8 Creative Uses of IT: Dual Use Governance, Assessment and Design

Thea Riebe · Stefka Schmid · Christian Reuter
Science and Technology for Peace and Security (PEASEC), TU Darmstadt

Abstract

Dual-use of IT is relevant to many applications and technology areas: how can we prevent, control, or manage the risk of misuse of IT? How can dual-use awareness and regulation help to mitigate the risks to peace and security on the national and international levels? As cyberspace has been declared a military domain, IT is increasingly important for civil and military infrastructures. How can researchers, developers and decision-makers ensure that IT is not misused to cause harm? Scholars have debated on the dual-use problem for nuclear, biological, and chemical technologies. This chapter introduces different dual-use concepts and illustrates, by considering cryptography, intrusion software, and artificial intelligence, how governance measures, including export control, are applied. Further, approaches of technology assessment, with a focus on the design process, are presented. The chapter also provides insight into the implementation of dual-use assessment guidelines at TU (Technische Universität) Darmstadt, the so-called Civil Clause.

1. Introduction

The latest invasion of Ukraine by Russian Forces in 2022 has led to a discourse on the combat readiness and defense capabilities of European countries. This shift in funding and attention to the forces has been called “Zeitenwende” (the end of an era) in Germany (Löffmann, 2023). In this context, the civil clauses have been criticized as hindering the equipping of the armed forces leading to demands for reform or even to abolish the clauses. Further, the distinction in research funding between civilian and military R&D was questioned by advisors at the German and the European level (Greenacre & Matthews, 2024; Matthews, 2024). As of 2024, established Civil Clauses at German Universities are under scrutiny, highlighting the importance of clarity on the issues at stake.

Technologies can be considered **dual-use**, when they are relevant for civilian and military applications, when they are critical to security and can be misused to cause significant harm, or when they can be used as part of an (improvised) weapons system. Considering a typical dual-use technology, most people would think of nuclear technologies, which can

both be a source of power production and provide fissile material for nuclear weapons. Others might first think of biotechnology, such as genome editing with CRISPR/Cas[1] due to its ability to modify genes in an accessible and much cheaper way than earlier methods. To raise awareness about the ambivalence of IT, the Student Council of Computer Science at TU Darmstadt used the image of a baby holding an assault rifle as their mascot as early as 1986 (Ottermann & Gries, 2018), reminding the members of the faculty of the ambivalent nature of innovation in computer science (Knappmeier, 2004; Leng, 2013). Since then, the association of dual-use and computer science has become more apparent. In computer science and engineering, students and researchers have shown awareness of dual-use in their fields. In a study, 11% of senior editors of peer-reviewed journals in engineering and technology stated that they came across dual-use questions in submitted research papers (Oltmann, 2015). Students are aware of ethical and dual-use risks regarding AI, as the study by Haunschild et al. (2023) has shown. Others, such as Lin (2016), argue that IT should not be classified as a dual-use technology in the same way as physics, biology, and chemistry because communication and information, integral to IT, are deemed **general-purpose** (for non-specific use) and not directly harmful in itself. Thus, interdisciplinary assessment of socio-technical systems needs constant reflection, training, and practice (Reuter et al., 2022).

Figure 8-1: Mascot of the Student Council of Computer Science at TU Darmstadt since 1986

In 2016, NATO declared that cyberspace should be categorized as a military domain (NATO, 2016), and many countries have invested in offensive and defensive IT capabilities (Neuneck, 2013). In the domains of land and sea, the use of unmanned armed vehicles (UAVs) and weapons systems with autonomous functions (AWS), are on the rise. Additionally, IT has been perceived as the driving force in the most recent **Revolution in**

[1] On the discourse regarding the dual-use potential of CRISPR/Cas, please read Mir et al. (2022).

Military Affairs (RMA), implying the transformation of the armed forces and their strategies using IT, such as the tactical use of real-time data for enhanced flexibility among smaller units (Adamsky, 2010). IT and digitalization are the main drivers of innovation in military and civilian infrastructures.

Once a technology is developed and has high relevance for civil and military actors, it can even set off a destabilizing dynamic in international security, feeding into mistrust and scenarios of a **security dilemma.** The so-called security dilemma is created by the need for states to increase their security in the anarchic international system by investing in their military. Realism, a prominent paradigm in International Relations, posits that the international system lacks a central authority, compelling it to adhere to the dominance of the strongest or most powerful nation (Waltz, 1979). Consequently, other states could feel threatened and increase their military spending, resulting in the effect of creating less security for all. This competitive dynamic for military superiority leads to arms races (Herz, 1950).

IT has become necessary for information, communication and control systems and might bear unintended risks for safety and security while its use holds great benefits. IT can be dual-use, both from the perspective of being used in a potentially harmful way, or from the perspective of being deployed in civilian and defense contexts. Therefore, this chapter provides an overview on the history and definitions of the concept of dual-use (Section 8.1~~8.2~~). It seeks to illustrate the governance of dual-use risks using three cases involving IT (Section 8.2~~8.3~~), and to provide methodological tools to assess dual-use technologies and to use dual-use sensitive design methods (Section 8.3~~8.4~~). Lastly, Section 8.5 dives into the case of the Civil Clause (*Zivilklausel*) at the Technical University of Darmstadt.

8.1 History and Definitions of Dual-Use

Dual-use as a concept describes the duality or dual-faced nature of technology, which can be used for good and intended purposes as well as misused to cause harm (Forge, 2010). Historically, evaluation of the potential uses and possible harms of dual-use technologies became prominent with nuclear energy and atomic weapons in the 1950s. Nuclear research has been considered “born classified” since then (Oltmann, 2015, p. 238). In the 1970s, advances in biology and biotechnology raised concerns about potential biological weapons. Research on viruses, bacteria, and toxins, as well as genome editing, has since then strongly shaped the understanding of dual-use (Oltmann, 2015).

In the scientific fields historically associated with dual-use applications, such as physics, biology, chemistry, and engineering, dual-use possibilities and their relevant scenarios are regularly assessed. Besides safety concerns, the security of nuclear and missile technology has been addressed with state actors in mind, while in the life sciences, terrorist scenarios have been dominant. Considering these cases, some authors question whether IT can be

categorized as dual-use technology. Unlike nuclear, biological, and chemical research, IT primarily serves communication and automatic data processing purposes, lacking direct potential to cause harm to individuals comparable to **weapons of mass destruction (WMD)**. WMD is defined by US legal code §2302 as

> any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of (A) toxic or poisonous chemicals or their precursors; (B) a disease organism; or (C) radiation or radioactivity.

Therefore, cyber weapons are not considered WMD, even though sabotaging critical infrastructures could lead to high casualties (Carr, 2013).

All parts of the research and development (R&D) process can be relevant to questions of **dual-use.** Dual-use potentials are difficult to assess in basic research and are more difficult to prevent with applied research. Further, it is important to note that the dual nature of technology cannot be completely resolved. However, the aim is to acknowledge certain risks and prevent specific scenarios or harmful uses of technologies (Liebert & Schmidt, 2018).

There are various concepts of the duality of the term *dual-use* (Riebe, 2023). Some define duality in terms of usage across both civilian and military applications, particularly relevant for technologies like nuclear ones with high technological barriers or strategic importance. Conversely, broader definitions encompass technologies like autonomous systems, essential for military purposes due to their strategic and logistical significance, beyond weaponry. Forge (2010, p. 117) defines dual-use as items that can be used as part of an (improvised) weapon system:

> An item (knowledge, technology, artifact) is dual use if there is a (sufficiently high) risk that it can be used to design or produce a weapon, or if there is a (sufficiently great) threat that it can be used in an improvised weapon, where in neither case is weapons development the intended or primary purpose.

This definition excludes any non-weapon technology that still might cause harm and does not distinguish between civilian and military application contexts as (improvised) weapons are used in civilian settings as well.

However, there are cases of dual-use technologies, which are not part of weapon systems but pose risks due to unintended accidents in security-relevant R&D, e.g. in the life sciences. Thus, the World Health Organization (WHO) and the life science research community have coined their own definition, which focuses on the outcome of the use of technology, either beneficial or harmful (or both) (see **Error! Reference source not found.**~~**Error! Reference source not found.**~~).

Organisation	Definition of dual-use research

World Health Organization	"Dual-use research of concern (DURC) describes research that is intended to provide a clear benefit, but which could easily be misapplied to do harm." (WHO, 2020)
Deutsche Forschungsgemeinschaft	"In dual-use research, which can have harmful as well as beneficial effects [...]". (Deutsche Forschungsgemeinschaft & Deutsche Akademie der Naturforscher Leopoldina e.V., 2014)
***Zivilklausel* at TU Darmstadt**	"Research, teaching and studies at Technische Universität Darmstadt exclusively pursue peaceful goals and serve civilian purposes; research, particularly relating to the development and optimisation of technical systems, as well as studies and teaching are focused on civilian use." (TU Darmstadt, 2018b)

Table 1: Definitions of dual-use research

The more developed a technology is, the easier it is to assess its potentially harmful application. Thus, for product development, much more stringent dual-use regulations are focused on the goods that are to be traded as products (Alavi & Khamichonak, 2017; Wassenaar Arrangement Secretariat, 2018).

To summarize, the concept of dual-use is often applied to consider military and civilian, harmful and beneficial usage or application or the plausible risk of such use. Historically, in the realm of nuclear technology, dual-use is applied regarding civil and military applications due to nation states' monopoly on nuclear technology. Conversely, in the life sciences, technologies are much more accessible and have even higher risks of being exploited by terrorist groups or causing severe accidents. For the life sciences, the dual-use concept for biological and chemical risks has been introduced as *Dual-use Research of Concern* (DURC) by the US National Academy of Sciences (Knowles, 2012, p. 54; NSABB, 2007) and the World Health Organization (WHO). Further, the scope of dual-use covers various items such as research, technologies, and goods that can all be dual-use. To determine the character of the risk of a harmful or military application, it is important to evaluate the item's potential contribution to a weapon system. The role of IT as such a component can be manifold: it can be part of a WMD or the weapon system itself.

8.2 Governing Dual-Use Information Technologies

Dual-use governance has three main objectives: first, limiting or even preventing the development of technologies that could serve hostile purposes. Second, controlling the access to dual-use technologies' materials, equipment, and information. Third, promoting the safe handling of equipment, information, and materials (Harris, 2016). There are different R&D levels, each addressed differently by governance measures.

> Assessing the safety and security risks of emerging technologies should be both flexible and capable of integrating new information as the development process

unfolds. The most effective way to achieve this objective is to incorporate an iterative process of technology assessment into the research and development cycle itself. Once the risks of an emerging dual use technology have been identified, it will be necessary to identify a tailored package of governance measures – made up of hard-law, soft-law, and informal elements – to ensure a reasonable balance of risks and benefits and their equitable distribution across the various stakeholders (Tucker, 2012).

Across the different stages of R&D, a spectrum of governance approaches is available to mitigate dual-use risks (see Figure 8--2~~Figure 8--2~~). On the one hand, less stringent and "softer" regulations such as "**risk education and awareness raising**" should help train researchers while at the same time leaving sufficient flexibility for the research process. On the other hand, **export controls** are often used to legally and broadly control the proliferation of dual-use materials and technologies that have already resulted from R&D. In the following, we focus on these "hard-law" measures regarding cases of dual-use IT.

Informal	Soft-law	Hard-law
Codes of Conduct	Security Guidelines	Statutory Regulations
Risk Education and Awareness Raising	Industry of Scientific Community Self-Governance	Mandatory Licensing, Certification, Registration
Whistle-Blowing Channels	Adoption of International Standards	Export Controls
Transparency Measures	Pre-Publication Review	Reporting Requirements

Less Stringent → More Stringent

Figure 8--2: Spectrum of governance approaches for dual-use, addressing the different stages of R&D (Tucker, 2012)

In the last decade, three cases of IT have been mostly discussed from the perspective of dual-use. First, cryptography and encryption software were the first IT dual-use "products" that were introduced to export and import regulations. Second, since 2013, intrusion software and spyware have been the focus of the Wassenaar Arrangement, which aims to control the proliferation of such software. Third, AI and its harmful potential have received more attention from legislators, such as the EU, as well as from ethics committees.

8.2.1 Cryptography

Internationally, encryption products are regulated by the **Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA)** established in 1995**.** a multilateral agreement among states, that regulates the trade of dual-use goods. This arrangement is not binding for the member states but serves as a declaration of intent to harmonize certain laws. Cryptography is the first IT to be regulated under the banner of dual-use. Following World War II, encryption products were mostly relevant for military purposes, and thus restricted by the US for trade. This includes control of export or import and licenses for international trade. However, digital technologies

proliferated especially with the use of the World Wide Web globally and made the process challenging, with civilian demand for encryption increasing. In 1992, the US repeatedly adjusted the threshold and excluded mass-market products, e.g. messengers or technology used for personal use (Vella, 2017, p. 108) from the restrictions. Since the 1990s, public discussions regarding the regulation of encryption have primarily focused on two approaches: setting key length as a threshold or proposing various forms of key escrow (key escrow involves a system where a key is retained to decrypt information for law enforcement purposes). This has strongly influenced the societal backlash due to concerns about privacy civil rights and led to the so called *crypto wars* (Buchanan, 2017; Koops & Kosta, 2018). Thereby, politically active developers and civil rights activists protested against the implementation of key-escrow by the US government and actively undermined export and import restrictions.

In the EU, IT products for military applications are controlled, and this can include software and encryption. However, the EU has adopted a General Technology Note and a General Software Note that excludes information and software within the public domain from the Control List (Vella, 2017). Additionally, the EU allows exceptions to its restrictions, when there are concerns regarding the violation of human rights (Vella, 2017).

To summarize, the regulation of encryption as a dual-use good reflects states' intentions to use the regulation to control the access to a technology for certain actors. As information and communication technologies have become popular, mass market products have been excluded. Social media platforms and messenging have led to the most successful distribution of end-to-end encryption, but also became important tools for mass surveillance (Riebe et al., 2021).

8.2.2 Intrusion Software

Intrusion software refers to tools that bypass defenses, gain access to computers, and extract data from them (Herr, 2016). The proliferation of intrusion software is also regulated in domestic and international arrangements, such as the WA and by the EU. The WA has added intrusion software by amendments in 2013 and adjusted the regulation by 2016. Building on Dullien et al. (2015) it is noted that the controls restrict infrastructure and support systems, which are

> any software, systems, equipment, components, or technology used to generate, operate, deliver, or communicate with intrusion software. In effect, Wassenaar targets how intrusion software is built, deployed, or communicated with. (Pissanidis et al., 2016, p. 182)

The EU adopted a similar approach in 2014 and implemented it in 2015. Since then, the EU restricts network surveillance and intrusion software by requiring individual export licenses. The EU export control regime requires states to validate export requests and deny them if "there is a clear risk that the […] equipment to be exported might be used for

internal repression" taking into account "all relevant considerations" including its possible usage for activities that might violate human rights (Reinhold, 2021). However, this is not implemented in a standardized way, and has left loopholes for *surveillance-as-a-service* in the past. For example, the German spyware Fin Fisher was exported and used by the Turkish government between 2016 and 2017 without having export approval by the German government (Gesellschaft für Freiheitsrechte, 2019).

The regulation of surveillance and intrusion software was also criticized by IT security companies, as the definition in the regulation was sometimes fuzzy and could put import R&D on security tools at risk (Ruohonen & Kimppa, 2019). Nevertheless, the WA defined some exceptions for

1. Debuggers, virtualization hypervisors, or software reverse engineering tools[2];
2. Software implementations for digital rights management (DRM);
3. Software that is installed by manufacturers, administrators, or end-users for "the purposes of asset tracking or recovery" (Ruohonen & Kimppa, 2019).

To sum up, surveillance technologies as well as intrusion software have been increasingly discussed with a focus on human rights violations, such as against activists and journalists. However, regulation of such technologies is far from straight forward as the common features of IT security tools make a robust regulation and respective implementation difficult.

8.2.3 Artificial Intelligence

AI has been distributed into many different areas of application, both in the civilian and defense sectors, and can be used in security critical contexts that potentially impact human wellbeing (Brundage et al., 2018). However, it has not yet been covered by the WA, whereas the EU has moved the international normative discourse on ethical and trustworthy AI forward. First, the EU has proposed the *Trustworthy AI* framework in 2019, according to which AI should be

1. lawful - respecting all applicable laws and regulations
2. ethical - respecting ethical principles and values
3. robust - both from a technical perspective while taking into account its social environment (European Commission, 2019)

Additionally, AI should follow four ethical principles (respect for human autonomy, prevention of harm, fairness and explicability) and seven requirements (such as human agency and oversight, technical robustness and safety, privacy, transparency, non-discrimination, societal and environmental well-being and accountability) to be considered

[2] Reverse engineering tools are software tools that help developers to disassemble and understand finished and complex software products.

trustworthy (for more details, see European Commission, 2019). Still, this is an ethical framework, which is not legally binding but instead setting normative rules for R&D, thus considered "soft-law". In 2023, the EU has put forward a legal proposal to regulate AI called the *Artificial Intelligence Act*, which categorizes AI into three risk groups (general AI, high-risk system and banned systems). The act bans the use of AI for biometric categorization systems by law enforcement, or social scoring of users. However, there are some exceptions for

> the use of biometric identification systems (RBI) in publicly accessible spaces for law enforcement purposes, subject to prior judicial authorization and for strictly defined lists of crime (European Parliament, 2023).

Further, there are safeguards for high-risk systems that require

> model evaluations, assess and mitigate systemic risks, conduct adversarial testing, report to the Commission on serious incidents, ensure cybersecurity and report on their energy efficiency (European Parliament, 2023).

Lastly, there is the possibility of imposing fines on non-compliant companies "ranging from 35 million euro or 7% of global turnover to 7.5 million or 1.5 % of turnover" (ibid.) which will help to implement the new law.

The EU has proven to be a significant actor in developing and shaping norms related to the R&D of AI systems. This influence is expected to improve products developed by tech companies around the globe due to the market relevance of the European consumers. Additionally, companies and governments now possess a blueprint on both a normative and a legal framework that can serve as a reference point for those seeking to regulate the risks associated with AI.

8.3 Technology Assessment and Design

As described above, there are multiple aspects that need to be considered by those working with high-risk or security critical technologies, which can be considered dual-use. How can researchers or developers assess the risks of R&D projects?

Technology Assessment (TA) focuses on the effects of technology on society to give policy advice and to inform the public about possible consequences of technology application to society and democratic institutions (see Figure 3~~Figure 3~~). TA is both a theoretical and a practical approach, in which the scientific endeavor is driven by the practical challenges of the emergence of technology for society, which will then induce the theoretical reasoning (Grunwald, 2018, p. 1). The three practical aims of TA are (1) policy advice, (2) engaging in public debate, and (3) contributing to the making of technology (Grunwald, 2018, p. 92). TA theory aims to facilitate the reflexivity of technology design and development. Grunwald (2018) defines TA as a socio-epistemic

practice with institutions, projects, and methods which is embedded in a societal framework.

TA is based on the so-called **precautionary principle**. With the advancement of sciences and technologies with potential irreversible harms for ecosystems and societies, the need to evaluate technology before implementation, even before conducting experiments, has become more relevant. Such unintended effects on the environment and the society have made philosopher Hans Jonas emphasize the precautionary principle as the guiding principle to the ethics of responsibility (Jonas, 1980). Considering (long-term) environmental effects of technology usage, scholars identified the need for actions to be taken with *in dubio pro natura*, meaning "if in doubt, decide in favor of the environment" (Ahteensuu & Sandin, 2012).

To assess the dual-use potential, it is necessary to foresee possible use scenarios and apply the precautionary principle. The principle helps to navigate actions in situations of uncertainty when decisions can have a significant or harmful influence on humankind, as with climate and environmental change. Especially when cause-and-effect mechanisms are not scientifically established, precautionary measures must be taken (Lösch et al., 2008). Precaution can be executed, according to Jonas (1980), if the *imperative of responsibility* is followed, meaning if there are two scenarios, then the pessimistic, not the optimistic, scenario should guide the decision. The precautionary principle is implemented in research agendas by the EU using the concept of **Responsible Research and Innovation (RRI)**:

> Responsible Research and Innovation is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view on the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society) (Owen et al., 2012; von Schomberg, 2011, p. 9).

Additionally, precaution is needed, as R&D of technologies can lead to a path dependency, which makes change difficult. This phenomenon is called the **Collingridge Dilemma.** The dilemma describes that in the process of R&D, it is not always easy to anticipate the potential risks of the outcome. Because early in its life, when still easy to change, the application and consequences of technology are difficult to predict, and later on, they are expensive to adjust: "When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time-consuming" (Collingridge, 1980). As a result, dual-use technology regulations range from informal to legally binding depending on the advancement of the R&D (see Section 8.2~~8.3~~).

Due to its societal and political relevance, TA has been institutionalized within established organizations, notably the Office for Technology Assessment of the German Bundestag in 1973 (TAB, 2014). Moreover, it has informally influenced the norms of research funding programs, such as the EU's *Horizon 2020* program (European Commission, 2018). Today, the Network OpenTA lists 55 German speaking institutes in Germany, Austria, and

Switzerland, albeit not exclusively working on questions of TA (OpenTA, 2024). Nonetheless, the Network EPTA (European Parliamentary Technology Assessment) has 14 full members and 12 associates, some of whom are not European, such as Chile, Mexico, and Japan which all have parliamentary TA institutes (EPTA, 2024). The US Congress was served by the US Office of Technology Assessment between 1972 and 1995, since closed by funding cuts. However, since 2002, the Office for Government Accountability has taken over some of the tasks (Knezo, 2005). TA is not a uniform theory or method but a framework to anticipate the effects of R&D. Thus, there are many forms of TA that can account for its central aims or relevant methodology; see Figure 3~~Figure 3~~ for some examples.

Common Forms of TA	
Participatory TA (pTA)	Including a variety of social and political groups in the process of deliberation and discussion of the undesired effects.
Parliamentary TA	Some parliaments, like the German Bundestag, employ TA experts who advise the members of the parliament on TA with regard to specific technologies.
Expert TA	Experts give mostly written statements about the effects of technology.
Prospective TA (ProTA)	Early assessment approach aims at designing technology during R&D in a way that limits the negative effects.

Figure 3: Common forms of TA (see (Grunwald, 2002, pp. 123–158).

One approach to assessing the potential harms of a project is **ethical assessment.** Especially for research designs involving animals or humans, standardized ethics questionnaires help to identify potential risks and set boundaries for certain types of design. Many organizations that deal with critical research or procedures have established ethics committees to ensure **compliance** with ethics standards. **Ethical standards** in research aim to avoid unnecessary harm to individuals or animals in experiments by ensuring the necessity of the experiments in addressing the research question. Associated with these discourses, within IT development, there is a debate about **information ethics** and how to deal with the private information of users (Capurro, 2017).

In TA, as well as in technology design, the "participatory turn" has led to the inclusion of relevant stakeholders and public dialog as a central paradigm of technology design (Boden et al., 2021). This approach follows the assumption that the design of technologies influences socio-technical futures (Lösch et al., 2019) and practices (Stevens et al., 2018). Here, design is perceived as an enabler of possibilities (Grunwald, 2018, p. 25). Van den Hoven (2010, p. 75) describes IT architects as "choice architects, who have responsibilities for organizing the context in which people make decisions." Therefore, IT artifacts interfere with and even change socio-technical practices, underscoring why socio-technical interactions are the subjects of participatory design research (Wulf et al., 2011).

Methodologically, participatory approaches have worked towards reflecting, accounting, and including values in technology design, such as Value Sensitive Design (Friedman et al., 2013). In VSD, the concept of doing "good" means to include legitimate values in technology design (Friedman et al., 2013, p. 2). The determination of what constitutes "good" is answered empirically, often through user-centered design research. Moreover, identifying conflicts between these values allows for a reflection on possible design solutions (Friedman et al., 2013)

Looking at the development of IT products and their assessment, project management can use a sequential waterfall model as well as iterative and agile project management processes, aiming to offer shorter iterations of development and testing. While agile development has become more popular and common (Bogdan-Alexandru et al., 2019), can such iterative and agile methods help in the early identification and mitigation of dual-use risks or do they make assessment harder due to their speed and agility? First of all, such approaches have increased the efficiency of IT development in contrast to the waterfall model. However, due to their agile nature, implementing non-functional requirements poses challenges as constant changes occur, and measuring non-functional requirements often proves difficult (Gogoll et al., 2021). Additionally, such non-functional requirements might escalate the product costs and complexity. In the case of ethical AI, there has been increasing research on tools aimed at aiding researchers and developers in integrating risk deliberation and ethical requirements during agile development, locating responsibilities to different levels of decision-making (Floridi & Cowls, 2022). In **ethical deliberation**, Gogoll et al. (2021, p. 1089) found that most questions are decided either at the legal level, which decides which technologies and are desirable for a society and under which conditions, or on the business level, where business cases are defined. However, during the design and development process, there can still decisions be made, which might be far reaching, e.g. by choosing a certain AI model or database. In the process of deliberation (see

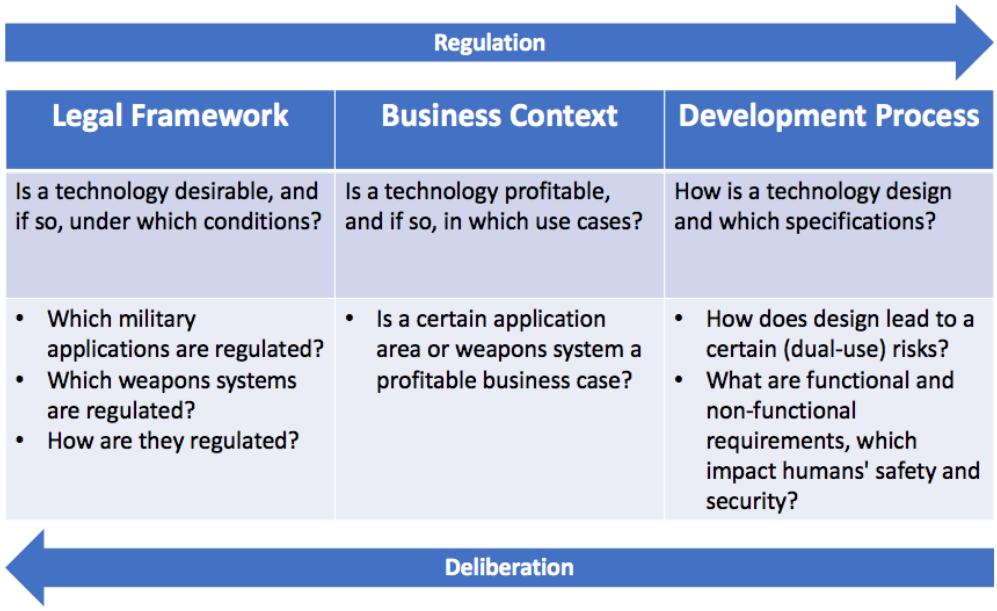

Figure ~~Figure 3~~), developers and designers can also use their expert knowledge to inform and influence the discourse on the business and the legal level.

Regulation
Legal Framework
Business Context
Development Process
Is a technology desirable, and if so, under which conditions?
Is a technology profitable, and if so, in which use cases?
How is a technology design and which specifications?
• Which military applications are regulated?
• Which weapons systems are regulated?
• How are they regulated?
• Is a certain application area or weapons system a profitable business case?
• How does design lead to a certain (dual-use) risks?
• What are functional and non-functional requirements, which impact humans' safety and security?
Deliberation

Figure 3: Dual-use Deliberation (following the framework by Gogoll et al., 2021)

Occasionally, conflicting requirements and values result in trade-offs that need prioritization. However, for matters within the developers' field of duties, it is important

to adopt a structured, guided, and systematic approach to the assessment of values, their trade-offs, and implementation (Zuber et al., 2020).

8.4 The Civil Clause at TU Darmstadt

Offering a concluding example of local, institutionalized ethical assessment, this chapter gives insight into the emergence and set-up of the Civil Clause at TU Darmstadt. In Japan and Germany, some universities prohibit military research entirely by a voluntary commitment, called **Civil Clause** (**Zivilklausel)** (Hummel, 2017; Nielebock et al., 2012; TU Darmstadt, 2018b). So far 76 German Universities have self-committed to Civil Clauses to assure the public they are not engaged in military research (Initiative Hochschule für den Frieden, 2024). The idea for this restriction at universities became popular in Germany during the pacifist movement of the 1980s amidst the Cold War. The wish to implement Civil Clauses was directly linked to anti-war and disarmament movements.

The Civil Clause is criticized for potentially limiting researchers' funding opportunities, seen as counterproductive to the freedom of research, especially when a lot of money is at stake (Hummel, 2017). Further, the Civil Clause does not aim to discredit the military, which is democratically legitimized and has to be mandated to participate in peacekeeping missions or self-defense, which would require personnel and equipment to preserve peace and security. At the same time, it is quite difficult to effectively separate between contexts due to spill-over effects between military and non-military applications (Schlögl-Flierl & Merkl, 2018; Utz et al., 2019). Spill-over effects are understood as knowledge, products and technology "spilling over" to each of the dual-use application sides. All these obstacles have hindered many universities from implementing more than voluntary commitments (ibid.).

At **TU Darmstadt**, the first commitment to conducting non-military research only was published in 1973, aiming not at the prevention of military research but at the sources for research funding that it considered should be non-military (Hubig, 2012). When the senate agreed to adopt the Civil Clause in 2012, the executive committee of the university not only affirmed research should solely serve non-military purposes but also, distinct from many other universities that only adopted a declaration without any procedures, they unanimously adopted a procedure that guides researchers using a questionnaire (see Figure 4~~Figure 4~~) and helps to identify research of concern (Utz et al., 2019). The purpose of the questionnaire is not to "name-and-shame" disqualified research but to support scientists through questions to see the research context. To do so, the Civil Clause differentiates between three decisive differences: (1) the aims of the research, either peaceful or not; (2) the means that serve either civilian or military purposes and (3) the application that can be either military or civilian.

Thus, the Civil Clause is defined as:

> Research, education and the course of studies at the Technical University of Darmstadt are exclusively dedicated towards peaceful aims, the means should serve civil purposes, especially in terms of development and optimization of technical systems, as well as education and the course of studies should be in alignment with civilian application. (TU Darmstadt, 2018b).

Therefore, as a result of extensive discussions among students, researchers and the senate of the university, a procedure was agreed to implement the Civil Clause in 2014, and a questionnaire designed to support researchers in technology assessment (see Figure 4~~Figure 4~~) (TU Darmstadt, 2018a). The questionnaire's function is to support researchers' awareness and responsibility and their ability to engage in a discourse of potential risks. If the project is considered to be of concern, the ethics committee will be consulted to provide a vote as a recommendation for the university administration (TU Darmstadt, 2018b).

	Research
1	Is your research focusing on fundamentals?
2	Does your research follow a peaceful intent?
	Project design
3	Does the project serve a civilian purpose (considering that there is a civilian and legitimate monopoly and use of force)?
4	Suppose in the case of application-oriented projects a military purpose is served, or this purpose cannot be excluded. Are the project's purposes other than the optimization of the protection, supply, intelligence or immediate defense?
5	Is the project designed in a way, that these application-oriented scenarios have a peaceful intent?
	Funding and Organizational Setting
6	Is the remitter*[3] a military organization, close to a military institution, or an enterprise that sells to the military?
7	Is there a risk of being financially or structurally dependent on this remitter, for example, to not disclose research with regard to the Civil Clause?
	Publishing and Transfer
8	Is there an agreement to possibly delay or even prohibit parts or all of the publication of research results due to the military nondisclosure policy?

Figure 4: Questionnaire Civil Clause (TU Darmstadt, 2018a)

In the context of the invasion of Ukraine and the German and European "Zeitenwende" (Löffmann, 2023), the civil clauses have been criticized as hindering the equipping of the armed forces leading to demands for reform or even to abolish the clauses. However, it is important to note that civil clauses do not prevent all military-related research but offer

[3] funder

questions for discourse and restrict the role of funding by defense firms as well as non-disclosure agreements regarding research results. How the civil clauses are interpreted and used can also change over time and differ between organizations. Whatever the case, an iterative and adaptive discourse on using the civil clauses should be the aim. In summary, the questionnaire supports a detailed discourse about the aims, purposes, and applications of R&D, enabling a transparent process and debate about R&D that might bear risks to peaceful aims, civil objectives, and applications.

8.5 Conclusion

Technologies can be considered dual-use, when they are relevant for civilian and military applications, when they are critical to security and can be misused to cause significant harm, or when they can be used as part of an (improvised) weapons system. Therefore, R&D of dual-use technologies needs safety and security measures, such as technology assessment and responsible methods of design, such as VSD and ethical deliberation. TA aims to anticipate the effects of the research and implementation of a technology within a socio-technical system and support design approaches to use the gained insight to inform the technology design to shape the socio-technical system. In computer science, dual-use questions arise in the context of IT security research, cryptography, and surveillance, as well as with regard to human-computer interaction and assistance systems using AI and robotics to create autonomous systems. The dual-use assessment, just like the ethical assessments, needs to be done in a systematic and iterative manner as part of the research and development design. Some universities offer ethical questionnaires as well as civil clauses for assessment and (self-)positioning of research endeavors.

8.6 Acknowledgements

This chapter builds on our previously written textbook chapter on dual use in information technology (Riebe et al., 2024). For this volume and to consider our context of research, it has been reframed as a contribution from a European perspective.

8.7 References

Adamsky, D. (2010). *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Stanford: Stanford University Press. doi:10.1515/9780804773805

Ahteensuu, M., & Sandin, P. (2012). The Precautionary Principle. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), *Handbook of Risk Theory* (pp. 961–978). Springer Netherlands. doi:10.1007/978-94-007-1433-5_38

Alavi, H., & Khamichonak, T. (2017). EU and US export control regimes for dual use goods: An overview of existing frameworks. *Romanian Journal of European Affairs*, *17*(1), 59–74. http://rjea.ier.gov.ro/wp-content/uploads/articole/RJEA_2017_vol17_no1_art4.pdf, last accessed June 13, 2024.

Boden, A., Liegl, M., & Büscher, M. (2021). Ethische, rechtliche und soziale Implikationen (ELSI). In C. Reuter (Ed.), *Sicherheitskritische Mensch-Computer-Interaktion* (pp. 185–205). Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-32795-8_9

Bogdan-Alexandru, A., Casu-Pop, A.-C., Gheorghe, S.-C., & Bioangiu, C.-A. (2019). A study on using waterfall and agile methods in software project management. *Journal of Information Systems & Operations Management*, 125–135. https://web.rau.ro/websites/jisom/Vol.13%20No.1%20-%202019/JISOM-SU19-A12.pdf, last accessed June 12, 2024.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., … Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217, last accessed June 12, 2024.

Buchanan, B. (2017). *The Cybersecurity Dilemma* (Vol. 1). Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780190665012.001.0001

Capurro, R. (2017). *Homo Digitalis: Beiträge zur Ontologie, Anthropologie und Ethik der digitalen Technik*. Wiesbaden: Springer VS. doi: 10.1007/978-3-658-17131-5

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

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

Deutsche Forschungsgemeinschaft & Deutsche Akademie der Naturforscher Leopoldina e.V. (2014). Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-Relevant Research. https://www.leopoldina.org/uploads/tx_leopublication/2014_06_DFG-Leopoldina_Scientific_Freedom_Responsibility_EN.pdf, last accessed June 14, 2024.

Dullien, T., Vincenzo, I., & Tam, M. (2015). *Surveillance, Software, Security, and Export Controls* [Draft Report]. https://tac.bis.doc.gov/index.php/documents/pdfs/299-surveillance-software-security-and-export-controls-mara-tam/file, last accessed June 13, 2024.

EPTA. (2024). *European Parliamentary Technology Assessment*. https://eptanetwork.org/members, last accessed June 12, 2024.

European Commission. (2018). *Horizon 2020 Programme—Guidance How to complete your ethics self-assessment*. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, last accessed June 14, 2024.

European Commission. (2019). *Ethics Guidelines for Trustworthy AI*. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, last accessed June 14, 2024.

European Parliament. (2023). *Artificial Intelligence Act: Deal on comprehensive rules for trustworthy AI*. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai, last accessed June 13, 2024.

Floridi, L., & Cowls, J. (2022). A Unified Framework of Five Principles for AI in Society. In S. Carta (Ed.), *Machine Learning and the City* (1st ed., pp. 535–545). Wiley. doi:10.1002/9781119815075.ch45

Forge, J. (2010). A Note on the Definition of "Dual Use". *Science and Engineering Ethics*, *16*(1), 111–118. doi:10.1007/s11948-009-9159-9

Friedman, B., Kahn, P. H., Borning, A., & Huldtgren, A. (2013). Value Sensitive Design and Information Systems. *Philosophy of Engineering and Technology*, *16*, 55–95. doi:10.1007/978-94-007-7844-3_4

Gesellschaft für Freiheitsrechte. (2019). *Illegal Spyware Exports*. GFF. https://freiheitsrechte.org/en/themen/digitale-grundrechte/export-von-uberwachungssoftware, last accessed June 13, 2024.

Gogoll, J., Zuber, N., Kacianka, S., Greger, T., Pretschner, A., & Nida-Rümelin, J. (2021). Ethics in the Software Development Process: From Codes of Conduct to Ethical Deliberation. *Philosophy & Technology*, *34*(4), 1085–1108. doi:10.1007/s13347-021-00451-w

Greenacre, M., & Matthews, D. (2024). EU Commission launches bid to expand funding of dual-use research in Horizon Europe's successor. *Science Business*. https://sciencebusiness.net/news/dual-use/eu-commission-launches-bid-expand-funding-dual-use-research-horizon-europes-successor, last accessed June 13, 2024.

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

Grunwald, A. (2018). *Technology assessment in practice and theory.* London: Routledge. doi:10.4324/9780429442643

Harris, E. D. (Ed.). (2016). *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge MA: American Academy of Arts & Sciences. https://www.amacad.org/publication/governance-dual-use-technologies-theory-and-practice, last accessed June 14, 2024.

Haunschild, J., Jung, L., & Reuter, C. (2023). Dual-use in volunteer operations? Attitudes of computer science students regarding the establishment of a cyber security volunteer force. In N. Gerber & V. Zimmermann (Eds.), *International Symposium on Technikpsychologie (TecPsy) 2023* (pp. 66–81). Sciendo. doi:10.2478/9788366675896-006

Herr, T. (2016). Malware counter-proliferation and the Wassenaar Arrangement. *8th International Conference on Cyber Conflict (CyCon)*, 175–190. Estonia. doi:10.2139/ssrn.2711070

Herz, J. H. (1950). Idealist Internationalism and the Security Dilemma. *World Politics*, *2*(2), 157–180. doi:10.2307/2009187

Hubig, C. (2012). Zivilklausel an Universitäten. *Forschung & Lehre*, *October*. https://www.wissenschaftsmanagement-online.de/sites/www.wissenschaftsmanagement-online.de/files/migrated_wimoarticle/ful_10-2012_Hubig.pdf, last accessed June 13, 2024.

Hummel, H. (2017). Zivilklausel auf japanisch: Japanische Universitäten ächten Militärforschung. *Wissenschaft & Frieden*, *2*. https://wissenschaft-und-frieden.de/artikel/militarisierung-oder-zivilisierung/, last accessed June 13, 2024.

Initiative Hochschule für den Frieden. (2024). *Liste aktueller Zivilklauseln sortiert nach dem Datum ihres Bestehens*. http://zivilklausel.de/index.php/bestehende-zivilklauseln, last accessed June 13, 2024.

Jonas, H. (1980). *Das Prinzip Verantwortung: Versuch einer Ethik für die technologische Zivilisation*. Frankfurt am Main: Insel-Verlag.

Knappmeier, N. (2004). Das Wesen der Informatik. In *Fachschaft Informatik TU Darmstadt (Hrsg.), Info*rz, Vol. 1.

Knezo, G. J. (2005). *Technology Assessment in Congress: History and Legislative Options* (pp. 1–6). Congressional Research Service. https://digital.library.unt.edu/ark:/67531/metadc820299/, last accessed June 13, 2024.

Knowles, L. P. (2012). Current Dual-Use Governance Measures. In J. B. Tucker (Ed.), *Innovation, Dual Use, Security: Managing The Risks of Emerging Biological and Chemical Technologies* (pp. 45–66). MIT Press. doi:10.1016/j.clsr.2018.06.003

Koops, B.-J., & Kosta, E. (2018). Looking for some light through the lens of

"cryptowar" history: Policy options for law enforcement authorities against "going dark". *Computer Law & Security Review*, *34*(4), 890–900. doi:10.1016/j.clsr.2018.06.003

Leng, C. (2013). *Die dunkle Seite: Informatik als Dual-Use-Technologie*. https://gi.de/meldung/die-dunkle-seite-informatik-als-dual-use-technologie, last accessed June 13, 2024.

Liebert, W., & Schmidt, J. C. (2018). Ambivalenzen im Kern der wissenschaftlich-technischen Dynamik: Ergänzende Anforderungen an eine Theorie der Technikfolgenabschätzung. *TATuP - Zeitschrift Für Technikfolgenabschätzung in Theorie Und Praxis*, *27*(1), 52–58. doi:10.14512/tatup.27.1.52

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.

Löffmann, G. (2023). *Germany's Zeitenwende: Wind of Change or Hot Air?* 49Security. https://fourninesecurity.de/2023/03/30/germanys-zeitenwende-wind-of-change-or-hot-air, last accessed June 12, 2024.

Lösch, A., Böhle, K., Coenen, C., Dobroc, P., Heil, R., Grunwald, A., Scheer, D., Schneider, C., Ferrari, A., Hommrich, D., Sand, M., Aykut, S. C., Dickel, S., Fuchs, D., Kastenhofer, K., Torgersen, H., Gransche, B., Hausstein, A., Konrad, K., … Wentland, A. (2019). Technology Assessment of Socio-Technical Futures—A Discussion Paper. In A. Lösch, A. Grunwald, M. Meister, & I. Schulz-Schaeffer (Eds.), *Socio-Technical Futures Shaping the Present* (pp. 285–308). Springer Fachmedien Wiesbaden. doi:10.1007/978-3-658-27155-8_13

Lösch, A., Gammel, S., & Nordmann, A. (2008). *Observieren – Sondieren – Regulieren: Zur gesellschaftlichen Einbettung nanotechnologischer Entwicklungsprozesse*. Schlussbericht des Büros für Interdisziplinäre Nanotechnikforschung (nanobüro). Technische Universität Darmstadt.

Matthews, D. (2024). German science minister calls for a rethink of "strong wall" between civilian and military research. *Science Business*. https://sciencebusiness.net/news/dual-use/german-science-minister-calls-rethink-strong-wall-between-civilian-and-military, last accessed June 12, 2024.

Mir, T. U. G., Wani, A. K., Akhtar, N., & Shukla, S. (2022). CRISPR/Cas9: Regulations and challenges for law enforcement to combat its dual-use. *Forensic Science International*, *334*. doi:10.1016/j.forsciint.2022.111274

NATO. (2016). *Warsaw Summit Communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm, last accessed June 12, 2024.

Neuneck, G. (2013). Assessment of International and Regional Organizations and Activities. In J. A. Lewis & G. Neuneck (Eds.), *The Cyber Index—International Security Trends and Realities* (pp. 91–109). UNIDIR. https://unidir.org/files/publication/pdfs/cyber-index-2013-en-463.pdf, last accessed June 12, 2024.

Nielebock, T., Meisch, S., & Harms, V. (Eds.). (2012). *Zivilklauseln für Forschung, Lehre und Studium: Hochschulen zum Frieden verpflichten*. Baden-Baden: Nomos.

NSABB. (2007). *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information* (Issue June). https://osp.od.nih.gov/wp-content/uploads/Proposed-Oversight-Framework-for-Dual-Use-Research.pdf, last accessed June 12, 2024.

Oltmann, S. (2015). Dual use research: Investigation across multiple science disciplines. *Science and Engineering Ethics*, *21*(2), 327–341. doi:10.1007/s11948-014-9535-y

OpenTA. (2024). *OpenTA:NTA Mitglieder*. https://www.openta.net/de/mitglieder, last accessed June 12, 2024.

Ottermann, T., & Gries, S. (2018). Das Wesen der Informatik. In *Fachschaft Informatik TU Darmstadt (Hrsg.)*, *Inforz.*, 16–17.

Owen, R., Macnaghten, P., & Stilgoe, J. (2012). Responsible research and innovation: From science in society to science for society, with society. *Science and Public Policy*, *39*(6), 751–760. doi:10.1093/scipol/scs093

Pissanidis, N., Rõigas, H., & Veenendaal, M. (Eds.). (2016). *2016 8th International Conference on Cyber Conflict: Cyber Power: 30 May - 03 June 2016, Tallinn, Estonia*. NATO CCD COE Publications. https://ccdcoe.org/uploads/2018/10/CyCon_2016_book.pdf, last accessed June 12, 2024.

Reinhold, T. (2021). *Export Control of Surveillance Software from Germany and Europe—Regulations, Limits and Weaknesses*. Heinrich Böll Stiftung. https://il.boell.org/en/2021/12/27/export-control-surveillance-software-germany-and-europe-regulations-limits-and, last accessed June 12, 2024.

Reuter, C., Riebe, T., Haunschild, J., Reinhold, T., & Schmid, S. (2022). Zur Schnittmenge von Informatik mit Friedens- und Sicherheitsforschung: Erfahrungen aus der interdisziplinären Lehre in der Friedensinformatik. *Zeitschrift für Friedens- und Konfliktforschung*, *11*(2), 129–140. doi:10.1007/s42597-022-00078-4

Riebe, T. (2023). *Technology Assessment of Dual-Use ICTs: How to Assess Diffusion, Governance and Design*. Wiesbaden: Springer Fachmedien. doi:10.1007/978-3-658-41667-6

Riebe, T., Schmid, S., Reuter, C. (2024). Dual-Use Technology: Research, Development and Governance of Security-relevant IT. In: Reuter, C.: *Information Technology for Peace and Security – IT-Applications and Infrastructures in Conflicts, Crises, War, and Peace*. Wiesbaden: Springer Vieweg.

Riebe, T., Wirth, T., Bayer, M., Kühn, P., Kaufhold, M.-A., Knauthe, V., Guthe, S., & Reuter, C. (2021). CySecAlert: An Alert Generation System for Cyber Security Events Using Open Source Intelligence Data. In D. Gao, Q. Li, X. Guan, & X. Liao (Eds.), *Information and Communications Security* (pp. 429–446). Springer International Publishing. doi:10.1007/978-3-030-86890-1_24

Ruohonen, J., & Kimppa, K. K. (2019). Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity. *Journal of Information Technology & Politics*, *16*(2), 169–186. doi:10.1080/19331681.2019.1616646

Schlögl-Flierl, K., & Merkl, A. (2018). Introducing Civil Clauses against Expanding Military Research at German Universities? A Descriptive and Ethical Analysis of the Discussion. *Sicherheit & Frieden*, *36*(2), 98–103. doi:10.5771/0175-274X-2018-2-98

Stevens, G., Rohde, M., Korn, M., & Wulf, V. (2018). Grounded Design: A Research Paradigm in Practice-based Computing. In V. Wulf, V. Pipek, D. Randall, M. Rohde, K. Schmidt, & G. Stevens (Eds.), *Socio Informatics – A Practice-based Perspective on the Design and Use of IT Artefacts*. Oxford University Press. doi:10.1093/oso/9780198733249.003.0002

TAB. (2014). *TA at the German Bundestag A brief history of the Office of Technology Assessment at the German Bundestag (TAB)*. http://www.tab-beim-bundestag.de/en/about-tab/history.html, last accessed June 12, 2024.

TU Darmstadt. (2018a). EK_Formular_inkl._ZK-Checkliste_2022. Word Document to download. https://www.intern.tu-darmstadt.de/media/dezernat_i/id_gremien_ordner/ethikkommission/formulare_2019/EK_Formular_inkl._ZK-Checkliste_2022.docx, last accessed June 12, 2024.

TU Darmstadt. (2018b). The Zivilklausel of TU Darmstadt. https://www.intern.tu-darmstadt.de/gremien/ethikkommisson/auftrag/index.de.jsp, last accessed June 12, 2024.

Tucker, J. B. (2012). *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies*. Cambridge: MIT Press. doi:10.7551/mitpress/9147.003.0003

Utz, L., Schickert, N., & Dutschka, S. (2019). *Die Zivilklausel der TU Darmstadt im Vergleich Wie behandeln verschiedene Zivilklauseln die Dual-Use Problematik der IT?* Conference of Aspiring Students in Tech (CAST), TU Darmstadt. https://cast.informatik.tu-darmstadt.de/files/2019/paper_utz.pdf, last accessed June

12, 2024.

Van Den Hoven, J. (2010). The use of normative theories in computer ethics. In L. Floridi (Ed.), *The Cambridge Handbook of Information and Computer Ethics* (1st ed., pp. 59–76). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511845239.005

Vella, V. (2017). Is There a Common Understanding of Dual-Use?: The Case of Cryptography. *Strategic Trade Review*, *3*(4), 03—122. https://strategictraderesearch.org/wp-content/uploads/2017/09/Is-there-a-Common-Understanding-of-Dual-use-The-Case-of-Cryptography.pdf, last accessed June 12, 2024.

von Schomberg, R. (2011). Introduction. In R. von Schomberg (Ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (pp. 7–16). European Commission. https://op.europa.eu/s/y980, last accessed June 12, 2024.

Waltz, K. (1979). *Theory of International Politics*. New York: Random House.

Wassenaar Arrangement Secretariat. (2018). *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. https://www.wto.org/english/res_e/booksp_e/int_exp_regs_part3_5_e.pdf, last accessed June 14, 2024.

WHO. (2020). *What is dual-use research of concern?* WHO. https://www.who.int/news-room/questions-and-answers/item/what-is-dual-use-research-of-concern, last accessed June 12, 2024.

Wulf, V., Rohde, M., Pipek, V., & Stevens, G. (2011). Engaging with practices: Design case studies as a research framework in CSCW. *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work*, 505–512. doi:10.1145/1958824.1958902

Zuber, N., Kacianka, S., Nida-Rümelin, J., & Pretschner, A. (2020). Ethical deliberation for Agile software processes: EDAP manual. In M. Hengstschläger (Ed.), *Digital Transformation and Ethics*. Australian Council for Research and Technology Development. https://www.bidt.digital/wp-content/uploads/sites/2/2022/08/Digital-Transformation-and-Ethics_Zuber-et-al_EN.pdf, last accessed June 12, 2024.