

Modulhandbuch des Studiengangs
Intelligence and Security Studies
(Master of Arts)

an der
Universität der Bundeswehr München

(Version 2020)

Stand: 08. Dezember 2020

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" oder "Regionale Sicherheit" 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

Prolog	2
Pflichtmodule - MISS 2020	
3468 Einführung in Intelligence and Security Studies.....	4
3469 Menschenrechte und Sicherheit in normativer Perspektive.....	7
3470 Digitalisierung.....	10
3471 Theoretische Zugänge und Methoden der Intelligence and Security Studies.....	12
3472 Intelligence Governance.....	15
3473 Intelligence Collection.....	19
3474 Globale Bedrohungen und Herausforderungen.....	21
3475 Kommunikation und Führung in den Nachrichtendiensten.....	24
3476 Intelligence Accountability.....	26
3477 Intelligence Analysis.....	28
3478 Umgang mit Unsicherheit.....	30
3479 Intelligence and Cyber Security.....	32
Pflichtmodule der Vertiefungsrichtung "Cyber Defence" - MISS 2020	
3480 Cyber Defence I.....	35
3481 Cyber Defence II.....	38
Pflichtmodule der Vertiefungsrichtung „Nachrichtendienste und öffentliche Sicherheit“ - MISS 2020	
3482 Verfassungsschutz in der wehrhaften Demokratie.....	41
3483 Politischer Extremismus.....	44
Pflichtmodule der Vertiefungsrichtung „Terrorismusbekämpfung“ - MISS 2020	
3484 Advanced Intelligence Collection and Analysis.....	46
3485 Terrorismusforschung.....	48
Pflichtmodule der Vertiefungsrichtung „Regionale Sicherheit“ - MISS 2020	
3486 Regionale Sicherheit I.....	50
3487 Regionale Sicherheit II.....	52
Master-Arbeit - MISS 2020	
3488 Master-Arbeit.....	56
Übersicht des Studiengangs: Konten und Module	57
Übersicht des Studiengangs: Lehrveranstaltungen	58

Modulname	Modulnummer
Einführung in Intelligence and Security Studies	3468

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

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

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3468-V1	SE	Einführung in Intelligence and Security Studies	Pflicht	2
3468-V2	SE	Einführung in Intelligence History	Pflicht	2
3468-V3	UE	Einführung in Intelligence Studies	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Qualifikationsziele
<p>Studierende sollen befähigt werden unterschiedliche IB-Theorien auf Themenkomplexe der internationalen Politik anzuwenden, durch Erhöhung des Abstraktionsniveaus komplexe Sachverhalte verstehen und erklären können, sowie sicherheitspolitische Zusammenhänge im Kontext IB-Theorien einzuordnen. Darüber hinaus werden Studenten grundlegende Erklärungsschemata aus dem Bereich der Sicherheitsforschung und Kriegsursachenforschung als Grundlage für das weitere Studium vermittelt und deren Einfluss auf Intelligence diskutiert. Die Studierenden werden mit der Rolle und den Aufgaben von „Intelligence“ in moderner staatlicher Sicherheitsarchitektur vertraut gemacht. Sie erhalten erste Einblicke in nationale und internationale „Intelligence Communities“ sowie deren Geschichte.</p> <p>Die Studierenden können aktuelle Herausforderungen von Intelligence erkennen und differenzieren. 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 internationalen Nachrichtendiensten mit Bezug auf ihre rechtliche Einbettung, Rolle im politischen Entscheidungsprozess und öffentliche Wahrnehmung zu identifizieren.</p>

Inhalt
<p>Das Modul legt Grundlagen. Die Studierenden lernen 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. Das Seminar 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 und Politik, die Rolle von Nachrichten- bzw. Geheimdiensten in Demokratien, und 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.</p> <p>Um die Arbeitsweise der Intelligence-Akteure nachvollziehen zu können, werden Facetten nachrichtendienstlicher Arbeit wie „Intelligence Analysis“ „Intelligence Collection“ oder „Covert Action“ behandelt. Zudem ist es Ziel des Moduls grundlegende Einsichten im Bereich der internationalen Beziehungen, internationale Sicherheit, Krieg und Frieden und intelligence studies zu vermitteln. Dieses Einführungsmodul befasst sich mit einer Vielzahl der bedeutendsten Herausforderungen internationaler Sicherheit. In diesem Zusammenhang sind folgende Themengebiete von übergeordneter Bedeutung: Theoretische und methodische Ansätze der Theorien der Internationalen Beziehungen, Fragenkomplexe aus dem Bereich Krieg und Frieden sowie der Informationsgewinnung und des Nachrichtenwesens. Neben einem grundsätzlichen Verständnis über die zentralen Akteure der internationalen Beziehungen wird insbesondere auf die sicherheitspolitischen Herausforderungen im Informationszeitalter eingegangen. Dabei spielen vor allen nicht-staatliche Akteure eine entscheidende Rolle, da sie oftmals diametral zu traditionellen Sicherheitsbedenken und –Lösungsansätzen stehen.</p>
Literatur
<p>Intelligence History:</p> <ul style="list-style-type: none">• Adams, Jefferson, Strategic intelligence in the Cold War and beyond, London: Routledge 2015.• 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.• Immerman, Richard, The Hidden Hand: A Brief History of the CIA, Malden, MA: John Wiley & 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, Geheimdienste in der Weltgeschichte. Spionage und verdeckte Aktionen von der Antike bis zur Gegenwart, 3., aktualisierte und erweiterte Aufl. München: Beck, 2014.
- Oxford handbook of national security intelligence, ed. by Loch K. Johnson, Oxford: Oxford University Press, 2010 (paperback ed. 2012).
- Moravcsik, Andrew: Taking Preferences Seriously: A Liberal Theory of International Politics, in: International Organization 51, 4 (Autumn 1997), S. 513-553.
- Rittberger, Volker: Regime Theory and International Relations, Oxford et al. 2002.

English School:

- Bull, Hedley: The Anarchical Society. A Study of Order in World Politics, 4. Auflage, Basingstoke et al. 2012.

Interdependence theory:

- Keohane, Robert/Nye, Joseph: Power and Interdependence. World Politics in Transition, Boston 1977.
- Keohane, Robert: After Hegemony. Cooperation and Discord in the World Political Economy, Princeton 1984.

Social Constructivism:

- Wendt, Alexander: A Social Theory of International Politics, Cambridge 2003.
- Wendt, Alexander: Anarchy is What States Make of It: The Social Construction of Power Politics, in: International Organization 46, 2 (March 1992), S. 391-425.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Menschenrechte und Sicherheit in normativer Perspektive	3469

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Christina Binder	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3469-V1	VS	Der moderne Staat: Zwischen Freiheitsnorm und einer Ethik der Sicherheit	Pflicht	2
3469-V2	VÜ	Grundrechte, Menschenrechte und modernes Sicherheitsrecht	Pflicht	2
3469-V3	VÜ	Einführung in das Recht der Nachrichtendienste	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

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 Nachrichten-dienste 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 in normativer Perspektive“.

Ideengeschichtlich formiert sich der moderne Staat wesentlich im politischen Denken der Aufklärung des 17. und 18. Jahrhunderts. Die Veranstaltung „Der moderne Staat“ untersucht die hier grundlegende Legitimation und Einhegung des Staates und seiner Exekutivorgane, aber auch die notwendige Weiterentwicklung dieser Grundlegung unter globalen Bedingungen. In einem sicherheitsethischen Seminaranteil werden dann in aktualisierender und anwendungsorientierter Perspektive Geltungsansprüche reflektiert, mit denen sich die Sicherheitsbehörden als Institutionen, aber auch die Sicherheitsakteure als Individuen konfrontiert sehen und die es sicherheitsethisch angemessen zu handhaben gilt. Verschiedene Sicherheitsentscheidungen, Sicherheitshandlungen und Sicherheitstechniken werden im Kontext der größeren Frage nach dem richtigen, guten und gerechten Handeln auf ihre mögliche Begründung und Rechtfertigung hin überprüft.

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 Konfliktlösungsformeln, 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.
- Brocker, Manfred (Hg.): Geschichte des politischen Denkens. Ein Handbuch (= Suhrkamp Taschen-buch Wissenschaft, Bd. 1818), Frankfurt a.M. 2007.
- Hassemer, Winfried u.a. (Hg.): Einführung in die Rechtsphilosophie und Rechtstheorie der Gegenwart (= Schwerpunktbereich), 9. neu bearb. u. erw. Aufl., Heidelberg 2016.

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 (= Tutzing 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: Intelligence Law and Policies in Europe, München/Oxford 2018 (i.E.).
- Tanneberger, Steffen: Die Sicherheitsverfassung: Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts. Zugleich ein Beitrag zu einer induktiven Methodenlehre (= Freiburger rechtswissenschaftliche Abhandlungen, Bd. 11), Tübingen 2014.

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.

Modulname	Modulnummer
Digitalisierung	3470

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Dr. apl. Prof. Lothar Schmitz	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3470-V1	VS	Digitalisierung	Pflicht	4
3470-V2	P	Praktikum zur Digitalisierung	Pflicht	4
Summe (Pflicht und Wahlpflicht)				8

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.

Über diesen Leistungsnachweis hinaus werden im Praktikum unbenotete Arbeitsaufträge erteilt, die erfüllt und bestanden werden müssen.

Modulname	Modulnummer
Theoretische Zugänge und Methoden der Intelligence and Security Studies	3471

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. jur. 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
3471-V1	VS	Intelligence and Security Studies als wissenschaftlicher Ansatz (Ringvorlesung)	Pflicht	4
3471-V2	SE	Wissenschaftliches Arbeiten	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Qualifikationsziele
Die Studierenden können „Intelligence“ und „Security“ als Gegenstände von Forschung und Lehre wissenschaftssystematisch einordnen. Dabei haben sie ein vertieftes Verständnis von disziplinären Zugängen und methodischen Ansätzen, so dass sie in der Lage sind, sich mit fachspezifischen Kontroversen auseinanderzusetzen. Mit den Perspektiven der „Intelligence Studies“ und der „Security Studies“ sind sie vertraut und können deren Leistungspotential für die Praxis erklären.
Inhalt
Ziel des Moduls ist es, die theoretischen und methodischen Zusammenhänge und Herangehensweisen bei der Bewältigung zentraler Forschungsfragen der Intelligence und Security Studies zu vermitteln. Die Studierenden wiederholen und vertiefen wissenschaftliche Zugänge und methodische Ansätze der „Intelligence and Security Studies“ zunächst in einer Ringvorlesung. Im Fokus stehen dabei rechts-, politik-, verwaltungs- und geschichtswissenschaftliche Perspektiven auf „Sicherheit“ und „Intelligence“. Auf diese Weise werden die Studierenden in zweifacher Hinsicht auf die Veranstaltungen im Kernstudium vorbereitet: zum einen wird das notwendige methodische Rüstzeug vor Augen geführt, zum anderen werden die Studierenden bereits frühzeitig mit Dozentinnen und Dozenten bekannt gemacht, die später entsprechende Veranstaltungen leiten.
Die Ringvorlesung wird ergänzt durch ein Seminar zum wissenschaftlichen Arbeiten. Das Seminar verfolgt den Zweck, auf die sehr heterogenen Vorkenntnisse und Methodenkompetenzen der Studierenden (in Bezug auf Vorwissen, Abschlüsse usw.) einzugehen und Standards insb. geisteswissenschaftlicher Arbeit zu setzen.

Literatur**Intelligence:**

- John Baylis/ James J. Wirtz/ Colin S. Gray, *Strategy in the Contemporary World: An Introduction to Strategic Studies*, 4th edition, 2015.
- Michael Herman, *Intelligence power in peace and war*, 1996/2005.
- Bob de Graaff/ James M. Nyce, *The Handbook of European Intelligence Cultures*, 2016.
- Peter Gill/ Stephen Marrin/ Mark Phythian, *Intelligence Theory*, 2009.
- Loch K. Johnson (ed.), *The Oxford Handbook of National Security Intelligence*, 2010.
- David Omand, *Securing the State*, 2010
- John Baylis/ James J. Wirtz/ Colin S. Gray, *Strategy in the Contemporary World: An Introduction to Strategic Studies*, 4th edition, 2015.
- Wolfgang Krieger, *Geschichte der Geheimdienste, Von den Pharaonen bis zur NSA*, 3. Aufl., 2014.
- Christopher Daase/ Philipp Offermann/ Valentin Rauer (Hrsg.), *Sicherheitskultur*, 2012.

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.
- Goertz, Gary (2006): *Social Science Concepts. A User's Guide*. Princeton University Press, Princeton.
- Keller, Reiner et al. (Hg.) (2007/2008): *Handbuch Sozialwissenschaftliche Diskursanalyse*. Bd. 1 und 2. VS Verlag, Wiesbaden.
- Krämer, W. (2015): *So lügt man mit Statistik*, Campus-Verlag.
- Mertens, P./Rässler, S. (2012): *Prognoserechnung*, Physica-Verlag
- Ragin, Charles C. (2008): *Redesigning Social Inquiry - Fuzzy Sets and Beyond*. Chicago University Press, Chicago.
- Rose, Gillian (2001): *Visual Methodologies: An Introduction to the Interpretation of Visual Materials*. Sage, London.
- Singer, David J./ Small, Melvin: *The wages of war 1816–1965. A statistical handbook*. New York 1972.
- Singer, David J./Small, Melvin: *Patterns in International Warfare 1816-1980*, in: Singer, David J./Small, Melvin(ed.): *International War. An Anthology*. Second Edition. Chicago: The Dorsey Press 1989, p. 26-37.
- Siegfried Schieder/ Manuela Spindler (Hrsg.), *Theories of International Relations*, Abingdon 2014.

- Scott, John (2000): Social Network Analysis - A Handbook. Sage, London.
- Van Evera, Stephen (1997): Guide to Methods for Students of Political Science. Cornell University Press, Ithaca

Leistungsnachweis

Der Notenschein wird auf der Grundlage eines Referats und einer Hausarbeit in jedem der beiden gewählten Seminare vergeben. Die Leistungen aus den beiden Seminaren gehen gleichwertig in die Gesamtnote ein. Die Leistungen aus beiden Seminaren müssen jeweils mit mindestens der Note 4,0 bestanden sein.

Modulname	Modulnummer
Intelligence Governance	3472

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

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

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3472-V1	VL	Einführung in Intelligence Governance	Pflicht	2
3472-V2	UE	Intelligence Governance – Analyse und Diskussion empirischer Beispiele sowie ausgewählte Probleme des Rechts der Nachrichtendienste	Pflicht	2
3472-V3	SE	Intelligence Governance in Practice	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Qualifikationsziele

- Fachwissen (Theorie/Empirie) zu zentralen Akteuren verschiedener (inter)nationaler Intelligence Communities bzw. Systeme sowie Herausforderungen und Lösungsansätze für Steuerungs- und Kontrollprozesse.
- Analytisches Denken: Systematisches (theoriegeleitetes) Analysieren von Steuerungs- und Kontrollprozessen anhand empirischen Beispielen, Identifikation von Herausforderungen, Widersprüchen etc.
- Basiskompetenzen: Perspektivwechsel (Draufsicht versus Binnenperspektive, deskriptive vs. analytische vs. normative Perspektive), systematischer Umgang mit Informationen (Informationsauswahl, Priorisieren, Informationsverdichtung, Informationsvermittlung), Arbeit in und mit Gruppen, Zeitmanagement.

Inhalt

Intelligence Governance ist ein junges Forschungsfeld im Rahmen der ebenfalls noch recht jungen Intelligence Studies. Allgemein gesprochen werden im Rahmen von Intelligence Governance die zentralen Akteure bzw. Akteurskonstellationen nationaler und internationaler Intelligence Systeme sowie die Strukturen und Prozesse der Steuerung und Kontrolle nachrichtendienstlicher Tätigkeit beschrieben, analysiert und bewertet. Anlass für die wissenschaftliche Beschäftigung mit diesem Thema waren (und sind weiterhin) politische Skandale rund um Misserfolge von nachrichtendienstlicher Tätigkeit sowie die Systemtransformationen („Demokratisierung“), die auf das Ende des Ost-West-Konfliktes folgten, und zur Neuordnung der jeweiligen nationalen Intelligence Systemen führten. Damit besteht ein zentraler Ausgangspunkt der Intelligence Governance-Forschung in der Einsicht: „[I]ntelligence is not produced in a vacuum“ (Walsh 2018).

Nachrichtendienste sind eingebettet in ein historisch gewachsenes und Wandlungsprozessen unterliegendes politisches und gesellschaftliches Gefüge. Die hieraus resultierenden unterschiedlichen Erwartungen und Anforderungen an die Intelligence Community spiegeln sich in den Steuerungs- und Kontrollinstrumenten wider, die die Community adressieren und damit den Intelligence Prozess zum einen von außen („external intelligence governance“, Walsh 2018) zu beeinflussen suchen sowie sich in internen Steuerungs- und Kontrollmechanismen („internal intelligence governance“, Walsh 2018) niederschlagen. In diesem Sinne liegt der Schwerpunkt des Moduls auf drei Aspekten:

Das Modul vermittelt eine (vergleichende) Übersicht über nationale und internationale Intelligence Communities bzw. Systeme sowie die zentralen Instrumente der Steuerung und Kontrolle nachrichtendienstlicher Tätigkeit („external intelligence governance“), die diese adressieren.

Das Modul vermittelt unter Rückgriff auf Überlegungen der angelsächsischen Intelligence Governance-Forschung sowie der politikwissenschaftlichen Governance-Forschung bzw. Steuerungstheorie (sowie weitere politikwissenschaftliche/soziologische Ansätze) die Fähigkeit, die Steuerung und Kontrolle nachrichtendienstlicher Tätigkeit systematisch zu analysieren.

Für die theoriegeleitete Analyse werden empirische Beispiele ausgewählt, die die praktischen Herausforderungen der Steuerung und Kontrolle nachrichtendienstlicher Tätigkeit exemplarisch nachvollziehbar machen.

In der Übung sollen die in der Vorlesung vermittelten Lehrinhalte praktisch angewendet und auch über ausgewählte Probleme des Rechts der Nachrichtendienste diskutiert werden. Ergänzend zur Vorlesung und der Übung sollen in einem Seminar praktische Beispiele aus dem Bereich der Kontrolle von Nachrichtendiensten gemeinsam diskutiert werden.

Literatur

- Bartodziej, Peter (2017): Parlamentarische Kontrolle. In: Jan-Hendrik Dietrich und Sven-R. Eiffler (Hg.): Handbuch des Rechts der Nachrichtendienste. Stuttgart: Boorberg, S. 1533–1606.
- Bogumil, Jörg/Jann, Werner (2009): Verwaltung und Verwaltungswissenschaft in Deutschland. Einführung in die Verwaltungswissenschaft. 2., völlig überarbeitete Auflage. Wiesbaden: VS Verlag.
- Born, Hans (2004): Towards Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices. In: Connections 4 (3), S. 1–12.
- Born, Hans/Leigh, Ian (2007): Intelligence Accountability. A Comparative Perspective. In: Loch K. Johnson (Hg.): Strategic Intelligence. Intelligence and Accountability. Westport, CT: Praeger, S. 141–164.
- Campbell, Tony (2009): Bedmates or Sparring Partners? Canadian Perspectives on the Media-Intelligence Relationship in "The New Propaganda Age". In: Dover,

- Robert/Goodman, Michael (Hg.): *Spinning Intelligence. Why Intelligence Needs the Media, Why the Media Needs Intelligence*. London: Hurst, S. 165–183.
- Chopin, Olivier (2017): *Intelligence Reform and the Transformation of the State: The End of a French Exception*. In: *The Journal of Strategic Studies* 40 (4), S. 532–533.
 - Daun, Anna (2011): *Auge um Auge? Intelligence-Kooperation in den deutsch-amerikanischen Beziehungen*. Wiesbaden: VS-Verlag.
 - Denécé, Eric (2016): *France: The Intelligence Service' Historical and Cultural Context*. In: de Graaff, Bob/Nyce, James M. (Hg.): *The Handbook of European Intelligence Cultures*. Plymouth: Rowman & Littlefield, S. 135–147.
 - 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.
 - Döhler, Marian (2007): *Hierarchie*. In: Benz, Arthur/Lütz, Susanne/Schimank, Uwe/Simonis, Georg (Hg.): *Handbuch Governance. Theoretische Grundlagen und empirische Anwendungsfelder*. Wiesbaden: Springer, S. 46–53.
 - 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.
 - Gill, Peter/Pythian, Mark (2018): *Intelligence in an Insecure World*. Third Edition. Cambridge: Polity Press.
 - Goodman, Michael (2014). *The United Kingdom*. In: Dover, Robert/Goodman, Michael/Hillebrand, Claudia (Hg.): *Routledge Companion to Intelligence Studies*. Abingdon: Routledge, S. 135–144.
 - Gusy, Christoph (2011): *Grundrecht und Verfassungsschutz*. Wiesbaden: VS Verlag.
 - Gusy, Christoph (2014): *Kontrolle der Nachrichtendienste*. In: *Verwaltungsarchiv* 106, S. 437–458.
 - 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.
 - Hillebrand, Claudia (2012): *The Role of News Media in Intelligence Oversight*. In: *Intelligence and National Security* 27 (5), S. 689–706.
 - Hillebrand, Claudia (2014): *Intelligence Oversight and Accountability*. In: Dover, Robert/Goodman, Michael/Hillebrand, Claudia (Hg.): *Routledge Companion to Intelligence Studies*. Abingdon: Routledge, S. 305–312.
 - 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.
 - Mayntz, Renate (2005): *Governance Theory als fortentwickelte Steuerungstheorie*. In: Gunnar Folke Schuppert (Hg.): *Governance-Forschung. Vergewisserung über Stand und Entwicklungslinie*. Baden-Baden: Nomos, S. 11–20.
 - Pythian, Mark (2010): *"A Very British Institution". The Intelligence and Security Committee and Intelligence Accountability in the United Kingdom*. In: Loch K. Johnson (Hg.): *The Oxford Handbook of National Security Intelligence*. Oxford: Oxford University Press, S. 699–718.
 - Pythian, Mark (2015): *The British Experience with Accountability*. In: Loch K. Johnson (Hg.): *Essentials of Strategic Intelligence*. Santa Barbara/Cal.: Praeger, S. 447–469.

- Rüss, Oliver (2017): International nachrichtendienstliche Zusammenarbeit. In: Jan-Hendrik Dietrich und Sven-R. Eiffler (Hg.): Handbuch des Rechts der Nachrichtendienste. Stuttgart: Boorberg, S. 453–505.
- Warusfel, Bertrand (2019): The Intensification of French Intelligence and its Oversight under the Impact of Counter-Terrorism. In: Leigh, Ian/Wegge, Njord (Hg.): Intelligence Oversight in the Twenty-First Century. Abingdon: Routledge, S. 124–134.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Klausur von 120 Minuten, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Intelligence Collection	3473

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Markus Denzler Prof. Dr. Raimund Jokiel	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
125	56	69	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3473-V1	VS	Intelligence Collection	Pflicht	2
3473-V2	SE	Intelligence Collection – Aktuelle Herausforderungen in der Praxis	Pflicht	2
3473-V3	VS	Intelligence Collection - Ringvorlesung	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Qualifikationsziele
Die Studierenden verfügen über vertiefte Kenntnisse der Methoden nachrichtendienstlicher Beschaffung. Auf der Grundlage wissenschaftlicher Methodik können sie Beschaffungsvorgänge hinterfragen, vergleichen und bewerten. So sind sie beispielsweise 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.
Inhalt
Die Beschaffung von Informationen beschreibt eine zentrale Aufgabe der Nachrichtendienste. Die Methoden der Beschaffung 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 oder OSINT) eingenommen. Sie werden kontextualisiert und hinterfragt; Probleme und Potentiale werden offengelegt. Im Fokus der wissenschaftlichen Analyse steht dabei die aktuelle nachrichtendienstliche Praxis.
Literatur
<ul style="list-style-type: none"> • Robert M. Clark, Intelligence Collection, 2014. • Wayne Michael Hall/ Gary Citrenbaum, Intelligence Collection, 2012. • Stephan Blancke, Private Intelligence, 2011. • Michael Bazell, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 2018. • Mark M. Lowenthal/ Robert M. Clark, The Five Disciplines of Intelligence Collection, 2015.

Leistungsnachweis

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

Modulname	Modulnummer
Globale Bedrohungen und Herausforderungen	3474

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

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
3474-V1	SE	Kriegsursachenforschung, Asymmetrische, ethnische und hybride Konflikte, moderner Krieg und Staatszerfall	Pflicht	3
Summe (Pflicht und Wahlpflicht)				2

Qualifikationsziele

Erweiterung des Fachwissens, vertieftes Verständnis interdisziplinärer Zugänge zu sicherheitspolitischen Themen aus unterschiedlichen fachspezifischen Sichtweisen und Forschungsinstrumentarien heraus, Auseinandersetzung mit Forschungsdebatten, Interpretationen und Kontroversen in den Security Studies. 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 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.

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 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

Pflichtliteratur:

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

Empfohlene Literatur (optional):

- Hahn, Henning: Globale Gerechtigkeit. Eine philosophische Einführung, Frankfurt a.M./New York 2009.
- 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
- Fukuyama, Francis/Ley Brian: Development strategies. Integrating Governance and Growth. World Bank Policy research paper 5196. 2010. Online at: <http://issrb.ru/content/program/436.pdf>.
- Hartzell, Caroline/Hoddie Matthew: Institutionalizing Peace: Power Sharing and Post-Civil War Conflict Management, in: American Journal of Political Science 47:2, April 2003, p. 318–332.

Asymmetrische Konflikte, Terror, moderner Krieg und Staatszerfall:

- Abrahams, Max: Why Terrorism Does not work, in: International Security 31:2, Fall 2006, 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.
- Hoffmann, Bruce: Inside Terrorism, New York 2006, p 1-41.
- Fearon, J.D. & Laitin, D. D.: Ethnicity, Insurgency, and Civil War. American Political Science Review 97, 2003, p. 75-90.
- 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.

Rise and Fall of Empires:

- Gilpin, Robert (1980): „The Theory of Hegemonic War“, in: Rotberg, Robert; Rabb, Theodore: „The Origin and Prevention of Major Wars“, 15-37
- 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
- Modelski, George; Thompson, William R. (1989): „Long Cycles and Global War“, in: Midlarsky, Manus: „Handbook of War Studies“, Boston, 23-54

- Thompson, William R. (1986): „Polarity, the Long Cycle, and Global Welfare”, *Journal of Conflict Resolution* (30/4), 587-615

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit, die mit mindestens der Note 4,0 bestanden sein muss. Alternativ kann, nach Rücksprache mit dem Modulverantwortlichen, eine andere schriftliche Prüfung abgelegt werden.

Modulname	Modulnummer
Kommunikation und Führung in den Nachrichtendiensten	3475

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Raimund Jokiel 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
3475-V1	VL	Grundlagen in Kommunikation und Führung	Pflicht	2
3475-V1	SE	Führung in den Nachrichtendiensten	Pflicht	2
3475-V3	UE	Kommunikation und Präsentation	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Qualifikationsziele
Nach erfolgreicher Teilnahme an dem Modul kennen und verstehen die Studierenden Erkenntnisse der wissenschaftlichen Psychologie zu Kommunikations- und Führungsprozessen. Sie können ihre eigenen Kommunikationsfähigkeiten reflektieren und nachrichtendienstliche Produkte fachlich, glaubhaft und nachvollziehbar gegenüber Abnehmern vertreten. Sie sind in der Lage, den nachrichtendienstlichen Produktionsprozess strategisch zu planen und verfügen über praxisbezogene Führungskompetenzen.
Inhalt
Das Modul setzt am nachrichtendienstlichen Produktionsprozess an. Dieser umfasst zum einen die bedarfsadäquate Aufbereitung und Präsentation nachrichtendienstlicher Erkenntnisse, die die Verwertbarkeit und Akzeptanz des nachrichtendienstlichen Produkts bei Entscheidungs- bzw. Bedarfsträgern steigern kann. Zum anderen umfasst er den optimalen Einsatz von Personalressourcen und die Übernahme von Personalverantwortung im spezifischen Umfeld von Sicherheitsbehörden. Im ersten Teil des Moduls werden psychologische Prozesse im Rahmen von Kommunikation und Führung grundlegend behandelt. Darauf aufbauend werden im zweiten Teil des Moduls kommunikative Kompetenzen erlernt sowie Führungskompetenzen mit spezifischem Fokus auf die nachrichtendienstliche Tätigkeit vertieft.
In der Vorlesung werden Grundlagen zu Kommunikations- und Führungsprozessen vermittelt. Dabei stehen u.a. folgende Themen im Zentrum: kommunikative

Grundlagen, Gruppen-prozesse, Konflikt und Konfliktlösung, soziale Gesundheit, Mitarbeitercommitment, Führungs-ansätze, Personalpsychologie sowie berufliche Belastungen und Bewältigungsmöglichkeiten.

Im Seminar werden Theorien und Erkenntnisse zu Führung und Personalpsychologie weiter vertieft und auf den spezifischen nachrichtendienstlichen Prozess adaptiert (u.a. berufliche Eignung, Leitbilder). Diese Vertiefung erfolgt in Gruppenarbeiten (Referate) und in Interaktion mit Gastdozenten mit Führungserfahrung.

In der Übung werden Erkenntnisse zu Kommunikation (u.a. Impression Management, Präsentationstechniken, aktives Zuhören, Umgang mit Stress und Störungen) durch Selbsterfahrung vertieft. Hierzu werden Übungen und Rollenspiele mit Videofeedback eingesetzt.

Literatur

- 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.
- De Dreu, C. K. W. (1997). Productive conflict: The importance of conflict management and conflict issue. In C. K. W. De Dreu & E. Van De Vliert (Eds.), *Using conflict in organizations* (pp. 9-22). London: Sage.
- Siegel, P. A., Post, C., Brockner, J., Fishman, A. Y., & Garden, C. (2005). The moderating influence of procedural fairness on the relationship between work-life conflict and organizational commitment. *Journal of Applied Psychology*, 90(1), 13-24.
- Schuler, H. (2014). Gegenstand und Aufgaben der Personalpsychologie. In H. Schuler & U. P. Kanning, *Lehrbuch der Personalpsychologie* (S. 13-24). Göttingen: Hogrefe.
- Felfe, J. (2009). *Mitarbeiterführung*. Göttingen: Hogrefe.
- Nerdinger, F. (2003). *Motivation von Mitarbeitern*. Göttingen: Hogrefe.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Klausur von 120 Minuten, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Intelligence Accountabilitiy	3476

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

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

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3476-V1	VL	Ideengeschichtliche Grundlagen der Rechenschaftspflicht von Nachrichtendiensten	Pflicht	2
3476-V2	VL	Entwicklung der ‚Intelligence Accountability‘ in der BRD	Pflicht	2
3476-V 3a	SE	Ethik der nachrichtendienstlichen Tätigkeit	Wahlpflicht	2
3476-V 3b	SE	Nachrichtendienste und Massenmedien seit 1945	Wahlpflicht	2
3476-V 3c	SE	Gegen den ‚inneren Feind‘: Spionageabwehr in Demokratie und Diktatur	Wahlpflicht	2
Summe (Pflicht und Wahlpflicht)				6

Qualifikationsziele

Die Studierenden kennen 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 vertretbare Lösungen zu entwickeln.

Inhalt

Allein durch Gesetze werden Nachrichtendienste in demokratischen Rechtsstaaten zu empfindlichen Eingriffen in individuelle Rechte von Bürger/-innen ermächtigt. Daraus resultiert eine demokratische Verantwortung der Dienste, deren Facetten Gegenstand dieses Moduls sind. Zivilgesellschaftliche Anliegen werden in den Veranstaltungen in den Kontext nachrichtendienstlicher Arbeit gestellt. Von besonderer Bedeutung ist dabei eine kontrastierende geschichtswissenschaftliche Perspektive auf die Rolle von Nachrichtendiensten in Diktaturen deutscher Vergangenheit.

Literatur

- Dover, Robert/Goodman, Michael S. (Hrsg.), Spinning Intelligence, Why Intelligence needs the Media, why the Media needs Intelligence, 2009.
- Dietrich, Jan-H./Eiffler, Sven (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017.
- Greenwald, Glenn, Die globale Überwachung – Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, 2014.Zweites Thema:
- Gieseke, Jens, Die Stasi 1945-1990, 2011.
- Born, Hans/Leigh, Ian/Wills, Aiden (Hrsg.), International Intelligence – Cooperation and Accountability, 2011.
- Bellaby, Ross W., The ethics of intelligence, A new framework, 2014.
- Galliot, Jai/Reed, Warren (Hrsg.), Ethics and the future of spying, 2016.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer schriftlichen Prüfung von 180 Minuten, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Intelligence Analysis	3477

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Christian Haas Juniorprof. Dr. Andreas Lutsch	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3477-V1	VL	Grundlagen der Intelligence Analysis	Pflicht	2
3477-V2	UE	Technik und Methodik der Intelligence Analysis	Pflicht	2
3477-V3	SE	Umgang mit Unsicherheit	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Qualifikationsziele
Die Studierenden beherrschen Wissensverknüpfung und kritisches Denken im Sinne der Intelligence Analysis. Sie sind der Lage, die Methoden der Intelligence Analysis auf praktische Fälle anzuwenden. Typische Fehlerquellen im Rahmen der Analyse können sie identifizieren und Vermeidungsstrategien entwickeln.
Inhalt
„Intelligence Analysis“ bezeichnet nicht nur eine wichtige gesetzliche Aufgabe der Nachrichtendienste („Auswertung“), sondern auch eine tragende Teildisziplin der Intelligence Studies. In diesem Sinne verbindet die Intelligence Analysis Auswertungsinstrumente der Praxis mit einer wissenschaftlichen Perspektive. Es geht – mit Richards J. Heuer gesprochen – um „Thinking about Thinking“. Anknüpfend an die bereits vermittelten Grundlagen der Intelligence Analysis setzen sich die Studierenden in diesem Modul mit den immer wiederkehrenden Herausforderungen nachrichtendienstlicher Analyse auseinander: Unvollständigkeit und Unsicherheit der verfügbaren Informationen, Zukunftsgerichtetheit der Analyse, Fokussierung und Pointierung der Ergebnisse unter Berücksichtigung des Abnehmerinteresses. Zur Vermeidung klassischer Wahrnehmungsfehler vertiefen sie die Anwendung und Anpassung strukturierter Analysemethoden aus verschiedenen Wissenschaftsdisziplinen, darunter auch entscheidungstheoretischer Methoden zur Prognose des Entscheidungsverhaltens von Akteuren in Zielländern und Zielorganisationen nachrichtendienstlicher Analyse. In einer Ex-post-Perspektive werden Fälle nachrichtendienstlichen Scheiterns („Intelligence Failures“) und nachrichtendienstlicher Erfolge („Intelligence Successes“) analysiert und damit das Verständnis für Grenzen und Möglichkeiten der Intelligence Analysis vermittelt.

Literatur

- George, Roger Z./ Bruce, James B. (Hrsg.) Analyzing Intelligence: National Security Practitioners' Perspectives, 2014.
- Heuer, Richards J./ Pherson, Randolph H. (Hrsg.), Structured Analytic Techniques for Intelligence Analysis, 2015.
- Moore, David T., Critical Thinking and Intelligence Analysis, 2016. Heuer, Richards J., Psychology of Intelligence Analysis, 2013.
- Beebe, Sarah/ Pherson, Randolph H., Cases in Intelligence Analysis, Structured Analytic Techniques in Action, 2014.
- Lahneman, William J./ Arcos, Rubén, The Art of Intelligence, Simulations, Exercises and Games, 2014.
- Maddrell, Paul, The Image of the Enemy: Intelligence Analysis of Adversaries since 1945, 2015.
- Bar-Joseph, Uri/ McDermott, Rose, Intelligence Success and Failures, 2017.
- Wirtz, James J., Understanding Intelligence Failure, 2016.
- Tetlock, Philip E./ Gardner, Dan, Superforecasting: The Art and Science of Prediction, 2015.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer schriftlichen Prüfung von 180 Minuten, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Umgang mit Unsicherheit	3478

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. pol. Karl Morasch	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3478-V1	SE	Umgang mit Unsicherheit	Pflicht	2
3478-V2	UE	Übung zum Umgang mit Unsicherheit	Pflicht	2
Summe (Pflicht und Wahlpflicht)				4

Qualifikationsziele

Die Studierenden sollen ein grundsätzliches Verständnis der für den Umgang mit Unsicherheit zentralen entscheidungs- und spieltheoretischen Konzepte erlangen und befähigt werden, diese Konzepte auf gesellschaftliche und politische Fragestellungen anzuwenden.

Inhalt

Menschliches Entscheiden und Handeln findet grundsätzlich in einer Situation der Unsicherheit statt. Dies gilt auch dann, wenn im Vorfeld der Entscheidungen versucht wird, diese Unsicherheit durch Informationsgewinnung zu reduzieren.

Eine rationale Entscheidung unter Unsicherheit setzt voraus, dass die Konsequenzen der potentiellen Handlungsalternativen für alle verschiedene Szenarien bestimmt und die Wahrscheinlichkeiten für den Eintritt dieser möglichen Szenarien abgeschätzt werden. In der Veranstaltung werden zentrale Konzepte der Theorie rationalen Entscheidens vermittelt, wie beispielsweise das Erwartungsnutzenkonzept oder die Verwertung zusätzlicher Informationen mittels Bayes'schem Updating. Dabei werden sowohl normative Aspekte (wie sollte eine Entscheidung getroffen werden?) als auch positive Aspekte (wie werden Entscheidungen in der Realität tatsächlich getroffen?) berücksichtigt.

Gerade im Kontext politischen Handelns liegt zudem häufig strategische Unsicherheit vor, da die Ergebnisse vom Handeln mehrerer Akteure abhängig sind, die sich dieser Interaktion bewusst sind. Der in der Veranstaltung vermittelte Ansatz der Spieltheorie liefert ein geeignetes Instrumentarium zur systematischen Analyse solcher Interaktionen und zur Bestimmung der bestmöglichen Strategie für einen beteiligten Akteur. Zur Vereinfachung der Analyse wird dabei zunächst nur von strategischer Unsicherheit ausgegangen. In einem zweiten Schritt erfolgt dann eine Verknüpfung mit der Unsicherheit über Umweltzustände

und Eigenschaften der anderen Akteure, wie sie vorher im entscheidungstheoretischen Rahmen behandelt wurden.

An praktischen Beispielen wird aufgezeigt, wie die Entscheidungs- und spieltheoretischen Konzepte ein besseres Verständnis der Problemsituation ermöglichen und wie diese Konzepte im konkreten Fall angewendet werden können. Themenfelder sind dabei unter anderem die Bereitstellung öffentliche Güter, internationale Konflikte und Terrorismusbekämpfung.

Literatur

- Behnke, J. (2013), Entscheidungs- und Spieltheorie (Studienkurs Politikwissenschaft, Band 3761), Baden Baden: Nomos.
- Dixit, A.K., Skeath, S., Reiley, D. (2015), Games of Strategy, 4th ed., W.W. Norton: New York.
- Morasch, K., Bartholomae, F. W., Wiens, M. (2010), Spieltheoretische Grundkonzepte, wisu 39 (8#9), 1135#1140.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer schriftlichen Prüfung von 60 Minuten, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Intelligence and Cyber Security	3479

Konto	Pflichtmodule - MISS MA 2020
-------	------------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	

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, Kenntnisse über Aufbau und Funktionsweise von Rechnersystemen sowie Daten- und Rechnernetzen, wie sie in einem technischen Bachelor-Studium oder im Modul Digitalisierung vermittelt werden.

Qualifikationsziele

Das Modul vermittelt theoretische, praktische und anwendungsbezogene Kompetenzen, um Bedrohungen, Schwachstellen und Risiken bei der Informationsverarbeitung und -übertragung, insbesondere in einer vernetzten IT-Infrastruktur, zu erkennen und einzuschätzen. Die Studierenden lernen Verfahren und Methoden kennen, die zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen eingesetzt werden, und können die Leistungsfähigkeit und Grenzen dieser Verfahren beurteilen. 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. Die Studierenden kennen die grundlegenden Konzepte und Verfahren der angewandten Kryptographie und erlangen die Befähigung, diese sowie ausgewählte Sicherheitswerkzeuge exemplarisch einzusetzen und anzuwenden.

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 Randbedingungen 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, 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.

In der Lehrveranstaltung "Methoden der Cyber Security" wird 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, kryptographische 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. steganographische Techniken, Anonymisierungs- und Pseudonymisierungsverfahren sowie Onion Routing.

Inhaltliche Schwerpunkte der Wissensvermittlung sind:

- Grundlagen der IT-Sicherheit: Sicherheitsanforderungen, Schutzziele, Bedrohungen, Sicherheitsmaßnahmen
- Bedrohungen von IT-Systemen und Netzen: Malicious Software, Angriffszyklus, passive Angriffe, aktive Angriffe, Social Engineering, Bedrohungsanalyse
- Kryptographische Konzepte und Verfahren: Symmetrische vs. asymmetrische Verschlüsselung, Transport- vs. Ende-zu-Ende-Verschlüsselung, kryptographische Primitive und Protokolle, digitale Signaturen und Zertifikate, Perfect Forward Secrecy
- Methoden der Counter Intelligence: Anonymisierung, Mix Networks, Onion Routing, Steganographie
- Grundlagen der Netzwerksicherheit: Sicherheitsprotokolle, Firewalls, Intrusion Prevention, Intrusion Detection.

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 dieses Moduls legen die Grundlage für die Pflichtmodule der Vertiefungsrichtung „Cyber“.

Modulname	Modulnummer
Cyber Defence I	3480

Konto	Pflichtmodule der Vertiefungsrichtung "Cyber Defence" - MISS 2020
-------	---

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

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10107	VÜ	Sichere vernetzte Anwendungen	Pflicht	3
3480-V1	VÜ	Sichere Netze und Protokolle	Pflicht	4
3480-V2	VÜ	Hardware- und Betriebssystemsicherheit	Pflicht	3
Summe (Pflicht und Wahlpflicht)				10

Empfohlene Voraussetzungen
Die Inhalte des Moduls „Intelligence and Cyber Security“ werden vorausgesetzt.

Qualifikationsziele

Das Modul vermittelt Kompetenzen zur Analyse, Bewertung und Absicherung von IT-Infrastrukturen und deren Bestandteilen auf den drei komplementären Ebenen

1. einzelner Systeme (Hardware und Betriebssysteme),
2. darauf betriebener Anwendungen und
3. im Verbund von Rechnernetzen mit verschiedenen Übertragungsmedien und -protokollen.

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 Härtingsmaßnahmen und können Verfahren wie Penetration-Tests in der Praxis gezielt einsetzen. Die Studierenden sind in der Lage, Methoden zur Bewertung und Erhöhung der IT-Sicherheit in allen Lebenszyklusphasen der eingesetzten Hard- und Software anzuwenden.

Inhalt

Die Vorlesung "Sichere Netze und Protokolle" vermittelt Wissen über 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 werden

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.

In der Vorlesung Hardware- und Betriebssystemssicherheit erhalten Studierende einen vertieften Einblick in Fragestellungen der Systemsicherheit. Die Grundlage bildet ein Überblick über die Systemarchitekturen mit einem 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 Betriebssystemssicherheit werden klassische Sicherheitsprobleme von Betriebssystemen diskutiert. Ausgewählte Fallbeispiele zeigen die konkrete Umsetzung am Windows- und Linux-Kernel und dienen als Ausgangsbasis für die Vermittlung grundlegender Analyse- und Reverse-Engineering-Methoden zur Diskussion systemnaher Sicherheitslücken.

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.

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
- 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, 4. Auflage

Leistungsnachweis

Schriftliche Prüfung (120 Minuten) oder mündliche Prüfung (30 Minuten) oder kombinierte schriftlich-mündliche Leistungsnachweise mit Notenschein gemäß Prüfungsordnung. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

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. Sie lassen sich unmittelbar in der Masterarbeit anwenden.

Modulname	Modulnummer
Cyber Defence II	3481

Konto	Pflichtmodule der Vertiefungsrichtung "Cyber Defence" - MISS 2020
-------	---

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

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
3481-V1	VÜ	Data Science and Analytics	Pflicht	3
3481-V2	P	Security Engineering	Pflicht	4
Summe (Pflicht und Wahlpflicht)				10

Empfohlene Voraussetzungen
Die Inhalte des Moduls „Intelligence and Cyber Security“ werden vorausgesetzt.

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. 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 durch internationale Normen und Zertifizierungskriterien zu beurteilen und Maßnahmen zu planen, um identifizierte Defizite zu beseitigen. Sie haben praktische Erfahrungen im Betrieb von Systemen unter Sicherheitsaspekten gesammelt.

Inhalt

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.

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 Themen und Fragestellungen der Absicherung von IT-Systemen. Zu Beginn werden einfache Angriffe auf den Ebenen 2 bis 4 sowie 7 des ISO/OSI-Referenzmodells vorgestellt, bspw. durch die Manipulation von ARP oder Angriffe auf Webanwendungen. Entsprechende Gegenmaßnahmen werden untersucht und integriert, u.a. durch die Einrichtung von Firewalls, die Härtung von Webservern und den Betrieb sicherer Managementzugänge. 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, um deren Beiträge zur Absicherung der Infrastruktur bewerten zu können. 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 Virtualisierer und Disassembler werden zudem die Möglichkeiten der Forensischen Analyse von Betriebssoftware sowohl klassischer, als auch mobiler Endgeräte vorgestellt und anhand praktischer Beispiele durchgeführt.

Literatur

- Michael Brenner et al.: Praxisbuch ISO/IEC 27001, Hanser-Verlag, 3. Auflage, 2019
- Th. Harich, IT-Sicherheitsmanagement – Arbeitsplatz IT Security Manager, mitpProfessional Verlag, 2012

- Chris Eagle: „The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler“. No Starch Press, 2011, 2. Auflage
- Kris Kaspersky: „Hacker Disassembling Uncovered“. A-List Publishing, 2007, 2. Auflage
- Jon Erickson: „Hacking: Die Kunst des Exploits“. dpunkt Verlag, 2008, 2. Auflage

Leistungsnachweis

Schriftliche Prüfung (120 Minuten) oder mündliche Prüfung (30 Minuten) oder kombinierte schriftlich-mündliche Leistungsnachweise mit Notenschein gemäß Prüfungsordnung. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

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. Sie lassen sich unmittelbar in der Masterarbeit anwenden.

Modulname	Modulnummer
Verfassungsschutz in der wehrhaften Demokratie	3482

Konto	Pflichtmodule der Vertiefungsrichtung „Nachrichtendienste und öffentliche Sicherheit“ - MISS 2020
-------	---

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Gunter Warg	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3482-V1	VS	Verfassungsschutz i. d. w. D.	Pflicht	10
Summe (Pflicht und Wahlpflicht)				10

Qualifikationsziele
<p>In diesem Modul werden die Studierenden mit dem Konzept der wehrhaften Demokratie vertraut gemacht, erörtern dessen sicherheitspolitische Notwendigkeit und gesellschaftliche Akzeptanz und können daraus Anforderungen an die Wahrnehmung des Auftrags der Verfassungsschutzbehörden ableiten. Sie werden in die Lage versetzt, ein eigenständiges Rollen- und Selbstverständnis bzw. Profil des Verfassungsschutzes in der Sicherheitsarchitektur zu entwickeln bzw. zu schärfen und etwaige Alleinstellungsmerkmale eines Inlandsnachrichtendienstes im Vergleich zu „law enforcement agencies“ zu identifizieren. Dabei verstehen sie die unterschiedliche Rolle und Aufgaben von Polizeibehörden und Nachrichtendiensten und bewerten selbständig, ob und inwieweit eine organisatorische, funktionelle, befugnisrechtliche und informationelle Abgrenzung zur Polizei zeitgemäß und rechtsstaatlich geboten ist. Die Studierenden sollen in die Lage versetzt werden, innovative Ideen zur Stärkung der Prognose- und Analysefähigkeit der Verfassungsschutzbehörden zu entwickeln. Dabei sind sie sich den Möglichkeiten und Grenzen eines „Frühwarnsystems“ und seiner (in einer freiheitlichen Demokratie eingeschränkten) Einflussmöglichkeit in der Öffentlichkeit bewusst. Sie analysieren und reflektieren in diesem Zusammenhang kritisch die Möglichkeiten einer Einflussnahme auf das „gesellschaftliche Bewusstsein“ durch Öffentlichkeitsarbeit und andere Teilhabe am gesellschaftlichen Diskurs.</p> <p>Des Weiteren können die Studierenden den historisch gewachsenen Aufgabenkatalog der Verfassungsschutzbehörden beschreiben und mit Blick auf aktuelle sicherheitspolitische Herausforderungen auf etwaige Änderungsbedarfe (etwa mit Blick auf die Organisierte Kriminalität) – jeweils im Licht verfassungsrechtlicher Determinanten – bewerten. Sie haben ein Verständnis für die Notwendigkeit aufgabenadäquater Befugnisse und können die Möglichkeiten und Grenzen nachrichtendienstlichen Eingriffshandelns beschreiben. Sie sind in die Lage kritisch zu evaluieren, ob der rechtlich eingeräumte Handlungsspielraum im Angesicht terroristischer und sonstiger elementarer Bedrohungen (etwa aus dem</p>

Cyberraum) der Staatsaufgabe einer situationsangepassten Sicherheitsgewährleistung ausreichend gerecht wird.

Die Studierenden sind sich der Bedeutung sicherheitsbehördlicher Kooperationen bewusst und können die Notwendigkeit der Zusammenarbeit mit einzelnen Gefahrenabwehr- und Strafverfolgungsbehörden sowie Gerichten je nach Fallkonstellation eigenständig bewerten. Sie sind in der Lage, die geltenden Regeln des Informationsaustauschs zu beschreiben, anzuwenden und hinsichtlich ihrer Reichweite mit Blick auf verfassungsrechtliche bzw. verfassungsgerichtliche Vorgaben zu kontextualisieren. Die Frage, ob die Regeln über Amtshilfe bestimmte Formen der Zusammenarbeit bzw. Hilfeleistung ermöglichen und ggf. sogar Zuständigkeits- oder Befugnisschranken überwinden können, bewerten die Studierenden aufgrund eines profunden Wissens über Möglichkeiten und Grenzen der Amtshilfe eigenständig und können dies auf praktische Problemstellungen der behördenübergreifenden Zusammenarbeit innerhalb der „ND-Community“, aber auch zwischen Nachrichtendiensten und „law enforcement agencies“ anwenden. Die institutionellen und informellen Formen der Zusammenarbeit mit anderen Akteuren öffentlicher Sicherheit (etwa in Terrorismusabwehrzentren) sind den Studierenden bekannt. Auf alledem aufbauend entwickeln sie die Fähigkeit, über das (zeugenschaftliche) Einbringen nachrichtendienstlicher Erkenntnisse in offene behördliche und gerichtliche Verfahren eigenverantwortlich zu befinden und auf der Basis realitätsnaher Übungen mithilfe von Verfahrenssimulationen auch in öffentlichen Gerichtsverhandlungen anzuwenden.

Als übergreifende Fach- und Methodenkompetenz erlangen die Studierenden ein kritisches Bewusstsein der Grundrechtssensibilität aller nachrichtendienstlichen Handlungen. Die Einhegung sicherheitsbehördlicher Tätigkeit durch Grund- und Menschenrechte können sie erklären und auf einzelne praxisrelevante Fallgestaltungen (insbesondere bei der Anwendung nachrichtendienstlicher Mittel) anwenden. Durch Kenntnis der verfassungsschutzrelevanten Grundrechte können sie eigenständig prüfen, wann eine nachrichtendienstliche Tätigkeit grundrechtsrelevant ist und ein Eingriff verfassungsrechtlich gerechtfertigt bzw. nicht gerechtfertigt ist. So entwickeln sie ein rechtsstaatliches Problembewusstsein und eine praktische Handlungssicherheit, welche Maßnahmen (insbesondere mit Blick auf eine mögliche öffentliche, parlamentarische oder gerichtliche Bewertung) als zu eingriffssensibel bzw. nicht vertretbar einzuschätzen sind.

Inhalt

Die Bedrohungen durch Extremismus, Terrorismus und aus dem Cyberraum haben das Bewusstsein geschärft, dass Nachrichtendienste in einer vernetzten Sicherheitsarchitektur zusammen mit Polizei- und Strafverfolgungsbehörden einen wichtigen Anteil an der staatlichen Sicherheitsgewährleistung wahrnehmen und die Funktionsbedingungen einer freiheitlichen Gesellschaft schützen. Darüber hinaus sehen sie sich in Bezug auf gesamtstaatliche Bedrohungen als „Frühwarnsysteme“ und „Informationsdienstleister“ für Politik und Gesellschaft. Das Modul „Verfassungsschutz in der wehrhaften Demokratie“ adressiert die gesamte Bandbreite der Teilhabe von Nachrichtendiensten an der Gewährleistung der inneren Sicherheit. Es richtet sich daher im Schwerpunkt an Studierende aus den Verfassungsschutz-behörden des Bundes und der Länder (einschließlich BAMAD) sowie aus den Polizeibehörden, bietet darüber hinaus jedoch auch für künftige Beschäftigte anderer Sicherheitsbehörden breite Einblicke in zentrale aktuelle

Themen der inneren Sicherheit. Im Mittelpunkt stehen rechtliche und rechtspolitische Fragen im Zusammenhang mit der Tätigkeit der Verfassungsschutzbehörden. Da letztere zur Informationsverarbeitung in vielfacher Hinsicht in Grundrechte eingreifen, sind Fragen nach bedarfsgerechten und rechtsstaatskonformen gesetzlichen Grundlagen ebenso zu adressieren wie politische Grundbedingungen des Verfassungsschutzes, insbesondere nach Aktualität und Akzeptanz des Konzepts einer „wehrhaften Demokratie“ sowie der Zulässigkeit einer Einwirkung des Verfassungsschutzes auf den gesellschaftliche Diskurs. Von besonderer Bedeutung sind phänomenologische Zugänge und damit der Blick auf die aktuellen Bedrohungslagen in den Bereichen Islamismus, Rechts- und Linksextremismus, säkularer Ausländerextremismus sowie der staatlichen Spionage einschließlich der unerlaubten ausländischen Einflussnahme (s. dazu auch das Modul „Politischer Extremismus“). Die Entwicklungen in allen Beobachtungsfeldern des Verfassungsschutzes (z.B. Radikalisierungstendenzen einschließlich politisch motivierter Straftaten, Wirtschaftsspionage, Bedrohungen aus dem Cyberraum) werden in Bezug zur aktuellen Gesetzeslage gesetzt und die behördliche Praxis daraufhin reflektiert, ob Aufgaben- und Befugnisregeln den jeweiligen Herausforderungen gerecht werden. Auch ist grundlegend die Frage aufzuwerfen, welche Funktion Nachrichtendiensten bei der Gewährleistung der öffentlichen Sicherheit überhaupt zukommen soll und ob ihre Tätigkeit im Vergleich mit anderen Sicherheitsbehörden Alleinstellungsmerkmale aufweist, die ihnen einen indisponiblen Mehrwert bei der Sicherheitsgewährleistung verschafft.

Literatur

- Fleischer, Dirk, Wirtschaftsspionage: Phänomenologie – Erklärungsansätze – Handlungsoptionen, 2016.
- Schwind, Hans-Dieter, Kriminologie und Kriminalpolitik, 2016.
- Allum, Felia/Gilmour, Stan, Routledge Handbook of Transnational Organized Crime, 2015.
- Droste, Bernadette, Handbuch des Verfassungsschutzrechts, 2007.
- Möller/Warg, Allgemeines Polizei- und Ordnungsrecht, 2011.
- Sinn, Arndt, Organisierte Kriminalität 3.0, 2016
- Dietrich, Jan-H./Sven Eiffler (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017.
- Sule, Satish, Spionage – Völkerrechtliche, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage, 2006.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer mündlichen Prüfung von 30 Minuten Dauer, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Politischer Extremismus	3483

Konto	Pflichtmodule der Vertiefungsrichtung „Nachrichtendienste und öffentliche Sicherheit“ - MISS 2020
-------	---

Modulverantwortliche/r	Modultyp	Empf. Trimester
N.N.	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3483-V1	VS	Politischer Extremismus	Pflicht	10
Summe (Pflicht und Wahlpflicht)				10

Qualifikationsziele
Die Studierenden sollen über das reine Faktenwissen zu extremistischen Bestrebungen hinaus diese als politische Akteure in unterschiedlichen Kontexten wahrnehmen. Den vergleichenden Blick auf die Besonderheiten von Ideologie, Organisation, Strategie und Wirkung gilt es so zu schärfen. Dadurch können bezüglich der Aufgabe eines Frühwarnsystems sowohl Gefahrenpotentialeinschätzungen wie Prognosen systematischer vorgenommen werden.
Inhalt
Auf der Grundlage von bisherigem Basiswissen über den Linksextremismus, Rechtsextremismus (incl. der Erscheinungsformen mit Migrationshintergrund) und Islamismus bzw. Djihadismus in Deutschland werden Methoden der vergleichenden Extremismus-forschung hinsichtlich der Analyse der gemeinten Phänomene vermittelt. Dabei geht es insbesondere um eine Betrachtung entlang des E-IO-S-W-Schemas, wobei nach Extremismusintensität, Ideologie, Organisation und Wirkung gefragt wird. Der systematische Blick soll dabei auf Gemeinsamkeiten und Unterschiede fallen. Erst die so feststellbaren Besonderheiten erlauben eine genaue Beschreibung und Einschätzung der untersuchten Phänomene. Es soll darüber hinaus um deren Bedeutung im jeweiligen Extremismus und in der Gesamtgesellschaft gehen. Bei all dem geht es auch um Einschätzungen des Gefahrenpotentials und Prognosemöglichkeiten zu Verlaufsformen.
Literatur
<ul style="list-style-type: none"> • Backes, Uwe, Politischer Extremismus in demokratischen Verfassungsstaaten. Elemente einer normativen Rahmentheorie, 1989. • Backes, Uwe/Jesse, Eckhard, Politischer Extremismus in der Bundesrepublik Deutschland, 1994. • Backes, Uwe/Jesse, Eckhard (Hrsg.), Jahrbuch Extremismus & Demokratie 1989 ff. • Jesse, Eckhard (Hrsg.), Handbuch Extremismusforschung 2017 i. E.

- Kandel, Johannes, Islamismus in Deutschland. Zwischen Panikmache und Naivität, 2011.
- Möllers, Martin H. W./Van Ooyen, Robert Chr. (Hrsg.), Jahrbuch Öffentliche Sicherheit 2002 ff.
- Pfahl-Traughber, Armin, Linksextremismus in Deutschland. Eine kritische Bestandsaufnahme, 2014.
- Pfahl-Traughber, Armin, Rechtsextremismus in Deutschland. Eine kritische Bestandsaufnahme, 2018 i.E.
- Pfahl-Traughber, Armin (Hrsg.), Jahrbuch für Extremismus- und Terrorismusforschung 2008 ff.
- Seidensticker, Tilman, Islamismus. Geschichte, Vordenker, Organisationen, 2014.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit von 5000 Wörtern, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Advanced Intelligence Collection and Analysis	3484

Konto	Pflichtmodule der Vertiefungsrichtung „Terrorismusbekämpfung“ - MISS 2020
-------	---

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Markus Denzler	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3484-V1	VS	Advanced Intelligence Collection and Analysis	Pflicht	10
Summe (Pflicht und Wahlpflicht)				10

Qualifikationsziele
Im Mittelpunkt des Moduls stehen intelligence-spezifische Methoden mit Bedeutung für die nachrichtendienstliche Praxis (z.B. Methoden des „Targeting“ und „Profiling“). Die Studierenden vertiefen ihre zuvor erworbenen Kenntnisse am Beispiel von Erscheinungsformen des globalen Terrorismus, so dass sie nicht nur in der Lage sind, Vorgänge und Ansätze in der Praxis zu reflektieren. Vielmehr sind sie gleichzeitig auf der Basis eines intensiven Theorie-Praxis-Dialogs in der Lage, neue Methoden für die Praxis zu entwickeln und auf ihre Tauglichkeit hin zu überprüfen.
Inhalt
Die Studienkonzentration „Terrorismus und Terrorismusbekämpfung“ richtet sich insbesondere an Studierende, die für eine anschließende Verwendung im Bereich der Terrorismus-aufklärung vorgesehen sind. Im Mittelpunkt des Moduls „Advanced Intelligence Collection and Analysis (Geheim)“ stehen intelligence-spezifische Methoden mit Bedeutung für die nachrichtendienstliche Praxis (z.B. Methoden des „Targeting“ und „Profiling“). Im Modul erhalten die Studierenden die Möglichkeit, nicht nur ihre methodenspezifischen Kenntnisse aus vorangegangenen Modulen zu vertiefen und auf Erscheinungsformen des globalen Terrorismus zu beziehen, sondern gleichzeitig Fragestellungen und Probleme der nachrichtendienstlichen Praxis unter der Anleitung der Lehrenden im Sinne forschenden Lernens selbst zu untersuchen und einer Lösung zuzuführen. Auf diese Weise sollen methodisch begründete Impulse für die Praxis erzielt werden. Insoweit versteht sich das Modul als Fortführung der Vermittlung intelligence-spezifischer Methodologie. Das Modul greift z.T. auf eingestuftes VS-Material zurück und bedingt ein vertieftes Verständnis der Anwendung nachrichtendienstlicher Methoden. Daher kann der Zugang zu diesem Modul nur einem eingeschränkten Kreis der Studierenden ermöglicht werden. Übrige Studierende sind gehalten, andere Studienkonzentrationen zu belegen.

Literatur

- Clark, Robert M., Intelligence Analysis: A target-centric approach, 2016.
- Heuer, Richards J., Psychology of Intelligence Analysis, 2013.
- Beebe, Sarah/Pherson, Randolph H., Cases in Intelligence Analysis, Structured Analytic Techniques in Action, 2014.
- Moore, David T., Critical Thinking and Intelligence Analysis, 2016.
- Huddy, Leonie/Sears, David O./Levy, Jack S. (Hrsg.), The Oxford Handbook of Political Psychology, 2013.
- Heuer, Richards J./Pherson, Randolph H. (Hrsg.), Structured Analytic Techniques for Intelligence Analysis, 2014.
- Hall, Wayne Michael/Citrenbaum, Gary, Intelligence Collection, 2012.
- Lowenthal, Mark M./Clark, Robert M., The Five Disciplines of Intelligence Collection, 2015.
- Bloom, Richard, Foundations of Psychological Profiling: Terrorism, Espionage, and Deception, 2013.
- Tetlock, Philip/Gardner, Dan, Superforecasting: The Art and Science of Prediction, 2015.
- Fischhoff, Baruch/Chauvin, Cherie (Hrsg.), Intelligence Analysis: Behavioral and Social Scientific Foundations, 2011.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit von 5000 Wörtern, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Terrorismusforschung	3485

Konto	Pflichtmodule der Vertiefungsrichtung „Terrorismusbekämpfung“ - MISS 2020
-------	---

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Christian Haas	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3485-V1	VS	Terrorismusforschung	Pflicht	10
Summe (Pflicht und Wahlpflicht)				10

Qualifikationsziele
Die Teilnehmerinnen und Teilnehmer des Moduls verfügen über vertiefte Kenntnisse von verschiedenen Erscheinungsformen des internationalen Terrorismus und können verschiedene Terrorstrategien einordnen. Sie besitzen ein besonderes Verständnis von Radikalisierungsprozessen und können terroristische Propagandamittel und ihre Wirkung analysieren. Die Studierenden sind mit den nationalen und internationalen Instrumentarien der Terrorismusbekämpfung vertraut und haben ein Bewusstsein für ihre rechtlichen und ethischen Grenzen entwickelt. Auf dieser Basis können sie Strategien der Terrorismusbekämpfung – inklusive des zugehörigen nachrichtendienstlichen Beitrags – auf ihre Wirksamkeit hin kritisch überprüfen und bewerten.
Inhalt
Das Modul verbindet Erkenntnisse, Methoden und Perspektiven aus verschiedenen Wissenschaftsdisziplinen zum Gesamtphänomen Terrorismus und Terrorismusbekämpfung. Wesentliche Inhalte sind: Entstehung, Phänomenologie und Historie terroristischer Gruppierungen, Analyse terroristischer Netzwerke, Ideologien und Strategien terroristischer Gruppierungen, Radikalisierungsprozesse von Einzelpersonen und Mittel zur Rekrutierung bzw. Propaganda, rechtliche Rahmenbedingungen der Terrorismusbekämpfung, Strategien zur Terrorismusbekämpfung, Analyse von Bedrohungspotenzialen, Aufklärung von Anschlägen, Beitrag von Nachrichtendiensten zur Terrorismusbekämpfung, Wege zur Deradikalisierung. Die organisatorischen und ideologischen Erscheinungsformen des jihadistisch motivierten Terrorismus stehen hierbei im Mittelpunkt, gleichzeitig soll jedoch der Blick auf nicht-jihadistische Formen des Terrorismus gewahrt bleiben. Die Studierenden sollen mit Kenntnis der unterschiedlichen Wissenschaftsperspektiven Methoden und Strategien der Terrorismusaufklärung und Terrorismusbekämpfung im Zusammenspiel der Sicherheitsbehörden im demokratischen Rechtsstaat kennenlernen, vertieft reflektieren und zielgerichtet anwenden können.
Literatur
<ul style="list-style-type: none"> • Armbrorst, Andreas, Jihadi Violence. A Study of al-Qaeda's Media, 2012. • Chalk, Peter (Hrsg.), Encyclopedia of Terrorism, 2013.

- Graulich, Kurt/Simon, Dieter (Hrsg.), Terrorismus und Rechtsstaatlichkeit, 2009.
- Harmon et al., Christopher C. (Hrsg.), Toward a Grand Strategy against Terrorism, 2011.
- Hoffman, Bruce, Inside Terrorism, 2006.
- Horgan, John, The Psychology of Terrorism, 2014.
- Johnson, Loch K. (Hrsg.), Strategic Intelligence: Counterintelligence and Counterterrorism, 2007.
- Koomen, Willem/Pligt, Joop van der, The Psychology of Radicalization and Terrorism, 2015.
- Mobley, Blake W., Terrorism and Counterintelligence, 2012.
- Neumann, Peter, Die neuen Dschihadisten: IS, Europa und die nächste Welle des Terrorismus, 2015.
- Sageman, Marc, Leaderless Jihad: Terror Networks in the Twenty-First Century, 2008.
- Said, Behnam T., Islamischer Staat: IS-Miliz, al-Qaida und die deutschen Brigaden, 2014.
- Schmidt, Alex P. (Hrsg.), The Routledge Handbook of Terrorism Research, 2011.
- Silke, Andrew, The Psychology of Counter-Terrorism, 2010.
- Urban, Johannes, Die Bekämpfung des Internationalen Islamistischen Terrorismus, 2006.
- Wenger, Andreas/Wilner, Alex (Hrsg.), Deterring Terrorism: Theory and Practice, 2012.
- Pearse, John (Hrsg.), Investigating Terrorism: Current Political, Legal, and Psychological Issues, 2015.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit von 5000 Wörtern, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Regionale Sicherheit I	3486

Konto	Pflichtmodule der Vertiefungsrichtung „Regionale Sicherheit“ - MISS 2020
-------	--

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Martin Wagener	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3486-V1	VS	Regionale Sicherheit I	Pflicht	10
Summe (Pflicht und Wahlpflicht)				10

Qualifikationsziele
Die Studierenden vertiefen ihre Kenntnisse in Bezug auf die Außen- und Sicherheitspolitik Ostasiens. Auf dieser Grundlage können sie das Zustandekommen außenpolitischer Entscheidungen und das Verhalten der daran beteiligten Akteure erklären und kritisch hinterfragen. Methodengeleitet können sie Modelle zukünftiger regionaler Entwicklungen generieren, die zu einer konkreten Bedrohung deutscher Interessen werden können.
Inhalt
Die Studienkonzentration „Regionale Sicherheit“ bezieht sich auf geographische Regionen der Welt mit Bedeutung für die deutsche Außen- und Sicherheitspolitik. Die Studierenden erhalten vertiefte Einblicke in geschichtliche, wirtschaftliche, kulturelle und politische Zusammenhänge und sind in der Lage, Bezüge zu außen- und sicherheitspolitischen Interessen der Bundesrepublik herzustellen. Auf diese Weise sollen regionale und globale Konfliktdynamiken nicht nur richtig eingeschätzt, sondern auch interregional aufeinander bezogen werden können. Das Modul „Regional Security I“ widmet sich aktuellen außen- und sicherheitspolitischen Entwicklungen im asiatischen Raum. Ein besonderes Augenmerk gilt dabei der Rolle Chinas als sicherheitspolitischem Akteur. Dabei werden z.B. die chinesisch-japanischen Beziehungen und die Taiwan-Frage in den Blick genommen. Zudem werden die Situation auf der koreanischen Halbinsel sowie neuere Ansätze eines strategischen Regionalismus thematisiert.
Literatur
<ul style="list-style-type: none"> • Inkster, Nigel, China's Cyber Power, 2016. • Heginbotham, Eric, The U.S.-China Military Scorecard. Forces, Geography, and the Evolving Balance of Power 1996-2017, 2015. • Swaine, Michael D. u.a., Conflict and Cooperation in the Asia-Pacific Region: a strategic assessment, 2015.

- Shambaugh, David, Tangled Titans. The United States and China, Lanham – Plymouth 2013.
- Wagener, Martin, Hegemonialer Wandel in Südostasien? Der machtpolitische Aufstieg Chinas als sicherheitsstrategische Herausforderung der USA, 2009.

Leistungsnachweis

Der Leistungsnachweis besteht aus einer Seminararbeit von 5000 Wörtern, die mit mindestens der Note 4,0 bestanden sein muss.

Modulname	Modulnummer
Regionale Sicherheit II	3487

Konto	Pflichtmodule der Vertiefungsrichtung „Regionale Sicherheit“ - MISS 2020
-------	--

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Martin Wagener	Pflicht	

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3487-V1	SE	Regionale Sicherheit II	Pflicht	10
Summe (Pflicht und Wahlpflicht)				10

Qualifikationsziele

Die Studierenden erhalten vertiefte Kenntnisse über außen- und sicherheitspolitische Entwicklungen in Osteuropa sowie die ihnen zugrundeliegenden historisch-kulturellen, sozioökonomischen und innenpolitischen Determinanten. Das Modul fokussiert dabei auf den postsowjetischen Raum mit besonderer Beachtung Russlands, zieht bei Bedarf aber auch Entwicklungen in Mittelost- und Südosteuropa heran.

Das Modul baut auf der Kenntnis grundlegender Theorien und Ansätze der „Internationalen Beziehungen“ auf, erweitert und vertieft diese aber um zentrale Aspekte der „Security Studies“ und „Regional Studies“. Die Studierenden werden befähigt, die Theorien, Ansätze und Konzepte auf Themenkomplexe der regionalen Sicherheit in Osteuropa anzuwenden und dadurch außen- und sicherheitspolitische Prozesse (z.B. Entscheidungsprozesse, Konfliktodynamiken) und Strukturen (z.B. Akteurs- und Konfliktkonstellationen, Institutionengefüge) zu analysieren. Darüber hinaus sollen die Studierenden in der Lage sein, zentrale Herausforderungen zu identifizieren, die sich aus der Region heraus für deutsche und europäische Politik ergeben, sowie die Kosten und Nutzen verschiedener Handlungsoptionen kritisch zu bewerten.

Inhalt

Im Fokus des Moduls stehen die Außen- und Sicherheitspolitik der regionalen Akteure sowie die regionalen und internationalen Strukturen, innerhalb derer sie agieren. Sicherheitspolitik wird dabei in einem umfassenden Sinn verstanden. Neben der militärischen Dimension von Sicherheit (z.B. Bedrohungspotentiale und -perzeptionen, Rüstungskontrolle und Abrüstung, „hybride Kriege“) werden daher auch die ökonomische (z.B. Energiesicherheit), menschliche (z.B. Rechtstaatlichkeit, Minderheiten) und gesellschaftlich-politische Dimension (z.B. Regimesicherheit, Elitenkonflikte und Protestbewegungen) regionaler Sicherheit behandelt. Einen weiteren Fokus bildet die Analyse der zahlreichen sicherheitspolitischen Konflikte in Osteuropa sowie ihrer Ursachen und Dynamiken – von ethnoterritorialen (z.B. Tschetschenien, Abchasien)

über zwischenstaatliche (z.B. Georgienkrieg, Krim-Annexion) bis hin zu regionalen Ordnungskonflikten (z.B. über die Ausgestaltung der europäischen Sicherheitsordnung). Das Modul bettet die Außen- und Sicherheitspolitik Osteuropas dabei in den breiteren internationalen Kontext ein. Im Rahmen dessen werden sowohl die Einflüsse von NATO und EU als auch externer Akteure (USA und China) und globaler Kräfteverschiebungen auf die regionale Sicherheit als auch die Implikationen regionaler Entwicklungen auf internationale Sicherheit kritisch beleuchtet.

Literatur

- Tsygankov, Andrei, *Russia's Foreign Policy: Change and Continuity in National Identity*, 2016.
- Alpern Engel, Barbara/Martin, Janet, *Russia in World History*, 2015.
- Hill, Fiona/ Gaddy, Clifford G., *Mr. Putin: Operative in the Kremlin*, 2015.
- Charap, Samuel/Colton, Timothy J., *Everyone Loses. The Ukraine Crisis and the Ruinous Contest for Post-Soviet Eurasia*, 2017.
- Zürcher, Christoph, *The Post-Soviet Wars: Rebellion, Ethnic Conflict, and Nationhood in the Caucasus*, 2007.
- Trenin, Dmitri, *Should we fear Russia?* 2016.
- Oliker, Olga u.a., *Russian Foreign Policy. Sources and Implications*, 2009.
- Stent, Angela E., *The Limits of Partnership: US Russian Relations in the Twenty-First Century*. 2015.

Empfehlungen:

- Dima Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy*, 2015.
- John Baylis/ James J. Wirtz/ Colin S. Gray, *Strategy in the Contemporary World: an Introduction to Strategic Studies*, 5th edition 2016.
- Sabine Fischer, *Nicht eingefroren! Die ungelösten Konflikte um Transnistrien, Abchasien, Südossetien und Berg-Karabach im Lichte der Krise um die Ukraine*, 2016.
- Keir Giles, *Moscow Rules. What Drives Russia to Confront the West*, 2019.
- International Institute for Strategic Studies (ed.), *Military Review* 2019, 2019.
- Roger Kanet (ed.), *The Russian Challenge to the European Security Environment*, 2017.
- Roger Kanet (ed.), *Routledge Handbook of Russian Security*, 2019.
- Margarete Klein, *Russlands Militärpolitik im postsowjetischen Raum. Ziele, Instrumente und Perspektiven*, 2018.
- Gudrun Persson/ Carolina Vendil Pallin/ Tommy Jeppsson (eds.), *Military Thinking in the 21st Century*, 2015.
- Nicu Popescu/ Stanislav Secrieu (eds.), *Third Powers in Europe's East*, 2018.
- Siegfried Schieder/Manuela Spindler (Hrsg.), *Theories of International Relations*, Abingdon 2014.
- Dmitrij V. Trenin, *European Security: from managing adversity to a new equilibrium*, 2018.
- Andrei Tsygankov, *Routledge handbook of Russian foreign policy*, 2018.

Fachzeitschriften:

- Belarusanalysen
- Communist and Post-Communist Studies
- Europe-Asia Studies
- Jane´s Intelligence Review
- Journal of Slavic Military Studies
- New eastern europe
- Osteuropa
- Russian Analytical Digest
- Russlandsanalysen
- Ukraineanalysen
- Voennaja Mysl´/Military Thought (Zeitschrift des russischen Verteidigungsministeriums)
- Zentralasienanalysen
- Weblinks:
- <https://thebulletin.org/> (Bulletin of Atomic Scientists)
- <https://jamestown.org/programs/edm/> (Eurasia Daily Monitor der Jamestown Foundation, USA; Artikelsammlung zu Osteuropa/Eurasien)
- <https://www.hybridcoe.fi/> (The European Centre of Excellence for Counterin Hybrid Threats, Helsinki)
- <https://www.foi.se/en/foi.html> (Swedish Defence Research Agency, Stockholm)
- <https://inmoscowsshadows.wordpress.com/> (Blog von Mark Galeotti)
- <http://www.ponarseurasia.org/> (PONARS Eurasia: Artikel zu (Sicherheits)politik in Osteuropa)
- <https://russiamil.wordpress.com/author/gorenbur/> (Blog von Dmitry Gorenburg)
- <https://www.russiamatters.org/> (Linksammlung von Simon Saradzhyan von Belfer Centre in Harvard, USA)
- <http://russianforces.org/podvig/> (Russian Forces: Blog von Pavel Podvig zur Nuklearwaffenpolitik Russlands)
- <https://www.sipri.org/> (Stockholm International Peace Research Institute)
- <https://www.osw.waw.pl/en> (Centre for Eastern Studies, Warschau)
- [www. swp-berlin.org](http://www.swp-berlin.org) (Stiftung Wissenschaft und Politik, Berlin)
- [fondation pour la recherche strategique](http://www.fondationpourlarecherche.org)
- [iiss](http://www.iiss.org)
- [ifri](http://www.ifri.org)
- [dgap](http://www.dgap.org)
- [nupi](http://www.nupi.org)
- [ecfr](http://www.ecfr.eu)
- [kennan institute](http://www.kennaninstitute.org)
- [carnegie](http://www.carnegie.org)
- [hsfk](http://www.hsfk.org)
- <https://warontherocks.com> (War on the Rocks)

Leistungsnachweis

Als benoteter Leistungsnachweis wird von der Dozentin eine von drei Möglichkeiten festgelegt: eine Hausarbeit (5000 Wörter), ein Referat mit Arbeitsskizze und Kurzesay oder eine Klausur mit einer Länge von 180 Minuten. Für ein Bestehen ist mindestens die Note 4,0 zu erreichen. Welche der drei Formen des Leistungsnachweises für den jeweiligen Durchgang gewählt wird, erfahren die Seminarteilnehmer rechtzeitig. Über den benoteten

Leistungsnachweis hinaus werden nicht benotete Arbeitsaufträge erteilt, die erfüllt und bestanden werden müssen. Im Modul herrscht Anwesenheitspflicht.

Modulname	Modulnummer
Master-Arbeit	3488

Konto	Master-Arbeit - MISS 2020
-------	---------------------------

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. rer. nat. Uwe M. Borghoff	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
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.
Dauer und Häufigkeit
Das Modul dauert sechs Monate und beginnt im Juli des zweiten 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 2020		75
	1	3468	Einführung in Intelligence and Security Studies	J. Dietrich	10
	1	3469	Menschenrechte und Sicherheit in normativer Perspektive	C. Binder	10
	1	3470	Digitalisierung	L. Schmitz	10
		3471	Theoretische Zugänge und Methoden der Intelligence and Security Studies	J. Dietrich	5
	0	3472	Intelligence Governance	S. Fischer	5
		3473	Intelligence Collection	M. Denzler	5
		3474	Globale Bedrohungen und Herausforderungen	C. Masala	5
		3475	Kommunikation und Führung in den Nachrichtendiensten	R. Jokiel	3
		3476	Intelligence Accountability	J. Dietrich	5
		3477	Intelligence Analysis	C. Haas	5
		3478	Umgang mit Unsicherheit	K. Morasch	5
		3479	Intelligence and Cyber Security	S. Pickl	7
		8	Pflichtmodule der Vertiefungsrichtung "Cyber Defence" - MISS 2020		20
	2	3480	Cyber Defence I	W. Hommel	10
	2	3481	Cyber Defence II	W. Hommel	10
		9	Pflichtmodule der Vertiefungsrichtung „Nachrichtendienste und öffentliche Sicherheit“ - MISS 2020		20
		3482	Verfassungsschutz in der wehrhaften Demokratie	G. Warg	10
		3483	Politischer Extremismus	N. N.	10
		10	Pflichtmodule der Vertiefungsrichtung „Terrorismusbekämpfung“ - MISS 2020		20
		3484	Advanced Intelligence Collection and Analysis	M. Denzler	10
		3485	Terrorismusforschung	C. Haas	10
		11	Pflichtmodule der Vertiefungsrichtung „Regionale Sicherheit“ - MISS 2020		20
		3486	Regionale Sicherheit I	M. Wagener	10
		3487	Regionale Sicherheit II	M. Wagener	10
		12	Master-Arbeit - MISS 2020		25
		3488	Master-Arbeit	U. Borghoff	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
	3468-V3	Einführung in Intelligence Studies	Übung	Pf	2
	3470-V2	Praktikum zur Digitalisierung	Praktikum	Pf	4
	3471-V1	Intelligence and Security Studies als wissenschaftlicher Ansatz	Vorlesung/Seminar	Pf	4
	3471-V2	Wissenschaftliches Arbeiten	Seminar	Pf	2
	3472-V1	Einführung in Intelligence Governance	Vorlesung	Pf	2
0	3472-V2	Intelligence Governance – Analyse und Diskussion empirischer Beispiele sowie ausgewählte Probleme des Rechts der Nachrichtendienste	Übung	Pf	2
	3472-V3	Intelligence Governance in Practice	Seminar	Pf	2
	3473-V1	Intelligence Collection	Vorlesung/Seminar	Pf	2
	3473-V2	Intelligence Collection – Aktuelle Herausforderungen in der Praxis	Seminar	Pf	2
	3473-V3	Intelligence Collection - Ringvorlesung	Vorlesung/Seminar	Pf	2
	3474-V1	Kriegsursachenforschung, Asymmetrische, ethnische und hybride Konflikte, moderner Krieg und Staatszerfall	Seminar	Pf	3
	3475-V1	Führung in den Nachrichtendiensten	Seminar	Pf	2
	3475-V1	Grundlagen in Kommunikation und Führung	Vorlesung	Pf	2
	3475-V3	Kommunikation und Präsentation	Übung	Pf	2
	3476-V1	Ideengeschichtliche Grundlagen der Rechenschaftspflicht von Nachrichtendiensten	Vorlesung	Pf	2
	3476-V2	Entwicklung der ‚Intelligence Accountability‘ in der BRD	Vorlesung	Pf	2
	3476-V 3a	Ethik der nachrichtendienstlichen Tätigkeit	Seminar	WPf	2
	3476-V 3b	Nachrichtendienste und Massenmedien seit 1945	Seminar	WPf	2
	3476-V 3c	Gegen den ‚inneren Feind‘: Spionageabwehr in Demokratie und Diktatur	Seminar	WPf	2
	3477-V1	Grundlagen der Intelligence Analysis	Vorlesung	Pf	2
	3477-V2	Technik und Methodik der Intelligence Analysis	Übung	Pf	2
	3477-V3	Umgang mit Unsicherheit	Seminar	Pf	2
	3478-V1	Umgang mit Unsicherheit	Seminar	Pf	2
	3478-V2	Übung zum Umgang mit Unsicherheit	Übung	Pf	2
	3479-V1	Intelligence	Vorlesung	Pf	4
	3479-V2	Methoden der Cyber Security	Vorlesung	Pf	2
	3479-V3	Methoden der Cyber Security	Übung	Pf	1
	3481-V2	Security Engineering	Praktikum	Pf	4
	3482-V1	Verfassungsschutz i. d. w. D.	Vorlesung/Seminar	Pf	10
	3483-V1	Politischer Extremismus	Vorlesung/Seminar	Pf	10
	3484-V1	Advanced Intelligence Collection and Analysis	Vorlesung/Seminar	Pf	10
	3485-V1	Terrorismusforschung	Vorlesung/Seminar	Pf	10

	3486-V1	Regionale Sicherheit I	Vorlesung/Seminar	Pf	10
	3487-V1	Regionale Sicherheit II	Seminar	Pf	10
	3488-V1	Master-Arbeit	Projekt	Pf	,
	5544-V1	Ostasien und die Theorien der Internationalen Beziehungen	Vorlesung	Pf	2
	5544-V2	Die Geschichte Ostasiens sowie ihre Bedeutung für die Gegenwart	Seminar	Pf	1
	5544-V3	Die Interessen der Großmächte Ostasiens	Vorlesung	Pf	2
	5544-V4	Die Konflikte Ostasiens	Seminar	Pf	1
	5544-V5	Gastvorträge aus der Praxis	Seminar	Pf	1
	5544-V6	Politikberater in Ostasien	Übung	Pf	1
	5544-V7	Konkurrierende Ideen zur Sicherheitsarchitektur Ostasiens	Vorlesung	Pf	1
	5544-V8	Vorbereitung auf die Erstellung einer Masterarbeit	Übung	Pf	1
1	3468-V1	Einführung in Intelligence and Security Studies	Seminar	Pf	2
1	3468-V2	Einführung in Intelligence History	Seminar	Pf	2
1	3469-V1	Der moderne Staat: Zwischen Freiheitsnorm und einer Ethik der Sicherheit	Vorlesung/Seminar	Pf	2
1	3469-V2	Grundrechte, Menschenrechte und modernes Sicherheitsrecht	Vorlesung/Übung	Pf	2
1	3469-V3	Einführung in das Recht der Nachrichtendienste	Vorlesung/Übung	Pf	2
1	3470-V1	Digitalisierung	Vorlesung/Seminar	Pf	4
2	10106	Sicherheitsmanagement	Vorlesung/Übung	Pf	3
2	10107	Sichere vernetzte Anwendungen	Vorlesung/Übung	Pf	3
2	3480-V1	Sichere Netze und Protokolle	Vorlesung/Übung	Pf	4
2	3480-V2	Hardware- und Betriebssystemsicherheit	Vorlesung/Übung	Pf	3
2	3481-V1	Data Science and Analytics	Vorlesung/Übung	Pf	3

