bringen. Das ist in den letzten Jahren oft gelungen, könnte aber noch intensiviert werden. W&F ist ein passendes Publikationsorgan für das Thema Rüstung und Informatik in all seinen Facetten, wenn eine Leser:innenschaft weit jenseits der Informatik erreicht werden soll.

Wenn eine seit 40 Jahren bestehende Zeitschrift wie auch das fast so alte FIfF „Frieden" im Namen führen, dann muss man leider konstatieren, dass diese Thematik weiterhin schreckliche Aktualität besitzt, weil Krieg eine alltägliche Realität darstellt, weil Konflikte in vielen Teilen der Welt zu eskalieren drohen und weil Politik regional bis weltweit wenig erfolgreich dagegen arbeitet, wenn sie sich überhaupt darum kümmert. Ein betrübliches, ja skandalöses Beispiel hat gerade der deutsche Verteidigungsminister Boris Pistorius gegeben, der bei *Berlin direkt*[1] sagt: „Wir müssen kriegstüchtig werden." Sein Versuch, diesen Begriff als synonym zu „verteidigungsfähig" hinzustellen, ist irreführend. Denn hätte er „verteidigungsfähig" gemeint, hätte er das ja auch sagen können. „Kriegstüchtig" bedeutet laut Duden, für einen Krieg gut gerüstet zu sein. Für welchen Krieg? Wo und gegen wen soll Deutschland Krieg führen? Krieg ist nach der UN-Charta verboten. Wozu müssen wir, Deutschland, die Bundeswehr „tüchtig" sein, Verbotenes zu tun? Es gibt allerdings zwei Ausnahmen: Wenn ein Staat angegriffen wird, darf er sich verteidigen; und wenn die UN einen Krieg beenden oder verhindern will, darf sie militärisch eingreifen. „Verteidigungsfähig" ist

Hans-Jörg Kreowski auf dem Jubiläumssymposium

also das viel richtigere Wort, das auch durch das Grundgesetz gedeckt ist. Der Kriegsminister Pistorius muss also wohl etwas anderes meinen, und er steht da in der Regierung anscheinend nicht allein. Wie wäre es mit „friedenstüchtig"?

Um einen berühmten Dichter des 20. Jahrhunderts zu zitieren: *„Imagine all the people living life in peace"* (John Lennon 1971).

1 *Verteidigungsminister Pistorius im Interview mit Dominik Rzepka, zdfheute am 29.10.2023 um 20:37 h*

Anja-Liisa Gonsior, Thea Riebe, Stefka Schmid, Thomas Reinhold und Christian Reuter

Friedensinformatik: heute und morgen

Fortschritte in Wissenschaft und Technologie spielen eine entscheidende Rolle im Zusammenhang mit Frieden, Konflikt und Sicherheit (Reuter 2019). Insbesondere die Rolle der Informatik in der Friedens- und Konfliktforschung hat sich durch die Digitalisierung der Gesellschaft gewandelt. Die Bewältigung der damit verbundenen Herausforderungen für Frieden und Sicherheit durch die akademische Forschung erfordert die Anwendung und Etablierung interdisziplinärer Ansätze (Reuter et al. 2020). An dieser Stelle kann die naturwissenschaftlich-technische Friedens- und Konfliktforschung entscheidende Beiträge leisten, um aktuelle Themen und damit verbundene Problemstellungen aus verschiedenen disziplinären Perspektiven zu analysieren und zu bewerten. So müssen beispielsweise Fragen im Kontext von Cyberangriffen oder Cyberwaffen sowohl aus der Perspektive der Informatik als auch der Politikwissenschaft betrachtet werden (Reuter et al. 2020).

Einleitung

Das Forschungsfeld der *Friedensinformatik* kann als Subdisziplin der naturwissenschaftlich-technischen Friedens- und Konfliktforschung bezeichnet werden. Diese beschäftigt sich mit der Rolle informationstechnischer Artefakte in Konflikten und Kriegen sowie mit der Gestaltung von informationstechnischen Systemen, welche zur Gewaltvermeidung oder friedlichen Transformation von Konflikten beitragen können. Dazu gehören Aspekte wie die Widerstandsfähigkeit von informationstechnischen Infrastrukturen, beispielsweise als Zielscheibe in Konfliktsituationen, aber auch die Rolle von IT-Anwendungen bei der Prävention und Bewältigung von Konflikten, Krisen und Katastrophen (Reuter 2019). Darüber hinaus behandelt die Friedensinformatik unter anderem Themen in den Bereichen Cyber-Rüstungskontrolle, *Dual-Use*-Forschung, künstliche Intelligenz (KI) und autonome Systeme. Es werden interdisziplinär Konzepte und Methoden aus der Informatik und den Sozialwissenschaften zusammengeführt, wie der Mensch-Computer-Interaktion, IT-Sicherheit, Technikfolgenabschätzung und Politikwissenschaft. In den *Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung* wies der deutsche Wissenschaftsrat 2019 auf den dringenden Handlungsbedarf zur Stärkung der naturwissenschaftlich-technischen Friedens- und Konfliktforschung hin, die in Deutschland derzeit strukturell zu schwach ist, um den massiven Bedarf an Politikberatung zu decken (Wissenschaftsrat 2019). Dieser Beitrag möchte einen Einblick in ausgewählte aktuelle Arbeitsthemen und Bereiche der Friedensinformatik am Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit* (PEASEC) der Technischen Universität Darmstadt geben.

Cyberwaffen, die Militarisierung des Cyberspace und Cyber-Rüstungskontrolle

Mit Blick auf die zunehmende Militarisierung des Cyberspace und die damit verbundenen Gefahren und Bedrohungen erge-

ben sich in diesem Bereich vielfältige Herausforderungen. In diesem Kontext wappnen sich weltweit bereits viele nationale und internationale Sicherheitsdoktrinen gegen Software, die entwickelt wurde, um in IT-Systeme eingespeist zu werden mit dem Ziel der Spionage oder Sabotage (Reinhold & Reuter 2022). Das prominenteste Beispiel ist sicher der Einsatz der Schadsoftware *Stuxnet*, die im Jahr 2010 entdeckt wurde und die das industrielle Kontrollsystem einer Nuklearanlage im Iran manipulierte mit dem Ziel, Schwellenwerte und Parameter der Kontrollsoftware heimlich zu ändern, um dadurch den Produktionsprozess zu sabotieren (Langner 2013). Das Beispiel demonstriert, wie Bedrohungen aus dem Cyberraum Einfluss auf physische Infrastrukturen haben können. Vor dem Hintergrund derartiger Bedrohungen versuchen nationale Regierungen und Geheimdienste nicht nur, geeignete Verteidigungsmaßnahmen gegen Schwachstellen von Computersystemen zu etablieren, sondern teilweise gleichzeitig auch, dies für die offensive Planung von eigenen Cyberangriffen zu nutzen (Reinhold & Reuter 2022).

Durch die steigende Abhängigkeit von Informationstechnologien in ökonomischen, gesellschaftlichen und politischen Bereichen ergeben sich zahlreiche Herausforderungen. Dennoch bzw. gerade deswegen besteht derzeit kein einheitliches international anerkanntes Verständnis über die Bedrohung durch Cyberwaffen und ihre Verhinderung, geschweige denn über ein verbindliches Rechtsinstrument. Eine weitere Herausforderung stellt das sogenannte *Attributionsproblem* dar, also der forensische und politische Prozess der Gewinnung gesicherter Erkenntnisse über den Ursprung eines Cyberangriffs (Saalbach 2019). Attribution stellt ein wichtiges Instrument dar, um die Wirksamkeit und Durchsetzbarkeit völkerrechtlicher Normen und Grundlagen auch im Cyberspace zu verbessern, indem der Akteur hinter einem Angriff klar benannt und in Verantwortung genommen werden kann. Dies gilt beispielsweise für den gebotenen Schutz der Zivilbevölkerung oder die Rechtmäßigkeit von Verteidigungsmaßnahmen eines angegriffenen Staates. Auch für die Rüstungskontrolle ist es sinnvoll, den Einsatz einer bestimmten Cyberwaffe und deren Ursprung zu ermitteln. Neben einer fehlenden Definition von Cyberwaffen und dem Attributionsproblem erschweren zudem die Virtualität des Cyberspace, die fehlende physische Form von Sicherheitslücken und Schadsoftware, ständige technologische Weiterentwicklung, fehlender politischer Wille, Verifizierung sowie der Einfluss zahlreicher Akteure den Umgang mit Cyberwaffen (Reinhold et al. 2023). Daher versagen vielfach etablierte Konzepte der Rüstungskontrolle für den Cyberspace und neue Ansätze, die den technischen Besonderheiten dieses Raumes Rechnung tragen, sind dringend von Nöten. Die *Friedensinformatik* kann hier wertvolle Beiträge leisten. So etwa bei der Frage danach, wie sich *Cyberwaffen* bewerten lassen (Reinhold & Reuter 2021), aber auch anhand welcher technischen mess- und erfassbaren Parameter eine Schadsoftware vor deren Einsatz und unabhängig von mutmaßlichen Absichten klassifiziert und reguliert werden kann.

Autonomie in Waffensystemen

Die Anwendung von KI in vielfältigen gesellschaftlichen Bereichen ist derzeit in aller Munde. Ein besonders schnell voranschreitender und kritischer Anwendungskontext ist die Integration von Autonomie in Waffensystemen – sogenannten *(lethal) autonomous weapon systems* ((L)AWS). Die Debatte über die Entwicklung und den Einsatz von AWS als Technologie gewinnt zunehmend an Bedeutung, wobei internationale Verhandlungen ins Stocken geraten, während gleichzeitig die technologische Entwicklung immer weiter voranschreitet (Riebe et al. 2020). Stetige technologische Weiterentwicklungen sind nur ein Grund dafür, warum es bis heute keine allgemeingültige bzw. international anerkannte Definition von AWS gibt. Das *International Committee of the Red Cross* (ICRC) schreibt dazu: „Autonomous weapon systems select and apply force to targets without human intervention" (ICRC 2021). Das US-Verteidigungsministerium vertritt ein ähnliches Verständnis und definiert ein autonomes Waffensystem als „weapon system that, once activated, can select and engage targets without further intervention by an operator" (DoD 2023). Diese Definitionen verdeutlichen den Unterschied zwischen AWS und konventionellen Waffen, da Autonomie in Waffensystemen viel stärker im Hinblick auf den Anwendungs- bzw. Einsatzkontext definiert werden muss, weil es sich nicht um eine klar abgrenzbare Waffenkategorie handelt. Neben der definitorischen Problematik werfen autonome Waffensysteme technische, (völker-)rechtliche, sicherheitspolitische, ethische und humanitäre Fragen auf. Hier ist noch viel Forschung nötig, deren Ergebnisse zwischen Wissenschaft, Politik und Zivilgesellschaft diskutiert werden müssen. Außerdem sollten auch Vertreter:innen aus Militär und Industrie in Gespräche integriert werden.

Mit Blick auf eine angemessene politische und rechtliche Regulierung solcher neuartigen Waffensysteme müssen daher neue Konzepte im Rahmen der Rüstungskontrolle gefunden werden (Sauer 2021). Die Entwicklungen und möglichen Regulierungen rund um AWS werden seit einigen Jahren innerhalb der *UN-Konvention über bestimmte konventionelle Waffen* (engl. *Convention on Certain Conventional Weapons* (CCW)) im Rahmen einer *Group of Governmental Experts* (GGE) zwischen Mitgliedsstaaten, Zivilgesellschaft und Fachexpert:innen diskutiert. Das Element der menschlichen Kontrolle, Fragen im Kontext der Mensch-Maschine-Interaktion sowie die *human security* rücken dabei immer mehr in den Vordergrund. In diesem Kontext weist die internationale NGO-Kampagne *Campaign to Stop Killer Robots* auf die Bedeutung intersektionaler Ansätze hin und verdeutlicht beispielsweise, in welchem Ausmaß *Gender*- und *Race*-Bias in der Konzeption, Technologie und Anwendung von LAWS in der Kriegsführung vorhanden sind (Stop Killer Robots 2020). Auf dieser Basis skizziert die Kampagne zukünftige Herausforderungen für die Einordnung dieser Waffensysteme. Auch in der GGE werden diese Aspekte in den letzten Jahren vermehrt in den Gesprächen aufgegriffen, auch wenn technische, rechtliche und sicherheitspolitische Themen weiterhin im Fokus stehen.

Dual-Use-Technologien

Die Einordnung von Autonomie und KI in Waffensystemen wird durch ihre *Dual-Use*-Eigenschaften erschwert, denn Autonomie ist eine Eigenschaft, die potenziell in unterschiedliche Systeme integriert werden kann. Daher wird auch immer häufiger von *Autonomie in Waffensystemen* statt von *autonomen Waffen-*

systemen gesprochen, beispielsweise in der neuen Richtlinie des US-Verteidigungsministeriums (DoD 2023). *Dual-Use* bezeichnet hierbei die Möglichkeit, eine Technologie sowohl für militärische als auch für zivile Zwecke zu nutzen. Der Dual-Use-Charakter vieler Informations- und Kommunikationstechnologien (IKT) wirft neue Fragen für Forschung und Entwicklung sowie für die nationale, internationale und menschliche Sicherheit auf (Riebe 2023).

Die Herausforderungen für die Forschung ergeben sich hierbei durch die Kombination von konventionellen mit automatisierten oder autonomen Trägersystemen, aber auch durch völlig neuartige Systeme zum Mensch-Maschine-Teaming und zur Unterstützung von Menschen, zum Beispiel durch autonome Systeme wie Drohnen, Roboterhunde oder auch Exoskelette. Innerhalb der Disziplinen der Technikfolgenabschätzung, kritischer Sicherheitsforschung und Mensch-Computer-Interaktion können Fragen zum Beispiel im Hinblick auf die Einhaltung des Humanitären Völkerrechts, die Diffusion von Technologien und Wissen und effektive Rüstungskontrollmaßnahmen analysiert werden. Beispielweise müssen vor dem Hintergrund verantwortungsvoller Forschung und Entwicklung technologische Diffusionen von KI vom zivilen auf den militärischen Bereich berücksichtigt werden (Schmid et al. 2022). Auch in anderen Bereichen der IT – unter anderem in Bezug auf Software oder Kryptographie – spielt der Dual-Use-Charakter eine Rolle.

Maßnahmen zur Bewältigung der Risiken, die mit verschiedenen Dual-Use-Technologien einhergehen, beispielweise durch Proliferationskontrollen oder politische Maßnahmen, gestalten sich mitunter sehr unterschiedlich. Dabei werfen Innovationen in verschiedenen Bereichen – so etwa im Kontext von KI, Robotik und Cybersicherheit – neue Fragen zu jeweiligen Dual-Use-Risiken auf.

Internationale Visionen und Governance von Künstlicher Intelligenz

Jüngste Forschung und Entwicklung im Bereich der *KI* wird gesellschaftlich breit, auch im Hinblick auf Herausforderungen, diskutiert. Beispiele wie der Konversationsbot ChatGPT, *predictive maintenance* in der Logistik oder militärische KI verweisen darauf, dass Schlüsseltechnologien Anwendung in verschiedenen Formen und Kontexten finden und gesellschaftlich transformativ wirken können. Gleichzeitig können neben den Herausforderungen von KI für die Rüstungskontrolle einige dieser Verfahren aber auch als Werkzeug *für* die Rüstungskontrolle verstanden und eingesetzt werden (Reinhold & Reuter 2022), insbesondere wenn zum Teil enorme Informationssammlungen und Sensordaten analysiert werden müssen.

In Bezug auf internationale Sicherheit zeigt sich zudem der Trend der Geopolitisierung von Innovationen, welcher die Förderung von Technologien für nationale und machtpolitische Zwecke umfasst. Staatliche Akteure prägen durch Regulierung Innovationsprozesse entscheidend. Es lohnt daher eine Analyse ihrer Innovationspolitiken und damit verknüpften Visionen von Technologien sowie der Mensch-KI-Beziehung. In Bezug auf die Europäische Union (EU) zeigt sich beispielsweise, dass diese konkrete politische Maßnahmen zur Erforschung und Entwicklung von KI ergriffen hat. Hinsichtlich Debatten über die Technikfolgenabschätzung, die sich auf die Risiken für den Menschen und Fragen der Kontrolle von KI konzentrieren, vertritt die EU in diesem Zusammenhang einen ethischen, auf den Menschen ausgerichteten Ansatz für die Anwendung von KI. Um in diesem Zusammenhang die Entstehung von Normen zu verstehen, muss vor dem Hintergrund der Mensch-Computer-Interaktion das Verständnis des Akteurs für die Interaktion zwischen Mensch und KI analysiert werden, wobei die Konzeptualisierungen von Erklärbarkeit, Interpretierbarkeit und Risiken eine wichtige Rolle spielen. Hier wird zudem erneut die Relevanz interdisziplinärer Ansätze für das detailliertere Verständnis der Visionen unterschiedlicher Akteure über die menschliche Kontrolle von KI verdeutlicht, vor allem hinsichtlich der Bewertung und Governance solcher Technologien (Schmid 2022).

Ausblick auf zukünftige Fragen der Friedensinformatik

Der Einsatz von Informatik-Artefakten in Kriegen und Konflikten wird zunehmen. Daher wird auch die Friedensinformatik in Zukunft unter anderem Fragen zur Attribution und Verifikation von Cyberwaffen, zur Mensch-Maschine-Interaktion und deren Auswirkung auf die internationale Sicherheit erforschen. Konfliktdynamiken im Cyberspace, sowie der Einsatz autonomer Waffensysteme insbesondere vor dem Hintergrund der Nutzung von KI, stellen uns weiterhin vor relevante Forschungsfragen. Aus der *Governance*-Perspektive ist zudem von großer Bedeutung, welche Schwerpunkte bei der Innovationsförderung im Bereich der zivil-militärischen *Dual-Use*-Güter gesetzt werden, um technologische Trends zu beeinflussen. Da IT eine Querschnittstechnologie darstellt, werden durch neue Entwicklungen zahlreiche andere Bereiche mitbeeinflusst, so beispielsweise auch im Kontext konventioneller Waffen. Daher müssen auch Einflüsse auf bereits etablierte Forschungsbereiche berücksichtigt werden.

In Zukunft werden IT-Systeme – auch vor dem Hintergrund von KI – zunehmend untereinander und mit dem Cyberspace verbunden sein, was bedeutet, dass die Verteidigung gegen Cyberangriffe eine immer größere Bandbreite an verteilten digitalen Geräten umfassen wird, die entsprechend noch widerstandsfähiger gegen Angriffe und Abhängigkeiten gemacht werden müssen. Dadurch sowie durch die zunehmende Menge an Informationen wird sich auch das Spektrum möglicher Angriffsvektoren vergrößern und diversifizieren (Reinhold & Reuter 2022). In Bezug auf Autonomie in Waffensystemen und andere Dual-Use-Technologien muss in Zukunft weiterhin erörtert werden, wie eine potentielle Rüstungskontrolle aussehen könnte oder ob eventuell weichere Formen der Regulierung – beispielweise in Form sogenannter *soft-law*-Mechanismen – wirkungsvoller sein können hinsichtlich der Bildung neuer starker Normen (Rosert 2021). Dabei können politische Aushandlungsprozesse, bei denen verschiedene Akteursperspektiven aufeinandertreffen, maßgeblich für eine wertgeleitete und zukunftsgerichtete Technikfolgenabschätzung und verantwortungsbewusste Designprozesse sein.

Referenzen

DoD. (2023): DoD Directive 3000.09. Autonomy in Weapon Systems, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

ICRC. (2021): ICRC position on autonomous weapon systems, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

Langner, R. (2013): A Technical Analysis of What Stuxnet's Creators Tried to Achieve, https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Reinhold, T.; H. Pleil & C. Reuter (2023). Challenges for Cyber Arms Control: A Qualitative Expert Interview Study. Zeitschrift Für Außen- Und Sicherheitspolitik, 16(3), 289–310. https://doi.org/10.1007/s12399-023-00960-w.

Reinhold, T. & C. Reuter (2022): Cyber Weapons and Artificial Intelligence: Impact, Influence and the Challenges for Arms Control. In Reinhold, T. & N. Schörnig (Eds.), Armament, arms control and artificial intelligence: The janus-faced nature of machine learning in the military realm. Springer. https://doi.org/10.1007/978-3-031-11043-6.

Reinhold, T. & C. Reuter (2021): Towards a Cyber Weapons Assessment Model – Assessment of the Technical Features of Malicious Software. IEEE Transactions on Technology and Society.

Reuter, C. (Ed.). (2019): Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-25652-4.

Reuter, C.; J. Altmann; M. Göttsche & M. Himmel (2020): Natural Science and Technical Peace Research: Definition, History, and Current Work. Sicherheit Und Frieden (S+F), 38(1).

Riebe, T. (2023): Technology Assessment of Dual-Use ICTs—How to Assess Diffusion, Governance and Design, https://doi.org/10.26083/TU-PRINTS-00022849.

Riebe, T.; S. Schmid & C. Reuter (2020): Meaningful Human Control of Lethal Autonomous Weapon Systems: The CCW-Debate and Its Implications for VSD. IEEE Technology and Society Magazine, 39(4), 36–51, https://doi.org/10.1109/MTS.2020.3031846.

Rosert, E. (2021): Autonomie in Waffensystemen: Menschliche Kontrolle verbindlich vorschreiben, die UNCCW stärken. In U. Kühn (Ed.), Research Report: Rüstungskontrolle für die nächste Bundesregierung. Ein Empfehlungsbericht (pp. 48–53). IFSH. https://ifsh.de/publikationen/research-report-006.

Saalbach, K.-P. (2019): Attribution of Cyber Attacks. In C. Reuter (Ed.), Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace.

Sauer, F. (2021): Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible. International Review of the Red Cross, 102(913), 235–259. https://doi.org/10.1017/S1816383120000466.

Schmid, S. (2022): Trustworthy and Explainable: A European Vision of (Weaponised) Artificial Intelligence. Die Friedens-Warte, 95(3–4), 290. https://doi.org/10.35998/fw-2022-0013.

Schmid, S.; T. Riebe, & C. Reuter (2022): Dual-Use and Trustworthy? A Mixed Methods Analysis of AI Diffusion Between Civilian and Defense R&D. Science and Engineering Ethics, 28(2), 12. https://doi.org/10.1007/s11948-022-00364-7.

Stop Killer Robots (2020): Intersectionality and Racism, https://www.stopkillerrobots.org/resource/intersectionality-and-racism/.

Wissenschaftsrat. (2019): Empfehlungen zur Weiterentwicklung der Friedens- und Konfliktforschung, (Drs. 7827-19), pp. 1–178, https://www. wissenschaftsrat.de/download/2019/7827-19.html.

Anja-Liisa Gonsior, Thea Riebe, Stefka Schmid, Thomas Reinhold und Christian Reuter

Anja-Liisa Gonsior ist wissenschaftliche Mitarbeiterin und Doktorandin am Lehrstuhl *Wissenschaft und Technik für Frieden und Sicherheit* (PEASEC) am Fachbereich Informatik der Technischen Universität Darmstadt. Ihre Forschungsinteressen liegen in den Bereichen autonome Waffensysteme, Meaningful Human Control, (Cyber-) Rüstungskontrolle, (naturwissenschaftlich-technische) Friedens- und Konfliktforschung sowie kritische Sicherheitsstudien.

Dr. **Thea Riebe** ist wissenschaftliche Mitarbeiterin und Postdoktorandin am Lehrstuhl PEASEC und forscht zu Technikfolgenabschätzung von Dual-Use-Technologien in der Informatik und verbindet Ansätze aus Technikfolgenabschätzung, Kritischer Sicherheitsforschung und Mensch-Computer-Interaktion.

Stefka Schmid ist wissenschaftliche Mitarbeiterin am Lehrstuhl PEASEC. Ihre Forschungsinteressen sind Innovationspolitiken als Gegenstand kritischer Sicherheitsstudien, die naturwissenschaftlich-technische Friedens- und Konfliktforschung sowie Mensch-Computer-Interaktion in Krisenszenarien. In ihrer Promotion setzt sie sich mit der Nutzung von Technologien seitens kollektiver Akteure im Kontext globaler Sicherheitspolitiken auseinander.

Dr. **Thomas Reinhold** ist wissenschaftlicher Mitarbeiter sowie Postdoktorand im gemeinsamen Projekt *Cluster Natur- und Technikwissenschaftliche Rüstungskontrollforschung (CNTR)* des Leibniz-Institut für Friedens- und Konfliktforschung (PRIF) sowie des Lehrstuhls PEASEC. Im Mittelpunkt seines wissenschaftlichen Interesses stehen die Bedrohungen im Cyberspace und das Problem der zunehmenden Militarisierung dieser Domäne.

Prof. Dr. Dr. **Christian Reuter** ist Universitätsprofessor und Dekan am Fachbereich Informatik der Technischen Universität Darmstadt. Sein Lehrstuhl Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) verbindet Informatik mit Friedens- und Sicherheitsforschung. Er hält Doktorgrade in Wirtschaftsinformatik (Universität Siegen) sowie in Sicherheitspolitik (Radboud Universiteit Nijmegen).