstützen und ausführen. In begleitenden Praktikumsteilen lernen die Studierenden, wie man Aufgaben erfasst und praktisch mittels Programmierung löst. Dabei werden neben den gängigen Kontroll- und Datenstrukturen auch Modulbausteine aus Programmbibliotheken eingesetzt. In der Vorlesung dargestellte Inhalte werden zum Teil durch Programme operationalisiert und dadurch vertieft. Problemfelder und Herausforderungen der Digitalisierung werden benannt, erläutert und diskutiert.

Literatur
• Helmut Herold, Bruno Lurz, Jürgen Wohlrab, Matthias Hopf: Grundlagen der Informatik. Pearson-Verlag, 3. Auflage 2017, ISBN 978-3-86894-316-0 • Gumm, Heinz-Peter; Sommer, Manfred: Einführung in die Informatik. Oldenbourg Verlag, 10. Auflage 2013, ISBN 978-3-486-70641-3 • Ulrich Freyer: Nachrichten-Übertragungstechnik: Grundlagen, Komponenten, Verfahren und Anwendungen der Informations-, Kommunikations- und Medientechnik. Hanser-Verlag, 7. Auflage, 2017, ISBN 978-3-446-44211-5 • Bernd Klein: Einführung in Python 3. Carl Hanser Verlag, 3. Auflage 2018, ISBN 978-3-446-54208-4 • Johannes Ernesti, Peter Kaiser: Python 3 - Das umfassende Handbuch: Sprachgrundlagen, Objektorientierung, Modularisierung. Verlag Rheinwerk Computing, 2. Auflage 2016, ISBN 978-3-8362-3633-1 • Mark Lutz: Learning Python. O'Reilly Verlag, 5. Auflage 2017, ISBN 978-1-449-35573-9
Leistungsnachweis
Der Leistungsnachweis besteht aus einer schriftlichen Prüfung mit einer Dauer von 120 Minuten, die mit mindestens der Note 4,0 bestanden sein muss.
Verwendbarkeit
Die Inhalte des Moduls legen die Grundlage für das Modul 5535, sowie die Vertiefungsrichtung Cyber Defence.
Dauer und Häufigkeit
Das Modul dauert 6 Monate (Jan-Jun) und beginnt jeweils im Wintertrimester des 1. Studienjahres.

Modulname	Modulnummer
Einführung in Intelligence and Security Studies	5524

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Eva Herschinger	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
250	90	160	10

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5524-V1	VL	Einführung in Internationalen Beziehungen und Security Studies	Pflicht	2
5524-V2	SE	Einführung in Intelligence History	Pflicht	2
5524-V3	SE	Intelligence Essentials - Nachrichtendienstliche Operationen	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Es werden keine besonderen Vorkenntnisse vorausgesetzt.

Qualifikationsziele

Die Studierenden sind mit der nationalen und internationalen Sicherheitsarchitektur vertraut. Sie verfügen über die notwendigen methodischen Zugänge, um sicherheitspolitische Bedingungen und Prozesse der Friedenserhaltung und Krisenbewältigung zwischen und gegenüber staatlichen, staatsähnlichen und nichtstaatlichen Akteuren erklären zu können. Auf dieser Grundlage können sie aktuelle sicherheitspolitische Herausforderungen bewerten. Mit der üblichen Arbeitsweise von Intelligence-Akteuren, insbesondere dem „Intelligence Cycle“ und den Methoden der „Intelligence Analysis“, sind sie vertraut und kennen die verschiedenen Methoden der Informationsbeschaffung (bspw. HUMINT, SOCMINT, SIGINT). Zudem sind sie in der Lage, Gemeinsamkeiten und Unterschiede zwischen verschiedenen nationalen und ausländischen Nachrichtendiensten in Bezug auf ihre Geschichte, ihre rechtliche Einbettung, ihre Rolle im politischen Entscheidungsprozess und ihre öffentliche Wahrnehmung zu identifizieren.

Inhalt

Das Modul legt Grundlagen. Die Studierenden erhalten grundlegende Einsichten im Bereich der internationalen Beziehungen, internationaler Sicherheit sowie Krieg und Frieden. Sie lernen darüber hinaus Geschichte, Organisation und Aufgaben verschiedener in- und ausländischer Nachrichtendienste kennen und werden mit der Funktion von „Intelligence“ in der deutschen und internationalen Sicherheitsarchitektur vertraut gemacht.

Die Vorlesung stellt aktuelle Herausforderungen internationaler Sicherheit in den Mittelpunkt. In diesem Zusammenhang sind insb. theoretische und methodische Ansätze der Theorien der „Internationalen Beziehungen“ von Bedeutung. Ziel ist es, die Studierenden mit den zentralen Theorien und Akteuren der Internationalen Beziehungen vertraut zu machen und sie v.a. für sicherheitspolitischen Herausforderungen des Informationszeitalters zu sensibilisieren.

Das Seminar „Einführung in Intelligence History“ führt ein in die Geschichte vorwiegend westlicher Nachrichten- bzw. Geheimdienste seit dem Zweiten Weltkrieg. Diskutiert werden Organisation und Struktur des Nachrichten- bzw. Geheimdienstwesens, das Verhältnis zwischen Institutionen, Politik und (medialer) Öffentlichkeit, die Rolle von Nachrichten- bzw. Geheimdiensten in Demokratien sowie die Wechselwirkungen von technologischer Innovation und der Produktion, Analyse und Interpretation von Informationen. Anhand ausgewählter Beispiele werden operative Merkmale geheimdienstlicher Tätigkeit erarbeitet und im Kontext historischer Prozesse bewertet.

Um die Arbeitsweise der Intelligence-Akteure nachvollziehen zu können, werden im Seminar „Intelligence Essentials“ unterschiedliche Facetten nachrichtendienstlicher Arbeit wie „Intelligence Analysis“ „Intelligence Collection“ oder „Covert Action“ behandelt und reflektiert.

Literatur

Intelligence History:

• Adams, Jefferson, Strategic Intelligence in the Cold War and Beyond, London: Routledge 2015.

• Andrew, Christopher: The Secret World: A History of Intelligence, New Haven: Yale University Press 2018.Andrew, Christopher, Secret Intelligence: A Reader, London: Routledge 2009.

• Haslam, Jonathan, Near and Distant Neighbors: A New History of Soviet Intelligence, Oxford: Oxford University Press 2015.

• Goschler, Constantin/Wala, Michael, „Keine neue Gestapo“. Das Bundesamt für Verfassungsschutz und die NS-Vergangenheit, Reinbek bei Hamburg: Rowohlt 2015.

• Immerman, Richard, The Hidden Hand: A Brief History of the CIA, Malden, MA: JohnWiley & Sons 2014.

• Jeffreys-Jones, Rhodri, In Spies We Trust: The Story of Western Intelligence, Oxford: Oxford University Press 2013.

• Johnson, Loch K., Intelligence: The Secret World of Spies: An Anthology, Oxford: Oxford University Press 2015.

• Johnson, Loch K., National Security Intelligence, Malden, MA: Polity 2017.

• Krieger, Wolfgang, Die deutschen Geheimdienste. Vom Wiener Kongress bis zum Cyber War, München: C.H.Beck 2021.

• Krieger, Wolfgang, Geheimdienste in der Weltgeschichte. Spionage und verdeckte Aktionen von der Antike bis zur Gegenwart, 3., aktualisierte und erweiterte Aufl. München: C.H.Beck, 2014.

• Lapid, Ephraim, The Israeli Intelligence Community: An Insider's View, Jerusalem/New York: Gefen Publishing House 2020.

• Omand, David: How Spies Think: Ten Lessons in Intelligence, London: Penguin Books 2021.

• Oxford Handbook of National Security Intelligence, ed. by Loch K. Johnson, Oxford: Oxford University Press, 2010 (paperback ed. 2012).

• West, Nigel, Historical dictionary of international intelligence, Lanham, MD: Rowman& Littlefield 2015.

• Zegart, Amy B., Spies, Lies, and Algorithms: The History and Future of American Intelligence, Princeton: Princeton University Press 2022.

Intelligence:

• Mark M. Lowenthal, Intelligence, From Secrets to Policy, 7th edition, 2016.

• Christopher Andrew/ Richard J. Aldrich/ Wesley K. Wark (eds.), Secret Intelligence, A Reader, 2009.

• Robert Dover (ed.), Routledge Companion to Intelligence Studies, 2015.

• Mark Pythian (ed.), Understanding the Intelligence Cycle, 2013.

• Loch K. Johnson (ed.), The Oxford Handbook of National Security Intelligence, 2010.

• David Omand, Securing the State, 2010.

• Carl J. Jensen/ David H. McElreath/ Melissa Graves, Introduction to Intelligence Studies, 2013.

• Wolfgang Krieger, Geschichte der Geheimdienste, Von den Pharaonen bis zur NSA, 3. Aufl., 2014.

• Thomas Jäger/ Anna Daun (Hrsg.), Geheimdienste in Europa. Transformation, Kooperation und Kontrolle, 2009.

Internationale Beziehungen und Security Studies:

• Balzacq, Thierry/Cavelty-Dunn, Myriam (Hrsg.): The Routledge Handbook of Security Studies, New York, 2016.

• Baylis, John/ Smith, Steve/ Owens, Jessica (Hrsg.): The Globalization of World Politics. An Introduction to International Relations, 6. überarb. Aufl., Oxford, 2014.

• Baylis, John/Wirtz, James J./Johnson, Jeannie L.: Strategy in the Contemporary World: An Introduction to Strategic Studies, 7. Aufl., Oxford, 2022.

• Buzan, Barry/ Wæver, Ole/de Wilde, Jaap: Security. A New Framework for Analysis, Boulder, CO, 1998.

• Bull, Hedley: The Anarchical Society. A Study of Order in World Politics, 4. Auf., Basingstoke, 2012.

• Campbell, David: Writing Security. United States Foreign Policy and the Politics of Identity, Minneapolis, überabeitete Aufl., 1998.

• Edkins, Jenny/Zehfuss, Maja (Hrsg.), Global Politics: A New Introduction, 3. Aufl., New York, 2019.

• Moravcsik, Andrew: Taking Preferences Seriously: A Liberal Theory of International Politics, in: International Organization 51: 4, S. 513-553, 1997.

• Morgenthau, Hans.: Politics among Nations: The Struggle for Power and Peace, NewYork, 1993.

• Sauer, Frank/Masala, Carlo (Hrsg.): Handbuch Internationale Beziehungen, Wiesbaden, 2017.

• Schieder, Siegfried/Spindler, Manuela (Hrsg.): Theorien der Internationalen Beziehungen, 3. Aufl., Opladen& Farmington Hills, 2010.

• Waltz, Kenneth N.: Theory of International Politics, New York, 1979.Wendt, Alexander: Social Theory of International Politics, Cambridge, 1999.

• Wendt, Alexander: Anarchy is What States Make of It: The Social Construction of Power Politics, in: International Organization 46: 2, S. 391-425, 1992.

Leistungsnachweis
Der Leistungsnachweis besteht aus einer Seminararbeit (2500-3000 Wörter/ Bearbeitungszeit vier bis acht Wochen, die konkrete Bearbeitungszeit wird zu Beginn der Lehrveranstaltung bekannt gegeben), die mit mindestens der Note 4,0 bestanden sein muss.
Verwendbarkeit
Die Inhalte des Moduls legen die Grundlagen für die Module 5528, 5530, 5532 und 5534, sowie die Vertiefungsrichtungen Regionale Sicherheit und Intelligence Cooperation.
Dauer und Häufigkeit
Das Modul dauert 6 Monate (Jan-Jun) und beginnt jeweils im Wintertrimester des 1. Studienjahres.

Modulname	Modulnummer
Globale Bedrohungen und Herausforderungen	5530

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Carlo Antonio Masala	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	36	89	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5530-V1	VL	Einführung in hybride und asymmetrische Konflikte	Pflicht	3
5530-V2	SE	Einführung in die Kriegsursachenforschung (Übungsanteil: Vorausschau durch Szenarioanalyse)	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen
erste Vorkenntnisse aus den Modulen 5524 und 5527 erforderlich.

Qualifikationsziele
Die Studierenden kennen zentralen Debatten der Kriegsursachen- und Konfliktforschung, können unterschiedliche Konfliktypen unterscheiden und erkennen aktuelle Trends. Sie verstehen, dass unterschiedliche Fragenkomplexe und Konfliktarten auf unterschiedlichen Analysebenen angesiedelt sind und verschiedene Methoden zur Erklärung herangezogen werden können. Sie können das Zusammenwirken verschiedener Faktoren bezogen auf spezifische historische Kontexte erklären. Sie können ferner interdisziplinärer Zugänge zu sicherheitspolitischen Themen aus unterschiedlichen fachspezifischen Sichtweisen und Forschungsinstrumentarien heraus abzuleiten. Zudem können Teilnehmer szanarioanalytische Herangehensweisen umsetzen, die es ermöglichen die zukünftige Entwicklung aktueller sicherheitspolitischer Herausforderungen methodengeleitet und strukturiert zu bewerten sowie Handlungsanweisungen abzuleiten.

Inhalt
Ziel des Moduls ist es, den Teilnehmern die aktuellen Bedrohungen und Risiken für die westliche Staatengemeinschaft anhand verschiedenster Herausforderungen zu vermitteln. Das Modul konzentriert sich dabei auf die Themenkomplexe des Staatenzerfalls, des internationalen Terrorismus, der Kriegsursachenforschung, der maritimen Sicherheit sowie politische, soziale und ökonomische Interdependenzen. Dabei sollen vor allem Kenntnisse im Bereich der Krisenfrüherkennung, strategischen Vorausschau, strategischen Dimension, Konfliktbewältigung sowie Konfliktverhütung vermittelt werden. Die klassischen Fragen der Politischen Philosophie nach Legitimität

und Struktur politischer Ordnungen stellen sich im Zeitalter der Globalisierung angesichts zunehmender Komplexität und Kontingenz neu. Idee und Praxis nationalstaatlicher Souveränität stoßen an ihre Grenzen und verlieren ihre Überzeugungskraft. Politik muss daher auch jenseits des Nationalstaates neu gedacht werden.

Literatur

• Abrahams, Max: Why Terrorism Does not work, in: International Security 31:2, Fall2006, p. 42-78.

• Arreguin-Toft, Ivan: How the weak win wars. A Theory of Asymmetric Conflict, in: International Security 26:1, Spring 2001, p. 93–128.

• Ballentine, K./H. Nietzsche (Ed.): Profiting from Peace. Managing the Resource Dimension of Civil War. Boulder 1996.

• Chandler, David: From Kosovo to Kabul and Beyond: Human Rights and International Intervention, Ann Arbor 2006.

• Cook, Martin (2002): „On Being a Sole Remaining Superpower: Lessons from History", Journal of Military Ethics (1/2), 77-90.

• Fearon, J.D. & Laitin, D. D.: Ethnicity, Insurgency, and Civil War. American Political Science Review 97, 2003, p. 75-90.

• Hartzell, Caroline/Hoddie Matthew: Institutionalizing Peace: Power Sharing and Post-Civil War Conflict Management, in: American Journal of Political Science47:2, April 2003, p. 318–332.

• Hoffmann, Bruce: Inside Terrorism, New York 2006, p 1-41.

• Kugler, Jacek; Organski, A.F.K. (1989): „The Power Transition: A Retrospective and Prospective Evaluation", in: Midlarsky, Manus (Hrsg.): „Handbook of War Studies", Unwin Hyman, Boston, 171–194.

• Levy, Jack S. and William R. Thompson. 2010. Causes of War. Malden, MA: Wiley-Blackwell.

• Lynn-Jones, Sean M. 1995. Offense-Defense Theory and Its Critics. Security Studies. Vol 4, No 4, pp. 660-691.

• Modelski, George; Thompson, William R. (1989): „Long Cycles and Global War", in: Midlarsky, Manus: „Handbook of War Studies", Boston, 23-54

• Rotberg, R. I (Ed.): State Failure and State Weakness in a Time of Terror, Washington, D.C., 2003.

• Sambanis, N.: Do Ethnic or Non-ethnic Civil Wars Have the Same Causes? Journal of Conflict Resolution 45, 2001, p. 259-282. Gilpin, Robert (1980): „The Theory of Hegemonic War", in: Rotberg, Robert; Rabb, Theodore: „The Origin and Preventionof Major Wars", 15-37.

• Thompson, William R. (1986): „Polarity, the Long Cycle, and Global Welfare”
Leistungsnachweis
Der Leistungsnachweis besteht aus einer Seminararbeit von 5000 Wörtern (Bearbeitungszeit vier bis acht Wochen, die konkrete Bearbeitungszeit wird zu Beginn der Lehrveranstaltung bekannt gegeben), die mit mindestens der Note 4,0 bestanden sein muss.
Verwendbarkeit
Die Inhalte des Moduls sind grundlegend für die Vertiefungsrichtungen Terrorismusbekämpfung und Regionale Sicherheit, finden aber in allen Folgemodulen als Hintergrundwissen Anwendung.
Dauer und Häufigkeit
Das Modul dauert 3 Monate (Sept.-Nov.) und beginnt jeweils im Herbsttrimester des 1. Studienjahres

Modulname	Modulnummer
Grundlagen der Extremismusforschung: Analysemethoden und Bekämpfungsstrategien	5534

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Hendrik Hansen	Pflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	36	89	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5534-V1	VSU	Einführung in die Extremismusforschung für Nachrichtendienste	Pflicht	4
5534-V2	SE	Extremismus- und Terrorismusstrafrecht I	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
erste Vorkenntnisse aus den Modulen 5524 und 5527 erforderlich.

Qualifikationsziele
Die Studierenden können die Grundlagen der vergleichenden Extremismus- und Terrorismusforschung sowie der Strategien ihrer strafrechtlichen Bekämpfung erklären. Sie eignen sich die Methoden der vergleichenden Extremismusforschung an und können den Begriff des Extremismus sowie die Methoden der Extremismusforschung kritisch reflektieren. Sie erhalten die Kompetenz, extremistische Bestrebungen zu erkennen, deren transnationale Vernetzungsstrategien zu analysieren und die Bedrohung von Sicherheitsbehörden durch extremistische Bestrebungen einzelner Mitarbeiter zu reflektieren. Darüber hinaus kennen sie die Institutionen, die für die strafrechtliche Verfolgung von Extremismus und Terrorismus zuständig sind sowie die rechtlichen Grundlagen der Bekämpfung von Extremismus und Terrorismus.

Inhalt
Die Studierenden erhalten eine inhaltliche und methodische Einführung in die Extremismusforschung, analysieren aktuelle Entwicklungen im Extremismus und Terrorismus, die für die Nachrichtendienste im internationalen Kontext neue Herausforderungen schaffen und eignen sich die Grundlagen der Extremismus- und Terrorismusbekämpfung durch das Strafrecht unter besonderer Berücksichtigung der hierbei gegebenen Schnittstellen zum Aufgabenbereich der deutschen Nachrichtendienste an. In der politikwissenschaftlich orientierten Lehrveranstaltung erhalten die Studierenden eine grundlegende Einführung in Gegenstand und Methode der vergleichenden Extremismusforschung. Darüber hinaus werden sie mit aktuellen Fragen der Extremismusforschung vertraut gemacht, die für die Angehörigen aller

Nachrichtendienste von besonderem Interesse sind: zum einen die transnationale Vernetzung von Extremisten und Terroristen, die im Islamismus ein bekanntes Phänomen ist, die aber auch im Rechts- und Linksextremismus stattfindet, zum anderen die Gefährdung von Sicherheitsbehörden durch den Extremismus einzelner Mitarbeiter. Die Studierenden lernen dabei an Fallbeispielen, Formen des Extremismus zu erfassen und zu analysieren, die die Anschlussfähigkeit an demokratische Bereiche der Gesellschaft suchen und deshalb schwerer zu erkennen sind (z.B. der intellektuelle Rechtsextremismus der „Neuen Rechten“).

In dem rechtswissenschaftlich orientierten Seminar eignen sich die Studierenden Kenntnisse über die grundsätzliche Bekämpfungsstrategie von Extremismus und Terrorismus, den strafrechtlichen Terrorismusbegriff und die völker- und unionsrechtlichen Vorgaben des deutschen Terrorismusstrafrechts an. Sie lernen die einzelnen Tatbestände des deutschen Strafrechts getrennt nach drei Gruppen zu unterscheiden (1. Basisstraftaten, 2. Straftaten im Zusammenhang mit einer terroristischen Vereinigung, 3. Straftaten im Zusammenhang mit terroristischen Aktivitäten). In verfahrensrechtlicher Hinsicht werden sie mit den Zuständigkeiten der Landes- und der Bundesjustiz, der Kooperation mit den Nachrichtendiensten sowie – insbesondere – mit der Vorgehensweise der Strafverfolgungsbehörden bei der Verwertung von ND-Erkenntnissen vertraut gemacht.

Literatur

- Böse, Die Harmonisierung des materiellen Strafrechts durch das Völker- und Europarecht ZJS 2019 1.
- Bock, Der Generalbundesanwalt beim Bundesgerichtshof, Jura 2017, 895;
- Engelstätter, Die Richtlinie zur Terrorismusbekämpfung (EU) 2017/541 – Deutsches Staatsschutzstrafrecht unter Anpassungsdruck? GSZ 2019 95.
- Engelstätter/Lohse, Die Bekämpfung staatsgefährdender rechtsextremistischer Gewalt durch den Generalbundesanwalt beim Bundesgerichtshof GSZ 2020, 156.
- Engelstätter, Prävention durch Intervention – Terrorismusbekämpfung im Vorfeld der Rechtsgutverletzung in Fischer/Hilgendorf „Gefahr“, Baden-Badener Gespräche Bd. 5, (2020) S. 181.
- Greßmann, Nachrichtendienste u. Strafverfolgung in Dietrich/Eifler (Hrsg.) Handbuch des Rechts der Nachrichtendienste (2017) § 3.
- Jesse, Eckhard/Mannewitz, Tom (Hg.): Extremismusforschung. Handbuch für Wissenschaft und Praxis, Baden-Baden 2018.
- Hansen, Hendrik/Kainz, Peter: Radical Islamism and Totalitarian Ideology. A Comparison of Sayyid Qutb’s Islamism with Marxism and National Socialism, in: Totalitarian Movements and Political Religions Band 8 (1), 2007, S. 55-76.
- Pfahl-Traughber, Armin: Linksextremismus in Deutschland, Wiesbaden 2020 (2. Aufl.).
- Pfahl-Traughber, Armin: Rechtsextremismus in Deutschland, Wiesbaden 2019.
- Pfahl-Traughber, Armin: Extremismusintensität, Ideologie, Organisation, Strategie und Wirkung. Das E-IOS-W-Schema zur Analyse extremistischer Bestrebungen, in: Jahrbuch für Extremismus- und Terrorismusforschung 2011/12, Teilband I, Brühl 2012.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer schriftlichen Prüfung (90 Minuten) oder einer Seminararbeit (5000 Wörter / Bearbeitungszeit vier bis acht Wochen,

die konkrete Bearbeitungszeit wird zu Beginn der Lehrveranstaltung bekannt gegeben), die mit mindestens der Note 4,0 bestanden sein muss. Die konkrete Form des Leistungsnachweises wird durch den Modulverantwortlichen zu Beginn der Lehrveranstaltung bekanntgegeben.
Verwendbarkeit
Die Inhalte des Moduls sind grundlegend für die Vertiefungsrichtungen Nachrichtendienste und öffentliche SIcherheit und Terrorismusbekämpfung.
Dauer und Häufigkeit
Das Modul dauert 4 Monate (Dez.-Mrz.) und beginnt jeweils gegen Ende des Herbsttrimester des 1. Studienjahres.

Modulname	Modulnummer
Intelligence Accountability	5532

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Rüdiger Bergien	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	48	77	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5532-V1	VL	Grundlagen der nachrichtendienstlichen Rechenschaftspflicht	Pflicht	3
5532-V2	SE	Ethik der Nachrichtendienste	Wahlpflicht	2
5532-V3	SE	Nachrichtendienste und Gesellschaft seit 1945	Wahlpflicht	2
5532-V4	SE	Geheimdienste und Geheimpolizeien in deutschen Diktaturen	Wahlpflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen
erste Vorkenntnisse aus den Modulen 5524 und 5527 erforderlich.

Qualifikationsziele
Die Studierenden kennen die historische Entwicklung nachrichtendienstlicher Rechenschaftspflicht nach 1945 und können diese in das Spannungsverhältnis einordnen, das in den meisten liberalen Demokratien zwischen Nachrichtendiensten und Gesellschaft bestand. Sie verstehen, dass die Zunahme von gesellschaftlichen Transparenzforderungen in einem engen Zusammenhang mit dem Bedeutungsgewinn von Freiheits- und Persönlichkeitsrechten einerseits und der Medialisierung von Politik und Gesellschaft andererseits stand. Bezogen auf Deutschland wissen die Studierenden um die besondere Rolle, die die Erfahrung der Repressionspraxis von Geheimdiensten in Diktaturen für die Perzeption nachrichtendienstlichen Handelns in der Demokratie spielte. Zudem kennen sie die besonderen ethischen Herausforderungen nachrichtendienstlicher Tätigkeit und können sie erklären. Auf dieser Grundlage sind sie in der Lage, ethische Probleme in der Praxis zu identifizieren und unterschiedliche Paradigmen der Ethik beispielhaft auf Dilemmasituationen anzuwenden.

Inhalt
Das Modul „Intelligence Accountability“ führt über geschichtswissenschaftliche und politikwissenschaftliche Zugriffe in die Geschichte der nachrichtendienstlichen Rechenschaftspflicht, der nachrichtendienstlichen Ethik sowie, übergreifend,

des Spannungsverhältnisses zwischen demokratischem Transparenzideal und nachrichtendienstlicher Praxis ein. Die Studierenden erhalten die Möglichkeit, anhand von archivalischen Quellen ihre Methodenkenntnisse zu erweitern. Sie werden zudem, anhand der Geschichte der Nachrichtendienste der deutschen Diktaturen des 20. Jahrhunderts, mit der Erfahrung geheimdienstlicher Grenzüberschreitungen vertraut gemacht, die eine wichtige Grundlage für die kritische Reflektion des eigenen nachrichtendienstlichen Handelns darstellen. Hinsichtlich der Ethik der Nachrichtendienste werden die wesentlichen Paradigmen der Ethik behandelt und auf die nachrichtendienstliche Praxis angewandt.

Literatur

• Bellaby, Ross, The Ethics of Intelligence, in: Dover, Robert et al. (Hg.), The Palgrave Handbook of Security, Risk and Intelligence, London 2017, S. 395-409.

• Dover, Robert/Goodman, Michael S. (Hg.), Spinning Intelligence, Why Intelligence needs the Media, why the Media needs Intelligence, New York 2009.

• Frisk, R./Johansson, Linda (2021) From Samurais to Borgs: Reflections on the Importance of Intelligence Ethics, International Journal of Intelligence and CounterIntelligence, Bd. 34 (1), 2021, S. 70-96.

• Galliott, Jai/Reed, Warren (Hg.): Ethics and the Future of Spying. Technology, national security and intelligence collection, London/New York 2016.

• Gieseke, Jens, Die Stasi 1945-1990, München 2011.

• Goschler, Constantin, Intelligence, Mistrust and Transparency. A Case Study of the German Office for the Protection of the Constitution. In: Stefan Berger und Dimitrij Owetschkin (Hg.): Contested Transparencies. Social Movements and the Public Sphere, Palgrave Macmillan UK 2019, S. 153–171.

• Henke, Klaus-Dietmar: Geheime Dienste. Die politische Inlandsspionage des BND in der Ära Adenauer, 2 Bde, Berlin 2018, 2022.

• Johnson, Loch K., Spy watching. Intelligence accountability in the United States, New York 2018.

• Loewenstein, Karl, Militant Democracy and Fundamental Rights, Teil I, in: The American Political Science Review, Bd. 31 (3), 1937), S. 417#432 und Teil II, in: ebenda, Bd. 31 (4), 1937, S. 638-658.

• Miller, Seumas, Rethinking the Just Intelligence Theory of National Security Intelligence Collection and Analysis: The Principles of Discrimination, Necessity, Proportionality and Reciprocity, Social Epistemology, Bd. 35 (3), 2021, S. 211-231.

• Wildt, Michael (Hg.), Nachrichtendienst, politische Elite und Mordeinheit. Der Sicherheitsdienst des Reichsführers SS, Hamburg 2003.

Leistungsnachweis
Der Leistungsnachweis besteht aus einer Seminararbeit von 5000 Wörtern (Bearbeitungszeit vier bis acht Wochen, die konkrete Bearbeitungszeit wird zu Beginn der Lehrveranstaltung bekannt gegeben), die mit mindestens der Note 4,0 bestanden sein muss.
Verwendbarkeit
Die Inhalte des Moduls sind grundlegend für die Vertiefungsrichtungen Nachrichtendienste und öffentliche Sicherheit sowie Intelligence Cooperation.
Dauer und Häufigkeit
Das Modul dauert 4 Monate (Dez.-Mrz.) und beginnt jeweils gegen Ende des Herbsttrimester des 1. Studienjahres.

Modulname	Modulnummer
Intelligence Analysis	5533

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Juniorprof. Dr. Andreas Lutsch	Pflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	48	77	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5533-V1	VL	Grundlagen der Intelligence Analysis	Pflicht	2
5533-V2	UE	Fallstudien zur Methodenanwendung	Pflicht	1
5533-V3	SE	Analysemethodische Probleme (Vertiefungen)	Wahlpflicht	1
Summe (Pflicht und Wahlpflicht)				4

Empfohlene Voraussetzungen
erste Vorkenntnisse aus dem Modul 5527 erforderlich.

Qualifikationsziele
Auf dem aktuellen Stand internationaler Forschung erschließen die Studierenden aus wissenschaftlichen Perspektiven Ziele, Grundlagen, Herausforderungen, Probleme, Konzepte und Methoden der Intelligence Analysis. Sie erlangen spezifisches und kompaktes Fachwissen, werden für Irrtums- und Fehlerquellen in der Analysearbeit sensibilisiert, erwerben Methodenkenntnisse und können methodische Zugänge im Blick auf Erfordernisse nachrichtendienstlicher Analyse kritisch reflektieren. Weitere Fachkompetenzen erlangen die Studierenden, indem sie auf der Basis des erworbenen Wissens selbstständig Transferleistungen herstellen und Methoden auf praktische Fälle anwenden. Zudem stärken die Studierenden ihre Selbstkompetenzen durch eigene Beiträge in Übungen und Seminaren, Literaturstudium sowie Fachaustausch mit Gastreferenten auf Deutsch und Englisch.

Inhalt
„Intelligence Analysis“ bezeichnet eine wichtige gesetzliche Aufgabe der Nachrichtendienste („Auswertung“) und ein Spezialfachgebiet in den Intelligence Studies und Security Studies. Die Funktion der Analyse ist es, sicherheitsrelevante Entscheidungsprozesse auch unter Zeitdruck inhaltlich bestmöglich und zeitgerecht zu informieren, indem sie im Rahmen der Lagefortschreibung Ungewissheit reduziert, zukunftsorientierte Einschätzungen präsentiert und einen spezifischen nachrichtendienstlichen Mehrwert beisteuert. Im Modul Intelligence Analysis werden wissenschaftliche Perspektiven auf Analyseinstrumente, -verfahren und -erfahrungen in Gegenwart und Vergangenheit

eröffnet, um Ziele, Grundlagen, Herausforderungen, Probleme, Konzepte und Methoden in Bezug auf Praktiken der Auslandsaufklärung, des militärischen Nachrichtenwesens und des Verfassungsschutzes zu erschließen. Das Modul besteht aus drei konsekutiven Lehrveranstaltungen.

Im Rahmen der Vorlesung werden Ansätze vorgestellt und diskutiert, wie die Rigorosität nachrichtendienstlicher Auswertung als Kognitionsprozess sui generis gesteigert werden kann. Unter anderem werden Ansätze adaptiven Denkens und Urteilens vermittelt, um Studierende für Wahrnehmungs- und Urteilsfehler zu sensibilisieren und Verbesserungspotenziale aufzuzeigen. Einen weiteren Schwerpunkt bildet die Intelligence- spezifische Beweis- und Argumentationslehre, wobei hypothesengeleitetes Vorgehen, der Umgang mit Evidenzen und Robustheitstests im Vordergrund stehen. Abschließend werden Probleme und Methoden der Vorausschau thematisiert.

In der Übung werden Fallstudien zur Methodenanwendung durchgeführt. Als Grundlage dienen VS-Meldungsmaterial und deklassifizierte Akten. Bei großen Studierendengruppen werden Parallelübungen angeboten.

Abschließend nehmen die Studierenden an einem von vier Wahlpflichtseminaren teil:

A. Analysemethodische Probleme in historischer Perspektive

B. Analysemethodische Probleme der strategischen Auslandsaufklärung

C. Analysemethodische Probleme der Defence Intelligence

D. Analysemethodische Probleme der Inlandsaufklärung.

Hinzukommen können ausgewählte Gastvorträge.

Literatur

• Robert Clark, Intelligence Analysis. A Target-Centric Approach. Seventh Edition (Thousand Oaks, CA: CQ Press, 2022).

• Jerome Clauser, An Introduction to Intelligence Research and Analysis (Lanham, MD: Scarecrow Press, 2008).

• Thomas Fingar, Reducing Uncertainty. Intelligence Analysis and National Security (Stanford, CA: Stanford University Press, 2011).

• Roger Z. George und James B. Bruce (Hg.), Analyzing Intelligence. National Security Practitioners' Perspectives. Second Edition (Washington DC: Georgetown University Press, 2014).

• Noel Hendrickson, Reasoning for Intelligence Analysts. A Multidimensional Approach of Traits, Techniques, and Targets (Lanham et al: Rowman & Littlefield, 2018).

• Richards J. Heuer, Psychology of Intelligence Analysis (Washington DC: CIA Center for the Study of Intelligence, 1999).

• Robert Jervis, Why Intelligence Fails. Lessons from the Iranian Revolution and the Iraq War (Ithaca, NY: Cornell University Press 2010).

• Sherman Kent, Strategic Intelligence for American World Policy (Princeton, NJ: 1949).

• David Omand, How Spies Think. 10 Lessons in Intelligence (London: Viking, 2020).

• Randolph H. Pherson und Richards J. Heuer, Structured Analytic Techniques for Intelligence Analysis. Third Edition (Thousand Oaks, CA: CQ Press, 2021).

Leistungsnachweis
Der Leistungsnachweis besteht aus einer schriftlichen Prüfung (120-180 Minuten), die mit mindestens der Note 4,0 bestanden sein muss. Der konkrete Umfang der Prüfung wird durch den Modulverantwortlichen zu Beginn der Lehrveranstaltung bekanntgegeben.
Verwendbarkeit
Die Inhalte des Moduls sind grundlegend für den gesamten Studiengang und finden in allen nichttechnischen Folgemodulen Verwendung.
Dauer und Häufigkeit
Das Modul dauert 4 Monate (Dez.-Mrz.) und beginnt jeweils gegen Ende des Herbsttrimester des 1. Studienjahres.

Modulname	Modulnummer
Intelligence and Cyber Security	3479

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Juniorprof. Dr. rer. nat. Maximilian Moll Univ.-Prof. Dr. Stefan Pickl	Pflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
175	84	91	7

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3479-V1	VL	Intelligence	Pflicht	4
3479-V2	VL	Methoden der Cyber Security	Pflicht	2
3479-V3	UE	Methoden der Cyber Security	Pflicht	1
Summe (Pflicht und Wahlpflicht)				7

Empfohlene Voraussetzungen

Die Studierenden benötigen Grundkenntnisse der Informatik, wie sie in einem technischen Bachelor-Studium oder im Modul 5526 vermittelt werden.

Qualifikationsziele

Das Modul vermittelt grundlegende Kompetenzen in den Bereichen Intelligence und Cyber Security. Die Lehrveranstaltung „Intelligence“ vermittelt theoretische, praktische und anwendungsbezogenen Kompetenzen, um IT-basierte Entscheidungsunterstützung im Intelligence Bereich eigenständig durchführen zu können. Die Studierenden können eigenständig Modelle entwickeln, vorhandene Modelle bewerten, Analysen durchführen und Optimierungspotentiale erkennen sowie Optimierungsvorhaben im Sinne des Operations Research und Management Science entwickeln.

In der Lehrveranstaltung "Methoden der Cyber Security" verstehen die Studierenden verstehen den Angriffszyklus sowie ausgewählte Cyberangriffe. Basierend darauf lernen die Studierenden Verfahren und Methoden kennen, die zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen eingesetzt werden, und können Anwendungsbereiche, Leistungsfähigkeiten und Grenzen dieser Verfahren beurteilen. Sie verstehen die grundlegenden Konzepte und Verfahren der angewandten Kryptografie und erlangen die Befähigung, diese sowie ausgewählte Sicherheitswerkzeuge exemplarisch einzusetzen und anzuwenden. Sie sind in der Lage, Methoden und Mechanismen, wie Anonymisierung und Verschleierung der Kommunikation, die eine nachrichtendienstliche Aufklärung erschweren oder unterbinden können, zu verstehen und deren Möglichkeiten und Grenzen einzuschätzen.

Inhalt
Frühe Anfänge von „Intelligence Security“ gehen bereits auf Sun Tzu und Clausewitz zurück. Einen Höhepunkt erreicht dieses Gebiet zurzeit und kurz nach dem zweiten Weltkrieg, als Forschungen der RAND Corporation und insbesondere zentrale spieltheoretische Arbeiten hohe Aufmerksamkeit auf sich zogen. Die Lehrveranstaltung „Intelligence“ vermittelt ein Grundverständnis für die Denkweise dieses zentralen Sicherheits-Gebietes. Es wird ein inhaltlicher Bogen bis hin zu heutigen analytischen Zugängen wie Mining, Big Data Ansätzen und forensischen Verfahren entwickelt. Da hierbei den technischen Grundbedingungen und Verfahren eine besondere Bedeutung zukommt wird ein enger inhaltlicher Bezug zu der begleitenden Lehrveranstaltung „Methoden der Cyber Security“ in diesem Modul bestehen und immer wieder hergestellt werden. Ferner wird ein Überblick über aktuelle Methoden und Verfahren im Bereich des Operations Research/ Management Science, die als sogenannte analytische Tools innerhalb von „Intelligence Security“ zur Verfügung stehen, gegeben. Hierbei wird auf Themen wie Crisis Management, Foresight Analysis sowie Counter Intelligence explizit eingegangen werden. Es ist geplant, ein bis zwei Exkursionen bzw. aktive Planspielphasen zu integrieren. Die Lehrveranstaltung „Intelligence“ gibt zunächst einen historischen Überblick über die spezielle Modellentwicklung im Intelligence Bereich von Anfang der 40er Jahre über die Etablierung von Operations Research/ Management Science bis zu heutigen Anwendungen im Bereich der datengetriebene Analyse und datenbasierten Optimierung („Analytics“/ „Business Intelligence“). Inhaltliche Schwerpunkte sind: • Modellentwicklung im Bereich sicherheitsrelevanter Anwendungen • Entwicklung eines spieltheoretischen Verständnisses und Überblick über spieltheoretische Verfahren • Einführung in Optimierungsverfahren im Rahmen der IT-basierten Entscheidungsunterstützung • Eigenständige Szenarienentwicklung und Bewertung • Analyse von Kritischen Infrastrukturen und Cyber Intelligence • Entwicklung von geeigneten Frühwarnsysteme • Ausblick: Rolle der KI und Big Data im Intelligence Bereich In der Lehrveranstaltung "Methoden der Cyber Security" wird, basierend auf einem Überblick über Bedrohungen und Cyberangriffen, der Schutz von ruhenden und bewegten Daten sowie die Sicherheit der technischen Systeme, welche die Übertragung, Verarbeitung und Speicherung dieser Daten und Informationen ermöglichen und unterstützen, aus zwei Blickwinkeln betrachtet: Zum einen lernen

die Studierenden Techniken und Werkzeuge kennen, um die gängigen Schutzziele von Daten, Sendern und Empfängern sowie der beteiligten technischen Systeme sicherzustellen. Dazu gehören Verschlüsselungsverfahren, kryptografische Protokolle, Authentifizierungsverfahren und Mechanismen der Zugriffskontrolle.
Zum anderen werden die mannigfaltigen technischen Möglichkeiten, den Austausch von Informationen per se zu verbergen sowie Ursprung und Empfänger bzw. den Weg der Daten zu verschleiern und zu tarnen, betrachtet. Die vorgestellten und diskutierten Verfahren umfassen u.a. steganografische Techniken, Anonymisierungs- und Pseudonymisierungsverfahren sowie Onion Routing.

Inhaltliche Schwerpunkte der Wissensvermittlung sind:

• Grundlagen der IT-Sicherheit: Grundbegriffe, wie Sicherheitsanforderungen und Schutzziele.

• Bedrohungen von IT-Systemen und Netzen: Angriffszyklus, verschiedene passive und aktive Angriffe, wie Malware und Social Engineering, zudem Bedrohungsanalyse.

• Grundlegende Sicherheitsmaßnahmen und -mechanismen: Risikoanalyse und Sicherheitsmaßnahmen zur Erreichung der Schutzziele

• Kryptografische Konzepte und Verfahren: Symmetrische vs. asymmetrische Verschlüsselung, kryptografische Primitive und Protokolle, digitale Signaturen und Zertifikate.

• Grundlagen der Netzwerksicherheit: Sicherheitsprotokolle, Firewalls und Intrusion Detection.

Methoden der Counter Intelligence: Anonymisierung, Onion Routing und Steganografie.

Literatur

- Baruch Fischhoff; Cherie Chauvin (Editors): Intelligence Analysis - Behavioral and Sozial Scientific Foundations, 2011, ISBN 978-0-309-17689-9
- Claudia Eckert: IT-Sicherheit - Konzepte - Verfahren - Protokolle, ISBN 978-3-11-055158-7
- Christof Paar, Jan Pelzl: Understanding Cryptography, 2010, ISBN 978-3-642-041006

Leistungsnachweis

Der Leistungsnachweis besteht aus einer schriftlichen Prüfung mit 150 Minuten Dauer, die mit mindestens der Note 4,0 bestanden sein muss.

Verwendbarkeit

Die Inhalte des Moduls legen die Grundlage für Vertiefungsrichtung Cyber Defence. Für alle anderen Vertiefungsrichtungen schaffen sie ein grundsätzliches technisches Problemverständnis, das als Hintergrundwissen auch in den nichttechnischen Vertiefungen zentral ist.

Dauer und Häufigkeit
Das Modul dauert 3 Monate (Sept.-Nov.) und beginnt jeweils im Herbsttrimester des 1. Studienjahres

Modulname	Modulnummer
Intelligence Collection	5529

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Juniorprof. Dr. Stephan Lau	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	59	66	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5529-V1	VS	Intelligence Collection - Ringvorlesung	Pflicht	1
5529-V2	SE	HUMINT in den Grenzen des Rechtsstaats	Pflicht	1
5529-V3	VS	Psychologie der HUMINT-Collection	Pflicht	3
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

erste Vorkenntnisse aus den Modulen 5525 und 5527 erforderlich.

Qualifikationsziele

Die Studierenden verfügen über ein breites Verständnis der Methoden nachrichtendienstlicher Informationsgewinnung, deren Abhängigkeiten und Wechselwirkungen im 21. Jahrhundert. Auf der Grundlage wissenschaftlicher Erkenntnissen können die Studierenden vor allem Vorgänge der Informationsgewinnung mit menschlichen Quellen (HUMINT) hinterfragen, vergleichen und bewerten. So sind sie in der Lage, psychologische Determinanten des Erfolgs bzw. Misserfolgs von HUMINT-Operationen zu identifizieren. Ihnen gelingt dadurch der „Shift from Tradecraft to Science“, der sich später förderlich in ihrer Verwendung in der Praxis auswirken wird. Die Studierenden kennen zudem die verfassungsrechtlichen Problematiken der nachrichtendienstlichen Informationsgewinnung, insbesondere im Bereich HUMINT, und verfügen über vertiefte Kenntnisse ihrer einfachrechtlichen Grundlagen.

Inhalt

Informationsgewinnung beschreibt eine zentrale Aufgabe von Nachrichtendiensten. Die Methoden der Informationsgewinnung sind zahlreich und vielfältig. Ihre Beherrschung zählt zum nachrichtendienstlichen Handwerk. Gegenstand dieses Moduls ist es jedoch nicht, die Studierenden in Beschaffungsmethodik zu trainieren. Vielmehr wird eine (fach-) wissenschaftliche Perspektive auf verschiedene Beschaffungsmethoden (wie z.B. HUMINT) eingenommen. Sie werden kontextualisiert und hinterfragt; Probleme und Potentiale werden offengelegt. Im Fokus der wissenschaftlichen Analyse steht dabei die aktuelle nachrichtendienstliche Praxis. Die rechtlichen Rahmenbedingungen dieser Tätigkeit unterliegen einem dynamischen Wandel und sind zum Teil ungeklärt. Die

Studierenden werden mit der rechtsstaatlichen Einhegung der nachrichtendienstlichen Informationsgewinnung vertraut gemacht.

Literatur

Intelligence Studies und Praxis

• Robert M. Clark, Intelligence Collection, 2014.

• Mark M. Lowenthal/ Robert M. Clark, The Five Disciplines of Intelligence Collection, 2015.

Rechtliche Aspekte der HUMINT Collection

• Dietrich, in: Dietrich/Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, S. 1017-1091.

• Löffelmann/Zöller, Nachrichtendienstrecht, 2022, S. 106-125, 169-173

Psychologie der HUMINT Collection

• Loftus, E. F. (2011). Intelligence gathering post-9/11. American Psychologist, 66(6), 532–541.

• Evans, J. R., Meissner, C. A., Brandon, S. E., Russano, M. B., & Kleinman, S. M. (2010). Criminal versus HUMINT interrogations: The importance of psychological science to improving interrogative practice. The Journal of Psychiatry & Law, 38(1-2), 215-249.

Diese Werke sind für Sie als erster Einblick und/oder Überblick in die Facetten des Themas Intelligence Collection gedacht. Mehr und spezifischere Literatur wird im Rahmen der einzelnen Veranstaltungen gegeben (vgl. Veranstaltungssyllabi).

Leistungsnachweis

Der Leistungsnachweis besteht aus einer zweiteiligen schriftlichen Prüfung (120 Minuten) zu den Inhalten der Lehrveranstaltungen 5529-V2 und 5529-V3. Beide Teile der Prüfung müssen jeweils mit mindestens der Note 4,0 bestanden werden und fließen zu 30 Prozent (5529-V2) bzw. 70 Prozent (5529-V3) in die Gesamtnote ein.

Durch das separate Bestehenserfordernis für beide Prüfungsteile wird dem Umstand Rechnung getragen, dass sowohl ausreichende Psychologie- als auch Rechtskompetenzen zu den unverzichtbaren Merkmalen des Anforderungsprofils zählen. Die Gewichtung der Teilnoten bei der Bildung der Gesamtnote spiegelt den Anteil der jeweiligen Fächer an den Präsenzveranstaltungen.

Verwendbarkeit

Die Inhalte des Moduls sind grundlegend für den gesamten Studiengang, besonders die Module 5531, 5532, 5533 sowie die Vertiefungsrichtung Terrorismusbekämpfung.

Dauer und Häufigkeit

Das Modul dauert 3 Monate (Sept.-Nov.) und beginnt jeweils im Herbsttrimester des 1. Studienjahres

Modulname	Modulnummer
Intelligence Governance	5528

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Susanne Fischer	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	46	79	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5528-V1	VS	Einführung in Intelligence Governance	Pflicht	2
5528-V2	SE	Seminar zur Einführungsvorlesung – Dimensionen von Intelligence Oversight	Wahlpflicht	1
5528-V3	SE	Seminar zur Einführungsvorlesung – Dimensionen von Intelligence Oversight	Wahlpflicht	1
5528-V4	SE	Seminar zur Einführungsvorlesung – Defense Intelligence Architekturen	Wahlpflicht	1
5528-V5	SE	Seminar zur Einführungsvorlesung – National Intelligence Architekturen	Wahlpflicht	1
5528-V6	SE	Intelligence Governance in Practice	Pflicht	1
5528-V7	SE	Intelligence Governance in Practice	Pflicht	1
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen
erste Vorkenntnisse aus den Modulen 5524 und 5527 erforderlich.

Qualifikationsziele
Fachkompetenz: Theoretisches und empirisches Fachwissen zu den skizzierten Themenbereichen von Intelligence Governance. Methodenkompetenz: Durch die theoriegeleitete Analyse empirischer Beispiele vertiefen die Studierenden die Fähigkeit zum analytischen Denken und methodischen/ systematischen Vorgehen, d.h. es werden die grundlegenden Fertigkeiten wissenschaftlichen Arbeitens sowie Fertigkeiten der empirischen Sozialforschung vertieft. Zudem wird der Umgang mit bzw. die Interpretation von Rechtsquellen vertieft. Selbstkompetenz: Studierende vertiefen ihre Fähigkeiten der Selbstmotivation und Selbstorganisation [Priorisieren, Zeitmanagement, Disziplin und Konzentration beim Selbststudium] sowie die Fähigkeit zur Arbeit in und mit Gruppen und die damit verbundenen Fähigkeiten der Organisation von Teamarbeit [gemeinsame Definition von Arbeitszielen, Aufgabenverteilung, Führen im Team etc.].

Inhalt
Intelligence Governance ist ein junges Forschungsfeld im Rahmen der ebenfalls noch recht jungen Intelligence Studies. Intelligence Governance führt politikwissenschaftliche, rechtswissenschaftliche und soziologische Perspektiven zusammen – inhaltlich deckt Intelligence Governance in diesem Modul zwei Themenfelder ab, die im Folgenden idealtypisch getrennt dargestellt werden: **Intelligence Oversight** Die Forschung in diesem Feld befasst sich mit den zentralen Akteuren, Strukturen und Prozessen der Kontrolle nachrichtendienstlicher Tätigkeit. Dabei wird zwischen Kontrolle von außen sowie behördeninterner Kontrolle unterschieden. Das Modul befasst sich empirisch insbesondere mit parlamentarischer Kontrolle, Fachaufsicht und der Rolle der Medien („external intelligence governance“). Ausgangspunkt ist die Intelligence Community in Deutschland. Da Governance vor allem „Governance durch Regelungsstrukturen [ist]“ (Schuppert 2011, S. 168), kommt zudem dem Recht, als regelungstheoretische Perspektive verstanden, eine zentrale Bedeutung zu. Daher widmet sich das Modul insbesondere auch den Rechtsgrundlagen nachrichtendienstlicher Arbeit, d.h. die Studierenden vertiefe n ihre Kenntnis des deutschen Rechts der Nachrichtendienste und setzen sich in diesem Zusammenhang z.B. mit der höchstrichterlichen Rechtsprechung und den Auswirkungen dieser Rechtsprechung auf die nachrichtendienstliche Tätigkeit auseinander. **Intelligence Architekturen** Eine zentrale Erkenntnis der Intelligence Governance-Forschung besteht in der Einsicht: „[I]ntelligence is not produced in a vacuum “(Walsh 2008). Forschung im Bereich Intelligence Architekturen beschreibt und analysiert Akteure bzw. Akteurskonstellationen (verschiedener) nationaler Intelligence Communities und reflektiert ihre Ausprägung im Lichte der Einbettung in den jeweils spezifischen historisch gewachsenen gesellschaftlichen, institutionellen und regulativen Kontext. Der Blick auf die Intelligence Architekturen wird hierbei durch verschiedene analytische Perspektiven (z.B. Intelligence Culture, Bureaucratic Politics, Koordination und Recht) vor genommen. Ausgangspunkt ist die Intelligence Community in Deutschland (u.a. Verfassungsschutzverbund, MilNW etc.) – partiell werden Vergleiche zu Intelligence Communities anderer Länder, z.B. Canada, USA etc. gezogen. **Wie verhalten sich die einzelnen Unterrichtseinheiten im Modul zueinander?** Die **Einführungsvorlesung** führt in die grundlegenden Fragestellungen und Diskussionspunkte des Forschungsfeldes Intelligence Governance ein. Ziel der Vorlesung ist es, einen Überblick über Intelligence Governance zu vermitteln. Die zwei thematischen Schwerpunkte von Intelligence Governance werden jeweils in Kombination aus eher konzeptionellen und empirischen Unterrichtseinheiten behandelt. Über diese enge

Verknüpfung soll ein Verständnis für theoriegeleitetes systematisches Vorgehen bei der Analyse empirischer Sachverhalte entwickelt werden.

Die Einführungsvorlesung ist mit verschiedenen **thematischen Wahlpflichtübungen** verbunden. Die Übungen sind jeweils einem der Themenfelder von Intelligence Governance zugeordnet und vertiefen dementsprechend ausgewählte Teilaspekte aus diesem Feld. Ziel der Übungen ist neben der Vertiefung von Fachwissen vor allem auch das Einüben spezifischer Fertigkeiten in einem ausgewählten Feld (z.B. Übertragen theoretischer Überlegung auf neues empirisches Feld).

Das Seminar **„Intelligence Governance in Practice“** ermöglicht den Austausch mit herausragenden Vertretern aus dem direkten (Um)Feld nachrichtendienstlicher Tätigkeit. Das Seminar gibt Einblicke in die „praktischen“ Herausforderungen von „Intelligence Governance“ und zielt damit auf die Vermittlung von praxisrelevantem Wissen. In diesem Sinne rundet das Seminar den Prozess der Wissensvermittlung ab.

Das **Methodenseminar** vertieft Fertigkeiten wissenschaftlichen Arbeitens (Forschungsfrage, Forschungsdesign, Fallauswahl) an konkreten „Forschungspuzzeln" im Bereich „Intelligence Governance“. Auf diese Weise verknüpft es Fach- und Methodenwissen, um die Fertigkeiten wissenschaftlichen Arbeitens mit Blick auf die Teilleistung „Seminararbeit“ und die Masterarbeit zu vertiefen.

In den Übungen können unbenotete Leistungen wie Referat, Thesenpapier, Poster oder Protokoll eingefordert werden. Hierdurch trainieren die Studierenden die Kompetenzen, die das Modul als Qualifikationsziel ausweist. Das Feedback zu diesen Leistungen ermöglicht den Studierenden zudem Fehlorientierung frühzeitig zu korrigieren. Alle eventuell begleitend zu erbringenden Leistungen führen damit unmittelbar zum Gesamtqualifikationsziel des Moduls.

Literatur

Intelligence Oversight (Auswahl)

Dietrich, Jan-Hendrik (2014): Die Reform der parlamentarischen Kontrolle der Nachrichtendienste als rechtsstaatliches Gebot und sicherheitspolitische Notwendigkeit. In: Zeitschrift für Rechtspolitik (ZRP) 47 (7), S. 205-208.

Eiffler, Sven-R. (2017): Exekutivkontrolle (Ministerielle Fachaufsicht und Koordinierung). In: Jan-Hendrik Dietrich und Sven-R. Eiffler (Hg): Handbuch des Rechts der Nachrichtendienste. Stuttgart: Boorberg, S. 1499-1532.

Friedel, Andreas (2018): Blackbox Parlamentarische Kontrollgremium des Bundestages. Defizite und Optimierungsstrategien bei der Kontrolle der Nachrichtendienste. Wiesbaden: Springer VS.

Gusy, Christoph (2014): Kontrolle der Nachrichtendienste. In: Verwaltungsarchiv 106, S. 437-458.

Hillebrand, Claudia (2012): The Role of News Media in Intelligence Oversight. In: Intelligence and National Security 27 (5), S. 689-706.

McCubbins, Mathew/Schwartz, Thomas (1984): Congressional Oversight Overlooked: Police Patrol versus Fire Alarm. In: American Journal of Political Science 28 (1), S. 165-179.

Intelligence Architekturen (Auswahl)

Davies, Philip (2009): Ideas of Intelligence: Divergent National Concepts and Institutions. In: Andrew, Christopher/Aldrich, Richard J./Wark, Wesley, K. (Hg): Secret Intelligence. A Reader. Abingdon: Routledge, S. 12-17.

Dietrich, Jan-Hendrik (2021): Verfassungsschutz in der föderalen Ordnung. In: Engelhart,

M. et al. (Hrsg.): Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber, Duncker&Hubmblot: Berlin, S.883-902.

Gusy, Christoph (2017): Organisation und Aufbau der deutschen Nachrichtendienste. In: Jan-Hendrik Dietrich und Sven-R. Eiffler (Hg.): Handbuch des Rechts der Nachrichtendienste. Stuttgart: Boorberg, S. 297–347.

Halperin, Morton H. (1974): Bureaucratic Politics and Foreign Policy. Washington: Brookings Institution.

Hensler, Alistair (2020): Creating a Canadian foreign intelligence service: revisited 25 years later. In: Canadian Foreign Policy Journal 26 (3), S. 360–365.

Jann, Werner/Wegrich, Kai (2010): Governance und Verwaltungspolitik: Leitbilder und Reformkonzepte. In: Benz, Arthur/Dose, Nicolai (Hg.): Governance-Regieren in komplexen Regelsystemen. Eine Einführung. 2., aktualisierte und veränderte Auflage. Wiesbaden: VS Verlag, S. 175–200.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit (3500-4500 Wörter / Bearbeitungszeit vier bis acht Wochen, die konkrete Bearbeitungszeit wird zu Beginn der Lehrveranstaltung bekannt gegeben), die mit mindestens der Note 4,0 bestanden sein muss.

Verwendbarkeit

Die Inhalte dieses Moduls sind grundlegend für die Module 5531, 5532, 5534 und die Vertiefungsrichtungen Nachrichtendienste und öffentliche Sicherheit sowie Intelligence Cooperation.

Dauer und Häufigkeit

Das Modul dauert 3 Monate (Sept.-Nov.) und beginnt jeweils im Herbsttrimester des 1. Studienjahres

Modulname	Modulnummer
Kommunikation und Führung in den Nachrichtendiensten	5531

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Michaela Pfundmair	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
75	36	39	3

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5531-V1	VL	Grundlagen in Kommunikation und Führung	Pflicht	2
5531-V2	SE	Führung in Nachrichtendiensten	Pflicht	2
5531-V3	UE	Kommunikation und Präsentation	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Keine besonderen Vorkenntnisse erforderlich.

Qualifikationsziele

Die Studierenden gewinnen ein vertieftes Verständnis über die wesentlichen psychologischen Konzepte, Theorieansätze und empirischen Befunde zu Kommunikations- und Führungsprozessen. Um den nachrichtendienstlichen Produktionsprozess strategisch und effektiv zu gestalten, sind die Studierenden in der Lage, situationsabhängig empirisch fundierte Instrumente zur Personalführung und - entwicklung einzusetzen und diese von empirisch haltlosen Instrumenten zu unterscheiden. Eigene Kommunikationsfähigkeiten können reflektiert und optimiert werden, um nachrichtendienstliche Produkte zu vertreten

Inhalt

In der Vorlesung werden psychologische Prozesse im Rahmen von Kommunikation und Führung grundlegend behandelt. Dabei stehen einerseits Themen wie Kommunikation, Gruppenprozesse, Konflikt und Konfliktlösung und andererseits Themen wie Personalführung, Mitarbeitermotivation und Personalentwicklung im Zentrum. Im Seminar findet eine Vertiefung ausgewählter personalpsychologischer Themen unter dem Gesichtspunkt der praktischen Anwendung im nachrichtendienstlichen Kontext statt.
In der Übung werden kommunikative Kompetenzen (u.a. Impression Management, Präsentationstechniken) geschult.

Literatur

• Aubé, C., Brunelle, E., & Rousseau, V. (2014). Flow experience and team performance: The role of team goal commitment and information exchange. Motivation and Emotion, 38(1), 120–130.

• Derue, D. S., Nahrgang, J. D., Wellman, N., & Humphrey, S. E. (2011). Trait and behavioral theories of leadership: An integration and meta#analytic test of their relative validity. Personnel Psychology, 64(1), 7–52.

• Feijó, F. R., Gräf, D. D., Pearce, N., & Fassa, A. G. (2019). Risk factors for workplace bullying: A systematic review. International Journal of Environmental Research and Public Health, 16(11), 1945.

• Kanning, U. P. (2021). Crashkurs Personalpsychologie. Haufe.

• Straus, S. G., Parker, A. M., & Bruce, J. B. (2011). The group matters: A review of processes and outcomes in intelligence analysis. Group Dynamics: Theory, Research, and Practice, 15(2), 128–146.

• Taylor, P. J., Russ-Eft, D. F., & Chan, D. W. L. (2005). A meta-analytic review of behavior modeling training. Journal of Applied Psychology, 90(4), 692–709.

Leistungsnachweis
Der Leistungsnachweis besteht aus einer schriftlichen Prüfung von 90 Minuten, die mit mindestens der Note 4,0 bestanden sein muss.
Verwendbarkeit
Die Inhalte des Moduls finden in allen Folgemodulen als Hintergrundwissen Anwendung bei besonderer Relevanz für die Module 5541 und 5546.
Dauer und Häufigkeit
Das Modul dauert 4 Monate (Dez.-Mrz.) und beginnt jeweils gegen Ende des Herbsttrimester des 1. Studienjahres.

Modulname	Modulnummer
Masterarbeit	3488

Konto	Masterarbeit - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Jan-Hendrik Dietrich	Pflicht	5

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
625	0	625	25

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3488-V1	PRO	Master-Arbeit	Pflicht	
Summe (Pflicht und Wahlpflicht)				

Empfohlene Voraussetzungen
Vorausgesetzt werden die allgemeinen Kenntnisse aus dem Master-Studium.

Qualifikationsziele
Die Studierenden können eine anspruchsvolle Aufgabe selbständig analysieren und mit wissenschaftlichen Methoden bearbeiten. Sie haben Erfahrung in der Entwicklung von Lösungsstrategien und in der Dokumentation ihres Vorgehens. Sie haben in einem speziellen Forschungsgebiet der Intelligence and Security Studies vertiefende Erfahrung gesammelt.

Inhalt
In der Master-Arbeit soll eine Aufgabe aus einem begrenzten Problemkreis unter Anleitung selbständig mit bekannten Methoden wissenschaftlich bearbeitet werden. In der Arbeit sind die erzielten Ergebnisse systematisch zu entwickeln und zu erläutern. Sie wird in der Regel individuell und eigenständig durch die Studierenden bearbeitet, kann aber je nach Thema auch in Gruppen von bis zu drei Studierenden bearbeitet werden.

Leistungsnachweis
Es ist eine schriftliche Ausarbeitung im Umfang von ca. 80 Seiten zu erstellen.

Verwendbarkeit
Das Modul schließt den Studiengang ab und ist daher nicht für Folgemodule verwendbar.

Dauer und Häufigkeit
Das Modul dauert sechs Monate (Jul-Dez) und beginnt im Frühjahrstrimester des 2.Studienjahres.

Modulname	Modulnummer
Menschenrechte und Sicherheit in normativer Perspektive	5525

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Jan-Hendrik Dietrich Prof. Dr. Carlo Antonio Masala	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
250	90	160	10

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5525-V1	VS	Der moderne Staat: Zwischen Freiheitsnorm und einer Ethik der Sicherheit	Pflicht	1
5525-V2	VÜ	Grundrechte, Menschenrechte und modernes Sicherheitsrecht	Pflicht	2
5525-V3	VÜ	Einführung in das Recht der Nachrichtendienste	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Es werden keine besonderen Vorkenntnisse vorausgesetzt.

Qualifikationsziele
Die Studierenden sind mit der normativen Begründung und Bindung des modernen Rechtsstaates vertraut. Sie beherrschen die ethischen Instrumentarien zur Bestimmung freiheitsgebundenen Sicherheitshandelns und können sie auf konkrete Fälle und Szenarien anwenden. Die Studierenden kennen das im Grundgesetz der Bundesrepublik Deutschland konkretisierte Verhältnis von Staat und Bürger, haben eine rechtsvergleichende Perspektive auf entsprechende Ordnungen anderer Staaten, ergänzt durch ein grundlegendes Verständnis für die Entwicklung verlässlicher Mechanismen eines internationalen Menschenrechtsschutzes. Sie wissen um aktuelle konzeptionelle Entwicklungen des bundesdeutschen und internationalen Sicherheitsrechts angesichts neuerer Bedrohungen und können diese normativ einordnen. Die Studierenden kennen die rechtlichen Bedingungen staatlicher Sicherheitsgewährleistung sowie das Zusammenspiel der Nachrichtendienste mit anderen verantwortlichen Akteuren. Sie sind in der Lage, verfassungsrechtliche Grenzen für die nachrichtendienstliche Tätigkeit abzuleiten und auf der Ebene einfacher Gesetze zur Geltung zu bringen. Mit der Dogmatik des Rechts der Nachrichtendienste sind die Studierenden so vertraut, dass unbekannte Rechtsprobleme gelöst werden können.

Inhalt
Der moderne demokratische Rechtsstaat versteht sich als sichernde Formgebung für die Praxis bürgerlicher Freiheit. Daraus ergibt sich einerseits die Forderung nach einem starken, Sicherheit garantierenden Staat, andererseits müssen alle Sicherheitsmaßnahmen immer freiheitsbegründet und freiheitsdienlich sein. Die so formulierte Grundorientierung staatlichen Handelns ist Gegenstand des Moduls „Menschenrechte und Sicherheit aus normativer Perspektive“. Die Lehrveranstaltung behandelt anhand zentraler ideengeschichtlicher Positionen die Auseinandersetzung mit möglichen Konflikten von Wertorientierung, Freiheit und Sicherheit in der Ethik. Ausgehend von konkreten Fragen wie Dilemmata zwischen Rechtsstaatlichkeit und Sicherheit oder der Frage nach der Bewertung der Lüge sollen paradigmatische Positionen der Ethik kontrastiert werden, um erstens die Grundzüge solcher Paradigmen zu vermitteln und zweitens den Umgang mit der Pluralität von Paradigmen in der Ethik zu diskutieren. Die Veranstaltung „Grundrechte, Menschenrechte und modernes Sicherheitsrecht“ sensibilisiert für Notwendigkeit, Besonderheit und Grenzen des modernen Rechts. Sie führt ein in die deutsche Grundrechtsordnung sowie – in rechtsvergleichender Absicht – in entsprechende Rechtsordnungen ausgewählter anderer Staaten. Hinzu tritt ein Überblick über das gewachsene und werdende System des globalen Menschenrechtsschutzes und die damit sich anbahnende Internationalisierung der normativen Ansprüche moderner Rechtsstaatlichkeit. Davon ausgehend werden neuere sicherheitsrechtliche Konzepte behandelt, in denen sich die Entwicklung des Staates zum „Präventionsstaat“ abzeichnet. Dieser Trend und die mit ihm einhergehenden Strukturen, Abgrenzungen und Handlungen von Sicherheitsbehörden werden im Blick sowohl auf bürgerliche Grundrechte als auch auf internationalen Menschenrechtsschutz, zu dem sich Deutschland verpflichtet hat, überdacht und beurteilt. Der Übungsanteil der Veranstaltung bietet die Gelegenheit, konkrete Fallbeispiele zu bearbeiten. Den deutschen Nachrichtendiensten ist gesetzlich ein wichtiger Teil staatlicher Sicherheitsgewährleistung überantwortet: Politischen Entscheidungsträgern dienen sie als Frühwarnsysteme für innere und äußere Gefährdungen, und im Wirkungsverbund mit Polizeibehörden und Staatsanwaltschaften tragen sie zur Verhinderung und Aufklärung von Straftaten bei. Bürgerinnen und Bürger erwarten von ihnen nicht zuletzt angesichts des internationalen Terrorismus ein hohes Maß an Sicherheitsfunktionalität. Bei der Erfüllung ihrer Aufgaben sind die Nachrichtendienste allerdings verpflichtet, individuelle Freiheitsverbürgungen des Grundgesetzes streng zu achten. An dieser Stelle setzt die Veranstaltung "Einführung in das Recht der Nachrichtendienste" an. Sie nimmt die Rechtsgrundlagen nachrichtendienstlicher Tätigkeit in den Blick und hinterfragt – insbesondere unter Berücksichtigung verfassungsgerichtlicher Judikatur – die gesetzlich niedergelegten Konfliktschlichtungsformeln, die den Schutz grundrechtlicher Freiheiten und die Gewährleistung öffentlicher Sicherheit in Einklang bringen sollen. Im Übungsanteil der Veranstaltung werden einschlägige Rechtsprobleme diskutiert und gelöst.
Literatur
1. „Der moderne Staat: Zwischen Freiheitsnorm und einer Ethik der Sicherheit“

• Ammicht Quinn, Regina (Hg.): Sicherheitsethik (= Studien zur Inneren Sicherheit, Bd. 16) Wiesbaden 2014.

• Grunwald, Armin/Hillerbrand, Rafaela (Hg.): Handbuch Technikethik, 2. akt. u. erw. Auflage, Berlin 2021.

2. „Grundrechte, Menschenrechte und modernes Sicherheitsrecht“

• Albrecht, Peter-A.: Der Weg in die Sicherheitsgesellschaft. Auf der Suche nach staatskritischen Absolutheitsregeln, Berlin 2010.

• Merten, Detlef/Papier, Hans-J. (Hg.): Handbuch der Grundrechte in Deutschland und Europa. 12 (Teil-)Bände, Heidelberg 2004 ff.

• Papier, Hans-J./Münch, Ursula/Kellermann, Gero (Hg.): Freiheit und Sicherheit. Verfassungspolitik, Grundrechtsschutz, Sicherheitsgesetze (= Tutzinger Studien zur Politik, Bd. 8), Baden-Baden 2016.

3. „Einführung in das Recht der Nachrichtendienste“

• Dietrich, Jan-H./Eiffler, Sven-R. (Hrsg.), Handbuch des Rechts der Nachrichtendienste, Stuttgart 2017.

• Dietrich, Jan-H./Sule, Satish (eds.), Intelligence Law and Policies in Europe, München/ Oxford 2019.

• Dietrich, Jan-H./Gärditz, Klaus et al. (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, Tübingen 2019.

Leistungsnachweis
Der Leistungsnachweis besteht aus einer schriftlichen Prüfung mit einer Dauer von 180 Minuten, die sich auf die drei Themenfelder des Moduls bezieht. Die schriftliche Prüfung muss mit der Note 4,0 bestanden werden.
Verwendbarkeit
Die Inhalte des Moduls legen die Grundlagen für die Module 5529 und 5532, sowie die Vertiefungsrichtung Nachrichtendienste und öffetnliche Sicherheit.
Dauer und Häufigkeit
Das Modul dauert 6 Monate (Jan-Jun) und beginnt jeweils im Wintertrimester des 1. Studienjahres.

Modulname	Modulnummer
Theoretische Zugänge und Methoden der Intelligence and Security Studies	5527

Konto	Pflichtmodule - MISS 2025 M.Sc.

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Jan-Hendrik Dietrich Prof. Dr. Carlo Antonio Masala	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	24	101	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
5527-V1	VS	Ringvorlesung Intelligence and Security Studies	Pflicht	4
5527-V2	SE	Wissenschaftliches Arbeiten	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Es werden keine besonderen Vorkenntnisse vorausgesetzt.

Qualifikationsziele
Die Studierenden wiederholen und vertiefen wissenschaftliche Zugänge zu „Intelligence“ und „Security“ aus unterschiedlichen wissenschaftlichen Disziplinen heraus. Sie kennen die jeweils wichtigsten Methoden und sind in der Lage, sie für unbekannte Sachverhalte nutzbar zu machen. Mit dem übergreifenden Ansatz der „Intelligence and Security Studies“ sind sie so weit vertraut, dass sie Schnittstellen zwischen verschiedenen Disziplinen erkennen können.

Inhalt
Das Modul soll methodische Grundlagen verfestigen und auf das Kernstudium vorbereiten. Dabei soll auf die Heterogenität der Studierenden eingegangen werden. Es verfügt über zwei Veranstaltungen. Die Ringvorlesung nimmt die unterschiedlichen disziplinären Zugänge zu „Intelligence“ und „Security“ in den Blick. Hier werden die wichtigsten Methoden der jeweiligen Disziplin exemplarisch erörtert und in Bezug zu „Intelligence“ bzw. „Security“ gesetzt. So werden z.B. rechtswissenschaftliche Ansätze und Methoden wie der Rechtsvergleich oder die Rechtstatsachenforschung vorgestellt und ihr Potential in Bezug auf die wissenschaftliche Untersuchung rechtlicher Rahmenbedingungen nachrichtendienstlicher Arbeit vertieft. Gleichzeitig werden Schnittstellen zwischen den Disziplinen offengelegt und die Leistungsfähigkeit des transdisziplinären Ansatzes von „Intelligence Studies“ bzw. „Security Studies“ hinterfragt. Das Seminar des Moduls ist dem wissenschaftlichen Arbeiten gewidmet. An praktischen Beispielen wiederholen die Studierenden die Erstellung eines Forschungsdesigns für eine Untersuchung im Bereich der Geistes- und Sozialwissenschaften. Ziel ist es, auf

diese Weise auf die unterschiedlichen Vorbildungen der Studierenden einzugehen und möglichst einen einheitlichen Kenntnisstand herzustellen.

Literatur

Intelligence Studies/ Security Studies:

- Paul D. Williams (ed.), Security Studies, An Introduction, 2nd edition, 2013.
- Thierry Balzacq/ Myriam Cavelty-Dunn (Hrsg.), The Routledge Handbook of Security Studies, 2016.
- Michael Herman, Intelligence power in peace and war, 1996/2005.
- Loch K. Johnson (ed.), The Oxford Handbook of National Security Intelligence, 2010.
- John Baylis/ James J. Wirtz/ Colin S. Gray, Strategy in the Contemporary World: An Introducation to Strategic Studies, 4th edition, 2015.
- Wolfgang Krieger, Geschichte der Geheimdienste, Von den Pharaonen bis zur NSA, 3. Aufl., 2014.

Methoden:

- Blatter, Joachim and Markus Haverland (2012): Designing Case Studies -
- Explanatory Approaches in Small-N Research. Palgrave MacMillan, Basingstoke.
- Blatter, Joachim, Frank Janning and Claudius Wagemann (2007): Qualitative Politikanalyse. Eine Einführung in Methoden und Forschungsansätze. VS Verlag, Wiesbaden.
- Fahrmeir, L./Heumann, C./Künstler, R./Pigeot, I./Tutz, G. (2016). Statistik: Der Weg zur Datenanalyse. Springer-Verlag.
- Früh, Werner (2007): Inhaltsanalyse: Theorie und Praxis. 6. Aufl., UVK Verlagsgesellschaft, Konstanz.
- George, Alexander L. and Andrew Bennett (2005): Case Studies and Theory Development in the Social Sciences. MIT Press, Cambridge.
- Gerring, John (2007): Case Study Research. Principles and Practices. Oxford University Press, Oxford.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit (3.500 Wörter/Bearbeitungszeit vier bis acht Wochen, die konkrete Bearbeitungszeit wird zu Beginn der Lehrveranstaltung bekannt gegeben), die mit mindestens der Note 4,0 bestanden sein muss. Die Seminararbeit kann bei allen an der Ringvorlesung beteiligten Lehrenden geschrieben werden.

Verwendbarkeit

Die Inhalte des Moduls sind grundlegend für alle weiteren Module des Kernstudiums sowie die nichttechnischen Vertiefungsrichtungen.

Dauer und Häufigkeit

Das Modul dauert 1 Monat (Juli) und beginnt jeweils im Frühjahrstrimester des 1. Studienjahres.

Übersicht des Studiengangs: Konten und Module

Legende:

FT	= Fachtrimester des Moduls
PrFT	= frühestes Trimester, in dem die Modulprüfung erstmals abgelegt werden kann
Nr	= Konto- bzw. Modulnummer
Name	= Konto- bzw. Modulname
M-Verantw.	= Modulverantwortliche/r
ECTS	= Anzahl der Credit-Points

FT	PrFT	Nr	Name	M-Verantw.	ECTS
		7	**Pflichtmodule - MISS 2025 M.Sc.**		**75**
1		5526	Digitalisierung	M. Moll	10
1		5524	Einführung in Intelligence and Security Studies	E. Herschinger	10
		5530	Globale Bedrohungen und Herausforderungen	C. Masala	5
4		5534	Grundlagen der Extremismusforschung: Analysemethoden und Bekämpfungsstrategien	H. Hansen	5
		5532	Intelligence Accountability	R. Bergien	5
4		5533	Intelligence Analysis	A. Lutsch	5
3		3479	Intelligence and Cyber Security	M. Moll	7
		5529	Intelligence Collection	S. Lau	5
		5528	Intelligence Governance	S. Fischer	5
		5531	Kommunikation und Führung in den Nachrichtendiensten	M. Pfundmair	3
1		5525	Menschenrechte und Sicherheit in normativer Perspektive	J. Dietrich	10
		5527	Theoretische Zugänge und Methoden der Intelligence and Security Studies	J. Dietrich	5
		8	**Pflichtmodule der Vertiefungsrichtung "Cyber Defence" - MISS 2025 M.Sc**		**20**
5		5537	Cyber Defence I	W. Hommel	10
5		5538	Cyber Defence II	W. Hommel	10
		14	**Masterarbeit - MISS 2025 M.Sc.**		**25**
5		3488	Masterarbeit	J. Dietrich	25

Übersicht des Studiengangs: Lehrveranstaltungen

Legende:

FT	= Fachtrimester der Veranstaltung
Nr	= Veranstaltungsnummer
Name	= Veranstaltungsname
Art	= Veranstaltungsart
P/Wp	= Pflicht / Wahlpflicht
TWS	= Trimesterwochenstunden

FT	Nr	Name	Art	P/Wp	TWS
	10106	Sicherheitsmanagement	Vorlesung/Übung	Pf	3
	10107	Sichere vernetzte Anwendungen	Vorlesung/Übung	Pf	3
	3479-V1	Intelligence	Vorlesung	Pf	4
	3479-V2	Methoden der Cyber Security	Vorlesung	Pf	2
	3479-V3	Methoden der Cyber Security	Übung	Pf	1
	3488-V1	Master-Arbeit	Projekt	Pf	,
	5524-V1	Einführung in Internationalen Beziehungen und Security Studies	Vorlesung	Pf	2
	5524-V2	Einführung in Intelligence History	Seminar	Pf	2
	5524-V3	Intelligence Essentials - Nachrichtendienstliche Operationen	Seminar	Pf	2
	5525-V1	Der moderne Staat: Zwischen Freiheitsnorm und einer Ethik der Sicherheit	Vorlesung/Seminar	Pf	1
	5525-V2	Grundrechte, Menschenrechte und modernes Sicherheitsrecht	Vorlesung/Übung	Pf	2
	5525-V3	Einführung in das Recht der Nachrichtendienste	Vorlesung/Übung	Pf	3
	5526-V1	Digitalisierung	Vorlesung/Seminar	Pf	4
	5526-V2	Praktikum zur Digitalisierung	Praktikum	Pf	4
	5527-V1	Ringvorlesung Intelligence and Security Studies	Vorlesung/Seminar	Pf	4
	5527-V2	Wissenschaftliches Arbeiten	Seminar	Pf	2
	5528-V1	Einführung in Intelligence Governance	Vorlesung/Seminar	Pf	2
	5528-V2	Seminar zur Einführungsvorlesung – Dimensionen von Intelligence Oversight	Seminar	WPf	1
	5528-V3	Seminar zur Einführungsvorlesung – Dimensionen von Intelligence Oversight	Seminar	WPf	1
	5528-V4	Seminar zur Einführungsvorlesung – Defense Intelligence Architekturen	Seminar	WPf	1
	5528-V5	Seminar zur Einführungsvorlesung – National Intelligence Architekturen	Seminar	WPf	1
	5528-V6	Intelligence Governance in Practice	Seminar	Pf	1
	5528-V7	Intelligence Governance in Practice	Seminar	Pf	1
	5529-V1	Intelligence Collection - Ringvorlesung	Vorlesung/Seminar	Pf	1
	5529-V2	HUMINT in den Grenzen des Rechtsstaats	Seminar	Pf	1
	5529-V3	Psychologie der HUMINT-Collection	Vorlesung/Seminar	Pf	3
	5530-V1	Einführung in hybride und asymmetrische Konflikte	Vorlesung	Pf	3
	5530-V2	Einführung in die Kriegsursachenforschung (Übungsanteil: Vorausschau durch Szenarioanalyse)	Seminar	Pf	2
	5531-V1	Grundlagen in Kommunikation und Führung	Vorlesung	Pf	2
	5531-V2	Führung in Nachrichtendiensten	Seminar	Pf	2
	5531-V3	Kommunikation und Präsentation	Übung	Pf	2
	5532-V1	Grundlagen der nachrichtendienstlichen Rechenschaftspflicht	Vorlesung	Pf	3
	5532-V2	Ethik der Nachrichtendienste	Seminar	WPf	2

	5532-V3	Nachrichtendienste und Gesellschaft seit 1945	Seminar	WPf	2
	5532-V4	Geheimdienste und Geheimpolizeien in deutschen Diktaturen	Seminar	WPf	2
	5533-V1	Grundlagen der Intelligence Analysis	Vorlesung	Pf	2
	5533-V2	Fallstudien zur Methodenanwendung	Übung	Pf	1
	5533-V3	Analysemethodische Probleme (Vertiefungen)	Seminar	WPf	1
	5534-V1	Einführung in die Extremismusforschung für Nachrichtendienste	Vorlesung/ Seminaristischer Unterricht	Pf	4
	5534-V2	Extremismus- und Terrorismusstrafrecht I	Seminar	Pf	2
	5537-V2	Sichere Netze und Protokolle	Vorlesung/Übung	Pf	4
	5538-V1	Hardware- und Betriebssystemsicherheit	Vorlesung/Übung	Pf	3
	5538-V2	Data Science and Analytics	Vorlesung/Übung	Pf	3
	5538-V3	Security Engineering	Praktikum	Pf	4