Accessing Dual-Use in IT Development

THEA RIEBE AND CHRISTIAN REUTER

SCIENCE AND TECHNOLOGY FOR PEACE AND SECURITY (PEASEC), TECHNISCHE UNIVERSITÄT DARMSTADT

[#5-PAPER]

ABSTRACT

The use of information technology (IT) in peace, conflict and security raises some questions, i.e. whether the use of IT can be limited exclusively to so-called advantageous purposes and applications and whether improper use can be prevented. This ambivalence is called a dual-use dilemma, meaning that objects, knowledge and technology can find both useful and harmful applications. Dual-use questions have been addressed in various disciplines, in particular in nuclear technology and the production of nuclear weapons, but also in chemistry and biology. In all these disciplines, dual-use topics in technical development and education have been discussed and addressed. Nevertheless, the importance of dual-use differs slightly, depending on the technology and its risks, as well as its distribution and application. Nuclear technology is less accessible than biotechnology, which in turn is less accessible than IT.

1. INTRODUCTION

In 2016, NATO states recognized cyberspace as a military domain, in order to assess cyber operations as an attack or to become active themselves (NATO, 2016). Cyberspace forces are expanding worldwide, while the use of IT in all areas of life is increasing. This raises more than ever the question of evaluating research and development in computer science with regard to potential military uses of software developed for civilian use. In atomic physics, biology and chemistry, the dual-use risks were intensively studied (Altmann et al., 2017; Liebert et al., 2009; Tucker, 2012). These studies have also helped to identify techniques for evaluating and controlling these same risks and have provided the basis for the concept of Dual-Use Research of Concern (DURC). DURC refers to research, (new) technologies, or information that has the potential for beneficial and harmful applications (Oltmann, 2015). The question is therefore whether computer science can also be used to define an IT Research and Development of Concern that requires a context-based dual-use impact assessment and, similar to the life sciences, helps to reduce the potential for misuse during software development.

The challenge is that the respective dual-use risk depends on the state and process of research and development of the respective work, while the technology remains inherently ambivalent. In particular, software is characterized by its versatility of use and adaptation in conducive and

harmful contexts, and by its indirect effect which differs substantially from directly harmful ABC weapons (Carr, 2013; Lin, 2016, 119). Nevertheless, in order to make evaluations and design decisions that take the dual-use risk into consideration, individual case studies are required which must be very context- and technology-specific. Such case studies not only evaluate a single technology, but also contribute to the development of formal and informal dual-use governance methods (Tucker, 2012, 30–39) and the evolution of the socio-technical safety culture.

2. STATE OF RESEARCH

Dual-use is widely and divergently applied and defined, as the term can refer to research, knowledge, as well as technologies and individual objects (Forge, 2010; Harris, 2016). An early assessment of the consequences or use of one's own research and development is particularly difficult if design decisions are possible with little effort (Collingridge, 1980). There are different methods for dual-use assessment, which are based on the assessment of technology consequences (Grunwald, 2002; Liebert, 2011). The methods are scenario-based and application-oriented, and must therefore always be integrated into the specific research or development project in order to be able to exclude the more pessimistic scenario by design adaptations on a case-by-case basis (von Schomberg, 2006).

For software development, it is precisely against the background of the securitization of cyberspace (Hansen & Nissenbaum, 2009), the military endeavour to comprehensively elucidate (Müller & Schörnig, 2006), and the increasing investment in strategic offensive development (Reinhold, 2016) the question of how developers can estimate the risk of misuse of their research and development.

So far, the dual-use debate in computer science has mainly led to cryptography (Vella, 2017) and to the proliferation of spyware through additions to the Wassenaar Agreement in 2013 and 2016 (Herr, 2016). And although software dual-use is becoming a problem again and again as part of weapons modernization (Bernhardt & Ruhmann, 2017; Reuter & Kaufhold, 2018b), empirical case studies on dual-use IT are lacking (Leng, 2013; Lin, 2016). On the one hand, modern software development is characterized by agile and iterative process models such as Extreme Programming and Scrum, in which developers and managers can react flexibly to changes in (customer) requirements (Dingsøyr et al., 2012). Therefore, it is obvious that dual-use potentials need to be checked not only in the initial planning of software, but process-accompanying. On the other hand, the flexibility in using software in different application contexts is the essential challenge for dual-use impact assessment and therefore must be fundamentally different from life sciences (Lin, 2016, 119). The aim is both to minimize risks by non-state actors, and to anticipate the risk of uncontrolled distribution of malware or misunderstandings between states.

Alongside the entrepreneurial analysis of influencers and moods, social media analytics tool are also playing an increasingly important role: On the one hand, they enable the identification of situations of use in social conflicts or crises (Reuter & Kaufhold, 2018a; Reuter et al., 2017), but also imply a particular potential for abuse in the context of cyber espionage (Neuneck, 2017) or (political) persecution. Therefore, the question arises how potential dual-use components and indicators can already be identified in software research and development.

3. REFERENCES

Altmann, J., Bernhardt, U., Nixdorff, K., Ruhmann, I., & Wöhrle, D. (2017). *Naturwissenschaft – Rüstung – Frieden*. (J. Altmann, U. Bernhardt, K. Nixdorff, I. Ruhmann, & D. Wöhrle, Eds.) (2nd ed.). Wiesbaden. https://doi.org/10.1007/978-3-658-01974-7

Bernhardt, U., & Ruhmann, I. (2017). Informatik. In J. Altmann, U. Bernhardt, K. Nixdorff, I. Ruhmann, & D. Wöhrle (Eds.), *Naturwissenschaft – Rüstung – Frieden* (pp. 337–448). https://doi.org/10.1007/978-3-658-01974-7

Carr, J. (2013). The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*, *69*(5), 32–37. https://doi.org/10.1177/0096340213501373

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*, *85*(6), 1213–1221. https://doi.org/10.1016/j.jss.2012.02.033

Forge, J. (2010). A note on the definition of "dual use." *Science and Engineering Ethics*, *16*(1), 111–118. https://doi.org/10.1007/s11948-009-9159-9

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*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

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. *International Conference on Cyber Conflict, CYCON*, *2016-Augus*, 175–190. https://doi.org/10.1109/CYCON.2016.7529434

Leng, C. (2013). *Die dunkle Seite: Informatik als Dual-Use-Technologie*. Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs00287-012-0675-7.pdf

Liebert, W. (2011). Wissenschaft und gesellschaftliche Verantwortung. In M. Eger, B. Gondani, & R. Kröger (Eds.), *Verantwortungsvolle Hochschuldidaktik* (pp. 15–34). Berlin: Lit.

Liebert, W., Englert, M., & Pistner, C. (2009). *Kernwaffenrelevante Materialien und Präventive Rüstungskontrolle : Uranfreie Brennstoffe zur Plutoniumbeseitigung und Spallationsneutronenquellen*. *Deutsche Stiftung Friedensforschung*.

Lin, H. (2016). Governance of Information Technology and Cyber Weapons. In E. D. Harris (Ed.), *Governance of Dual-Use Technologies: Theorie and Practice* (pp. 112–157). American Academy of Arts & Sciences.

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

NATO. Warsaw Summit Communiqué (2016). Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Neuneck, G. (2017). Krieg im Internet? Cyberwar in ethischer Reflexion. In I.-J. Werkner & K. Ebeling (Eds.), *Handbuch Friedensethik* (pp. 805–816). Wiesbaden. https://doi.org/10.1007/978-3-658-14686-3_58