



# Karrierperspektiven

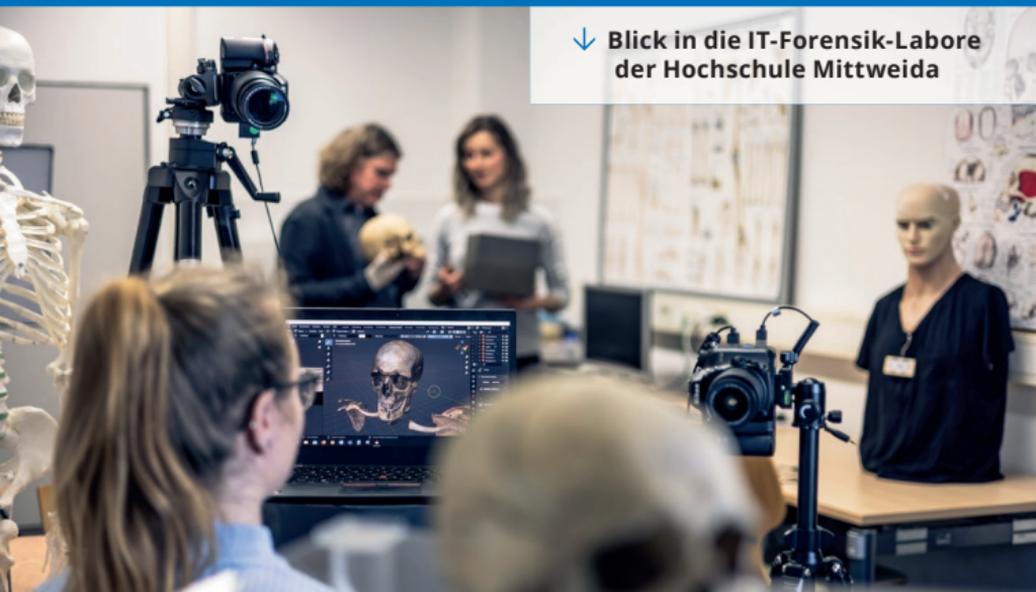
Gefragte Spezialist:innen in der Wirtschaft, bei Polizei und Kriminalämtern.

Die Berufsperspektiven für alle, die Cyber-Kriminalität aufklären oder verhindern wollen, sind extrem spannend. Angesichts aggressiver Handlungen von staatlichen Akteur:innen und individuellen Cyber-Kriminellen bauen Staat und Wirtschaft ihre Anstrengungen aus, um deren Angriffe abzuwehren oder zumindest aufzuklären.

Spezialist:innen werden von Unternehmen und Behörden mit Hochdruck gesucht, wobei an verschiedensten Wissenschaftseinrichtungen intensiv an Mitteln zur Gefahrenabwehr und Verbrechensaufklärung geforscht wird – unter anderem an der Hochschule Mittweida. Absolvent:innen des Studiengangs Cybercrime/Cybersecurity arbeiten folglich unter anderem an

- der Ermittlung von Straftäter:innen für die Polizei,
- der Abwehr von hybriden Angriffen auf kritische Infrastruktur für BKA, LKA und Bundeswehr,
- der Verhinderung von Angriffen auf Unternehmen,
- der Erforschung von wirksamen Abwehr- und Aufklärungsmechanismen gegen Cyber-Kriminalität.

Die Master-Absolvent:innen der Hochschule Mittweida sind durch ihr Studium dabei im Vergleich zu anderen Berufseinsteiger:innen in der Lage, früher komplett eigenständig zu arbeiten oder ganze Teams zu führen. Zudem steht den besten Mittweidaer Absolvent:innen an der HSMW die Möglichkeit der Promotion offen.



↓ Blick in die IT-Forensik-Labore der Hochschule Mittweida

# Studienziel

## Sicherheit für unsere digitale Welt.

Betrug, Fälschung, Sabotage, Spionage: Wer ins Bundeslagebild Cybercrime blickt, sieht eine Abbildung der Straftatbestände der analogen Welt. Dabei explodieren Fallzahlen und die Schadenssummen, die eigenständig agierende Cyber-Kriminelle bei staatlichen Institutionen verursachen. Das Bewusstsein für IT-Sicherheit ist geschärft. Doch es fehlen Fachleute.

Um Verbrechen im Internet aufzuklären oder durch die richtigen Maßnahmen schon vor der Tat zu verhindern, benötigen Firmen und Behörden wie Polizei, LKA und BKA Personal, das die Werkzeuge der Cyber-Kriminalität versteht. Viele Informatiker:innen erlernen dieses Wissen erst nach ihrem Studium auf eigene Faust. Das Masterstudium Cybercrime/Cybersecurity in Mittweida macht das überflüssig: IT-Schwachstellen zu identifizieren, die öffentliche und privatwirtschaftliche Infrastruktur gegen Angriffe abzusichern und Mittel der digitalen Forensik zur Verbrechensaufklärung zu nutzen, sind die Inhalte von Cybercrime/Cybersecurity.

## Eckdaten zum Studium

Regelstudienzeit  
Vollzeitstudium

4



Semester

Akkreditiert



Abschluss



Master of Science (M.Sc.)



Beginn  
Wintersemester

# Studienaufbau

## Verbrechen verhindern oder Verbrechen aufklären? Ein Studium, zwei Optionen.

Der Studiengang Cybercrime/Cybersecurity verzahnt digitale Forensik und IT-Sicherheit in einem deutschlandweit einzigartigen Masterstudium und steht allen Bachelor- und Master-Absolvent:innen offen, die sich in den Bereichen Cyber-Sicherheit und -Kriminalität weiterbilden möchten. Insbesondere richtet es sich an Absolvent:innen der Fachrichtungen Informatik, Elektrotechnik und Mathematik. Programmier-Vorkenntnisse sind deshalb zwar hilfreich, aber für ein erfolgreiches Studium nicht nötig.

Zu Beginn des Studiums wählen die Studierenden **sechs Qualifizierungslinien** und legen dadurch ihre Studienrichtung(en) und die Inhalte der ersten drei Semester fest. Im vierten Semester wird die Masterarbeit angefertigt.

### ■ Studienrichtung Cybercrime:

**Netzwerkforensik** und **Mobile Forensics** richten sich insbesondere an Studierende mit Interesse an IT-Forensik. Dabei steht das Aufdecken von Beweismitteln auf elektronischen Spurenlägern im Mittelpunkt.

### ■ Studienrichtung Cybersecurity:

**Softwarearchitektur** und **höhere Konzepte der Informatik** setzen den Schwerpunkt auf IT-Sicherheit. Die Studienrichtungen schließen das Entwerfen komplexer informatischer Systeme inklusive Datenbanken und Multimedia-Anwendungen ein.

### ■ Modellierung/Dunkelfeldforschung, Elektronische Forensik und Kryptologie

sind für beide Felder relevant und ergänzen die Kenntnisse der IT-Forensiker:innen und Cybercrime-Spezialist:innen.

Die Wahl der Qualifizierungslinien beeinflusst die Bezeichnung des Master-Abschluss. Werden die Studienrichtungen Cybercrime **und** Cybersecurity belegt, werden beide im Zeugnis aufgenommen.

Alle Qualifizierungslinien integrieren aktuelle Forschungserkenntnisse in IT-Sicherheit und digitaler Forensik. Dabei profitieren die Studierenden besonders von der Forschungsstärke der Hochschule Mittweida und den Tätigkeiten der Lehrenden als Gutachter:innen für Sicherheit- und Ermittlungsbehörden sowie Unternehmen.

# Studienablaufplan

Qualifizierungslinie <b>Netzwerkforensik</b>	1.	2.	3.	4.
Cybercrime I	■			
Cybercrime II		■		
Social Engineering und OSINT			■	
Qualifizierungslinie <b>Mobile Forensics</b>	1.	2.	3.	4.
Grundlagen der Mobilfunkforensik	■			
Der Sachverständige vor Gericht		■		
Komplexpraktikum Forensische Methoden			■	
Qualifizierungslinie <b>Elektronische Forensik</b>	1.	2.	3.	4.
Internet of Things	■			
Geoforensik und Reverse Engineering		■		
Car Forensics			■	
Qualifizierungslinie <b>Modellierung/Dunkelfeldforschung</b>	1.	2.	3.	4.
Stochastic Models	■			
Artificial Intelligence – Theory and Foundations		■		
Predictive Policing/Dunkelfeld			■	
Qualifizierungslinie <b>Kryptologie</b>	1.	2.	3.	4.
Foundations of Modern Cryptography	■			
Cryptanalysis		■		
Digitale Werte und Güter			■	
Qualifizierungslinie <b>Softwarearchitektur</b>	1.	2.	3.	4.
Datenbankprogrammierung	■			
Softwarepraktikum		■		
Entwurf sicherer Systeme			■	
Qualifizierungslinie <b>Höhere Konzepte der Informatik</b>	1.	2.	3.	4.
Intelligente Videoanalyse	■			
Datenkompression		■		
Datennetze/Cloud Forensik			■	
Masterarbeit (24 Wochen)				■

## Studienberatung

Unsere Studienberater:innen stehen jederzeit für ein unkompliziertes Gespräch bereit – egal ob du allgemeine Fragen oder fachbezogene zu den Inhalten des Studiums hast.

### Deine persönlichen Ansprechpartnerinnen:

Annika Gündel B.A. & Julia Gündel B.A.

Telefon +49 (0) 3727 58-1309

Whatsapp +49 (0) 151 115 42 900

studienberatung@hs-mittweida.de



## Social Media



@hochschulemittweida



@hochschulemittweida



@HochschuleMittweida



hs.mw/discord

## Bewerbung

Dein Interesse ist geweckt? Dann registrier dich unter [hs-mittweida.de/bewerben](https://hs-mittweida.de/bewerben). Sobald du alle Formulare und Nachweise übermittelt hast, kannst du dich in Cybercrime/ Cybersecurity immatrikulieren. Mit der Immatrikulation schreibst du dich für das Studium ein – und hast deinen Studienplatz sicher.

## Zulassungsvoraussetzungen

Der Masterstudiengang Cybercrime/Cybersecurity ist konsekutiv zu den Bachelor-Studienangeboten Allgemeine und Digitale Forensik, IT-Forensik/Cybercrime und IT-Sicherheit der Hochschule Mittweida angelegt, eignet sich jedoch für alle Interessierten, die ein erstes berufsqualifizierendes Hochschulstudium in Informatik, Elektrotechnik oder Mathematik abgeschlossen haben.