Dual-Use in der IT

Bewertung in der Softwareentwicklung

von Thea Riebe und Christian Reuter

Der Einsatz von Informationstechnologie (IT) im Frieden ebenso wie in Konflikten und für Sicherheitszwecke wirft einige Fragen auf (Reuter 2019), u.a. ob die Nutzung von IT auf so genannte förderliche Zwecke und Anwendungen begrenzt und eine schädliche Nutzung verhindert werden kann (Riebe und Reuter 2019). Diese Ambivalenz wird als Dual-use-Dilemma bezeichnet und bedeutet, dass Gegenstände, Wissen und Technologie sowohl nützliche als auch schädliche Anwendung finden können. Dual-use-Fragen stellen sich in ganz unterschiedlichen technischen und naturwissenschaftlichen Disziplinen, insbesondere in der Nukleartechnologie sowie in der Chemie und Biologie. Dabei unterscheidet sich die Bedeutung von Dual-use je nach Technologie, ihren spezifischen Risiken und Szenarien sowie ihrer Distribution und Anwendung. Konkret bedeutet dies: Sicherheitspolitische Risikoszenarien und Anwender der Nukleartechnologie unterscheiden sich erheblich von denen der IT.

Im Jahr 2016 erkannten die NATO-Staaten den Cyberspace als militärische Domäne an, um so Cyberoperationen als Angriffe bewerten und im Cyberraum selbst aktiv werden zu können (NATO 2016). Weltweit werden Streitkräfte für den Cyberspace ausgebaut, gleichzeitig nimmt der Einsatz von IT in allen Lebensbereichen zu. Es stellt sich dadurch mehr denn je die Frage nach der Bewertung von Forschung und Entwicklung in der Informatik hinsichtlich potenzieller militärischer Nutzungsbereiche von Software, die ursprünglich für den zivilen Einsatz entwickelt wurde. In der Nuklearphysik, der Biologie und der Chemie wurden die Dual-use-Risiken bereits intensiv untersucht (Altmann et al. 2017; Liebert et al. 2009; Tucker 2012). Diese Studien trugen dazu bei, für einzelne Technologien Verfahren zur Bewertung und Kontrolle eben dieser Risiken hervorzubringen, und lieferten die Grundlage für den Begriff »Dual Use Research of Concern« (DURC). Dieser Begriff bezeichnet Forschungsprojekte, (neue) Technologien oder Informationen, denen das Potential für förderliche und schädliche Anwendung innewohnt und die besonders verheerende Auswirkungen haben können (Oltmann 2015). Die Frage ist daher, ob auch in der Informatik ein »IT Research and Development of Concern« definiert werden kann, das heißt, ob solche besonders riskanten Technologien durch eine kontextbasierte Dual-use-Folgenabschätzung identifiziert werden können, die – ähnlich wie in den Naturwissenschaften – dazu beiträgt, das Potential für eine schädliche Verwendung bereits während der Softwareentwicklung zu verringern.

Die Herausforderung besteht darin, dass das jeweilige Dual-use-Risiko vom Stand und Prozess der Forschung und Entwicklung der jeweiligen Arbeit abhängt und die Technologie gleichzeitig inhärent ambivalent bleibt. Besonders Software zeichnet sich durch ihre vielfältigen Einsatz- und Anpassungsmöglichkeiten in förderlichen und schädlichen Kontexten aus und unterscheidet sich durch ihre mittelbare Wirkung wesentlich von unmittelbar schädlichen ABC-Waffen (Carr 2013; Lin 2016, S. 119). Um trotzdem Bewertungen und darauf aufbauend Designentscheidungen zu treffen, die das Dual-use-Risiko berücksichtigen, braucht es Einzelfallstudien, die sehr kontext- und technologiespezifisch sein müssen. Solche Fallstudien evaluieren nicht nur eine einzelne Technologie, sondern tragen auch insgesamt zur Entwicklung formeller und informeller Methoden der Dual-use-Governance (Tucker 2012, S. 30-39) und zum Wandel der sozio-technischen Sicherheitskultur bei.

Forschungsstand

Der Begriff »Dual-use« wird vielfältig und divergierend angewendet und definiert, da er sich sowohl auf die Forschung und das Wissen als auch auf Technologien und einzelne Gegenstände beziehen kann (Forge 2010; Harris 2016). Eine frühe Abschätzung der Folgen oder Verwendungsmöglichkeiten der eigenen Forschung und Entwicklung ist besonders dann schwierig, wenn Designentscheidungen mit geringem Aufwand möglich wären (Collingridge 1980). Dabei gibt es unterschiedliche Methoden zur Dual-use-Bewertung, die sich an der Technikfolgenabschätzung orientieren (Grunwald 2002; Liebert 2011). Die Methoden sind szenarienbasiert und anwendungsorientiert und müssen daher immer in das konkrete Forschungs- oder Entwicklungsvorhaben integriert werden, um fallbasiert das jeweils pessimistischere Szenario durch Designanpassungen ausschließen zu können (von Schomberg 2006).

Für die Softwareentwicklung[1] stellt sich gerade vor dem Hintergrund der Versicherheitlichung des Cyberspace (Hansen und Nissenbaum 2009), dem militärischem Bestreben nach umfassender Aufklärung (Müller und Schörnig 2006) und der zunehmenden Investition in die strategisch-offensive Erschließung

(Reinhold 2016) die Frage, auf welche Weise Entwickler Missbrauchsrisiken ihrer Forschung und Entwicklung abschätzen können.

Die Dual-use-Debatte in der Informatik wurde bisher vor allem zur Kryptographie (Vella 2017) und zur Proliferation von Spionagesoftware geführt und 2013 sowie 2016 durch Ergänzungen des Wassenaar-Abkommens[2] berücksichtigt (Herr 2016). Auch der Dual-use von

Software wurde immer wieder als Teil der waffentechnischen Modernisierung problematisiert (Bernhardt und Ruhmann 2017; Reuter und Kaufhold 2018b), dennoch fehlen entsprechende empirische Fallstudien (Leng 2013; Lin 2016). Einerseits ist die moderne Softwareentwicklung durch agile und iterative Vorgehensmodelle, wie Extreme Programming und Scrum, gekennzeichnet, in denen Entwickler und Manager flexibel auf die Änderungen von (Kunden-) Anforderungen reagieren können (Dingsøyr et al. 2012). Es ist daher naheliegend, dass Dual-use-Potenziale nicht nur in der Planungsphase von Softwareprojekten, sondern prozessbegleitend überprüft werden müssen. Andererseits stellt die Flexibilität in der Verwendung von Software in unterschiedlichen Anwendungskontexten die Dual-use-Folgenabschätzung vor eine spezielle Herausforderung und führt dazu, dass diese grundsätzlich anders erfolgen muss als in den Naturwissenschaften (Lin 2016, S. 119). Dabei geht es sowohl darum, Risiken durch nicht-staatliche Akteure zu minimieren, als auch darum, die Gefahr einer unkontrollierten Verbreitung von Schadsoftware oder von Missverständnissen zwischen Staaten zu antizipieren.

Neben der unternehmerischen Analyse von Einflussnehmern und Stimmungsbildern spielen auch Systeme der Social-media-Analyse eine zunehmend wichtige Rolle: Einerseits ermöglichen sie die Identifikation von Einsatzlagen in sozialen Konflikten oder Krisen (Reuter und Kaufhold 2018a; Reuter et al. 2017), gleichzeitig eröffnen sie aber auch ein besonderes Missbrauchspotential im Kontext der Cyberspionage (Neuneck 2017) oder der (politischen) Verfolgung. Deshalb stellt sich die Frage, wie potenzielle Dual-use-Komponenten und -Indikatoren bereits in der Forschung und Entwicklung von Software identifiziert werden können.

Ausblick

Um diese Frage zu beantworten, müssen auf Basis bestehender Ansätze zur Identifikation von Dual-use relevante Indikatoren für eine besonders sicherheitskritische Datenverarbeitung und IT identifiziert und die Gemeinsamkeiten systematisiert werden. Zur Proliferationskontrolle von Spionagesoftware wurden im Wassenaar-Abkommen erste Schritte unternommen, die sich weniger an die konkrete »Intrusion-Software« als an die sie unterstützende Infrastruktur richten (Dullien et al. 2015; Herr 2016). Allerdings wird die Effektivität dieser nicht-bindenden Maßnahmen bezweifelt (Herr 2016; Vella 2017) bzw. sie werden sogar als möglicherweise kontraproduktiv kritisiert (Dullien 2015). Dies zeigt einerseits die Herausforderungen, die sich angesichts der Vielzahl unterschiedlicher Akteure und Prozesse für die effektive Kontrolle von Dual-use-Risiken ergeben. Andererseits tun sich mit der Identifikation von Indikatoren für »Dual Use IT of Concern« und der daran anschließenden Dual-use-Governance von der Forschung zur anwendungsorientierten Entwicklung auch Möglichkeiten zur Verringerung von und zum Umgang mit solchen Risiken auf.

Fazit und Zusammenfassung

- Dual-use sind Forschungsprojekte, (neue) Technologien oder Informationen, denen das Potential für förderliche und schädliche Anwendung innewohnt und die besonders verheerende Auswirkungen haben können (Oltmann 2015).
- Dual-use-Risiken sind früh im Forschungsprozess, solange Anpassungen relativ leicht vorzunehmen sind, schwer feststellbar, während sie in der anwendungsorientierten Forschung, wenn sie leichter feststellbar sind, aufwendiger zu vermeiden sind (Collingridge-Dilemma).
- Dual-use-Risiken können Rüstungsdynamiken und die Stabilität der internationalen Gemeinschaft negativ beeinflussen.
- Um Dual-use-Risiken zu bewerten, gibt es verschiedene Ansätze der Technikfolgenabschätzung. Diese untersuchen die möglichen Effekte von Technologien auf die Gesellschaft, unter Berücksichtigung von Normen, wie dem Vorsorgeprinzip oder Pazifismus.
- Dual-use in der Informatik beinhaltet zahlreiche hier dargestellte Forschungsfragen, die wir aktuell in der Forschung adressieren.

Anmerkungen

1) Softwareentwicklung ist die *„zielorientierte Bereitstellung und systematische Verwendung von Prinzipien, Methoden und Werkzeugen für die arbeitsteilige, ingenieurmäßige Entwicklung und Anwendung von umfangreichen Softwaresystemen“* (Balzert 2000).

2) Dem Wassenaar-Abkommen für die Exportkontrolle konventioneller Rüstungsgüter und Güter mit doppeltem Verwendungszweck (Dual-use Güter) sowie darauf bezogene Technologien gehören 41 Staaten an. Es ist am 1. November 1996 in Kraft getreten.

Literatur

Altmann, J.; Bernhardt, U.; Nixdorff, K.; Ruhmann, I.; Wöhrle, D. (Hrsg). (2017): Naturwissenschaft – Rüstung – Frieden. Wiesbaden: Springer Fachmedien.

Balzert, H. (2000): Lehrbuch der Software-Technik – Software-Entwicklung. Heidelberg: Spektrum Akademischer Verlag.

Bernhardt, U.; Ruhmann, I. (2017): Informatik. In: Altmann et al. (Hrsg.): Naturwissenschaft – Rüstung – Frieden (pp. 337-448). Wiesbaden: Springer Fachmedien.

Carr, J. (2013): The misunderstood acronym – Why cyber weapons aren't WMD. Bulletin of the Atomic Scientists, Vol. 69, Nr. 5, S. 32-37.

Collingridge, D. (1980): The social control of technology. New York: St. Martins Press.

Dingsøyr, T.; Nerur, S.; Balijepally, V.; Moe, N. B. (2012). A decade of agile methodologies – Towards explaining agile software development. Journal of Systems and Software, Vol. 85, Nr. 6, S. 1213-1221.

Dullien, T. (2015): Why changes to Wassenaar make oppression and surveillance easier, not harder. Blog ADD / XOR / ROL, 2.10.2018; addxorrol.blogspot.com.

Dullien, T.; Iozzo, V.; Tam, M. (2015): Surveillance, Software, Security, and Export Controls – Reflections and recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting. Draft Report, 2.10.2015; tac.bis.doc.gov.

Forge, J. (2010): A note on the definition of »dual use«. Science and Engineering Ethics, Vol. 16, Nr. 1, S. 111-118.

Grunwald, A. (2002): Technikfolgenabschätzung – Eine Einführung. Berlin: Edition Sigma.

Hansen, L.; Nissenbaum, H. (2009): Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, Vol. 53, Nr. 4, S. 1155-1175.

Harris, E.D. (ed.) (2016): Governance of Dual-Use Technologies – Theory and Practice. Cambridge MA: American Academy of Arts & Sciences.

Herr, T. (2016): Malware counter-proliferation and the Wassenaar Arrangement. NATO Cooperative Cyber Defence Centre of Excellence, 8th International Conference on Cyber Conflict – CyCon 2016. Proceedings, S. 175-190.

Leng, C. (2013): Die dunkle Seite – Informatik als Dual-Use-Technologie. Gesellschaft für Informatik.

Liebert, W. (2011): Wissenschaft und gesellschaftliche Verantwortung. In: Eger, M.; Gondani, B.; Kröger, R. (Hrsg.): Verantwortungsvolle Hochschuldidaktik. Berlin: LIT, S. 15-34.

Liebert, W.; Englert, M.; Pistner, C. (2009): Kernwaffenrelevante Materialien und Präventive Rüstungskontrolle - Uranfreie Brennstoffe zur Plutoniumbeseitigung und Spallationsneutronenquellen. Osnabrück: Deutsche Stiftung Friedensforschung, Forschung DSF Nr. 20.

Lin, H. (2016): Governance of Information Technology and Cyber Weapons: In: Harris, E.D. (ed.), op.cit, S. 112-157).

Müller, H.; Schörnig, N. (2006): Rüstungsdynamik und Rüstungskontrolle – Eine exemplarische Einführung in die Internationalen Beziehungen. Baden-Baden: Nomos.

North Atlantic Treaty Organization/NATO (2016): Warsaw Summit Communiqué. nato.int.

Neuneck, G. (2017): Krieg im Internet? Cyberwar in ethischer Reflexion. In: Werkner, I.-J.; Ebeling, K. (Hrsg.). Wiesbaden: Springer Fachmedien, S. 805-816.

Oltmann, S. (2015): Dual use research – investigation across multiple science disciplines. Science and Engineering Ethics, Vol. 21, Nr. 2, S. 327-341.

Reinhold, T. (2016): Cyberspace als Kriegsschauplatz? Herausforderungen für Völkerrecht und Sicherheitspolitik. Aus Politik und Zeitgeschichte/APUZ 35-36/2016, S. 22-27.

Reuter, C. (2019): Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace. Wiesbaden: Springer Vieweg (im Erscheinen).

Reuter, C.; Kaufhold, M.-A. (2018a): Fifteen Years of Social Media in Emergencies – A Retrospective Review and Future Directions for Crisis Informatics. Journal of Contingencies and Crisis Management/JCCM, Vol. 26, Nr. 1, S. 1-17.

Reuter, C.; Kaufhold, M.-A. (2018b): Informatik für Frieden und Sicherheit. In: Reuter, C. (Hrsg.): Sicherheitskritische Mensch-Computer-Interaktion – Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement. Wiesbaden: Springer Vieweg, S. 577-597.

Reuter, C.; Kaufhold, M.-A.; Spielhofer, T.; Hahne, A.S. (2017): Social Media in Emergencies – A Representative Study on Citizens' Perception in Germany. Proceedings of the ACM on Human Computer Interaction, Computer-Supported Cooperative Work and Social Computing, Vol. 1, Nr. 2, S. 1-19.

Riebe, T.; Reuter, C. (2019): Dual Use and Dilemmas for Cybersecurity, Peace and Technology Assessment. In: Reuter, C. (ed.) (2019), op.cit.

Tucker, J.B. (ed.). (2012): Innovation, Dual Use, Security – Managing The Risks of Emerging Biological and Chemical Technologies. Cambridge MA: MIT Press.

Vella, V. (2017): Is There a Common Understanding of Dual-Use? The Case of Cryptography. Strategic Trade Review, Vol. 3, Nr. 4, S. 103-122.

von Schomberg, R. (2006): The Precautionary Principle and Its Normative Challenges. In: Fischer, E.; Jones, J.; von Schomberg, R. (eds.): Implementing the Precautionary Principle – Perspectives and Prospects. Cheltenham: Edward Elgar, S. 19-42.

Thea Riebe ist wissenschaftliche Mitarbeiterin an der Technischen Universität Darmstadt sowie der Universität Siegen und promoviert zu Dual-use in der Informatik. Christian Reuter ist Professor für Wissenschaft und Technik für Frieden und Sicherheit (PEASEC) an der Technischen Universität Darmstadt; peasec.de.