TATuP Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis
Journal for Technology Assessment in Theory and Practice

oekom science

RESEARCH ARTICLE

Rethinking participatory technology assessment in security governance

Dana Mahr*,1

Abstract · This article explores participatory technology assessment (pTA) in security contexts and asks whether it has a purely symbolic function or whether it can enable real democratic influence. Googles' involvement in the U.S. military's Project Maven serves as an example. At the time, Google employees publicly protested against their company's involvement in the military use of its AI, leading Google to drop its contract with the Pentagon. However, a literature review has shown that secrecy and power asymmetries are typical characteristics of security innovations, so formal pTA rarely goes beyond symbolic politics. Nonetheless, conflicts such as these can open up opportunities for public scrutiny and democratic influence.

Neue Ansätze zur partizipativen Technikfolgenabschätzung in der Sicherheitsgovernance

Zusammenfassung · *Dieser Beitrag geht der Frage nach, ob partizipative Technikfolgenabschätzung (pTA) in der Sicherheitsgovernance eine rein symbolische Funktion hat oder ob sie echte demokratische Einflussnahme ermöglicht. Die Beteiligung Googles am U.S.-Militärprojekt Maven dient als Beispiel. Google-Mitarbeiterinnen und -Mitarbeiter protestierten damals öffentlich gegen die Beteiligung ihres Unternehmens an der militärischen Nutzung seiner KI, woraufhin Google seinen Vertrag mit dem Pentagon nicht verlängerte. Eine Literaturanalyse hat jedoch gezeigt, dass Geheimhaltung und Machtasymmetrien typische Merkmale von sicherheitsrelevanten Innovationen sind und formale pTA somit selten über Symbolpolitik hinausgeht. Dennoch können Konfliktsituationen wie diese neue Möglichkeiten der öffentlichen Kontrolle und demokratischen Einflussnahme eröffnen.*

* *Corresponding author: dana.mahr@kit.edu*

[1] *Institute for Technology Assessment and Systems Analysis, Karlsruhe Institute of Technology, Karlsruhe, DE*

https://doi.org/10.14512/tatup.7231
Received: 22. 05. 2025; revised version accepted: 29. 10. 2025; published online: 23. 03. 2026 (peer review)

Keywords · *technology assessment, military research, public participation, arms control, artificial intelligence*

This article is part of the Special topic "Technology assessment and future warfare: The Good, the Bad, and the Ugly," *edited by K. Weber, M. Bresinsky. https://doi.org/10.14512/tatup.7286*

Introduction

Participatory technology assessment (pTA) refers to processes in which citizens and stakeholders are involved in decisions about new technologies (Hennen 2012). According to democratic principles, risk and ethical issues should not be determined solely by expert committees; the public affected should also be heard. In areas of security policy (i.e., technologies that affect the military, intelligence services, or issues of war and peace) these democratic demands face particular hurdles: secrecy, a discourse of urgency (emergency and threat rhetoric), and powerful, often hierarchical actors stand in the way of broad participation. This often means that participation processes in this sector remain rather formal or symbolic acts, without enabling actual co-creation (Heide and Villeneuve 2021).

A prominent example of this tension is the Pentagon's 'Project Maven' (2017–2019), which developed AI technology for object recognition in drone videos. Google was involved in the project as an industry partner at times, but this only became known after the fact. In April 2018, more than 3,100 Google employees protested in an open letter against their company's role in Maven and demanded that Google should not participate "in the business of war" (Google Employees 2018). The letter, with its core message 'Google should not be in the business of war,' made headlines around the world. This sparked a broad debate that revealed contradictions between the company's publicly proclaimed values and its involvement in military applications. Under pressure from internal protests and negative publicity, Google announced in June 2018 that it would allow the Maven contract with the Department of Defense to expire. This case illustrates, on the one hand, the desire for democratic influence on military technology developments, but on the other

hand, the narrow limits of such influence under security policy conditions: Despite Google's withdrawal, the actual project development continued unabated, now with other companies in the background.

Against this backdrop, the research question arises as to what participatory processes look like and how they work in areas of tight secrecy. Specifically, the article asks: Does pTA in the defense and security sector remain mere symbolic politics? Or are there ways in which participation can lead to real change despite power asymmetries and secrecy? How does this finding contribute to the debate on democratic control of security technologies? The aim of this article is to explore this tension and contribute to technology assessment (TA) and science and technology studies (STS) by examining participatory approaches in the hitherto neglected field of security governance.

Does participatory technology assessment in the defense and security sector remain mere symbolic politics?

Literature review

Early pTA scholarship argued that involving citizens in technology decisions (via citizens' juries, consensus conferences, etc.) enhances legitimacy (Hennen et al. 2023; Wesselink et al. 2011). In practice, however, critics observed that such exercises often reproduce existing hierarchies rather than disrupting them (Felt and Fochler 2008). This prompted STS scholars to reject the notion of a single 'public.' Instead, they emphasize multiple, context-specific publics (Warner 2002; Marres 2007). For example, Pesch et al. (2020) advocate forming dedicated 'local publics' so that acceptability is judged by diverse community stakeholders (including local communities) rather than an abstract general public, reflecting the co-production of knowledge and values (Witjes 2017). In short, contemporary literature suggests that meaningful pTA must engage various publics rather than treat participation as a one-size-fits-all or token gesture.

Security conditions create further challenges. Democratic theory holds that participation only matters when processes are transparent, inclusive, and answerable to citizens (Habermas 2001; Dryzek 2002). But secrecy in defense policymaking directly conflicts with these ideals. Analysts warn that secret policymaking produces a 'knowledge deficit' and prevents citizens from authorizing or contesting hidden actions (Mokrosinska 2023), while withholding information in military affairs erodes citizen consent (Perthes 2011). Appeals to 'necessary secrecy' may even cloak unethical practices (Born and Leigh 2007). Under such conditions, participatory exercises risk being purely symbolic. When urgency and confidentiality dominate, public forums tend to rubber-stamp pre-set outcomes (Taylor et al. 2017). In military contexts these pressures intensify: Secrecy is woven into operations (Mickan 2013) even as life-and-death technologies arguably demand popular scrutiny. Overall, scholars conclude that confidentiality requirements routinely undermine accountability, often relegating participation to a thin veneer that deepens public exclusion (Guerrero 2018).

Research on emerging military technologies shows that narrative framing also plays a performative role. Malmio (2023) finds that debates on AI (e.g., Project Maven) are framed by competing 'enabling' narratives (AI as life-saving precision tool) versus 'constraining' narratives (emphasizing human accountability), and that these frames actively shape technological trajectories by defining which ethical choices seem possible. More broadly, foresight studies note a consensus among experts on the need for civilian engagement in security innovation, but lament a lack of concrete participation models for defense (Vicente-Oliva 2025). As Hennen et al. (2023) and Ladikas et al. (2023) argue, transnational security challenges strain national TA designs, calling for new, cross-border engagement frameworks beyond the nation-state.

Nonetheless, informal or insurgent forms of influence can emerge. Whistleblowers, media exposés, or employee activism sometimes thrust hidden military R&D into public view. Lindelauf and Meerveld (2025) propose 'hybrid' transparency arrangements (for example, keeping military AI algorithms closed to the general market but open to audit by vetted, trusted partners) to build trust without fully sacrificing confidentiality. The Project Maven case exemplifies the limits of such bottom-up contestation: Google employees' protests forced the company to withdraw (imposing an internal pause and ethical commitment), but the Pentagon's AI program continued largely as planned (Xue and Guo 2024). Thus, while these episodes can expose value conflicts and impose constraints on some actors, entrenched secrecy and power asymmetries often mean that underlying innovation trajectories remain unaffected.

Methodology

This paper follows a qualitative case study design using Project Maven as an example. This case study was selected because Project Maven is a prominent current example of the intertwining of high technology and the security apparatus, and it can be partially reconstructed through public documents and debates. The case thus provides empirical insights into otherwise difficult-to-access processes at the interface between the technology

industry and the military. At the same time, Maven paradigmatically illustrates the thesis of the tension between (symbolic) participation and democratic conflict potential.

The analysis is divided into two steps: First, a comprehensive literature review was conducted, bringing together theoretical and conceptual foundations from the fields of TA, security research, STS, and democracy theory. Second, primary and secondary sources on the Project Maven case were evaluated. To this end, the available sources were systematically recorded: official government documents (e.g., reports from the U.S. Department of Defense and analyses from the Congressional Research Service), parliamentary hearings and debate contributions, press articles (international and US-internal, 2017–2024), reports from non-governmental organizations and think tanks, and public statements by the companies and actors involved (e.g., blog posts by Google executives, the published corporate mission statement on AI ethics, open letters from employees). The identified documents were examined using qualitative content analysis. Key events and decisions in the course of Maven were chronologically reconstructed, identifying key actors (Pentagon, Google management, Google employees, media, politicians) and their contributions to the discourse. Particular attention was paid to informal forms of participation (such as employee protests) and the institutional framework (e.g., the role of internal company forums vs. the lack of government participation formats). The case analysis is theory-driven: It embeds the empirical findings in discussions about participation and democracy in order to make empirical and normative classifications.

Research in security policy contexts poses specific methodological challenges. Much of it takes place in areas that are closed to the public; relevant documents are often subject to high levels of secrecy. The present study therefore relies on publicly available information. This entails limitations: The presentation is based on what has come to light (e.g., through media reports). It is naturally impossible to obtain a complete picture of internal decision-making processes at the Department of Defense or Google. In addition, the statements made by the actors must be viewed in the context of their possible self-interests (e.g., corporate statements may be strategically motivated). To counteract distortions, source triangulation was attempted: Wherever possible, information is corroborated by several independent sources (e.g., press reports are compared with official statements and subsequent analyses). Nevertheless, the results must be interpreted with the caveat that they primarily reflect publicly documented dynamics. These limitations are disclosed in the discussion in order to make the scope of the conclusions transparent.

Case study: Project Maven

Background of the project

Project Maven, formally known as the Algorithmic Warfare Cross-Functional Team, was launched in April 2017 by the U.S. Department of Defense. The goal was to accelerate the use of artificial intelligence in the military, in particular through the development of computer vision algorithms for object recognition in video recordings from drones (U.S. DoD 2017; Pellerin 2017; Jones 2018). The Pentagon was responding to a perceived gap: While AI (especially machine learning for image recognition) was making rapid progress in the civilian sector, military agencies were lagging behind. Instead of building AI capabilities exclusively in-house, the Department of Defense pursued a public-private partnership strategy and sought specific collaboration with the tech industry. By the end of 2017, Google had already joined Project Maven as its most important corporate partner (Malmio 2023). Google contributed its expertise in the development of machine learning models, cloud infrastructure, and mass data processing. Initially, this was done confidentially: The cooperation between Google and the Pentagon was not made public, presumably to avoid internal and external criticism in advance. Within Google itself, however, at least a circle of employees was aware that software was being adapted for military purposes. In early 2018, the first information about Maven reached the media, immediately triggering an ethical controversy (Crofts and van Rijswijk 2020). The public suddenly questioned whether a company whose products are used by billions of people should be involved in AI for the military.

The debate remained elitist and technocratic rather than democratic and participatory.

Protest by Google employees

The revelation of Google's contribution to Project Maven acted as a catalyst for internal protest within the company. In the spring of 2018, an unprecedented wave of employee activism formed at Google (Scheiber and Conger 2020). Over 3,100 employees signed an open letter to the company's management with the unambiguous demand: "Google should not be in the business of war" (Google Employees 2018). This letter, which was made public in April 2018, expressed a deep concern shared by many employees: Namely, that the AI tools they had developed could ultimately be used in drone missions to automate lethal decisions (Google Employees 2018). The signatories argued that their work should not be repurposed for military use without transparent debate and without their consent.

There were several remarkable aspects to the protest. First, it was one of the most visible cases of ethical dissent from within the tech industry. Google employees publicly took a stand

https://doi.org/10.14512/tatup.7231

against a lucrative defense project of their own employer – a move that was unprecedented on this scale. Scholars interpreted this event as an early example of 'bottom-up governance': It was not regulatory agencies or NGOs, but the company's own employees who pushed a technology company to rethink its role in military innovation (Crofts and van Rijswijk 2020). Second, the protest exposed the contradictions in Google's corporate culture. For years, Google had cultivated a certain moral identity with the slogan 'Don't be evil'; in 2018, however, this motto was quietly replaced by the more innocuous 'Do the right thing' (Google n.d.; Horwitz 2022). For the protesting employees, the collaboration with the Pentagon represented a clear betrayal of values – both the old and the new company credo. This was a clash between the pursuit of profit, public image, and ethical responsibility. The controversy thus exemplified how a private company can become a venue for social negotiation when government decision-making processes remain closed: The workforce sparked a debate that should have taken place on the socio-political stage, for example in parliaments.

Without technical transparency, meaningful debate is impossible.

Reactions from the company

In the face of growing criticism, Google's management felt compelled to act quickly. The management team, led by CEO Sundar Pichai and the head of the cloud division, Diane Greene, initially sought dialogue with the employees. Internal town hall meetings and discussion groups were organized, during which management promised to rethink its own guidelines for military contracts. In fact, two far-reaching announcements followed at the end of May/beginning of June 2018: First, Diane Greene informed employees that Google would not renew the current Maven contract when it expired in 2019 (Statt 2018). Second, on June 7, 2018, Google published a set of AI principles that would henceforth serve as ethical guidelines for Google's development of artificial intelligence (Pichai 2018). These principles explicitly prohibited the development of AI for weapons systems, but left open the possibility of continuing to operate in other areas of defense, such as cybersecurity and logistics (Shane and Wakabayashi 2018).

On the one hand, the announcement of these AI principles was a direct concession to employee protests: Google attempted to address ethical concerns and regain lost trust. On the other hand, it clearly served to enhance the company's external reputation: The aim was to signal that Google was handling AI responsibly. Nevertheless, criticism from various quarters was inevitable. Scientists and observers noted that voluntary commitments such as these 'ethical principles' are often non-binding in corporate practice and lack enforcement (Malmio 2023). Without external control mechanisms, such guidelines could easily be circumvented or adapted if commercial or political interests suggested it. Furthermore, it became clear that although Google's direct withdrawal from Maven represented a symbolic victory for the protesters, the Pentagon project itself continued unabated. In other words, the company's decision primarily affected its public image – military-technological development as such remained unaffected (Hogue 2021). This already suggests that symbolic successes are possible, but do little to change structural path dependencies.

Publicity and progress of the project

What is striking about the Project Maven conflict is the lack of institutionalized public deliberation beyond Google. Neither the Department of Defense nor the U.S. Congress initiated any public technology impact assessments or citizen dialogues on the ethical and social implications of the use of AI in the military during that period (Hogue 2021). The debate took place primarily in internal company forums, in expert circles (e.g., posts in technology and legal blogs), and in specialized media. Thus, to put it bluntly, the debate remained elitist and technocratic rather than democratic and participatory. Although mainstream media reported on the internal conflict at Google and there were comments from NGOs, there was no broad public participation or parliamentary hearing on Maven (U.S. Department of Defense 2017). This underscores the problematic fact that security policy technology decisions are often made without broad public feedback – unless internal whistleblowers or protests happen to make them public.

After Google's withdrawal, it soon became clear who would continue Maven's development. In 2019, media reports indicated that Palantir Technologies had assumed key parts of the project. According to Business Insider, the company internally launched the code-named project 'Tron' to deliver AI models for drone video analysis, thereby continuing Google's earlier work (Peterson 2019). The report noted that Palantir had taken over Project Maven after Google ended its Pentagon contract in March 2019 following employee protests. Palantir (long linked to the security sector) thus seamlessly replaced Google.

The seamless continuity of the project under different leadership highlights a core element of security-driven innovation: Even if a single company withdraws due to public pressure, the technological path remains intact as long as the need within the security apparatus persists. In the case of Maven, this is exactly what happened. The fundamental military demand for AI-supported analysis of surveillance data remained unbroken – and Palantir was found to be a willing replacement. In fact, the Department of Defense expanded its cooperation with Palantir in the following years. In May 2024, Reuters reported that the Pentagon had awarded Palantir a $480 million contract for an advanced Maven Smart System (Reuters 2024). The specialist portal C4ISRNet also reported that a five-year contract would

enable the wider use of this system (Albon 2024). It is clear that structural drivers (in this case, the strategic imperative to improve the evaluation of intelligence material through AI) ensure that a project like Maven continues, regardless of interim reputation crises or personnel changes on the provider side.

Overall, the Maven case demonstrates the limits of corporate-driven protests: While the action taken by Google employees was able to influence the behavior of a single company, it did not change the long-term course of government arms policy. This continues to be determined by geopolitical priorities (e.g., the technological race with rivals such as China) and the interests of security agencies. Thus, innovation remained in the world, only the constellation of actors shifted slightly. This presents a dilemma for democratic control: Even if interventions are successful in individual cases, they must be institutionally anchored in order to have more than a symbolic effect – otherwise, the development of military technology will take place under different circumstances.

Discussion

The Project Maven case highlights institutional, epistemic, and power-political barriers that restrict genuine participation in security innovation. Institutionally, there is a deep asymmetry between the security apparatus and the democratic public sphere. Military and intelligence agencies operate within a closed 'security zone,' shielded by secrecy rules, clearances, and black budgets that place decisions beyond public control. As Mickan (2013) notes, secrecy is a constitutive element of the military, yet this tension must not come at the expense of informed citizens. In Maven, no formal participation took place – basic information such as data use or algorithmic design remained classified. The only 'participants' were Google employees, whose protest mattered mainly because Google's public brand and dependence on skilled labor gave them leverage. By contrast, traditional defense contractors face no comparable pressure; their activities usually remain invisible and only surface through leaks or media scrutiny.

Epistemically, knowledge asymmetries further block participation. Maven's AI systems functioned as a black box: Neither internal actors nor the public knew how models operated or what data they used. Without technical transparency, meaningful debate is impossible. Even Google staff demanding insight into the project met resistance, while external observers had no access to relevant facts. As Lindelauf and Meerveld (2025) argue, limited openness toward trusted partners could strengthen accountability, but under current secrecy regimes participation remains largely superficial. The epistemic gap between experts with clearance and lay publics thus widens, reinforcing perceptions of incompetence on the latter's side.

Power-political barriers arise when urgency and threat narratives justify exceptional measures. In the Maven debate, references to a technological race with China served to sideline democratic procedures – a typical case of securitization. Born and Leigh (2007) warn that such appeals to 'necessary secrecy' can mask dubious practices. The decision to partner with Google was driven by efficiency, not public deliberation. Civil society's influence was indirect: Only when reputational risk threatened Google did management react. As Vicente-Oliva (2025) notes, experts call for more citizen involvement in defense foresight, yet no concrete models exist. Maven confirms that participatory impulses remain extra-institutional and symbolically charged.

To address these tensions, several reforms have been proposed. Advisory boards with security clearance could review classified projects while representing diverse perspectives, though confidentiality risks curbing critique. Confidential parliamentary hearings might allow selected experts and NGOs to advise defense committees behind closed doors, using existing democratic channels but offering limited public transparency. Simulated citizen forums could model deliberation through hypothetical scenarios, though their policy impact would remain uncertain. Each approach faces resistance from security institutions reluctant to share authority. Yet incremental steps (such as independent ombudsmen or periodic public reports on defense AI) could create 'embedded transparency' without endangering operational secrecy.

Overall, the Maven protests exposed systemic tensions rather than resolving them. Participation under secrecy remains ad hoc and largely symbolic: It can illuminate value conflicts but rarely transforms underlying power structures or decision-making in security policy.

Conclusion

PTA in security governance often remains largely symbolic because secrecy, urgency narratives, and hierarchical power structures render transparency and inclusion difficult. However, the Project Maven case illustrates that critical contestation can still emerge. Protests of these effects are contingent and fragile – Maven's AI project continued under other contractors, showing that symbolic resistance rarely changes structural power asymmetries. In sum, pTA in the security sector remains constrained but not futile: Even symbolic participation can become politically productive when moments of contestation are harnessed to uphold democratic oversight and accountability.

Funding • This article received no funding.

Competing interests • The author declares no competing interests.

Ethical oversight • The author confirms that all procedures were performed in compliance with relevant laws and institutional guidelines.

Acknowledgements • I would like to thank Nora Weinberger, whose sharp questions, generous feedback, and intellectual sparring were essential to this paper. Her critical reflections helped me see the text more clearly. This article carries her traces.

https://doi.org/10.14512/tatup.7231

References

Albon, Courtney (2024): Palantir wins contract to expand access to Project Maven AI tools. In: C4ISRNET, 30.05.2024. Available online at https://www.c4isrnet.com/artificial-intelligence/2024/05/30/palantir-wins-contract-to-expand-access-to-project-maven-ai-tools/, last accessed on 04.11.2025.

Born, Hans; Leigh, Ian (2007): Democratic accountability of intelligence services. Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Crofts, Penny; van Rijswijk, Honni (2020): Negotiating 'evil'. Google, Project Maven and the corporate form. In: Law, Technology and Humans 2 (1), pp. 75–90. https://doi.org/10.5204/lthj.v2i1.1313

Dryzek, John (2002): Deliberative democracy and beyond. Liberals, critics, contestations. Oxford: Oxford University Press. https://doi.org/10.1093/019925043X.001.0001

Felt, Ulrike; Fochler, Maximilian (2008): The bottom-up meanings of the concept of public participation in science and technology. In: Science and Public Policy 35 (7), pp. 489–499. https://doi.org/10.3152/030234208X329086

Google (n.d.): Our approach to information. How search works. Available online at https://www.google.com/intl/en_us/search/howsearchworks/our-approach/, last accessed on 04.11.2025.

Google Employees (2018): Open letter to Sundar Pichai. Available online at https://static01.nyt.com/files/2018/technology/googleletter.pdf, last accessed on 04.11.2025.

Guerrero, Alexander (2018): Defense and ignorance. War, secrecy, and the possibility of popular sovereignty. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780190922542.003.0016

Habermas, Jürgen; Rehg, William (2001): Between facts and norms. Contributions to a discourse theory of law and democracy. Cambridge, MA: MIT Press.

Heide, Marlen; Villeneuve, Jean-Patrick (2021): Framing national security secrecy. A conceptual review. In: International Journal: Canada's Journal of Global Policy Analysis 76 (2), pp. 238–256. https://doi.org/10.1177/00207020211016475

Hennen, Leonhard (2012): Why do we still need participatory technology assessment? In: Poiesis & Praxis 9 (1–2), pp. 27–41. https://doi.org/10.1007/s10202-012-0122-5

Hennen, Leonhard; Peissl, Walter; Hahn, Julia; Ladikas, Miltos; van Est, Rinie; Lindner, Ralf (2023): Introduction. Technology assessment beyond national boundaries. In: Leonhard Hennen, Julia Hahn, Miltos Ladikas, Ralf Lindner, Walter Peissl and Rinie van Est (eds.): Technology assessment in a globalized world. Cham: Springer, pp. 1–14. https://doi.org/10.1007/978-3-031-10617-0_1

Hogue, Simon (2021): Project Maven, big data, and ubiquitous knowledge. The impossible promises and hidden politics of algorithmic security vision. In: Aleš Završnik and Vasja Badalič (eds.): Automating crime prevention, surveillance, and military operations. Cham: Springer, pp. 203–221. https://doi.org/10.1007/978-3-030-73276-9_10

Horwitz, Josh (2022): Google is losing 'Don't be evil' in its code of conduct, and what's left is corporate jargon. In: Quartz, 20.07.2022. Available online at https://qz.com/1282892/google-is-losing-dont-be-evil-in-its-code-of-conduct-and-whats-left-is-corporate-jargon, last accessed on 31.10.2025.

Jones, Felicity (2018): Project Maven. Machine learning in the military target selection process. In: Technology and Operations Management, 13.11.2018. Available online at https://d3.harvard.edu/platform-rctom/submission/project-maven-machine-learning-in-the-military-target-selection-process/, last accessed on 04.11.2025.

Ladikas, Miltos; Hahn, Julia; Hennen, Leonhard; van Est, Rinie; Peissl, Walter; Lindner, Ralf (2023): The shape of global technology assessment. In: Leonhard Hennen, Julia Hahn, Miltos Ladikas, Ralf Lindner, Walter Peissl and Rinie van Est (eds.): Technology assessment in a globalized world. Cham: Springer, pp. 225–235. https://doi.org/10.1007/978-3-031-10617-0_11

Lindelauf, Roy; Meerveld, Herwin (2025): Building trust in military AI starts with opening the black box. In: War on the Rocks, 12.08.2025. Available online at https://warontherocks.com/2025/08/building-trust-in-military-ai-starts-with-opening-the-black-box/, last accessed on 31.10.2025.

Malmio, Irja (2023): Ethics as an enabler and a constraint. Narratives on technology development and artificial intelligence in military affairs through the case of Project Maven. In: Technology in Society 72, p. 102193. https://doi.org/10.1016/j.techsoc.2022.102193

Marres, Noortje (2007): The issues deserve more credit. Pragmatist contributions to the study of public involvement in controversy. In: Social Studies of Science 37 (5), pp. 759–780. https://doi.org/10.1177/0306312706077367

Mickan, Thomas (2013): Kommentar. Geheimhaltung, Demokratie und Militär. In: IMI-Standpunkt 34, 18.07.2013. Available online at https://www.imi-online.de/2013/07/18/kommentar-geheimhaltung-demokratie-und-militar, last accessed on 31.10.2025.

Mokrosinska, Dorota (2023): Necessary but illegitimate. On democracy's secrets. In: The Review of Politics 85 (1), pp. 73–97. https://doi.org/10.1017/S0034670522000936

Pellerin, Cheryl (2017): Project Maven industry day pursues artificial intelligence for DoD challenges. In: U.S. Department of Defense News, 27.10.2017. Available online at https://www.war.gov/News/News-Stories/Article/Article/1356172/project-maven-industry-day-pursues-artificial-intelligence-for-dod-challenges/, last accessed on 31.10.2025.

Perthes, Volker (2011): Wikileaks und warum Diskretion in der Außen- und Sicherheitspolitik wichtig ist. In: Eva Gilmer and Heinrich Geiselberger (eds.): Wikileaks und die Folgen. Netz – Medien – Politik. Frankfurt a. M.: Suhrkamp, pp. 164–174.

Pesch, Udo; Huijts, Nicole; Bombaerts, Gunter; Doorn, Neelke; Hunka, Agnieszka (2020): Creating 'local publics'. Responsibility and involvement in decision-making on technologies with local impacts. In: Science and Engineering Ethics 26 (4), pp. 2215–2234. https://doi.org/10.1007/s11948-020-00199-0

Peterson, Becky (2019): Palantir grabbed Project Maven defense contract after Google left the program. Sources. In: Business Insider, 10.12.2019. Available online at https://www.businessinsider.com/palantir-took-over-from-google-on-project-maven-2019-12, last accessed on 04.11.2025.

Pichai, Sundar (2018): AI at Google. Our principles. In: The Keyword (Google Blog), 07.06.2018. Available online at https://blog.google/technology/ai/ai-principles/, last accessed on 31.10.2025.

Reuters (2024): Pentagon awards $480 million deal to Palantir for 'Maven' prototype. In: Reuters, 30.05.2024. Available online at https://www.reuters.com/technology/palantir-wins-480-million-us-army-deal-maven-prototype-2024-05-29/, last accessed on 31.10.2025.

Scheiber, Noam; Conger, Kate (2020): The great Google revolt. In: The New York Times, 18.02.2020. Available online at https://www.nytimes.com/interactive/2020/02/18/magazine/google-revolt.html, last accessed on 31.10.2025.

Shane, Scott; Wakabayashi, Daisuke (2018): 'The business of war'. Google employees protest work for the Pentagon. In: The New York Times, 04.04.2018. Available online at https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html, last accessed on 04.11.2025.

Statt, Nick (2018): Google reportedly leaving Project Maven military AI program after 2019. In: The Verge, 01.06.2018. Available online at https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire, last accessed on 04.11.2025.

Taylor, Bryan; Bean, Hamilton; O'Gorman, Ned; Rice, Rebecca (2017): A fearful engine of power. Conceptualizing the communication–security relationship. In: Annals of the International Communication Association 41 (2), pp. 111–135. https://doi.org/10.1080/23808985.2017.1312482

U.S. DoD – United States Department of Defense (2017): Establishment of an algorithmic warfare cross-functional team (Project Maven). Washington, DC: United States Department of Defense. Available online at https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf, last accessed on 04.11.2025.

Vicente-Oliva, Silvia (2025): Participation of civil society in security and defense foresight exercises. In: Futures & Foresight Science 7 (1), p. e206. https://doi.org/10.1002/ffo2.206

Warner, Michael (2002): Publics and counterpublics. In: Public Culture 14 (1), pp. 49–90. https://doi.org/10.1215/08992363-14-1-49

Wesselink, Anna; Paavola, Jouni; Fritsch, Oliver; Renn, Ortwin (2011): Rationales for public participation in environmental policy and governance. Practitioners' perspectives. In: Environment and Planning A: Economy and Space 43 (11), pp. 2688–2704. https://doi.org/10.1068/a44161

Witjes, Nina (2017): The co-production of science, technology and global politics. Exploring emergent fields of knowledge and policy. Munich: Technische Universität München. Available online at https://mediatum.ub.tum.de/doc/1350479/document.pdf, last accessed on 04.11.2025.

Xue, Jonathan; Guo, Lifu (2024): AI Cold War with China? The advantage of public conversations about ethics. In: GRACE: Global Review of AI Community Ethics 2 (1), p. 1–18. https://doi.org/10.60690/vdnrw404

DR. DANA MAHR
is a researcher at the Institute for Technology Assessment and Systems Analysis (ITAS) at the Karlsruhe Institute of Technology (KIT). She earned her PhD from Bielefeld University in 2013 and previously held research positions at the Université de Genève and the Universität zu Lübeck.