Binaire

DAS MAGAZIN DES FORSCHUNGSZENTRUMS L3S

WWW.BINAIRE.DE

AUSGABE № 11/11111100100

SICHERHEIT
DATENSCHUTZ
ETHIK

Forschungszentrum · Research Center L3S

Leibniz Universität Hannover

Technische Universität Braunschweig

—› Foto:
Vitali Artiushenko

MIT SCHIRM, WERTEN UND INTELLIGENZ

Ein Gentleman hält seinen Schirm über einen Rechner – eine Metapher für den Schutz vor Cyberattacken, aber auch für ethische und rechtliche Standards gegen diskriminierende Algorithmen der künstlichen Intelligenz. Ließe man den Algorithmen freien Lauf, sie wären voreingenommen und ungerecht, weil sie oft auf Basis von Daten, die unsere eigenen Vorurteile widerspiegeln, trainiert werden. Der Mensch muss ihnen seine ethischen und rechtlichen Standards erst beibringen.
Sicherheit ist ein hohes Gut. Das gilt auch für die Sicherheit von Daten, die durch Diebstahl, Spionage, Manipulation oder Missbrauch bedroht sind. Solche Schäden können enorme Ausmaße annehmen. Umgekehrt können Daten auch für mehr Sicherheit sorgen: Datenanalysen mit Methoden der künstlichen Intelligenz können wichtige Erkenntnisse liefern, um Risiken zu erkennen, zu verhindern oder zu beheben – von Naturkatastrophen bis hin zur organisierten Kriminalität.

DAS FORSCHUNGSZENTRUM *L3S*

L3S-Forscher entwickeln im Bereich **Web Science** und **digitale Transformation** zukunftsweisende Methoden und Technologien, die einen intelligenten und nahtlosen Zugriff auf Informationen über das Web ermöglichen, Individuen und Gemeinschaften in allen Bereichen der Wissensgesellschaft vernetzen und das Internet an die reale Welt und ihre Einrichtungen anbinden. Das *L3S* erforscht die Auswirkungen des digitalen Wandels, um aus den Erkenntnissen Handlungsoptionen, -empfehlungen und Innovationsstrategien für die Wirtschaft, die Politik und Gesellschaft herzuleiten.
Durch Forschung, Entwicklung und Beratung trägt das *L3S* gemeinsam mit seinen Partnern zur digitalen Transformation insbesondere in den Bereichen Mobilität, Gesundheit, Produktion und Bildung bei.

Geschützt und diskriminierungsfrei

Liebe Leserin, lieber Leser,

wir verstärken uns: noch mehr künstliche Intelligenz, noch mehr IT-Sicherheit und neue Digitalisierungsprofessuren in Hannover und Braunschweig! Datensicherheit, Datenschutz und Ethik sind für die digitale Transformation unverzichtbar und daher auch wichtige Forschungsgebiete für das *L3S*.
Künstliche Intelligenz – ihre Auswirkungen auf die Gesellschaft von morgen: Dazu fördert die *Volkswagenstiftung* unser Projekt *BIAS*, in dem Informatiker, Rechtswissenschaftler und Philosophen intensiv daran arbeiten, Vorurteile und Diskriminierung bei der algorithmischen Verarbeitung großer Datenmengen zu verhindern. Das ist auch das Ziel des europäischen Graduiertenkollegs *NoBIAS:* Mit sieben Partnern entwickeln wir neue KI-Algorithmen für datengestützte und diskriminierungsfreie Entscheidungssysteme und bilden gleichzeitig europäisch vernetzte Doktorandinnen und Doktoranden aus.
Sicherheit und Datenschutz: In Kooperation mit dem *Helmholtz-Zentrum für Informationssicherheit (CISPA)* bauen wir die *Leibniz Universität* und die *Region Hannover/Braunschweig* zum führenden Standort für Cybersicherheits- und Datenschutzforschung in Norddeutschland aus – einmalig durch die enge Vernetzung von künstlicher Intelligenz und Sicherheit.
Gesellschaft und Arbeit von morgen: auch das ist ein Schwerpunkt am *L3S*. In unserem neuen Projekt *OPAL* arbeiten Soziologen des *L3S* daran, vor dem Hintergrund des Pflegenotstands den Erfolg der digitalisierten Pflege durch partizipative Technikgestaltung zu erhöhen.
Künstliche Intelligenz, Sicherheit, Datenschutz, Soziologie der Digitalisierung: Das *L3S* steht für Exzellenz und interdisziplinäre Kooperation in Forschung und Innovation. Wir freuen uns, mit Ihnen zusammenzuarbeiten!

Eine spannende Lektüre wünscht Ihnen

Prof. Dr. techn. Wolfgang Nejdl

ESSENZ

DURCH FORSCHUNG, ENTWICKLUNG UND BERATUNG gestaltet das *L3S* gemeinsam mit seinen Partnern die digitalen Transformation insbesondere in den Bereichen:

→ Intelligente Produktion
→ Digitale Bildung
→ Intelligente Mobilität
→ Personalisierte Medizin

»Nur wenn Informationen sicher geschützt und unter der Kontrolle ihrer Anwender bleiben, können die rasanten technischen Entwicklungen langfristig zum Wohl der Gesellschaft eingesetzt werden.«

PROF. DR. SASCHA FAHL
L3S-Mitglied und Leiter des Fachgebiets IT-Sicherheit am Institut für Praktische Informatik der Leibniz Universität Hannover.

ÜBERSICHT

BINAIRE-AUSGABE 3 / 2020

TERMIN | AUSZEICHNUNG

18. 2. 2021

KI-Schulung für Unternehmen: In fünf Schritten zur Implementierung

Wo liegen die Potentiale von KI für Unternehmen? In dieser Schulung für Fach- und Führungskräfte lernen die Teilnehmer fünf Schritte zur Implementierung von KI kennen – beginnend mit der Erhebung und Verarbeitung von Daten über die konkreten Methoden und Modelle von KI bis hin zur Ergebnisbewertung. Außerdem diskutieren die Teilnehmer Beispiele für den Einsatz von KI in KMU. Die kostenfreie dreistündige Veranstaltung soll ab Februar wieder monatlich am *L3S* stattfinden. → *mitunsdigital.de*

Mittelstand 4.0 Kompetenzzentrum Hannover
mit uns digital!
Individuell. Unabhängig. Vor Ort.

Maria-Esther Vidal, Volker Meyer-Guckel (stellvertretender Generalsekretär des Stifterverbandes) und Präsident der Leibniz-Gemeinschaft Matthias Kleiner (von links) bei der Preisverleihung in kleiner Runde. *–> Foto: TIB*

25. 11. 2020

Preis für Prof. Dr. Vidal

Der Wissenschaftspreis des *Stifterverbandes für die Deutsche Wissenschaft* »Forschung in Verantwortung« geht in diesem Jahr an *L3S*-Mitglied Maria-Esther Vidal, Leiterin der Forschungsgruppe *Scientific Data Management* an der *TIB – Leibniz-Informationszentrum für Technik und Naturwissenschaften* in Hannover. Die Auszeichnung würdigt die Arbeiten der Informatikerin zum wissenschaftlichen Datenmanagement. Der mit insgesamt 50.000 Euro dotierte Preis wurde im Rahmen der in diesem Jahr virtuell stattfindenden Jahrestagung der Leibniz-Gemeinschaft verliehen.

MELDUNGEN

INKLUSIV · INTELLIGENT · NACHHALTIG

Ein Manifest für das Web der Zukunft

Mehr als vier Milliarden Menschen nutzen das World Wide Web in allen Lebensbereichen. Es greift auch in das Leben derjenigen ein, die nicht einmal wissen, dass es existiert. Wie sollte sich das Web entwickeln, wie wird und wie sollte es sich auf uns alle auswirken? Mit diesen Fragen hat sich eine Gruppe von Wissenschaftlern 2018 beim Workshop *10 Years of Web Science* intensiv beschäftigt, darunter *L3S*-Mitglied Prof. Dr. Eirini Ntoutsi. Daraus hervorgegangen ist ein Manifest, das sich mit den Perspektiven befasst, die sich aus den Ambivalenzen des Web ergeben: Informationsfreiheit versus Informationsqualität, Personalisierung versus Datenschutz, Massenbeteiligung versus Manipulation der Massen, Inklusion und Fairness versus Ausbeutung, Nachhaltigkeit versus Wachstum. Künstliche Intelligenz kann diese Ambivalenzen zum Guten oder Schlechten verstärken. Die Autoren skizzieren Wege, wie das Web weiterentwickelt werden kann, wie Individuen, Gruppen, Organisationen und Staaten lokal und in globaler Kooperation die Ziele für ein »gutes« Web bestimmen und ihren Beitrag dazu leisten können. Das Manifest ist online veröffentlicht. ¶

→ *https://www.webscience.org/wp-content/uploads/sites/117/2020/07/main.pdf*

KONTAKT:
Prof. Dr. Eirini Ntoutsi
Manifest-Co-Autorin
Ntoutsi@L3S.de

MELDUNGEN

LEISTUNGSSTARK
UND EFFIZIENT

Schnellster Hochleistungsserver für KI geht in Betrieb

Am *L3S* ist der zurzeit schnellste Hochleistungsrechner für künstliche Intelligenz (KI) an den Start gegangen. Europaweit gehört das Forschungszentrum damit zu den ersten Anwendern, bei denen der *Nvidia DGX-A100* installiert wurde. Der neue Rechner ermöglicht mit fünf Billiarden Rechenoperationen pro Sekunde die zurzeit schnellste Bearbeitung im Bereich des maschinellen Lernens, verbraucht aber rund 75 Prozent weniger Strom als sein Vorgänger.
Das neue KI-System wird vor allem im Projekt *IIP-Ecosphere* eingesetzt, einem KI-Ökosystem für die **intelligente Produktion,** das die Partner eines interdisziplinären Konsortiums aus Wissenschaft und Wirtschaft unter Leitung des *L3S* und des *Instituts für Fertigungstechnik und Werkzeugmaschinen* der *Leibniz Universität Hannover* gemeinsam aufbauen. Ziel ist, den Einsatz von KI in der Produktion zu beschleunigen und zu optimieren. Die dafür erforderlichen Modelle des maschinellen Lernens – insbesondere des Deep Learning – benötigen für das Training sehr umfangreiche Datensätze, einen entsprechend großen Speicher sowie zahlreiche Grafikprozessoren mit einer extrem schnellen Verbindung untereinander. Mit einem GPU-Gesamtspeicher von 320 Gigabyte und einer Bandbreite von 12,4 Terabyte pro Sekunde bietet der neue Server am *L3S* eine KI-Leistung von fünf PetaFLOPS, also fünf Billiarden Rechenoperationen pro Sekunde, sowie die neuesten Hochgeschwindigkeitsverbindungen. Bereits seit Anfang des Jahres verfügt das *L3S* zudem über einen neuen GPU-gestützten Server mit einem Gesamtspeicher von einem halben Terabyte und damit über die notwendige Leistungsfähigkeit, um ein schnelleres Training der aktuellen KI-Modelle zu ermöglichen. **Mit dem DGX-A100 verdoppelt das L3S seine KI-Leistung** und ist damit auf die exponentiell wachsende Größe von KI-Modellen und -Daten hervorragend vorbereitet.

Geringer Platz- und Energieverbrauch bei extrem hoher Leistung: Das zurzeit fortschrittlichste KI-System, der NVDIA DGX-A100, wurde Ende September 2020 am L3S installiert, um die Forschung zu neuen Methoden des Deep Learning weiter zu beschleunigen. Davon können im Projekt IIP-Ecosphere bald auch Unternehmen profitieren, die mit KI ihre Produktion optimieren wollen.

Auch Unternehmen profitieren von dem neuen Hochleistungsserver am *L3S*. Im Projekt *IIP-Ecosphere* wird das System in ein Experimentierfeld für die intelligente Produktion eingebunden. Neben den Projektpartnern können dann kleinere Unternehmen mit Unterstützung des *L3S* KI-Ansätze erproben, ohne direkt in die Infrastruktur investieren zu müssen.
Mit dem neuen System bietet das *L3S* zudem seinen Wissenschaftlerinnen und Wissenschaftlern hervorragende Arbeitsbedingungen und steigert auf dem Gebiet der KI-Forschung seine internationale Wettbewerbsfähigkeit. Studierende und Doktoranden werden am *L3S* optimal auf ihr zukünftiges Wirkungsfeld vorbereitet. ¶

EXIST-GRÜNDER-STIPENDIUM FÜR INDAAQ

Passende Daten für die intelligente Produktion

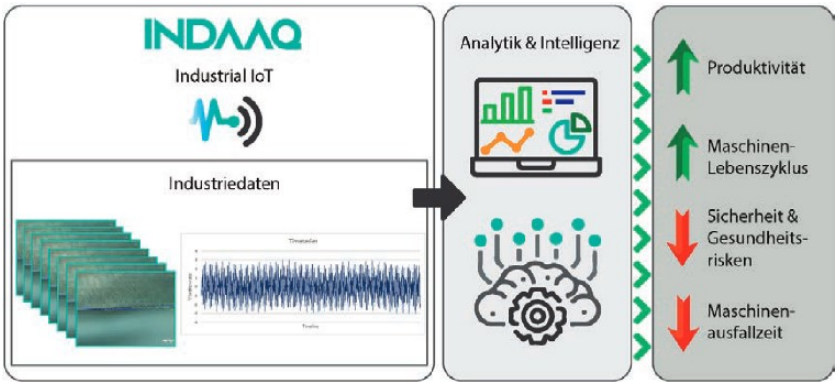
Seit November 2020 ist am *L3S* ein neues Gründerteam am Start. Hemanth Mandapati, Dimitrij Lewin und Siddhartha Giri erhalten ein Jahr lang das *EXIST*-Gründerstipendium des *Bundesministeriums für Wirtschaft und Energie*, um die Gründung ihres Unternehmens *INDAAQ (Industrial Data Acquisition)* vorzubereiten. *INDAAQ* will mit Datenbanken für intelligente Maschinen insbesondere kleinen und mittleren Unternehmen (KMU) den Einstieg in die digitale Transformation erleichtern. Bislang haben hauptsächlich größere Unternehmen die Digitalisierung vorangetrieben und unter dem Schlagwort Industrie 4.0 mit Technologien wie fortgeschrittener Robotik, Cloud-Anwendungen und Big Data einen großen Schritt in Richtung intelligente Fabrik getan. In vielen KMU sind die Produktions- und Fertigungsprozesse aber immer noch aus einer anderen Zeit. Aus vielen Umfragen geht hervor, dass kleinere Unternehmen gegenüber den Herausforderungen der digitalen Transformation weniger aufgeschlossen sind – sei es aus Angst vor Veränderungen, aus Mangel an Know-how oder fehlender Infrastruktur.

Hemanth Mandapati, Dimitrij Lewin, Siddhartha Giri (von links nach rechts).

Eine große Hürde ist der Mangel an spezifischen Industriedaten, die Unternehmen für den Aufbau einer auf künstlicher Intelligenz basierenden Fertigung benötigen. Der Prozess der Datenerfassung- und -verarbeitung ist aufwendig und erfordert besondere Fähigkeiten. *INDAAQ* bietet Lösungen an, um den Daten-Engpass zu überwinden. Das Startup erstellt Datenbanken, die den spezifischen Anforderungen der Kunden entsprechen.

Mit diesem Fundament bietet *INDAAQ* auch KMUs die Möglichkeit, die Chancen der intelligenten Produktion erfolgreich zu nutzen. Seit die Gründer ihre Idee erstmals ihrem jetzigen Mentor Prof. Dr. Wolfgang Nejdl und Dr. Sergej Zerr am Forschungszentrum *L3S* vorgestellt haben, sind ein Jahr und acht Monate vergangen. Während dieser Zeit haben das *L3S* und der Gründerservice *Starting Business* der *Leibniz Universität Hannover* das Team bei der Ausarbeitung der Idee und der Antragstellung für das *EXIST*-Programm unterstützt. Mit strategischen Partnerschaften und einer effektiven Kooperation mit der Universität will *INDAAQ* die verarbeitende Industrie nun zukunftssicher machen. ¶

→ *https://indaaq.com*



INDAAQ stellt Daten für die KI-Analytik zur Steigerung der industriellen Prozesse her. –> Abbildung: INDAAQ

Cybersicherheit und Datenschutz sind zentrale Herausforderungen für Smart Factories.
–> Foto: Adobe Stock

DIGITALISIERTE GESELLSCHAFT

Cybersicherheit, Mensch, Ethik

Die Digitalisierung der Gesellschaft ist in den letzten Jahrzehnten mit atemberaubender Geschwindigkeit vorangeschritten. Entwicklungen wie **Cloud- und Mobile Computing** sowie **Wearables**, die Verbreitung von **IoT-Geräten** in **Smart Homes**, **Smart Factories** und **Smart Cities**, das **autonome Fahren**, **personalisierte Medizin**, **Kryptowährungen** und der immer häufigere Einsatz von **künstlicher Intelligenz** in den unterschiedlichsten Anwendungsdomänen sind nur einige Beispiele, die Fragen der Cybersicherheit und des Datenschutzes zu zentralen Herausforderungen für die digitale Gesellschaft machen. Nur wenn Informationen sicher geschützt und unter der Kontrolle ihrer Anwender bleiben, können die rasanten technischen Entwicklungen langfristig zum Wohl der Gesellschaft eingesetzt werden.

Mit dem Fortschritt der Digitalisierung haben sich auch Angriffe auf IT-Systeme geändert. Während in den 90er Jahren einzelne Hacker und Script-Kiddiese IT-Systeme angegriffen haben, um ihre technischen Fähigkeiten zu erproben und auf unsichere Systeme hinzuweisen, fand in den letzten Jahren eine stetige Professionalisierung der Cyberangriffe statt. Dahinter stecken immer häufiger ressourcenstarke und mächtige Angreifer wie das organisierte Verbrechen oder staatliche Organisationen. Berichte von erfolgreichen Angriffen auf IT-Systeme und kritische Infrastrukturen in beinahe wöchentlicher Frequenz machen die Dramatik der Situation deutlich. Der Schutz der unterschiedlichsten IT-Systeme und Daten gegen moderne und mächtige Angriffe steht daher im Mittelpunkt aktueller Vorhaben der **Cybersicherheitsforschung**. ↗

IoT-Sicherheit zuhause: Das Smart Home kann aus der Ferne gesteuert werden. Ein Hacker kann das auch, indem er Sicherheitslücken nutzt. –> Foto: Adobe Stock

HERAUSFORDERUNGEN DER CYBERSICHERHEIT

Die Grundlage der Cybersicherheit bildet die Kryptographie. Sie erforscht grundlegende Primitive, die als Bausteine für komplexere Sicherheitssysteme und -anwendungen dienen. Eine große Herausforderung ist die Erforschung von **quantensicherer Kryptographie.** Gemeinsam mit dem Unternehmen *Tutanota* arbeiten wir daran, E-Mail-Verschlüsselung gegen Quantencomputer zu schützen (Binaire 2/2020, Seite 14). Eine zweite aktuelle Herausforderung ist die Entwicklung von Systemen, die immun gegen ganze Klassen von Angriffen sind. Hierbei kommen vermehrt Techniken des maschinellen Lernens zum Einsatz, um neuartige Angriffe auf Systeme erkennen zu können und wirkungsvolle Verteidigungsmechanismen zu erforschen. Neben den genannten technischen Innovationen, die eine wichtige Grundlage für hohe IT-Sicherheit bilden, gibt es eine weitere Herausforderung für die Forschung: Anwender müssen die Sicherheits- und Datenschutztechnologien möglichst fehlerfrei nutzen können. Prof. Fahl beschäftigt sich im Rahmen des DFG-Exzellenzclusters *CASA*, der an der *Ruhr-Universität Bochum* angesiedelt ist, und seiner Arbeitsgruppe *Human-Centered Security* am *L3S* mit Fragestellungen in den genannten Bereichen (Seite 14).

In einem vom BMWi geförderten Transferprojekt, in dem das *L3S* gemeinsam mit dem *Kriminologischen Forschungsinstitut Niedersachsen* in einer großangelegten Studie mit 5.000 kleinen und mittelständischen Unternehmen in Deutschland die Auswirkungen von Cyberangriffen auf KMUs untersucht, findet am *L3S* exzellente Grundlagenforschung Anwendung in der niedersächsischen und deutschen Wirtschaft (Seite 16).

HANNOVER WIRD FORSCHUNGSSTÄTTE FÜR CYBERSICHERHEIT

2021 wird das *CISPA Helmholtz-Zentrum für Informationssicherheit* in Kooperation mit der *Leibniz Universität Hannover (LUH)* und dem *L3S* eine Außenstelle in Hannover gründen und zu einer führenden Forschungsstätte für Cybersicherheit in Norddeutschland aufbauen. Das *CISPA Helmholtz-Zentrum für Informationssicherheit* ist eine nationale Forschungseinrichtung des Bundes innerhalb der *Helmholtz-Gemeinschaft* und erforscht alle großen Herausforderungen der Cybersicherheit. *L3S*-Mitglied Prof. Fahl wird im Rahmen einer gemeinsamen Berufung durch die *LUH* und das *CISPA* den Grundstein legen und mit der Zusammenarbeit im Bereich der Human-Centered Security beginnen. Verstärkt wird die Kooperation durch eine Forschungsgruppe im Bereich Industrial Security. Das *L3S* wird durch seine gute Vernetzung mit der niedersächsischen Industrie einen großen Beitrag leisten. Weitere Unterstützung bekommt die Initiative durch eine neue Berufung an der *LUH* auf die Professur zur IT-Sicherheit und eine Juniorprofes-

sur mit Schwerpunkt *Privacy-Friendly Software Systems.* Auch hier wird das *L3S* Kooperationspartner sein und von der neuen Initiative profitieren sowie seine langjährigen Erfahrungen einbringen.
Sicherheitsforschung betrifft nicht nur die virtuelle Welt, sondern die Gesellschaft als Ganzes. Die Europäische Union fördert Forschungs- und Innovationsprojekte, mit denen die **zivile Sicherheit der europäischen Gesellschaft und ihrer Bürger gestärkt** wird. Darunter sind auch zwei *L3S*-Projekte: *MIRROR* und *ROXANNE* (Seite 20). Im Projekt *MIRROR* wollen die beteiligten Projektpartner herausfinden, wie potentielle Zuwanderer Europa wahrnehmen und Diskrepanzen zwischen Wahrnehmung und Realität aufdecken. In *ROXANNE* geht es um die Bekämpfung organisierter Kriminalität mit Hilfe von künstlicher Intelligenz. Die Lösungskonzepte in den Projekten werden auch hinsichtlich ethischer, rechtlicher und datenschutzrechtlicher Gesichtspunkte bewertet.

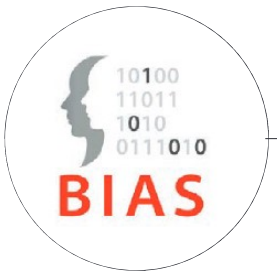
ETHIK FÜR KI

Um die Einbindung ethischer und rechtlicher Standards beim Einsatz von künstlicher Intelligenz geht es auch in den Projekten *BIAS* und *NoBias* (Seite 12). Algorithmen des maschinellen Lernens sind häufig voreingenommen, weil sie mit Daten trainiert werden, die gesellschaftliche Vorurteile widerspiegeln. Der Einsatz von Methoden der künstlichen Intelligenz führt daher nicht selten zu unfairen Ergebnissen. Um das enorme Potential von KI dennoch nutzen zu können, entwickeln die Wissenschaftler Algorithmen, die diskriminierungsfreie Entscheidungen treffen.
Im Zusammenhang mit KI tauchen auch viele neue juristische Fragen auf, die beantwortet werden müssen, um KI zum Erfolg zu führen – auch im Bereich der intelligenten Produktion. Das Projekt *IIP-Ecosphere* hat das Ziel, den Einsatz von KI in der Industrie zu vereinfachen und zu beschleunigen. Juristen des *L3S* befassen sich intensiv mit Themen wie Datenschutz, Eigentumsrechte und dem Schutz von Geschäftsgeheimnissen, wenn es etwa um Datenaustausch und die Nutzung von Plattformen geht (Seite 24).
Sicherheit ist ein vielschichtiges Thema. Dazu gehört auch, darauf vertrauen zu können, im Pflegefall angemessen versorgt zu werden. Angesichts einer immer älter werdenden Bevölkerung und einem jetzt schon gravierenden Mangel an Pflegepersonal sind die Hoffnungen groß, dass die **Digitalisierung die Lücke in der Pflege schließt** – bislang allerdings mit wenig Erfolg. Im Projekt *OPAL* sind *L3S*-Wissenschaftler daran beteiligt, die Akzeptanz von Digitalisierungsmaßnahmen mithilfe partizipativer Technikgestaltung zu erhöhen (Seite 22).
Künstliche Intelligenz, Sicherheit, Datenschutz – die Entwicklung neuer Technologien muss immer auch die Menschen als Anwender im Blick haben, um erfolgreich zu sein. Und zumindest in Europa muss die Anwendung von Technologien den Werten und Normen einer freien Gesellschaft Rechnung tragen. Dazu trägt das *L3S* mit seinen Forschungsprojekten bei. ¶

KONTAKT:
Prof. Dr. Sascha Fahl

Fahl@L3S.de

\\\ *L3S*-Mitglied Sascha Fahl leitet das Fachgebiet IT-Sicherheit am *Institut für Praktische Informatik* der *Leibniz Universität Hannover.* Er forscht im Kompetenzbereich Human-Centered Cybersecurity, das Themen der IT-Sicherheit mit Forschungsmethoden der Psychologie und Sozialwissenschaften kombiniert, um menschliche Faktoren in die Erforschung von IT-Sicherheitslösungen einzubeziehen. \\\



Ethische und rechtliche Standards

Auf künstlicher Intelligenz (KI) basierende Systeme treffen schon jetzt in vielen Bereichen **Entscheidungen,** die jeden Einzelnen überall und jederzeit betreffen können – mit weitreichenden Auswirkungen auch auf die Gesellschaft als Ganzes. Suchmaschinen, Internet-Empfehlungssysteme und Social-Media-Bots verwenden KI-Systeme und beeinflussen damit unsere Wahrnehmung politischer Entwicklungen und sogar wissenschaftlicher Erkenntnisse. Unternehmen nutzen KI in Einstellungsverfahren, Banken für die Kreditvergabe. Wenn aber künstliche Intelligenz Entscheidungen trifft, bringt das Risiken mit sich: zum Beispiel Diskriminierung. **Denn auch das maschinelle Gehirn ist nicht frei von Vorurteilen.** KI-Systeme übernehmen beim Lernen aus Datensätzen auch die darin enthaltenen Stereotypen. So könnten Unternehmen Chancen verpassen, weil Voreingenommenheit dazu führt, dass KI-getriebene Entscheidungen unterdurchschnittliche Leistungen erbringen; viel schlimmer noch: sie könnten gegen Menschenrechte verstoßen. Eine Frage, mit der sich Wissenschaftlerinnen und Wissenschaftler am *L3S* befassen, lautet daher: Wie können Standards für unvoreingenommene Einstellungen und nichtdiskriminierende Praktiken bei der Analyse großer Datenmengen und algorithmusbasierter Entscheidungsfindung eingehalten werden?

DISKRIMINIERUNG ERKENNEN UND BEHEBEN

Tatsächlich gibt es wachsende Bedenken, was die normative Qualität der KI-basierten Entscheidungen und Vorhersagen betrifft. Insbesondere mehren sich Hinweise, dass Algorithmen manchmal bestehende Verzerrungen und Diskriminierungen eher verstärken als beseitigen – mit möglichen negativen Auswirkungen auf den sozialen Zusammenhalt und auf demokratische Institutionen. Welche Rolle spielt also die Ethik bei solch einflussreichen Entscheidungsfindungssystemen?

In der Forschungsgruppe *BIAS* führen Expertinnen und Experten der *Leibniz Universität Hannover* die erkenntnistheoretischen sowie ethischen, rechtlichen und technischen Perspektiven zusammen. Die *Volkswagen-Stiftung* fördert die fakultätsübergreifende Forschungsinitiative im Rahmen der Ausschreibung »Künstliche Intelligenz – Ihre Auswirkungen auf die Gesellschaft von morgen«. Die Kernidee: Philosophen analysieren die ethische Dimension von Konzepten und Prinzipien im Kontext der KI (Voreingenommenheit, Diskriminierung, Fairness). Juristen untersuchen, ob sich die Prinzipien adäquat in den einschlägigen rechtlichen Rahmenbedingungen wiederfinden (Datenschutz, Verbraucher-, Wettbewerbs-, Antidiskriminierungsrecht). Und Informatiker entwickeln konkrete technische Lösungen, um Diskriminierung zu erkennen und mit Debiasing-Strategien zu beheben.
Neben Wissenschaftlern des *Instituts für Philosophie* ist das *L3S* an *BIAS* beteiligt: mit den Professoren Tina Krügel, Eirini Ntoutsi, Wolfgang Nejdl, Christian Heinze und Bodo Rosenhahn als leitenden Forschern. Sie alle eint das Verständnis, dass nicht nur die Algorithmen, sondern das gesamte System von Computerprognosen und menschlichen Entscheidungen **unvoreingenommen und**

für künstliche Intelligenz

nichtdiskriminierend sein sollte. Sie nehmen daher den gesamten Entscheidungsprozess und nicht nur einzelne Komponenten ins Visier.

→ *https://www.bias-project.org*

KÜNSTLICHE INTELLIGENZ MIT VERANTWORTUNG

Wie auf KI basierende Entscheidungen verantwortungsvoll gestaltet werden können, ist auch Thema des europäischen Promotionsprogramms *NoBias – Artificial Intelligence without Bias.* Fünfzehn Doktorandinnen und Doktoranden an acht Institutionen in fünf Ländern gehen das Problem gemeinsam an: mit multidisziplinärer Forschung in Informatik, Datenwissenschaften, maschinellem Lernen sowie den Rechts- und Sozialwissenschaften. Das *L3S* ist mit den Professoren Eirini Ntoutsi, Maria-Esther Vidal, Christian Heinze, Tina Krügel, Sören Auer und Wolfgang Nejdl an *NoBias* beteiligt.

Voreingenommenheit kann in allen Phasen von KI-basierten Entscheidungsprozessen auftreten: wenn Daten gesammelt werden, wenn Algorithmen Daten in Entscheidungsfindungskapazität umwandeln und wenn die Ergebnisse angewendet werden. Um Diskriminierung zu vermeiden, reichen die üblichen KI-Methoden nicht aus. Die Nachwuchswissenschaftler entwickeln daher **technische Lösungen,** die **ethische und rechtliche Prinzipien** in das Training, das Design und den Einsatz der Algorithmen einbetten. Dafür müssen sie zunächst die rechtlichen, sozialen und technischen Herausforderungen verstehen. Neben der Entwicklung fairer Algorithmen für eine unvoreingenommene Entscheidungsfindung gehört zu den Zielen von *NoBias*, KI-Ergebnisse automatisch zu erklären und den gesamten Prozess der Datenherkunft transparent zu dokumentieren.
Praxisnähe stellt *NoBias* durch die Kooperation mit mehr als zehn assoziierten Partnerunternehmen aus den Bereichen Telekommunikation, Finanzen, Marketing, Medien, Software und Rechtsberatung her, die mit dem Know-how der Forscher KI-Innovationen rechtskonform vorantreiben können. ¶

→ *https://nobias-project.eu*

KONTAKT:
Prof. Dr. Eirini Ntoutsi
ntoutsi@L3S.de

\\\ *L3S*-Mitglied Ntoutsi ist Projektkoordinatorin von NoBIAS und leitende Forscherin im Projekt *BIAS.* \\\

Dr. Vasileios Iosifidis
iosifidis@L3S.de

\\\ Iosifidis ist wissenschaftlicher Mitarbeiter am *L3S* und Projektleiter von *NoBIAS.* \\\

Arjun Roy
roy@L3S.de

\\\ Roy ist Doktorand am *L3S* und wissenschaftlicher Mitarbeiter im Projekt *BIAS.* \\\

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

CYBERSICHERHEIT IM ZEITALTER GROSSSKALIGER ANGREIFER (CASA)

Gewappnet für den Großangriff?

Technologische Entwicklungen wie das Cloud-Computing und das Internet der Dinge prägen unsere Gesellschaft. **Wir sind umgeben von Myriaden vernetzter digitaler Geräte.** Weitere Entwicklungen wie autonome Fahrzeuge, Kryptowährungen und intelligente medizinische Implantate werden das Leben in Zukunft noch einschneidender verändern – oder tun es bereits. Die digitale Gesellschaft steht dabei vor einer großen Herausforderung: der Cybersicherheit. In den letzten Jahren hat sich die Art der Bedrohung drastisch verändert. Viele der heutigen Cyberangriffe gehen von mächtigen Angreifern aus. Sorgen bereiten insbesondere staatliche Organisationen, da sie langfristig agieren und über erhebliche technische Fähigkeiten und Ressourcen verfügen. Die beinahe im Wochenrhythmus bekannt werdenden Vorfälle zeigen: Gegen Angriffe im großen Maßstab sind viele der bisherigen Sicherheitslösungen nahezu wirkungslos. Der von der *Deutschen Forschungsgemeinschaft* geförderte Exzellenzcluster *Cybersicherheit im Zeitalter großskaliger Angreifer (CASA)* soll nun nachhaltige Gegenmaßnahmen ermöglichen. An dem Großprojekt ist auch das *L3S* beteiligt. In erster Linie geht es um den Schutz vor mächtigen Angreifern. Die Maßnahmen versprechen aber auch Sicherheit vor schwächeren Widersachern, etwa vor Cyberkriminellen, die aus finanziellen Motiven handeln. Beheimatet ist *CASA* am *Horst Görtz Institut für IT-Sicherheit* der *Ruhr-Universität Bochum*, einer der international führenden Forschungsstätten auf diesem Gebiet.
In *CASA* arbeiten Forscher aus der Informatik, Kryptografie, Elektrotechnik, Mathematik und Psychologie in einer einzig-

CYBER-SICHERHEIT

Sicherheitstechnologien allein reichen nicht aus, um vor Cyberattacken zu schützen. Vielmehr müssen die Menschen die Maßnahmen mittragen. Daher befasst sich CASA auch mit der Nutzerfreundlichkeit von Sicherheitssoftware. –> Foto: Adobe Stock

artigen Konstellation zusammen. In vier sogenannten *Research Hubs* dreht sich die Forschung um grundlegende, eher theoretische Fragen zur Kryptographie der Zukunft, um Plattformsicherheit und um Lösungen für komplexe sichere Systeme.

AUCH MENSCHLICHES VERHALTEN IM BLICK

Was das Vorhaben international einzigartig macht, ist der ganzheitliche interdisziplinäre Ansatz. So befassen sich die *CASA*-Wissenschaftler nicht nur mit technischen Fragestellungen, sondern untersuchen auch das Zusammenspiel von menschlichem Verhalten und IT-Sicherheit. Für die Anwendungsbereiche intelligente Produktion, Logistik und E-Health wollen die Forscher evaluieren, wie nutzerfreundlich und praktikabel die Ergebnisse des Exzellenzclusters sind. Diese ganzheitliche Betrachtung der Cybersicherheit, die Spitzenforschung, Interdisziplinarität und Anwendung integriert, birgt großes Potential für bahnbrechende Ergebnisse, die nicht nur die Wissenschaft grundlegend beeinflussen, sondern auch die Sicherheit praktischer Systeme langfristig verbessern können. Das *L3S* ist durch Prof. Dr. Sascha Fahl vertreten. Der Preisträger des Heinz-Mayer-Leibnitz-Preises 2018 wechselte im Februar 2019 von der *Ruhr-Universität Bochum* an die *Leibniz Universität Hannover*. Als wissenschaftlicher Leiter des *Research Hub Nutzerfreundlichkeit* befasst sich Sascha Fahl vor allem mit den menschlichen Herausforderungen von IT-Sicherheit und Privatsphäre. In einem ersten interdisziplinären *CASA*-Projekt erforscht er gemeinsam mit Prof. Dr. Angela Sasse von der *Ruhr-Universität Bochum* die Herausforderungen rund um die Integration von benutzbarer Sicherheit in Softwareprodukten während der Entwicklung. ¶

KONTAKT:
Prof. Dr. Sascha Fahl
Fahl@L3S.de

IT-Sicherheit in der Wirtschaft

Wirtschaftsspionage, Sabotage oder Datendiebstahl – die zunehmende Digitalisierung birgt für die Wirtschaft ein großes Sicherheitsrisiko. Zahlreiche Unternehmen digitalisieren ihre gesamte Wertschöpfungskette: von der Geschäfts- oder Konstruktionsidee über das Produkt und die Dienstleistung bis hin zur Logistik. Damit steigt die Gefahr, **über das Internet Opfer krimineller Angriffe zu werden.** Gerade in kleinen und mittleren Unternehmen gibt es auf dem Gebiet der Cybersicherheit sehr viel Handlungsbedarf. Studien zeigen auch für größere Unternehmen und für einzelne Bereiche der Wirtschaft, etwa der Finanzbranche, dass eine große Zahl der Unternehmen von Cyberangriffen betroffen ist. Auf diese Bedrohungslage muss die gesamte deutsche Wirtschaft angemessen reagieren und sich mit dem Thema der Informationssicherheit gezielt auseinandersetzen. Dies kann besonders gut gelingen, wenn die Unternehmen anhand aktueller und sorgfältig erarbeiteter Informationen erkennen können, auf welche Weise die Cyberangriffe erfolgen und wie man sich effektiv dagegen schützen kann.

GRÖSSTE STUDIE ZU CYBERATTACKEN

Am *L3S* führt die Forschungsgruppe von Prof. Dr. Sascha Fahl gemeinsam mit dem *Kriminologischen Forschungsinstitut Niedersachsen e.V. (KFN)* zum Thema Cyberangriffe gegen Unternehmen eine breit angelegte Untersuchung durch. Sie soll differenziertes Wissen zu den Angriffsarten und ihren Häufigkeiten liefern. Zudem wollen die beteiligten Forscherinnen und Forscher herausfinden, wie verbreitet Präventionsmaßnahmen und IT-Sicherheitsstandards in Unternehmen sind. Damit der Transfer der daraus hergeleiteten wissenschaftlichen Erkenntnisse in die Praxis gelingt, entwickeln die Wissenschaftler Präventionsstrategien und konkrete Handlungsempfehlungen für Unternehmen.

Ein Schwerpunkt des Projekts liegt auf der Informationssicherheit kleiner und mittelständischer Unternehmen (KMU). Insbesondere geht es um die Frage, welche Faktoren die Angriffswahrscheinlichkeit und die IT-Sicherheit beeinflussen. Das könnten etwa die Mitarbeiterzahl, die finanzielle Situation, die Arbeitsorganisation oder die Arbeitsabläufe sein. Dazu wurden im Rahmen des Forschungsprojektes 5.000 Unternehmen befragt. Die repräsentative Umfrage zählt derzeit zu den größten und aussagekräftigsten Studien zum Thema Cyberangriffe gegen Unternehmen, die unabhängig und nach wissenschaftlichen Gütekriterien durchgeführt und transparent dokumentiert wurde.

40 PROZENT DER UNTERNEHMEN BETROFFEN

Demnach wurden in den letzten zwölf Monaten etwa 40 Prozent der befragten Unternehmen Opfer mindestens eines Cyberangriffs. Wie stark Unternehmen betroffen sind, hängt nicht nur vom Wirtschaftszweig und der Unternehmensgröße ab. Die Forscher fanden heraus, dass sich die Betroffenheitsraten kleiner und mittlerer Unternehmen zum Teil deutlich erhöhen, wenn sie mehrere Standorte in

Deutschland oder mindestens einen zusätzlichen Standort im Ausland haben oder Güter beziehungsweise Dienstleistungen exportieren. Die Befragung befasste sich auch mit den Folgen des jeweils schwerwiegendsten Cyberangriffs. Bei 70 Prozent der Unternehmen entstanden direkte Kosten, insbesondere durch Sofortmaßnahmen zur Abwehr und Aufklärung, Wiederherstellung oder Wiederbeschaffung sowie externe Beratung.

MITARBEITER SENSIBILISIEREN

Überraschenderweise sind technische Maßnahmen bereits weit verbreitet. Daher sollte es bei vielen Unternehmen jetzt darum gehen, diese noch besser in organisatorische Abläufe und Prozesse einzubinden und das Zusammenspiel von Mensch und Technik stärker in den Blick zu nehmen. Eine zentrale Erkenntnis lautet: Es reicht nicht aus, IT-Sicherheitsmaßnahmen zu implementieren. Vielmehr müssen diese auch innerhalb des Unternehmens von den Beschäftigten mitgetragen und umgesetzt werden. ¶

Mehr dazu in der Kurzfassung des Forschungsberichtes:
→ *https://cybercrime-forschung.de/forschung/Cyberangriffe_gegen_Unternehmen_kurz.pdf*

Außerdem steht auch eine Langfassung zur Verfügung:
→ *https://cybercrime-forschung.de/forschung/Cyberangriffe_gegen_Unternehmen_FB.pdf*

Abbildung aus dem Forschungsbericht »Cyberangriffe gegen Unternehmen« des Kriminologischen Forschungsinstituts Niedersachsen.

DAS KRIMINOLOGISCHE FORSCHUNGSINSTITUT NIEDERSACHSEN

Das Kriminologische Forschungsinstitut Niedersachsen e.V. ist eines der führenden kriminologischen Forschungsinstitute Deutschlands. Es verfügt über breite Erfahrungen in der Untersuchung unterschiedlicher Formen von Kriminalität. Die 1992 und 2011 durchgeführten Dunkelfeldbefragungen (mit bis 44.000 Personen) gelten bis heute als die zentralen viktimologischen Studien Deutschlands.
Eine besondere Stärke des Institutes liegt darin, dass es Phänomene der Kriminalität in ihrer gesellschaftlichen Dimension betrachtet. Daneben verfügt das KFN über eine praxisnahe Ausrichtung. Dies bedeutet, dass Forschungsvorhaben stets mit Vertretern der Praxis entwickelt und durchgeführt werden.

KONTAKT:
Prof. Dr. Sascha Fahl
Fahl@L3S.de

CISPA

HELMHOLTZ-ZENTRUM FÜR INFORMATIONSSICHERHEIT
UND LEIBNIZ UNIVERSITÄT HANNOVER

Neue Kooperation zu Cybersicherheitsforschung

Informationssicherheit und Datenschutz sind für die heutige Gesellschaft von zentraler Bedeutung. Sicherheitskritische Infrastrukturen wie die Energie- und Wasserversorgung, das Gesundheitswesen oder Kommunikations- und Transportnetze laufen ständig Gefahr, über fehlerhafte Computersysteme ausspioniert oder sabotiert zu werden. Die leichte Verfügbarkeit umfangreicher Datensätze birgt beispiellose Risiken für die Sicherheit von Unternehmen und für die Privatsphäre jedes Nutzers. Die zugrundeliegenden Fragestellungen sind hochkomplex und erfordern erhebliche Fortschritte in der Forschung zur Informationssicherheit und zum Schutz der Privatsphäre. Auf diese Situation hat die Bundesregierung mit umfangreichen Investitionen in die Sicherheitsforschung reagiert und – als Leuchtturm – ein neues Forschungszentrum ins Leben gerufen: das *Helmholtz-Zentrum für Informationssicherheit (CISPA)* in Saarbrücken. Seit seiner Gründung und der Aufnahme in die *Helmholtz-Gemeinschaft* im Jahr 2019 hat sich das *CISPA* zu einer der weltweit führenden Forschungseinrichtungen für Informationssicherheit und Datenschutz entwickelt.

Die Aufgabe des *CISPA* besteht darin, die drängenden und großen Herausforderungen unserer digitalen Gesellschaft im Bereich der Cybersicherheit und des Datenschutzes umfassend und ganzheitlich zu behandeln. Die derzeit 22 leitenden Wissenschaftlerinnen und Wissenschaftlern kombinieren Grundlagenforschung mit innovativer anwendungsorientierter Forschung, Technologietransfer und gesellschaftlichem Diskurs. Fünf Forschungsbereiche decken das gesamte Spektrum von der Theorie bis zur empirischen Forschung ab: vertrauenswürdige Informationsverarbeitung, zuverlässige Sicherheitsgarantien, Bedrohungserkennung und -abwehr, sichere mobile und autonome Systeme sowie empirische und verhaltensbasierte Sicherheit.

NUTZERORIENTIERTE TECHNIK

Einer der Gründe, warum wirkungsvolle Informationssicherheit so schwierig zu erreichen ist: Sie betrifft reale Nutzer und reale Softwaresysteme in der Praxis, nicht in der Theorie. Aus Sicherheitsperspektive handeln Nutzer nicht unbedingt rational. Da die Anwendungen und Systeme, mit denen sie interagieren,

CYBER-SICHERHEIT

Die strategische Zusammenarbeit wurde im Oktober 2020 in einem Kooperationsvertrag zwischen der LUH und CISPA sowie einer Absichtserklärungserklärung zwischen dem Land Niedersachsen und CISPA manifestiert. (V.l.n.r.) Björn Thümler, Niedersächsischer Minister für Wissenschaft und Kultur, Prof. Dr. Michael Backes, Gründungsdirektor CISPA Helmholtz-Zentrum für Informationssicherheit, Dr. Bernd Althusmann, Niedersachsens Minister für Wirtschaft, Arbeit, Verkehr und Digitalisierung, und Prof. Dr. Volker Epping, Präsident LUH. –> Screenshot: Niedersächsisches Ministerium für Wissenschaft und Kultur auf Youtube
→ https://www.youtube.com/watch?v=24FIDMAiac8&feature=emb_logo

ein enormes Maß an Komplexität erreicht haben, können Nutzer kaum einschätzen, was im Hinblick auf Informationssicherheit und Privatsphäre schiefgehen könnte. Verschärft wird dies durch einen gravierenden Mangel an Verständnis, wie Sicherheits- und Datenschutzmaßnahmen durchzuführen sind. Sie werden eher als Hindernis denn als Hilfe betrachtet und daher häufig ignoriert oder umgangen. Nun kann niemand von Nutzern verlangen, dass sie Sicherheitsexperten werden, um ihre Daten erfolgreich schützen zu können. Daher entwickeln *CISPA*-Wissenschaftler auf dem Gebiet der *Usable Security and Privacy* Technologien, die sich an den Fähigkeiten und Bedürfnissen ihrer Nutzer orientieren – als Beitrag zur Informationssicherheit in der realen Welt.

NIEDERSACHSEN FÖRDERT SICHERHEITSFORSCHUNG

Die niedersächsische Landesregierung hat die Bedeutung der Forschung zur Informationssicherheit und zum Datenschutz erkannt und stärkt diese Bereiche an der *Leibniz Universität Hannover (LUH).*

»Die neue Zusammenarbeit zwischen *CISPA* und der *Universität Hannover* mit seinem renommierten *Forschungszentrum L3S* ist ein großer Gewinn für den Forschungsstandort Niedersachsen – und ein Ausweis seiner Stärke im Bereich Künstliche Intelligenz, Data Science und IT-Sicherheit.«

BJÖRN THÜMLER, NIEDERSACHSENS MINISTER FÜR WISSENSCHAFT UND KULTUR

Mitte 2020 unterzeichneten das *CISPA* und die *LUH* eine Kooperationsvereinbarung über eine Zusammenarbeit auf dem Gebiet der Informationssicherheit, speziell der *Usable Security and Privacy*. Gemeinsam mit dem Land Niedersachsen haben *CISPA* und *LUH* nun die Gründung einer unselbständigen Betriebsstätte des *CISPA* in Hannover initiiert. Eingeleitet wird die Zusammenarbeit durch die gemeinsame Berufung von *L3S*-Mitglied Sascha Fahl, seit 2019 Professor an der *LUH* und Träger des Heinz Maier-Leibnitz-Preises 2018 der *Deutschen Forschungsgemeinschaft (DFG)*. Das Forschungsprofil von Professor Fahl auf dem Gebiet der Cybersicherheit passt hervorragend zum *CISPA*. Als weiterer Schritt ist für Anfang 2021 die Einrichtung einer Nachwuchsgruppe auf dem Gebiet der Informationssicherheit mit dem Schwerpunkt *Industrial Security* geplant. ¶

KONTAKT:
Prof. Dr. Sascha Fahl
Fahl@L3S.de

SICHERE GESELLSCHAFTEN

An dem EU-Forschungsprojekt ROXANNE ist unter anderem auch Interpol beteiligt – hier deren Hauptsitz in Lyon. –> Foto: Wikimedia

KI für eine gerechte EU

Eine sichere, freie und integrative Gesellschaft ist ein wesentliches Ziel der Europäischen Union – und zugleich eine große Herausforderung. Vor dem Hintergrund eines beispiellosen globalen Wandels, wachsender Abhängigkeiten und Risiken fördert die EU Forschungs- und Innovationsprojekte, mit denen die zivile Sicherheit der europäischen Gesellschaft und ihrer Bürger gestärkt werden soll. Die EU erhofft sich davon, sich entwickelnde Risiken früher erkennen und verhindern sowie besser handhaben zu können. Das *L3S* leistet mit den EU-Projekten *MIRROR* und *ROXANNE* einen Beitrag.

MIRROR: FEHLINFORMATIONEN ERKENNEN

Migration ist auch für die Europäische Union ein wichtiges Thema, das mit Chancen, aber auch mit Risiken verbunden ist – sowohl für die Migranten als auch für die Gesellschaften. Wie potentielle Zuwanderer die EU und ihre Mitgliedsstaaten wahrnehmen, hat einen hohen Einfluss auf Entscheidungen, die sie vor und auf dem risikoreichen Weg nach Europa treffen. Das Bild, das Menschen von Europa haben, kann jedoch von eingeschränkter Wahrnehmung und gezielten Desinformationskampagnen beeinflusst werden. Die daraus resultierenden Fehleinschätzungen beeinträchtigen die Entscheidungen im Kontext der Migration, etwa die Wahl der Route, und können zu zusätzlichen Risiken sowohl für Migranten als auch für die Grenzsicherheit führen. Behörden und politische Entscheidungsträger wollen daher besser einschätzen können, wie Europa wahrgenommen wird und welche Risiken sich daraus ergeben. Im EU-Projekt *MIRROR* entwickeln Wissenschaftler des *L3S* eine integrierte Plattform und eine systematische Methodik, um öffentlich zugängliche Quellen mit dieser Fragestellung umfassend zu analysieren. So sollen Diskrepanzen zwischen Erwartungen und Realität erkannt werden. Ein KI-basiertes Modell durchsucht dazu beispielsweise soziale Medien, Nachrichtenportale und andere Quellen nach migrationsrelevanten Texten, Bildern und Videos und schätzt die Stimmung im Hinblick auf ökonomische und soziale Faktoren ein, etwa die Lage auf dem Arbeitsmarkt oder die Situation von Minderheiten. Dabei stellt das Modell die Stimmungslage in Europa dem Bild Europas in den Herkunftsländern potentieller Zuwanderer gegenüber.

Bei der Entwicklung und dem Einsatz der Technologien berücksichtigt *MIRROR* auch ethische und rechtliche Aspekte sowie Fragen der gesellschaftlichen Akzeptanz. Um ein fundiertes Bild der Wahrnehmung Europas zeichnen zu können, vereint das Projekt Experten aus unterschiedlichen Diszplinen und Einrichtungen, darunter Hochschulen, IT-Unternehmen, Sicherheitsbehörden und Nichtregierungsorganisationen (NGOs). → *https://h2020mirror.eu*

ROXANNE: KRIMINELLE NETZWERKE AUFSPÜREN

In Sicherheitsfragen steht die Europäische Union vor wachsenden und zudem immer komplexer werdenden Herausforderungen. Eine erhebliche Bedrohung für die moderne Gesellschaft und die Sicherheit Europas ist die organisierte Kriminalität – die am schwierigsten zu untersuchende Form der Kriminalität. Beträchtliche Finanzströme verschaffen kriminellen Netzwerken Zugang zu Ressourcen und modernen Technologien. Die polizeilichen Ermittler überwachen zwar Datenkanäle und identifizieren relevante Personen und Orte, die sie anhand ihrer Beziehungen und Aktionen zu Netzwerken verknüpfen. Aber besonders in den größeren Fällen organisierter Kriminalität bleibt die Ermittlungsarbeit schwierig und zeitaufwändig – vor allem aufgrund der Komplexität der Netzwerke und der großen Datenmengen, die ausgewertet werden müssen und die mit Unsicherheiten behaftet sind. Ein zusätzliches Problem: Die Täter kommunizieren in unterschiedlichen Sprachen. In diesen Situationen übersteigt die Arbeitsbelastung häufig die Möglichkeiten des Ermittlerteams. Rund 80 Prozent des Zeitaufwands entfallen allein auf die Datenbereinigung und -normalisierung. Eine weitere Herausforderung bei der Fallbearbeitung ist das Herausfiltern relevanter Informationsquellen. Außerdem gibt es für bestimmte Aufgaben keine Softwarelösungen, etwa für die Analyse von Geodaten. Um dem entgegenzuwirken, befasst sich das *L3S* im EU-Forschungsprojekt *ROXANNE* mit Netzwerk-, Text- und Audio-Analyse für eine effektive Bekämpfung organisierter Kriminalität. Beteiligt sind weitere Forschungspartner und Sicherheitsbehörden, darunter Interpol und einer Reihe europäischer Strafverfolgungsbehörden. Die *ROXANNE*-Plattform ist in der Lage, schnell und automatisch Audioquellen zu verarbeiten und zu analysieren. Sie kann in den Datenquellen Bezüge zwischen den Quellen herstellen sowie Texte in mehreren Sprachen automatisch erkennen und verarbeiten, ergänzt durch Video- und geographische Meta-Informationsverarbeitung. Schließlich werden die Beziehungen zwischen relevanten Entitäten wie Personen oder Orte automatisch ermittelt und analysiert. Auf diese Weise erhalten die Ermittler ein verbessertes Bild der kriminellen Netzwerke. Allerdings spiegeln die zur Verfügung stehenden Informationen nur Vermutungen wider, die zudem durch die automatische Extraktion mit Unsicherheiten behaftet sind. In diesem Bereich forscht das *L3S* und entwickelt neuartige KI-Algorithmen, die auch bei Unsicherheiten in den Daten gute Ergebnisse liefern können. ¶

→ *https://roxanne-euproject.org*

KONTAKT:
Dr. Claudia Niederée

niederee@L3S.de

\\\ Claudia Niederée ist Forschungsgruppenleiterin am *L3S*. Sie koordiniert und leitet das Projekt *MIRROR*. \\\

Dr. Sergej Zerr

SZerr@L3S.de

\\\ Sergej Zerr ist Forschungsgruppenleiter am *L3S* und Projektleiter von *ROXANNE*. \\\

Dr. Erick Elejalde

Elejalde@L3S.de

\\\ Erick Elejalde ist Postdoc am *L3S* und Projektleiter von *MIRROR*. \\\

Die Digitalisierung der Pflege kann eher gelingen, wenn Pflegekräfte und Gepflegte in die Entwicklung neuer Technologien eingebunden werden. Im Forschungsprojekt OPAL *erforschen, koordinieren und begleiten Soziologen des* L3S *die Möglichkeiten der partizipativen Technikgestaltung. –> Foto: Adobe Stock*

DIGITALE LÖSUNGEN GEGEN DEN PFLEGENOTSTAND

Partizipative Technikentwicklung für die Pflege 4.0

Jeder zweite Deutsche ist älter als 45 Jahre. Wer wird sich in Zukunft um die steigende Zahl pflegebedürftiger Menschen kümmern? Schon heute herrscht in der Pflege ein Fachkräftemangel und die Pflegekräfte gehen in ihrem Arbeitsalltag an die Grenzen der Belastbarkeit. Wie bei kaum einem anderen gesellschaftlichen Problem sind die Hoffnungen groß, dass digitale Technologien zur Lösung des Pflegenotstandes beitragen werden. Und so erscheinen Informations- und Assistenzsysteme, E-Health-Anwendungen oder sogar Pflegeroboter als Chance für eine Pflege 4.0. Digitale Technologien sollen nicht nur die Pflegenden entlasten und die Lebensqualität der Gepflegten verbessern, sondern auch die Effizienz der Pflegeleistungen erhöhen. Pflege soll also langfristig digital werden. Dieser Zukunftsvision steht der immer noch sehr geringe Einsatz digitaler Technologien im Pflegealltag gegenüber. Trotz massiver Förderung sind nur wenige Anwendungen in den Pflegeheimen zu finden. Woran liegt das? Warum bleibt das Potential der digitalen Transformation in der Pflege bisher eindeutig hinter den Möglichkeiten zurück?

Der Grund liegt in der mangelnden Gebrauchstauglichkeit im pflegerischen Alltag. Die geringe Akzeptanz bei den Zielgruppen zeigt: Es reicht nicht, Technologien für die Pflege bereitzustellen. Vielmehr müssen sie gemeinsam mit den zukünftigen Nutzern entwickelt werden. Solch eine partizipative Technikgestaltung soll die unterschiedlichen Akteure aus der pflegerischen Praxis und den beteiligten wissenschaftlichen Disziplinen zusammenbringen – samt ihrer jeweiligen Perspektiven und Anforderungen an die Technologien. Dieses komplexe Verfahren kann nur gelingen, wenn neben Pflegekräften und Gepflegten auch Soziologen in die Technikentwicklung eingebunden werden. Sie sollen die komplexen Interaktionen während der Technikentwicklung koordinieren und bei Konflikten notfalls intervenieren.
Mit dem Projekt *Optimierung der Pflege in der Altenhilfe durch Sensornetzwerke*, kurz *OPAL*, fördert das Land Niedersachsen modellhaft die partizipative Einführung innovativer Sensortechnik, um die Situation der Bewohner und Pflegekräfte in Altenheimen zu verbessern. Im soziologischen Teilprojekt von *OPAL* erforschen Soziologen des *L3S*, wie

sich die Technikgenese zusammen mit Praxispartnern aus Pflege und Technikentwicklung möglichst partizipativ gestalten lässt. Mithilfe eines qualitativen Forschungsdesigns, das Interviews und Fokusgruppen-Diskussionen umfasst, begleiten Prof. Dr. Stefanie Büchner, Dr. Jannis Hergesell und Malte Weber vom *L3S* die Einführung von Sensorbetten in einem Altenheim. Die Wissenschaftler wollen herausfinden, wie sich digitale Anwendungen auf Arbeitsorganisation und Pflegepraktiken auswirken, wo mögliche Problemfelder liegen und Potentiale bisher ungenutzt bleiben. Der innovative Ansatz von *OPAL:* Die Implementierung der Sensorbetten wird kontinuierlich sozialwissenschaftlich evaluiert und alle Beteiligten stehen in engem Austausch. So kann partizipative Technikgestaltung erreichen, dass Pflegende und Gepflegte die digitalen Neuerungen akzeptieren und tatsächlich auch zu ihrem Vorteil nutzen. ¶

KONTAKT:

Jun.-Prof. Dr. Stefanie Büchner

Buechner@L3S.de

\\\ *L3S-Mitglied Stefanie Büchner leitet den Arbeitsbereich Soziologie der Digitalisierung am Institut für Soziologie der Leibniz Universität Hannover. Sie forscht zum Spannungsfeld von Digitalisierung und Organisationen.* \\\

Dr. Jannis Hergesell

Hergesell@L3S.de

\\\ Jannis Hergesell ist Postdoc am L3S und am Arbeitsbereich Soziologie der Digitalisierung am Institut für Soziologie der Leibniz Universität Hannover. Er leitet das Projekt OPAL operativ. \\\

Malte Weber, M. A.

mweber@L3S.de

\\\ Malte Weber ist wissenschaftlicher Mitarbeiter am L3S im Projekt OPAL und am Institut für Soziologie der Leibniz Universität Hannover. \\\

DATENNUTZUNG IN DER INDUSTRIE 4.0

Rechtliche Implikationen intelligenter Produktion

Künstliche Intelligenz (KI) in der Produktion – laut Studien sind dadurch Produktivitätssteigerungen von bis zu 50 Prozent möglich. Erforderlich ist der Einsatz von KI auf allen Ebenen der Produktion und – vor allem – über die jeweiligen Unternehmensgrenzen hinweg. Damit gehen jedoch vielfältige rechtliche wie technische Herausforderungen einher. Im Projekt *IIP-Ecosphere* arbeitet das *L3S* in einem Konsortium aus Forschungspartnern und Unternehmen daran, den Einsatz von KI in der Produktion zu erleichtern. *IIP-Ecosphere* hat das Ziel, Produktivität, Flexibilität und Effizienz der Produktion durch intelligente und vernetzte Systeme zu steigern. *L3S*-Wissenschaftler des *Instituts für Rechtsinformatik (IRI)* um Prof. Dr. Tina Krügel helfen dabei, die juristischen Hürden der intelligenten Produktion zu überwinden.

Drei Bereiche rücken die Juristen in den Fokus: Das Datenschutzrecht, geistiges Eigentum sowie das Wettbewerbs- und Kartellrecht. Beim Datenschutz geht es insbesondere um die Frage, wann ein Personenbezug bei der Datennutzung entstehen kann – etwa durch die Verarbeitung von Metadaten aus der Produktion, die gleichzeitig Rückschlüsse auf die Produktivität der Mitarbeiter zulassen könnten. Im Bereich des geistigen Eigentums sind insbesondere die Nutzungs- und Verwertungsmöglichkeiten automatisch generierter Daten, zum Beispiel Sensordaten, von Interesse. Im Wettbewerbs- und Kartellrecht geht es schließlich um den Schutz von Geschäftsgeheimnissen sowie allgemein um den Zugang zu Daten durch Plattformen wie *IIP-Ecosphere*.

Die Juristen verfolgen dabei einen anwendungsorientierten Ansatz, der neben wissenschaftlichen Publikationen auch Praxishilfen hervorbringen soll. In *IIP-Ecosphere* binden sie daher die Partnerunternehmen eng in ihre Forschung ein, so wie kürzlich durch eine Befragung und einen daran anknüpfenden Workshop. Die Kooperation dient nicht nur dazu, praxisrelevante Problemstellungen zu identifizieren, sondern auch Lösungsvorschläge und Hilfestellungen zu erarbeiten. ¶

→ *www.iip-ecosphere.eu*

KONTAKT:
Prof. Dr. Tina Krügel, LL.M.
kruegel@L3S.de

\\\ *L3S*-Mitglied Tina Krügel ist Inhaberin des Lehrstuhls für IT-Recht am *IRI*. \\\

KONTAKT:
Dipl.-Jur. Ricarda Puschky
puschky@L3S.de

\\\ Ricarda Puschky ist wissenschaftliche Mitarbeiterin am *L3S* und am *IRI*. \\\

DIE ZAHL

DIE AUSGABEN
FÜR IT-SICHERHEIT
IN DEUTSCHLAND IM JAHR 2019
BETRUGEN

4,9

MILLIARDEN EURO.
Im Jahr 2020 sollen in Deutschland rund 5,2 Milliarden Euro für IT-Sicherheit ausgegeben werden.
Quelle: Statista

NEUE MITGLIEDER AM *L3S*

Seit Oktober 2020 ist sie Universitätsprofessorin für Praktische Informatik, Data Science und Intelligente Systeme an der *Universität Bonn:* **Elena Demidova.** Zuvor war sie als Forschungsgruppenleiterin am *L3S* tätig sowie Senior Research Fellow bei der *Web and Internet Science Group der University of Southampton.* Elena Demidova studierte Information Engineering an der Universität Osnabrück in einem gemeinsamen Masterprogramm mit der Universität Twente. Anschließend promovierte sie an der *Leibniz Universität Hannover.* Ihre Forschungsschwerpunkte sind Datenwissenschaften, Open Data, Web und Semantic Web.

Ziawasch Abedjan ist Universitätsprofessor und Leiter des Fachgebietes *Datenbanken und Informationssysteme* an der *Leibniz Universität Hannover.* Studiert und promoviert hat er am *Hasso-Plattner-Institut* in Potsdam. Anschließend war er zwei Jahre als Postdoc am *Massachusetts Institute of Technology* tätig. Bevor er an die *Leibniz Universität Hannover* wechselte, war **Ziawasch Abedjan** Juniorprofessor an der *TU Berlin* und Senior Rearcher am *DFKI.* Er forscht an Methoden der Datenintegration und der Vorverarbeitung von Daten für Data-Science-Anwendungen. Seine Forschung wird durch Drittmittel der *DFG* und des *BMBF* gefördert. ¶

PROMOTIONEN AM *L3S*

Dr. rer. nat. Ran Yu
»Improving Knowledge Accessibility on the Web – from Knowledge Base Augmentation to Search as Learning«
FEBRUAR 2020
DOKTORVATER:
PROF. DR. STEFAN DIETZE

»Während meines Informatikstudiums hatte ich Gelegenheit, an Programmierwettbewerben teilzunehmen. Dabei wurde mir bewusst, wie viel Spaß mir das Lösen kniffliger Probleme mit Algorithmen und Computerprogrammen macht.« Nach ihrem Master-Abschluss an der Chinesischen Akademie der Wissenschaften entschied sich **Ran Yu** daher für eine Promotion am *L3S*. »In meiner Doktorarbeit befasste ich mich mit Methoden zur Erweiterung von Wissensgraphen mit Hilfe von Webdaten sowie zum Verständnis, zur Modellierung und zur Unterstützung des menschlichen Lernens bei der Websuche mit statistischen Methoden und Techniken des maschinellen Lernens. Meine Dissertation hat den *Preis der chinesischen Regierung 2019 für herausragende selbstfinanzierte Studenten im Ausland* gewonnen.« ¶
KONTAKT: yu@L3S.de

Dr. rer. nat. Christoph Hube
»Methods for Detecting and Mitigating Linguistic Bias in Text Corpora«
MAI 2020
DOKTORVATER:
PROF. DR. WOLFGANG NEJDL

»Ich wollte unbedingt etwas Zukunftsorientiertes studieren. Da lag Informatik nahe, zumal ich Erfahrungen mit Programmierung hatte.« **Christoph Hube** lernte an der *Leibniz Universität Hannover* das *L3S* kennen und schrieb dort später auch seine Masterarbeit. »Das Angebot einer Doktorandenstelle nahm ich gerne an. Meine Promotion befasst sich mit Voreingenommenheit und versteckten Meinungen in Textdaten, wie man sie auf Wikipedia oder auf News-Seiten findet. In meiner neuen Position als Data-Scientist bei *Concordia-Versicherungen* gestalte ich die Datenlandschaft des Unternehmens mit und wende moderne Verfahren des maschinellen Lernens an, um neue hilfreiche Erkenntnisse aus großen Datenmengen zu gewinnen. Die nötigen Grundlagen habe ich am *L3S* gelernt.« ¶
KONTAKT: hube@L3S.de

Dr. rer. nat. Vasileios Iosifidis
»Semi-supervised learning and fairness-aware learning under class imbalance«
JULI 2020
DOKTORMUTTER:
PROF. DR. EIRINI NTOUTSI
»Seit ich denken kann, wollte ich wissen, wie Computer funktionieren und was man mit ihnen machen kann. Im Jahr 2009 begann ich daher ein Informatikstudium.« Zum Promovieren kam **Vasileios Iosifidis** anschließend an das *L3S* nach Hannover. »Als Doktorand habe ich das Problem des Fairness-bewussten maschinellen Lernens untersucht. Algorithmen des maschinellen Lernens können diskriminierend gegenüber Einzelpersonen oder Gruppen mit bestimmten Merkmalen wirken. Aufgrund ungleichmäßiger Datenverteilung sind Algorithmen nicht in der Lage, genaue Vorhersagen für diese Gruppen zu liefern, sie klassifizieren also relativ mehr Personen dieser Gruppen falsch. Ich habe mehrere Modelle entwickelt, die sich mit diesem Problem befassen, und auf Top-Konferenzen vorgestellt.« ¶
KONTAKT: iosifidis@L3S.de

WEGE ZUR BINAIRE

BESTELLUNG:

Haben Sie Interesse an einzelnen Exemplaren oder möchten Sie ein Abo bestellen? Mailen Sie einfach an die Redaktion! Gerne senden wir Ihnen die *Binaire* kostenlos zu.

Innovation durch Forschung
→ *vergriffen*

Maschinelles Lernen
→ *vergriffen*

Digitale Bildung
→ *einzelne Exemplare bestellbar*

Mobilität von morgen
→ *bestellbar*

Big Data in der Medizin
→ *bestellbar*

Intelligente Produktion
→ *bestellbar*

Künstliche Intelligenz
→ *bestellbar*

Innovationen, Krisen, Startups
→ *bestellbar*

Sicherheit, Datenschutz, Ethik
→ *bestellbar*

Die Binaire können Sie als Pdf-Dokument auch online lesen.

www.binaire.de

Binaire
DAS MAGAZIN DES FORSCHUNGSZENTRUMS L3S

IMPRESSUM

HERAUSGEBER:
Forschungszentrum L3S
Leibniz Universität Hannover
Appelstraße 9a
30167 Hannover

VERANTWORTLICH:
Prof. Dr. techn. Wolfgang Nejdl
Geschäftsführender Direktor

REDAKTION:
Dipl.-Geogr. Susanne Oetzmann
Telefon: +49 511 762-177 34
E-Mail: Oetzmann@L3S.de

KONZEPT & DESIGN:
Dipl.-Des. Priska Tosch
www.tosch-kommunikation.de

DRUCK:
auf 100% Recyclingpapier
Ströher Druckerei und Verlag
GmbH & Co. KG
www.stroeher-druck.de

klimaneutral gedruckt
www.klima-druck.de
ID-Nr. 2097220
bvdm.

BILDQUELLEN:
Forschungszentrum L3S,
wenn nicht anders vermerkt.
Titelbild-Illustration:
Falko Lohrenscheit

www.L3S.de

Leibniz Universität Hannover

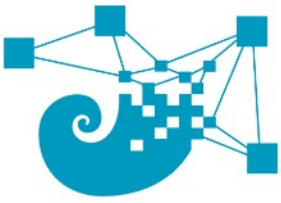
Technische Universität Braunschweig

IIP-Ecosphere

Next Level Ecosphere for
Intelligent Industrial Production

Gestalten Sie mit uns die KI-Plattform für die Produktion von morgen!

www.iip-ecosphere.eu



Wir entwickeln mit Ihnen ein KI-Ökosystem, das Industrie, Dienstleister, Verbände und Forschung vernetzt.

Wir gestalten gemeinsam eine digitale Plattform für KI- und datenbasierte Geschäftsmodelle.

Wir erarbeiten zusammen »Easy-to-use«-KI und ganzheitliche Optimierungs-algorithmen für die Produktion von morgen.

Wir bieten Workshops, Lehrgänge und Qualifikations-maßnahmen, um KI in die Praxis zu bringen.