Institut für Wirtschaftsinformatik - Information Engineering

Themenbereiche und Themen für wissenschaftliche Arbeiten

Institut für Wirtschaftsinformatik – Information Engineering

Betreuung durch David Rückel

(nur Bachelorarbeit)

Folgende **Themenbereiche** sind bei **David Rückel** generell möglich:

- Strategisches IT-Management
- Beteiligung von Practitioner Researcher im Forschungsprozess
- SDGs vs. IDGs
- Agiles Informationsmanagement
- Veränderung von Lehr- und Lernkonzepten durch LLMs

Betreuung durch René Riedl

Folgende **Themenbereiche** sind bei **René Riedl** generell möglich:

- Blockchain, Cryptocurrencies, Bitcoin
- Vorgehensweisen in der Softwareentwicklung (traditionellen Vorgehensweisen vs. agile Verfahren)
- Technostress / digitaler Stress
- Informationsnachfrage, Informationsangebot, Informationsgleichgewicht und organisationale Auswirkungen
- Vertrauen in Digitaltechnologien
- Digitale Transformation
- Large Language Models wie ChatGPT, insbesondere deren Veränderung von Arbeitsprozessen und -ergebnissen

---

Betreuung durch Barbara Krumay

Folgende **Themenbereiche** sind bei **Barbara Krumay** generell möglich:

- Auswirkungen der Digitalisierung auf Security Awareness
- Resilience, Agilität und Governance
- Security / Privacy Complacency
- Security und Privacy Messmodelle
- Green IT im Kontext von neuen Technologien
- Einfluss des EU AI Act auf die Anwendung von AI in Unternehmen
- Akzeptanzmessung

Konkrete Fragestellungen (Barbara Krumay)

Business Continuity Management & Digital Resilience

Die Bedrohung durch Cyberangriffe aber auch die Gefahr von Ausfällen durch Naturereignisse wie Lawinen wächst stetig. Für Organisationen heißt das, dass sie sich darauf vorbereiten müssen um langfristig bestehen zu können. Aber nicht alles kann vorhergesehen werden und manche Investitionen, die zum Schutz notwendig sind, sind nur schwer finanzierbar. Daraus ergeben sich unterschiedliche Fragestellungen, z.B. hinsichtlich der Implementierung von Business Continuity Management (BCM) und Ansätzen, die digitale Resilienz zu stärken. Die aktuellen Erkenntnisse sind vor allem praktischer Natur und die Anzahl der wissenschaftlich fundierten Ergebnisse ist noch relativ gering, insbesondere aus Managementsicht.

Föderierte, dezentrale Ansätze für Plattformen (NEU)

Plattformen und Plattformökonomie gelten als klares Zeichen der Digitalisierung. Die Vormachtstellung mancher Plattformen (wie z.B. Facebook, Twitter, Amazon) schien bis vor kurzem noch unbestritten. Änderungen z.B. in der Eigentümerstruktur (siehe Twitter) oder in der Ausrichtung (z.B. Meta / Facebook) haben Auswirkungen auf die Akzeptanz bei den User:innen. Bedenken bestehen unter anderem hinsichtlich Manipulation (z.B. Fakenews), der extensiven Sammlung von Daten und der dadurch möglichen Überwachung – um nur einige zu nennen. Föderierte, dezentrale Ansätze (z.B. Mastodon, DataSpaces) bieten andere Möglichkeiten, haben aber auch andere, für die Informationsgüterindustrie typische Herausforderungen (z.B. Erreichen der kritischen Masse). Dieses Thema adressiert diese Ansätze, deren Möglichkeiten sowie Herausforderungen.
Co-Betreuung mit Andreas Hutterer möglich

NEU! Szenarien zur Risikoklassifizierung im Rahmen EU AI Acts für KMUs

Der EU AI Act ist in Kraft getreten und von den EU-Mitgliedsstaaten innerhalb der nächsten Jahre umzusetzen. Das wird weitreichende Auswirkungen auf die Anwendung von AI in Unternehmen haben. Allerdings fehlt es an Instrumenten um die Risikoklassifizierung eindeutig umzusetzen. Für Organisationen stellt sich daher die Frage, wie sie mit möglichst geringen Kosten diese Klassifizierung selbst vornehmen können. Anhand von Beispielen aus der Praxis sollen unterschiedliche Instrumente entworfen und getestet werden.

Betreuung durch Manuel Mühlburger

Folgende **Themenbereiche** sind bei **Manuel Mühlburger** generell möglich:

- Digital Opportunity Recognition
- Digitale Technologien im Kontext der Digitalisierung und digitale Transformation
- KI-Einsatz in Unternehmen als digitale Technologie

Konkrete Fragestellungen (Manuel Mühlburger)

Potentiale der Digitalen Transformation

Digitalisierung und Digitale Transformation stellen Organisationen vor die Herausforderungen Potentiale digitaler Technologien zu identifizieren. Unabhängig ob diese Potentiale in der Automatisierung von Teilaufgaben, der Optimierung von Geschäftsprozessen oder der Transformation ganzer Geschäftsmodelle liegen ist die Fähigkeit dieser Potentialidentifikation wesentlich für moderne Organisationen. Master und Bachelorarbeiten in diesem Bereich können methodische, organisatorische oder individuelle Aspekte dieser Fähigkeit sowohl aus theoretischer als auch aus empirischer Sicht untersuchen und dabei auf Arbeiten des Instituts aufbauen.

Digitalisierung und Direktvertrieb in nicht-urbanen Gebieten
In nicht-urbanen Gebieten hat es in letzter Zeit einen regelrechten Boom hinsichtlich Direktverkaufs von Produkten gegeben. Dies reicht von Ab-Hof-Verkäufen von Lebensmitteln über Handwerkserzeugnisse bis hin zur Versorgung von Organisationen (Stichwort: Biokistl). Die Digitalisierung bietet hier viele Möglichkeiten, allerdings ist derzeit kein einheitliches Bild ersichtlich. Insbesondere durch den Einsatz von Plattformen, könnte es für alle hier zu positiven Effekten kommen. Dafür müssen die unterschiedlichen Bedingungen erhoben und mögliche positive und negative Einflussfaktoren auf die tatsächliche Nutzung einer gemeinsamen Plattform identifiziert werden.

Strukturierte Betrachtung von Anwendungen künstlicher Intelligenz in Organisationen
Künstliche Intelligenz als Feld umfasst verschiedenste Technologien, Methoden und Ansätze. Im praktischen Kontext werden KI-Ansätze aber oft nicht wirklich unterschieden und KI wird immer mehr zum Buzzword. Im Sinne des Wissenschaftsziels der Beschreibung ist es Aufgabe der Wirtschaftsinformatik Phänomene wie KI-Anwendungsmöglichkeiten in Organisationen strukturiert und einheitlich zu kategorisieren. Arbeiten in diesem Themenbereich sollten darauf ausgerichtet sein KI-Anwendungsszenarien in Organisationen zu identifizieren, zu strukturieren und in einer für die jeweiligen Zielgruppen geeigneten Sprache zu Beschreiben und aufzubereiten.

Betreuung durch Michaela Trierweiler
(bei Masterarbeit Co-Betreuung mit Barbara Krumay oder René Riedl)

Folgende **Themenbereich** sind bei **Michaela Trierweiler** generell möglich

- IT-Security & Cyber-Security - auch mit Fokus auf KMUs möglich
- IT-gestützte Betrugsprävention (IT/IS-supported Fraud Management) - auch mit Fokus auf KMUs möglich
- Cascading Artefacts in Design Science Research

Konkrete Fragestellungen (Michaela Trierweiler)
NEU! Datensicherheit in NGOs - Analyse von Herausforderungen und Mechanismen
Gemeinnützige Organisationen, die für den Umgang mit hochsensiblen persönlichen Daten verantwortlich sind (z.B. in der Pflege oder dem Medizinbereich), stehen vor wachsenden Herausforderungen in Bezug auf die Cyber- und Datensicherheit. Zwar müssen sie die Verfügbarkeit kritischer Informationen (z. B. Krankenakten) rund um die Uhr sicherstellen, doch fehlen ihnen häufig die finanziellen Mittel für eine umfassende Maßnahmen der IT-Security. Im Vergleich zu gewinnorientierten Unternehmen arbeiten gemeinnützige Organisationen mit einem anderen Schwerpunkt und einer anderen Struktur. Die Erbringung von Dienstleistungen steht über dem Gewinn, dennoch benötigen sie robuste Ansätze. Eine strukturierte Analyse der spezifischen Cybersicherheitsbedrohungen für NGOs, sowie Strategien zur Minderung dieser Risiken fehlt derzeit noch.

NEU! Cybersecurity - Vermittlung / Awareness / Training / Effektivitätsmessung von Cybersecurity-Awareness-Maßnahmen in Bildungseinrichtungen
Durch Angriffe auf die IT-Infrastruktur, insbesondere aus dem Cyberspace sind alle Organisationen gefordert, Cybersecurity-Maßnahmen zu entwickeln, um diesen Gefahren entgegen zu treten. Davon sind auch Bildungseinrichtungen im privatwirtschaftlichen Bereich betroffen. Aufgrund von fehlendem Know-how und anderen Schwerpunkten hinken Bildungseinrichtungen in der Weiterentwicklung von IT-Sicherheitsmaßnahmen aber hinterher. Es stellt sich daher die Frage, wie Wissen zum Thema Cybersecurity in Bildungseinrichtungen vermittelt und Bewusstsein aufgebaut werden kann. Wie findet

die Wissensvermittlung im Bereich Cybersecurity in Bildungseinrichtungen statt? Wie/wo könnte/sollte man dringend ansetzen? Welche Möglichkeiten gibt es, die Effektivität von Cybersecurity-Awarness-Maßnahmen zu messen?

NEU! EU AI-Act in Verbindung mit ISO 27001 und NIS2 --> Erhöhung der Cybersicherheit von KI-Produkten
Standards werden von vielen Unternehmen genutzt, um ein erwünschtes Level – z.B. an Sicherheit – zu erreichen und zu dokumentieren. Im Kontext des neuen EU AI Act werden manche bereits existierende Standards (z.B. ISO 27001, NIS2) aufgrund gleicher aber auch unterschiedlicher Zielsetzung eine besondere Rolle spielen. Daraus ergeben sich unterschiedliche Fragestellungen. Wie können die Standards ISO 27001 und die Vorgaben der NIS2-Richtlinie dazu beitragen, die Cybersicherheit von KI-Produktlösungen in den gemäß AI-Act definierten Risikoklassen „unannehmbar“, „hoch“ und „gering/minimal“ zu verbessern? Welche spezifischen Aspekte der Cybersicherheit werden durch den AI-Act bereits adressiert, und wo bestehen potenzielle Lücken, die durch die Implementierung von ISO 27001 oder NIS2 geschlossen werden könnten? (Anmerkung: siehe dazu z.B. Artikel 15 AI-Act Genauigkeit, Robustheit und Cybersicherheit).

NEU! Evaluation des Einsatzes von KI-Tools zur Unterstützung im Bereich der Betrugsprävention und Erkennung (nur für Masterarbeit geeignet)
IT/IS-Tools, wie z.B. Big Data Analytics Methoden haben in den letzten Jahren immer mehr an Bedeutung zur Erkennung von Betrugsversuchen gewonnen und sind in manchen Branchen zum Standard geworden. Mit der Weiterentwicklung der algorithmischen Analyse im Bereich der KI ergeben sich hier neue Chancen für die Erkennung und Prävention. Unklar bleiben bisher Nutzen und Nutzung von KI-Tools zur Prävention und Erkennung von Betrugsversuchen. Daher wäre es notwendig herauszufinden, ob KI als Mittel zu einem flächendeckenden Einsatz zum Betrugsmanagement gesehen wird und welche Chancen und Risiken Unternehmen damit verbunden sehen.

NEU! Teleworking und IT-Sicherheit in der Post-Covid-19-Ära
Durch die pandemiebedingten Einschränkungen waren Organisationen gezwungen, rasch Lösungen für Homeoffice bzw. Teleworking zu finden. Viele damals umgesetzte Lösungen existieren auch in der Post-Covid-19-Ära noch. Allerdings ist unklar, wie IT-Sicherheit (inkl. Physischer Sicherheit) damals und heute im Homeoffice bzw. Teleworking umgesetzt wurde und wird. Zahlreiche Untersuchungen für den Zeitraum der Covid-19-Pandemie haben gezeigt, dass Sicherheitsrisiken sprunghaft angestiegen sind, welche Sicherheitsrisiken das waren, aber auch die sogenannte „Schatten-IT“ ist angewachsen. Auch bei den aktuell vorherrschenden hybriden Arbeitsmodellen ist davon auszugehen, dass hier immer noch große Lücken und Nachholbedarf bestehen. Die aktuelle Situation ist unklar und kann z.B. in Anlehnung an die Auditierungen der ISO-Norm 27001 näher betrachtet werden.

Betreuung durch Ines Janusch
(ausschließlich Bachelorarbeitl)

Folgende Themenbereich sind bei Ines Janusch generell möglich

Künstliche Intelligenz im betrieblichen Umfeld insbesondere
- Bedarf / Machbarkeit
- Strategien
- Auswirkungen auf Datenschutz / Privatsphäre

Konkrete Fragestellungen (Ines Janusch)

NEU! Privacy Appropriate AI

Die zunehmende Nutzung von Künstlicher Intelligenz und deren Integration in datenintensive Anwendungen wirft zahlreiche datenschutzrechtliche Fragestellungen auf. Ein zentraler Aspekt eines datenschutzgerechten Einsatzes von KI liegt in der Einholung informierter Einwilligungen zur Datenverarbeitung. Doch auch wenn Daten im Einklang mit geltendem Datenschutzrecht erhoben werden, ergeben sich daraus zahlreiche Folgeproblematiken, wie zum Beispiel die Definition von Datenlöschstrategien für Trainingsdaten oder bereits im Einsatz befindlichen KI-Systeme, die oft außer Acht gelassen werden. Im Rahmen dieses Themas kann sowohl eine Auseinandersetzung mit den datenschutzrechtlichen Herausforderungen über die verschiedenen Phasen des KI-Lebenszyklus hinweg als auch die Erarbeitung von Strategien zur Gewährleistung eines datenschutzgerechten KI-Einsatzes in Organisationen erfolgen.