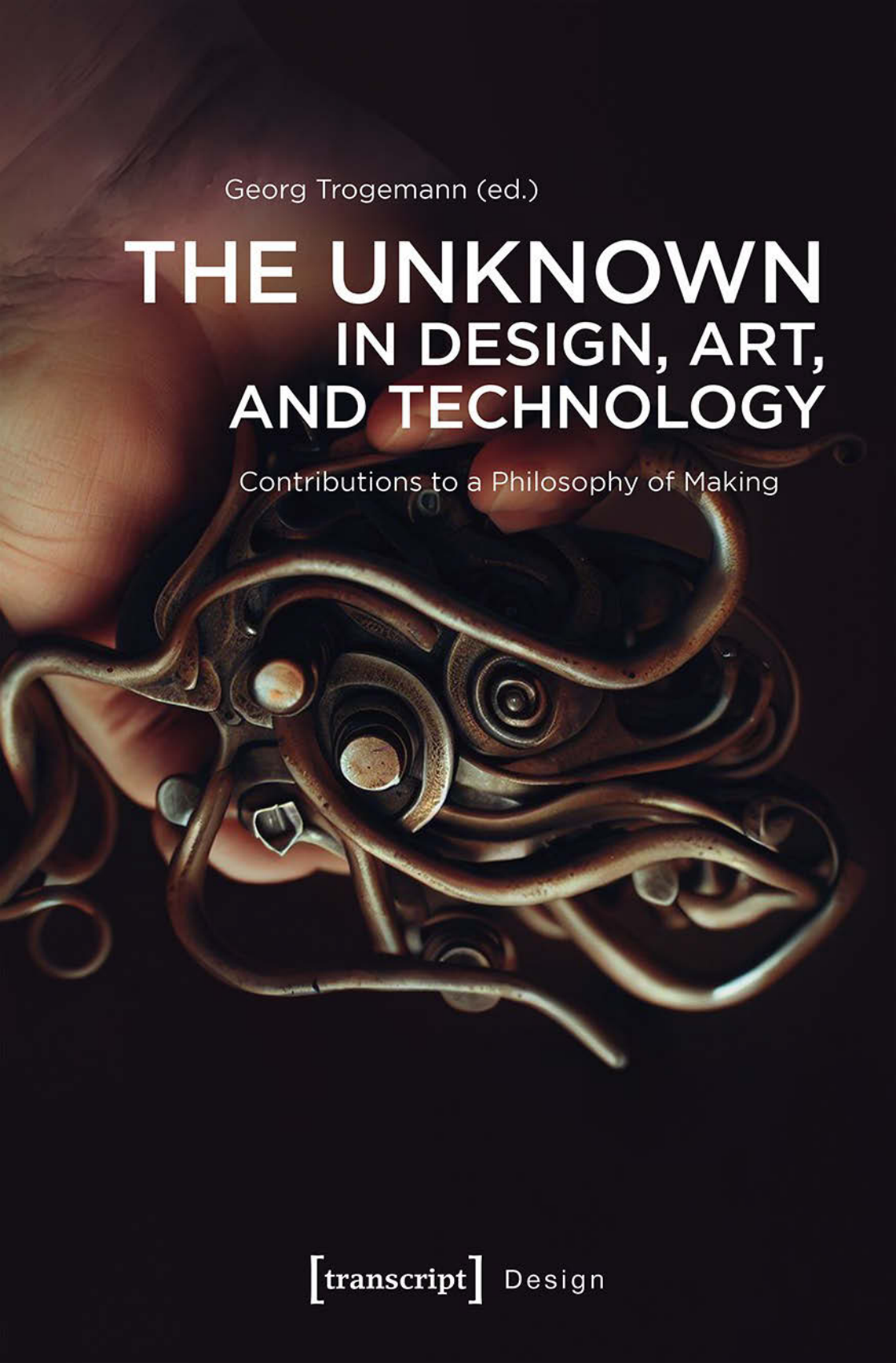
Georg Trogemann (ed.)
THE UNKNOWN
IN DESIGN, ART,
AND TECHNOLOGY
Contributions to a Philosophy of Making
[transcript] Design

Kunsthochschule für Medien Köln
Academy of Media Arts Cologne

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at https://dnb.dnb.de

First published in 2025 by transcript Verlag, Hermannstraße 26 | D-33602 Bielefeld | live@transcript-verlag.de

Cover layout: Zahra M.Ganjee, Somayyeh Shahhoseiny
Cover illustration: AI generated image from the workshop run by Steffen Mitschelen and Natalie Weinmann
Typeset: Zahra M.Ganjee, Somayyeh Shahhoseiny
Printed by docupoint GmbH, Magdeburg
Print-ISBN 978-3-8376-7681-5
PDF-ISBN 978-3-8394-7681-9
https://doi.org/10.14361/9783839476819
ISSN of series: 2702-8801
eISSN of series: 2702-881X

Printed on permanent acid-free text paper.

Imprisoning people for weeks to prevent them from participating in protests is incompatible with human rights and the rule of law.
Amnesty International[1]

Christian Heck

The Duty to Prevent

Prologue

In order to prevent further disruptive actions during the International Motor Show (IAA, Munich) in September 2021, nine activists from the Aktion Autofrei were taken into preventative custody (aka preventative detention) until the end of the trade fair.[2] The legal basis for this was provided by the tightening of the Bavarian Police Duties Act (Polizeiaufgabengesetz, PAG) in July 2021. While the expansion of the police laws in the federal states was originally initiated to prevent terrorist and extremist acts, this form of imprisonment is now permitted in the event of *"immediately impending committal/continuation of a criminal offense/infraction that is of considerable importance to the general public,"*[3] as it is phrased in the Bavarian Police Duties Act. In 2023, activists were also taken into preventative detention in connection with the IAA before they could even do anything. According to spokespersons from the *Last Generation*, sixteen of those affected were detained until September 10, and an additional eleven were detained by order of the Munich District Court until September 30. This is the case because many non-governmental organizations (NGOs) were

1 Amnesty International, "Deutschland: Präventivgewahrsam für Klimaschützer*innen ist klarer Verstoß gegen die Menschenrechte," *Amnesty.de,* September 4, 2021, https://www.amnesty.de/allgemein/pressemitteilung/deutschland-klimaschuetzerinnen-praeventivgewahrsam-verstoss-menschenrechte (accessed 1/8/2024).
2 See Michael Trammer, "Polizei stört Protest gegen IAA," taz, 9 September 2021, https://taz.de/Stoerer-bei-Automesse-in-Muenchen/!5795867/ (accessed 1/8/2024).
3 "Gewahrsam nach Maßgabe des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Polizei (PAG) (Munich, 2022)," https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2022-N-41850? (accessed 1/8/2024).

planning demonstrations, blockades, and other protests against the IAA 2023, as they do every year. The Bavarian Interior Minister Joachim Herrmann (CSU) anticipated protests, especially *"from the anti-capitalist and climate change camps."* He went on to say, *"We will not tolerate any criminal acts! Anyone who stops others in traffic, damages the property of others, becomes violent towards other people, or hinders emergency services must expect the police to take firm action."*[4] However, no such offenses were committed by those arrested prior to their detention. On the contrary, the offenses were anticipated by the politicians and law enforcement authorities. Nevertheless, around 1,500 climate activists gathered for the protest in the end, and they were confronted by 4,500 police officers.

This occurrence that took place at the IAA 2023 in Munich is part of a trend towards *preemptive security policy,* just like the clearing of the Hambach forest or the flyover of the G8 protest camp in Heiligendamm, both of which were later declared unlawful.[5] There are numerous other cases – such as the preemptive arrest near Biarritz of three Franconian youths during the G7 summit in the summer of 2019 – that attest to this emerging trend. These three youths, who were actually on their way to the Basque country, were listed in a Bavarian *State Criminal Police Office (Landeskriminalamt,* LKA) database along with 121 others in Germany's left-wing scene. German authorities passed them on to the French security authorities. The travelers had no criminal record and none of them had ever committed a criminal offense or possessed illegal items. When questioned about the specific details, the Bavarian State Criminal Police Office and the German government did not disclose any information, citing *"reasons of state interest."*[6]

4 See Editor, "Munich vor der IAA: Immer mehr Klimaaktivisten in bayerischer Präventivhaft," Der Globus Deutschland, September 2, 2023, https://www.globusdeutschland.de/2023/09/02/munchen-vor-der-iaa-immer-mehr-klimaaktivisten-in-bayerischer-praventivhaft/ (accessed 1/8/2024).

5 See Bernd Müllender, "Ein Schlag in die Magengrube," taz, September 8, 2021, https://taz.de/Urteil-zu-Raeumungen-im-Hambi/!5799019/ and Pascal Beucker, "Angsteinflößend und einschüchternd," taz, October 26, 2017, https://taz.de/Kampffliegereinsatz-in-Heiligendamm/!5455805/ (both accessed 1/8/2024).

6 See. Konrad Litschko, "Zehn Jochen Präventivhaft," taz, 15 November 2019, https://taz.de/Festgenommene-Deutsche-bei-G7/!5638399/ (accessed 1/8/2024).

Security Policy in the 21st Century

> *Many people have asked how close Saddam Hussein is to developing a nuclear weapon. Well, we don't know exactly, and that's the problem [...] Facing clear evidence of peril (the attacks of September 11), we cannot wait for the final proof – the smoking gun – that could come in the form of a mushroom cloud [...] Understanding the threats of our time, knowing the designs and deceptions of the Iraqi regime, we have every reason to assume the worst, and we have an urgent duty to prevent the worst from occurring.*[7]

The term prevention has gained prominence in Western industrialized nations. Simultaneously, its social implication has undergone a significant change, reaching a point where its application has started to have an impact on our daily lives and on our society, not only in the interests of private companies, scientific research, national and international security, federal and state investigation offices, the police, the military, the Office for the Protection of the Constitution, and the secret services, but also in the interest of the people. Preventative measures are increasingly encroaching upon our social interactions, disrupting the spaces where we gather and engage in conversation. These are the places where our sense of solidarity is nurtured and the social significance of concepts are derived, i.e. they are places where *sense-making* takes place.

In this millennium, Western societies are redefining concepts such as *catastrophe, danger, crisis, and risk,* and even the concept of *terrorism,* while integrating them into novel and at times *disruptive technologies.*[8] It is becoming increasingly important for society to respond to these new, critical developments as a whole. To this end, we need to mitigate risks and ideally prevent predicted crises, attacks, uprisings, and disasters before they unfold. Such shifts in the meaning of concepts align with a reconsideration of the acceptability of preventative and preemptive measures to minimize risk.[9] This occurs regarding new global crises, wars, military conflicts, and the threats posed by terrorism and weapons of mass destruction, to gain sovereignty in matters of interpretation.

7 "Transcript: George Bush's speech on Iraq," The Guardian, 7 October 2002, https://www.theguardian.com/world/2002/oct/07/usa.iraq (accessed 1/8/2024).

8 Disruptive technologies are technological developments that offer the market a different and entirely new value propostion. Startups, big tech or new tech, the elites of artificial intelligence research, deliberately produce immature (software) products in comparison to sustaining technologies. The social significance of these can only become manifest when they are used. See, for instance, Clayton M. Christensen, The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. (Boston, MA: Harvard Business School Press, 1997).

9 The term preemptive, or preemption, will be examined in further detail in the course of this article and distinguished from that of preventative (prevention). There is a risk that the respective measure within the technical system is considered final especially while attempting to implement preventative measures into technical systems. It is potentially presented as a variable in the functions of the system and can therefore be questioned increasingly less, the more automated the implementation processes take place.

Concurrent global events are fostering a new comprehension of interrelated crises, giving rise to complex *polycrises*.[10] Examples for this include the *dot-com* crash at the beginning of the millennium, the financial crisis in 2008, the Euro crisis in 2010, as well as 2015's refugee and migration crisis. Then came COVID-19, the crisis of democracy, the climate crisis, the Russian invasion of Ukraine, as well as other wars in Afghanistan, Iraq, Yemen, Libya, Mali, Syria, Israel and Gaza. Numerous environmental disasters have also occurred in this millennium, particularly in countries affected by war or in the process of rebuilding their devastated lives: earthquakes in Syria, Turkey, Morocco, Afghanistan, and Haiti have accounted for over 500,000 casualties, and floods in Pakistan, Libya, and Sumatra have claimed hundreds of thousands of lives due to a tsunami. Wildfires are breaking out all over the world. More than 43 million children are currently refugees in flight. Societies across the globe are called upon to address a wide range of concurrent challenges.
In order to avoid succumbing to a sense of powerlessness fueled by feelings of fear, uncertainty, anger, or helplessness, the traditional functions of technology have been reexamined and redesigned, in particular those that counteract spontaneous changes with stability. This means making the unexpected more predictable, risk factors more interpretable, and potential hazards more manageable. In addition to early crisis detection, crisis and conflict prevention also form a crucial foundation for minimizing risk. After all, no one denies that hundreds of thousands of lives can be saved every year by recognizing and preventing crises and conflicts in a timely manner. Much hope is attached to the analysis of new *big data* sources by artificial intelligence (AI) to enhance the predictive capacities of governments, institutions, universities and NGOs. In addition to *open-source intelligence* (OSINT), which can access media reports, academic papers, and publicly available statistics, early warning systems for crises must include reports from secret services, military intelligence, analyses from security agencies, findings from satellite reconnaissance, and a variety of other informational sources and encode them for computational processing.

10 See the definition of RiskNET, where "polycrises" are called "crises" that "reinforce one another." https://www.risknet.de/wissen/glossar-eintrag/polykrisen/ (accessed 1/8/2024).

After events from 2015, such as the arrival of a large number of refugees in a relatively unprepared Europe, political decision-makers sought ways to better anticipate flows of migration. Switzerland and Sweden have since started testing the prediction of asylum applications, and the European Union Agency for Asylum (EASO) has tested suitable prediction models as part of its *Early Warning and Preparedness System* (EPS). The Prediction, Visualization, Early Warning (PREVIEW) project at Germany's Federal Foreign Office also conducts early monitoring of crises. This is the case because – as the German Foreign Office postulates – *"Crises have their precursors. Problematic political, economic, and structural developments are often apparent before they erupt."*[11] In the Bundeswehr (German armed forces), programs like the IT support for the early detection of crises, which was developed by the German Federal Ministry of Defense. According to the ministry, the system has been an integral part of the German government's foreign, security, and development policy since 2017 and it was designed to *"determine the likelihood of crisis-related developments in militarily relevant contexts worldwide approximately one and a half to two years in advance."*[12] This early warning and assistance system links *"trade data, unemployment rates, crime rates, and also, for example, information about political violence from global event databases, such as the Global Terrorism Database (GTD), the Armed Conflict Location & Event Data Project (ACLED), and also the GDELT."*[13] Another project in this field – the Center for Crisis Early Warning (CCEW) – is currently being developed by the German Federal Ministry of Defense in cooperation the University of the German Federal Armed Forces in Munich. According to the Center for Intelligence and Security Studies (CISS), it conducts interdisciplinary research in advanced analytics and AI. Here, again the information is sourced from public or freely accessible sources, which the German Federal Ministry of Defense supplements with additional data sets.[14] Among other initiatives, IT-based early crisis detection

11 Auswärtiges Amt, "Krisenfrüherkennung, Konfliktanalyse und Strategische Vorausschau," https://www.auswaertiges-amt.de/de/aussenpolitik/krisenpraevention/-/2238138 (accessed 1/8/2024).
12 Bundesministerium der Verteidigung, "Auswärtiges Amt und BMVgBundesministerium der Verteidigung stärken gemeinsame Krisenfrüherkennung," https://www.bmvg.de/de/aktuelles/bmvg-auswaertiges-amt-staerken-gemeinsame-krisenfrueherkennung-4960694 (accessed 1/8/2024).
13 Ulf von Krause, "Potenziale der KI im Militär," in Künstliche Intelligenz im Militär: Chancen und Risiken für die Sicherheitspolitik (Wiesbaden: Springer Fachmedien Wiesbaden, 2021), 9–23.
14 Center for Intelligence and Security Studies (CISS), "Kompetenzzentrum Krisenfrüherkennung," https://www.unibw.de/ciss-en/ccew (accessed 1/8/2024).

with quantitative methods for national, foreign, and security policy is being further developed in collaboration with the German Federal Foreign Office. In May 2020, the *Data Innovation Directory* (DID) was also launched as part of the *Global Migration Data Portal of the International Organization for Migration* (IOM), which presented more than 50 projects that used AI, big data, mobile phone data, and satellite images to better understand the impact crises have on mobility. However, data sets concerning the market prices of goats in Somalia – for instance – also serve as a basis for AI early warning systems to predict refugee movements from the country of origin, such as within the UNHCR project *Jetson*.[15] Literary texts are also being analyzed as predictive instruments for the prevention of crisis and conflict. For three years, the project *Cassandra – Literature as an Early Warning System*[16] was commissioned by the German Federal Ministry of Defense to research the predictive potential of literature in crisis-prone regions: In Ukraine, Nigeria, Algeria, the Kuwait/Bidun- and the Nagorno Karabakh conflict.

It is especially essential for executives in public offices and companies who need to accurately validate the predictions from these at times still very experimental systems to acquire a basic understanding of the internal structures of these technical systems. A misjudgment in using these systems during a normal day of work could have concrete, sometimes devastating or fatal consequences for citizens. However, a growing challenge is that it will be increasingly difficult to assess the quality of each technical model as computer-assisted predictions become more automated. A prediction can only be as good as its model.

A Technically Generated Reality

> *That which has been coded, transmitted to thousand of machines, and has become part of our day-to-day lives because it has been repeated again and again will stabilize and ultimately become a culturally unquestioned sediment.*[17]

Software developers determine the fundamental behavior of the system via its internal structure and interfaces with the world. The system

15 Lauren Parater, "Jetson: Insights into Building a Predictive Analytics Platform for Displacement," UNHCR Innovation (blog), March 21, 2018, https://www.unhcr.org/innovation/jetson-insights-into-building-a-predictive-analytics-platform-for-displacement/ (accessed 1/8/2024).

16 See Markus Metz and Georg Seeßlen, "Kann Literatur Krisen prophezeien? - Cassandra," https://www.hoerspielundfeature.de/feature-cassandra-100.html (accessed 1/8/2024).

17 Georg Trogemann, "Code and Machine" in Code: Between Operation and Narration, Eds. Andrea Gleiniger and Georg Vrachliotis (Basel: Birkhäuser, 2010). 41–53.

only exerts its impact through the selection of the context in which it is employed, which also includes the involved users and their interactions with it. In other words, the external conditions of the system need to be maintained to ensure its continued functionality in the future. Modeling parts of the world and the predictions composed from such parts *"for linear systems that are well demarcated and that only interact loosely with their environment […] actually work out very well,"* but they fail in *"all areas for which interactions with the environment cannot be limited."*[18] Hence, the current settings need to be (re)configured to allow for the envisioned efficacy of the technical functions to be manifest in a particular context. This applies to all components involved in realizing the fictional model and the group of people who are included as datafied objects or operands; otherwise, their intended mode of operation would no longer be guaranteed. However, if it can be guaranteed, users of a particular technical system can rely on the deployment of the software's specified functions. Surprises are then only likely to be rare cases. The functions have a stabilizing effect. They counteract spontaneous changes or prevent them from ever being able to happen in the first place. They minimize the unexpected and preemptively prevent possible risks. The internal functions achieve this by predicting the future state of the environment to some extent. This means that in order for the systems to fulfill their functions, the internal operations have to lead from a specific initial situation to a target state as flawlessly as possible.

In the past 25 years, some predictive systems have worked better than others. However, criteria concerning *why* and *for whom* they have worked better or worse need to be defined from within society. They should be in the interest of the public and thus they should not be evaluated exclusively by communities of software developers but rather in conjunction with them. After all, humans have been deliberately intervening in their environment since time immemorial,where environment is understood as the environment of a living being that affects it and influences its living conditions.[19] Humans configure and manipulate their environment to create future habitats (for survival) and avoid exceptional circumstances as much

18 Georg Trogemann, "Reenacting Poiesis – More Anarchy in Technology!," in Reenactments in Kunst, Gestaltung, Wissenschaft und Technologie, Salon Digital Band / Vol. 1, Edited by: Ralf Baecker, Dennis Paul, Andrea Sick (Hamburg: Textem Verlag, 2020). 133–155.

19 See Jakob Johann von Uexküll, Umwelt und Innenwelt der Tiere (Berlin: Springer Verlag, 1909).

as possible. This way of stabilizing and reducing uncertainties has always been a fundamental quality of technical manufacturing processes; it is part of our world. A world that mankind created for itself and in which human life is at home: *"an artificial world of things, distinctly different from all natural surroundings."*[20] This in turn gave rise to new techniques and technologies. Some were developed intentionally, while others appeared as side effects, thus posing unforeseen challenges. They did this and still do via our technical interventions in the world. Whenever they become integrated into our behavior and significantly influence our lives and work, the initially liberated sense undergoes a reversal. A reversal that reimbues what had been previously removed through the process of abstraction, namely all of the ambiguities and inconsistencies of life itself. To make life readable for machines, phenomena must be detached from concrete reality, they have to be liberated from meaning. All that is abstracted away is then reimbued during the interaction between human and machine, where the abstract resurfaces through interfaces, in the intersections with the world. The abstract symbols are imbued with meaning, but these meanings are not identical to those previously removed. This reimbuing represents a fundamental aspect of *sense-making* when cultural values that were once inscribed in technologies start triggering new value debates in society.[21] Thus, whenever computer systems are used in real-world settings – i.e. whenever they are embedded in an environment – they activate new contexts of action. It is then up to society to extrapolate them, which is one of the reasons why political regulation often lags behind technological development.

The technologies discussed in this article are primarily used for *anticipatory intelligence*, i.e. to support military decision-making and in the realm of national security. They are integrated into existing contexts of action and recontextualize them when they appear via recharging during the computer-assisted acquisition of knowledge. The purpose of these systems is always to handle future crisis situations. With and through them, new spaces for experience and action are constantly emerging that did not exist before. In the first two decades of the new millennium, we thereby learned

20 Hannah Arendt, Human Condition (Chicago: University of Chicago Press, 1958), 7.
21 See Georg Trogemann, "The Wealth of the Concrete on the Skeleton of the Formal," 2014, https://georgtrogemann.de/wp-content/uploads/2021/04/Wealth_of_the_concrete_English.pdf (accessed 1/8/2024).

to acknowledge that technology increasingly outpaces our understanding of the world. *"that what we can cognize changes to the same extent as the technical modifications we make to our world."*[22] And with this realization, the technological predictions of our future life also change.

Prevention < Prediction > Preemption

In their study, "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy," researchers Ian Kerr and Jessica Earle introduced the concept *"predictive preemption."*[23] For this concept, they distinguished three models of technical prediction to gain a deeper understanding of the computer-assisted transformation of our living environment. Kerr and Earle divided technical prediction into *consequential, preferential,* and *preemptive* prediction. Various types of scenarios can be predicted with all of these models in which social processes and movements are not only recorded, analyzed, and shaped in the present, but also in which futures can be simulated. Some of these simulations are then optimized in a preventative fashion and steered in a specific predefined direction. Depending on the degree to which the future is technically possible, attempts are even made to preemptively prevent them. As mentioned above, these models have become a constituent part of our daily lives:

1. *Consequential predictions* are predictions that attempt to anticipate the likely consequences of an individual's or group's actions. The algorithms used in this process belong to classical risk management systems and ideally they are user-centered by providing future courses of action that align closely with the interests of the individual in question. This choice is intended to prevent unfavorable outcomes for the individual, such as in medical treatment or legal advice.
2. Algorithms that can be attributed to *preferential prediction* not only attempt to make predictions about possible or probable consequences of individual or group behavior but also seek to influence the preferences of individuals and groups to promote better sales of specific products or services. Even

22 Georg Trogemann, "The 18th Camel and The Habitats of Thought. On the Paradox of Teaching Technology in the Arts," in Shared Habitats, Eds.Ursula Damm / Mindaugas Gapsevicius (Bielefeld: transcript Verlag, 2021). P. 117 – 166. 163.
23 Ian R. Kerr und Jessica Earle, "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy," SSRN Scholarly Paper (Rochester, NY, September 3, 2013).

political opinion can be steered through their deployment. Google's *PageRank* algorithm and Facebook's *EdgeRank* algorithm fall into this category. Content moderation systems that implement such filtering and ranking algorithms play a crucial role in how information is located, accessed, and presented to us on the internet. Operating with specific parameters and values, they are constantly evolving through the intervention of humans and the technical systems themselves. Embedded in a complex combination of political, technical, cultural, and social interactions, these algorithms significantly influence worldviews. The boundaries between commercial risk management systems and those for preferential prediction, where choices can be intentionally directed, not only intersect with political agendas (like in the *Cambridge Analytica* scandal in 2018, for instance)[24] but also with models used in the military and national security. An opaque *"amalgam of commercial, private, military, and technological techniques"*[25] began to form that by the mid-2010s focused on solutions to identify unknown elements in (big) data mining. *"The commercial retailer's dream of an unknown consumer meets the state's nightmare of an unknown terrorist."*[26] Thus, preemptive security technologies, which emerged around the turn of the century, acquired an additional dimension by the 2010s.

3. While the first two models focus on the actions of an individual or group, preemptive systems assess probable consequences that could occur once a person or group is either permitted or forbidden to act in a certain way. The differentiation here is between legal and illegal actions, and between what is or will be allowed in the future and what is forbidden. *Preemptive predictions* therefore focus on predictions that are deliberately used to restrict the future range of actions for an individual or group and are only rarely used to expand such a scope. The suppositions of preemptive predictions are usually modeled from a state or company's

24 See Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," The New York Times, April 4, 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (accessed 1/8/2024).

25 Louise Amoore, The politics of possibility: risk and security beyond probability (Durham: Duke University Press, 2013). 2.

26 Ibid. 3.

perspective, meaning an entity that seeks to prevent or avert certain actions or perspectives. As such, one single actor gains so much power within a system that other parties and actors no longer have a chance to be or become their equal, and by definition, this is a system that is inherently unequal. This concept can be referred to as *hegemonic data processing*.[27] Big data combined with AI pattern recognition – for example – is one such technical system of hegemony, or rather, there are many such systems. They are hegemonic because a few (national and international authorities, IT companies, security services, etc.) entities collect data from citizens using machine learning algorithms, store such data in a black box, and recycle it *"with the aim of predicting events, states, or developments in the future."*[28] This usually occurs without citizens being aware of it. The increased use of big data in medium to large IT companies and the demands of security authorities to make predictions via *deep learning*[29] – i.e. creating automated databases through the design of data-driven algorithms – is further exacerbating this imbalance.

The efficacy of these systems becomes apparent in our everyday lives when – for example – a *social media* account classified as suspicious is suspended without any prior notice or explanation. Or when access to specific public or private infrastructures is denied to an individual based on a computed suspicion, whether to flights based on *no-fly* lists (see below), opening accounts based on a low-rated *Schufa score*,[30] access to public spaces online or out on the street due to a computed *endangerment index* (see below).

27 Following Gramsci, the concept of hegemony refers to a type of rule that is essentially based on the ability to define and assert one's own interests as the general social interests. See Antonio Gramsci, Gefängnishefte, Eds. Klaus Bochmann and Wolfgang Fritz Haug (Hamburg: Argument, 1991-2002).

28 Eric Mülling, "Workshop: Big Data und der digitale Ungehorsam," presentation slides, October 15, 2016, https://docplayer.org/177473931-Workshop-big-data-und-der-digitale-ungehorsam.html (accessed 8. 1.2024).

29 The technology of Deep Learning began to emerge at the turn of the millennium. The age of big data (ie the increase of data volumes due to the spread of internet technologies) began shortly after major processes had been made in computer technologies (i.e. in computing capacity, GPUs, and inexpensive storage capabilities). It was this technical infrastructure that allowed for the further development of artificial neural networks (ANN) to be possible for deep learning in research and increasingly also in the field of application. This is the technology we primarily talk about today when we hear about artificial intelligence: sub-symbolic artificial intelligence.

30 SCHUFA Holding AG is a company where information about consumers is sourced from utility suppliers, banks, internet providers, and more. The company tracks all bills or fines over time. Using this raw data and parsing it through an algorithm of their own, SCHUFA calculates the potential risk of default and translates this into a credit rating score for all German residents. The higher the score, the better the solvency. Scoring means in that sense, drawing up forecasts for the future based on experience from the past.

The Principles of Preemptive Security Policy

> *The message is that there are no knowns. There are things that we know that we know. There are known unknowns. That is to say there are things we now know we don't know. But there are also unknown unknowns – things we don't know we don't know.*[31]

If one follows this quote from former US Secretary of Defense Donald Rumsfeld, the world was faced with the need to transition into a preemptive security due to the security situation's unpredictable complexity. What had been coursing through Western societies in the previous century[32] now began to be inscribed into the countries' laws and into the existing security technologies. Numerous state-initiated measures aimed to assert sovereignty of interpretation over a security concept grounded in a logic of precaution and normalize the societal distrust of the Other.[33]

Reconfiguration of the Law:

The legal basis that enabled the Bavarian State Criminal Police Office to maintain the database from the prologue and disclose the names of the three youths has not been made public, due to *"reasons of state interest."* The case transpired in the summer of 2019, but it was not until a few months later, on January 1, 2020, that an amended EUROPOL regulation[34] came into effect that significantly expanded the power and prospects for cooperation between European police forces. It made the transferal of data and information to non-EU countries permissible as well as *loosely defined entities within the EU*. Hence, the legal basis for the preemptive actions by the French security authorities would have been established by 2020 at the latest. In the context of the new European security policy, several laws have been expanded or fundamentally changed in recent years. *"Preemptive security requires a radical reconfiguration of the law,"*[35] which has often

31 NATO Speeches Transcript, "Press Conference by US Secretary of Defence, Donald Rumsfeld," NATO HQ, Brussels, June 6, 2002, https://www.nato.int/docu/speech/2002/s020606g.htm (accessed 1/8/2024).
32 See Giorgio Agamben, State of Exception (Chicago: University of Chicago Press, 2005).
33 See Aradau, Claudia and Rens van Munster. "Taming the future: The dispositif of risk in the war on terror," in Risk and the War on Terror (Routledge, 2008).
34 REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0794 (accessed 1/8/2024).
35 See Richard V. Ericson, "The State of Preemption: managing terrorism through counter law," in Risk and the War on Terror (Routledge, 2008). 57.

been accompanied by *state-of-the-art* security technologies. According to Richard V. Ericson, this takes two forms: first, new laws are enacted or novel interpretations of existing laws are devised; and second, these are accompanied by the development of surveillance infrastructures and new possibilities to expand existing surveillance networks. Both are undertaken *"to erode or eliminate traditional principles, standards, and procedures of criminal law that get in the way of preempting imagined sources of harm."*[36] Arguably, the most important step in this direction in the UNITED STATES was the enactment of the *Patriot Act,* which repealed previously established principles, standards, and procedures of criminal law in the name of national security shortly after the events September 11, 2001. This act also introduced the concept of an *"unlawful enemy combatant"* From that moment on, this status could be assigned to individuals based on a categorical suspicion, namely being in the wrong place at the wrong time or moving or behaving incorrectly. *"'Unlawful enemy combatants' is a dangerous offender-like status that criminalizes suspects for imagined future harm they might cause, rather than past crime."*[37] U.S. law enforcement agencies now had extensive access to private spheres, locations, and communication networks. Everyone became a suspect and to a certain extent was treated as such. Every citizen posed a risk and was thus under general suspicion. The Patriot Act included *"a legalization of access to communication and database infrastructures that might yield signs of suspicious activity, for example those of telephone companies, Internet Service Providers (ISPs), libraries, retailers (e.g., book stores, travel agencies, car dealers) and schools (eg., under a 'foreign student monitoring program')."*[38]

Expansion of Surveillance Infrastructures:

In both the UNITED STATES and Europe, new surveillance infrastructures have been developed since the beginning of the millennium, accompanied by the expansion of existing surveillance networks to incorporate new modes of utilization. The second form of preemptive security logic, which Richard V. Ericson calls *surveillant*

36 Ibid.
37 Ibid. 62–3.
38 Ibid. 66.

assemblages,[39] has been investigated in several EU projects. A representative example of an assemblage of new perspectives to use existing surveillance infrastructures and new innovations in the sector is the project *Intelligent information system supporting observation, searching and detection for security of citizens in urban environments* (INDECT). Running from 2009 to 2014, this EU research project was part of the 7th Framework Program for Research in the field of *intelligent security systems*.

The main objective of the research project was to develop a central interface in which surveillance data from various sources could be linked and automatically analyzed by computer programs for potential *threats or abnormal behavior*. The intent was to support police authorities and other domestic agencies and intelligence services in monitoring and tracking suspects. INDECT also aimed to promote and intensify a cooperation with *FRONTEX,* the agency responsible for securing Europe's external borders. By networking and integrating numerous, often very divergent surveillance technologies, it was hoped that violence and abnormal behavior could be automatically detected and reported. *"In summary, the aim was/is to develop technologies to make police surveillance more effective than it was by connecting and linking existing systems and information sources."*[40]

Criminal Potential

The aforementioned and other extensive data feeds and acquisition of citizens' behavior in Europe were utilized to establish databases to implement predictive policing. *"The databases for predictive analytics are constantly being fed in real time. Everything from crime statistics to the current weather conditions are being captured."*[41] Probably the best-known database worldwide – at least in the context of preemptive security policy – is the *No-Fly List* and above all the *Terrorism Screening Database* (TSDB) in the United States, now known as the *Watchlist*. Managed by the Terrorist Screening Center (TSC), the database contains biographical and biometric data on 4,600 US

39 Ibid.

40 Sylvia Johnigk and Kai Nothdurft, "INDECT – ein weiterer Schritt zum Orwellschen Überwachungsstaat?," in FIfF-Kommunikation 1/2010 "Verantwortung 2.0," Eds. Forum of Computer Scientists for Peace and Social Responsibility (FIfF) e.V. (Bremen: 2010).

41 M. Rosenbach and H. Stark, Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung (Penguin Random House Verlagsgruppe GmbH, 2014). 283.

citizens and over one million residents in countries outside the United States who have been suspected by law enforcement or border officials in the United States and other countries of having ties to terrorism.

Being included in this list can have serious consequences for individuals and can lead – for example – to the loss of employment or inability to travel. Authorities need no evidence of criminal activity to add individuals to the watchlist. The United States shares the *TSDB Watchlist* with more than 60 countries, including the UK and countries in the EU, which can use it to detain and question listed individuals or deny them travel. The Obama administration silently authorized a significant expansion of *the terrorist watchlist system* and initiated a secret process that requires neither *concrete facts* nor *irrefutable evidence* to designate US citizens or foreign nationals as terrorists. These new guidelines made it possible to designate individuals as representatives of terrorist organizations without there being any evidence showing that they are actually associated with such organizations. Furthermore, they grant individual White House officials the authority to add entire *categories* of people to the list targeted by the government.

In Germany, this trend manifested itself in the term *"Gefährder"* (in English, a person likely to threaten public safety). It is a term that has become constantly employed in the language of security authorities over the past 20 years: *"a potential Gefährder is a person for whom certain facts justify the assumption that they will commit politically motivated crimes of considerable significance, especially those pertaining to the meaning of § 100a of the German Code of Criminal Procedure."*[42] The focus of the security authorities in dealing with the growing threat of Islamist-motivated terrorism, including in Germany, shifted from concrete to abstract, anticipated offenses. It has shifted, in other words, from criminal acts to a suspicion of behavior that does not fall within the realm of criminality. This was facilitated – among other things – by the legal framework established through the enactment of new police duties acts in Germany's federal states, which significantly expanded the powers of police against potential *Gefährder*. With the use of this concept, the

42 Deutscher Bundestag Drucksache 18/7151, http://dip21.bundestag.de/dip21/btd/18/071/1807151.pdf (accessed 1/8/2024).

criminal potential[43] was to be predicted, especially in preventing Islamist-motivated terrorist attacks, but in recent years also of right-wing extremist-motivated acts of violence and killings. For this purpose, software was developed in 2015 together with psychologists from the University of Konstanz: Rule-based Analysis of *Potentially Destructive Perpetrators to Assess Acute Risk – Islamist Terrorism* (RADAR-iTE),[44] and in 2022, together with the Central Criminological Office (KrimZ), the software RADAR-rechts.[45] The predictions generated by RADAR-iTE rely on an eight-stage predictive model for risk assessment. At level 1, the occurrence of a threatening event is to expected and at level 8 this is something that can be ruled out.[46] After Anis Amri's Islamist-motivated attack on the Christmas market in Berlin on December 19, 2016 – in which a total of thirteen people lost their lives and 67 visitors were injured, some seriously – few could comprehend how someone who was already under intense surveillance by the Berlin police could be capable of such an attack. Eventually, it was disclosed that the authorities had made a series of misjudgments and Amri was not considered an acute threat. Shortly after the attack, RADAR-iTE made its first appearance in the media as a new *"method to better expose top-level threats."*[47] Numerous media outlets at the time concluded that RADAR-iTE may have been able to prevent what happened. Before the attack, the data available on Amri had been cross-checked with RADAR-iTE and, unlike the Berlin police force, the prediction model would have *"classified Amri in the highest category – Red (high risk)."*[48]

Unrealizable Fictions

To a certain degree, the development of systems like RADAR-iTE, *watchlists*, or automated event databases implies the implementation of fictions in technical systems. Fictions that are functions

43 Deutscher Bundestag Drucksache 18/11163, https://www.bundestag.de/resource/blob/498694/76f82280dcc2c6f16722b181cada3b34/18-4-806-G-data.pdf (accessed 1/8/2024.

44 See Bundeskriminalamt (BKA), "RADAR (Regelbasierte Analyse potentiell destruktiver Täter zur Einschätzung des akuten Risikos)," BKA, https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/Radar/radar_node.html (accessed 1/8/2024).

45 See Bundeskriminalamt (BKA), "RADAR-rechts" BKA, https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/PMKrechts/RADAR/radar_node.html (accessed 1/8/2024).

46 See also the RADAT-iTE infographics of the BKA: https://www.bka.de/SharedDocs/Downloads/DE/AktuelleInformationen/Infografiken/Sonstige/infografikRADARiTE.jpg? – blob=publicationFile&v=8 (accessed 1/8/2024).

47 Fabienne Rzitki, "Radar-iTE: BKA-Methode soll Top-Gefährder besser entlarven," December 18, 2017, web.de, https://web.de/magazine/politik/radar-ite-bka-methode-top-gefaehrder-entlarven-32706414 (accessed 1/8/2024).

48 Ibid.

attempting to derive future events, such as a planned attack, as concretely as possible from individually observed processes, traces, and external actions. Of course, this practical approach requires an extremely high degree of speculation as well as thought experiments, given that this type of prediction can never achieve absolute certainty. A suspicion can only become more concrete if new actions align with the current prediction model, or this model has to be weakened or discarded should new data be in contradiction with it. However, as crisis and conflict prevention measures are implemented to detect crimes, attacks, crises, and conflicts promptly to prevent exceptional circumstances such as violent escalations, their efficacy needs to be proved before an individual or group decides to take action. Accordingly, before a terrorist attack is carried out or observable preparations for such an attack are made. This is one of the main reasons why crisis and conflict prevention are referred to as *"preventative diplomacy,"* in the programmatic UN document "Agenda for Peace"[49] from 1992. There, technical early warning systems are placed alongside diplomatic visits, talks, negotiations, trust-building measures, and preventative interventions in the form of establishing demilitarized zones. This is all undertaken because we do not have direct access to people's thoughts and intentions. To identify intentions and concrete plan with technical systems, they must always be derived from observable actions or statements. This means that only certain traces left by concrete intentions can actually be captured.

However, Western modern societies are characterized by the ways in which every day life is technologized since *"reproducible written traces are left everywhere,"* which *"in turn are the preconditions for further operations."*[50] In the interdisciplinary scientific field of *computational social science* (CSS),[51] traces such as those that "PREVIEW" and INDECT attempt to record are called *digital behavioral data*.

These traces are rendered interpretable by emerging digital technologies such that they can be used to examine social phenomena and their related epistemological practices. CSS, in particular, builds on

49 United Nations (UN), "Agenda für den Frieden (Bericht des Generalsekretärs), Ziffer 23," https://www.un.org/depts/german/friesi/afried/a47277-s24111.pdf (accessed 1/8/2024).

50 Armin Nassehi, Muster: Theorie der digitalen Gesellschaft (Munich: C.H.Beck, 2019). 136.

51 The CSS is a young field in the sciences where socio-cultural phenomena are treated with the aid of new technologies, such as machine learning, text and data mining, and network analysis.

the insights of *social network analysis* (SNA), a method of empirical social research to acquire and analyze social relationships and networks, which has been in use since the 1930s.

Can a Model Predict a War?

When criminologists such as Richard V. Ericson, philosophers such as Giorgio Agamben, or legal scholars such as Alan M. Dershowitz highlight that the American response to the terrorist attacks of September 11, 2001 illustrated a trend towards preemptive security that was nevertheless already underway in all Western societies, one inevitably has to come to terms with the so-called *revolution in military affairs* from the late 1990s, which is known as *Network Centric Warfare* (NCW).

The preemptive security logics of today have evolved from numerous spin-in and spin-off effects, i.e. innovations from industries, businesses, and society that were adopted by the military and vice versa. This is how military technologies found their way into our civilian spaces, into public and private spheres where we move and communicate or simply chat with one another. The knowledge, technologies, and skills from the SNA began to manifest themselves in the NCW as military-strategic, security-political, and operational ways of thinking. Their abilities were first demonstrated by the United States military in the Second Gulf War (1990) and from there they started to be developed in the US domestic and foreign security policies. Approximately three years later, on June 26, 1993, the first preemptive strike led by the United States was recorded under the term *"preventative military strike."* The United States used cruise missiles to attack the intelligence center near Baghdad and this strike resulted in 60 civilian casualties. According to former President Clinton, the operation was a measure taken against Iraq's alleged plans to assassinate Clinton's predecessor, George Bush, during a visit to Kuwait.

The quickly implemented reactions to the terrorist attacks of September 11, 2001, which included a NATO offensive against the Taliban that was led by the United States on October 7, 2001, would not have been possible without the longer-term asymmetric and hybrid warfare from the years and decades before. Or at least not in this dynamic. The possibility of quickly opening numerous sales offices of

technology companies in Washington and their rapid staffing *"with retired military and security officials"*[52] had also been established years before. Among the major companies included were Microsoft, IBM, Dell Computers, and the Oracle Corporation.[53] During this time, the Pentagon issued numerous funding programs in the field of SNA, regarding new forms of terrorist attacks and assassinations. Data analysis companies such as Palantir Technologies Inc. played a significant role during this period. These were companies that quickly specialized in monitoring individuals and consolidating data sets that had previously been separate. The CIA, the NSA, and the FBI quickly became Palantir customers. EUROPOL now also uses Palantir products for data analysis. Its software products are also in strong demand by NATO members countries and they play an important role in current wars such as the Russia Ukraine war and the Israel Gaza war. In Germany, Palantir's *database visualization and analysis software* Gotham[54] is used in Bavaria, among other places, as a *cross-procedural research and analysis platform* (Vera[55]). The police in North Rhine-Westphalia also use Palantir's *cross-database analysis and research software* (DAR[56]). In Hessen, Gotham has been used in the HessenData[57] police software since 2017. The state government in Hessen had approved the purchase of the software, but its use was deemed unconstitutional by the Federal Constitutional Court in Karlsruhe in February 2023. The judges of the Higher Regional Court in Karlsruhe gave the state legislature until September 2023 to make improvements to the law with regards the use of big data software by the police in Hessen. However, according to the *Society for Civil Liberities* (GFF), the second attempt is also incompatible with the supreme court's requirements. The GFF will submit a constitutional complaint to the Federal Constitutional Court. Hessendata can presumably be used *"if a person buys glue"* and could therefore be suspected of climate activism, criticizes

52 Richard V. Ericson, "The State of Preemption: managing terrorism through counter law," in Risk and the War on Terror (Routledge, 2008). 69.
53 Ibid.
54 See Bundeskriminalamt, "RADAR-rechts" BKA, https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/PMKrechts/RADAR/radar_node.html (accessed 1/8/2024).
55 See Bayrisches Landeskriminalamt, " Projekt VeRA: Ergebnis der Quellcodeüberprüfung" LKA Bayern, https://www.polizei.bayern.de/aktuelles/pressemitteilungen/045266/index.html (accessed 1/8/2024).
56 See report for the meeting of the Committee on Internal Affairs, "Wie begründet die Landesregierung die Kostenexplosion beim umstrittenen Palantir-Analysetool?" Ministerium des Inneren NRW, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV18-301.pdf (accessed 1/8/2024).
57 See Giel Ritzen, "Hessendata and its Impact on Personal Data Protection and Privacy" Police-IT, https://police-it.net/hessendata-and-its-impact-on-personal-data-protection-and-privacy (accessed 1/8/2024).

Simone Ruf from the GFF.[58] According to available data, the system technically merges digital behavioral data with entries in various police databases as well as connection data from telephone surveillance to identify possible criminals. However, the US Department of Defense also initiated its own innovative research and development programs such as the *Human, Social, Cultural, and Behavior Modelling Program (HSCB),*[59] which was sponsored by the *Office of the Under Secretary of Defense for Research and Engineering (OSD R&E)*. Most of them emerged and focused their main research areas and development core on predicting (abstract) future attacks as concretely as possible. New units were set up, such as the *Joint Improvised-Threat Defeat Organization* (JIEDDO), among others. This unit was one of the first units to test Palantir's Gotham for the war on terror. The JIEDDO was installed due to the need to address a rising number of attacks involving parcel bombs and *improvised explosive devices* (IEDs) during the Third Gulf War. In Baghdad, an increasing number of civilians and soldiers lost their lives.

The focus of methodological and technological developments shifted from the early detection or prediction of future attacks or the recording of the development of crises to the preemptive prediction of unrest, uprisings and wars. Ideally, the methods should also be able to prevent what they have detected and predicted. Prominent examples of the application of preemptive security technologies that emerged from this research approach are the networkalysis tool *Organization Risk Analyzer* (ORA)[60] and the *Spatial Cultural Abductive Reasoning Engine* (SCARE).[61] The latter was developed by V.S. Subrahmanian, among others, who was then the director of *the Laboratory for Computational Cultural Dynamics at the University of Maryland*. According to Subrahmanian, SCARE could predict the locations of weapons caches to within half a mile in Baghdad by using a combination of publicly available data on previous suicide attacks, geographic constraints, and cultural factors: first, attackers

58 See Simone Ruf, Jürgen Bering and Constanze Kurz, "Der sehende Stein der Polizeibehörden: Der Einsatz von Palantir Gotham aus technischer und rechtlicher Sicht,", presentation at Chaos Communication Congress 37C3, December 29, 2023, https://media.ccc.de/v/37c3-11989-der_sehende_stein_der_polizeibehorden (accessed 8. 1.2024).

59 See, for example, the introduction of the Defense Technical Information Center (DTIC®) into the program of HSCB: "INTRODUCTION TO THE HSCB PROGRAM," 2009: https://apps.dtic.mil/sti/tr/pdf/ADA496310.pdf

60 Kathleen Carley and Jeff Reminga, "ORA: Organization Risk Analyzer," July 1, 2004. P. 50.

61 See Paulo Shakarian, V Subrahmanian, and Maria Sapino, "SCARE: A Case Study with Baghdad," 2009. And the corresponding presentation slides: https://pdfs.semanticscholar.org/8a08/96fcf863ec937d72ecf98ffefc60ac6f01fa.pdf (accessed 1/8/2024).

could not carry their explosives very far in part for the fear of being caught; and second, most of the tracked attacks were carried out by Shiite groups with links to Iran, which meant that it was unlikely that the hideouts were in Sunni neighborhoods. Subrahmanian later stated that he had provided copies of the program to the military and stated that *"they're clearly trying it out."*[62] However, the extent to which remained classified.

Programs such as SCARE enhanced the efficacy of security policies through computer-assisted interpretations of observable intentions among groups and individuals, which evolved in tandem to the extent to which they could make an (abstract) future event concrete. The United Nation's reading that early crisis detection should not suggest 100% guaranteed predictions about the future but instead explicitly refer to the creation of risk prognoses based on solid indicators did not prevent individual actors in the military from using such systems for preemptive military strikes, i.e. for the proactive prevention of explicitly identified future attacks. Moreover, it also did not prevent them from further developing these systems, as we especially saw with the civilian costs of the US drone program; for instance, with the support of the SKYNET program that was leaked in 2016 and that *"may be killing thousands of innocent people."*[63] The event coding and prediction system *Integrated conflict early warning system* (ICEWS) is also representative of this type of development. The design of the ICEWS was also intended to focus on future suicide attacks and terrorist attacks. Nevertheless, the primary question of this predictive project was: "Can a model predict a war?"[64] ICEWS (2007) was developed by university researchers through financial support from the *Defense Advanced Research Projects Agency* (DARPA) in collaboration with the United States defense and technology company *Lockheed Martin Corporation*. The current version of ICEWS focuses on the IT-supported prediction of political events, such as uprisings, civil wars, or coups. In brief, this system works by obtaining data, primarily from the Reuters' online news feeds, then by combining these with models that correlate behavior of

62 Sharon Weinberger, "Social Science: Web of War," Nature 471, Nr. 7340 (March 1, 2011). 566–68.
63 Christian Grothoff and J.M. Porup, "The NSA's SKYNET Program May Be Killing Thousands of Innocent People," Ars Technica, February 16, 2016, https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/ (accessed 1/8/2024).
64 Sharon Weinberger, "Social Science: Web of War," Nature 471, Nr. 7340 (March 1, 2011). 566–68.

ethnic and/or political groups, economic factors such as the country's gross domestic product, and geopolitical relations with other nations. The resulting output is a so-called ICEWS forecast, which was able to predict the following: *"Country X has a 60 percent chance of entering a civil war."*[65] According to the then DARPA program manager Sean O'Brien, these models were already being used by the *United States Special Operations Command* and *the United States Africa Command* at the time although they had not yet been fully introduced.

Preemption in Modern International Law

International law recognizes neither preemptive wars nor preemptive strikes.[66]

The right to anticipatory self-defense is the subject of controversial debate in international legal studies. The British lawyer and professor for international law Christopher John Greenwood refers to it as perhaps *"the most controversial question"* in the context of the right to *self-defense*.[67] While the concept of preemptive self-defense tends to be approved of in the US, with the citation of customary international law and the right to self-defense, which existed before the adoption of the UN charter and has survived it,[68] the majority rejects the right to self-defense under customary international law. According to the latter, preventative and preemptive military measures are only permissible with the authorization of the UN Security Council.[69] *"A right to preemptive self-defense does not follow from the fact that Article 51 of the UN Charter*[70] *speaks of the 'inherent right to … self-defense.'"*[71] According to the Professor of Law Mary Ellen O'Connell, consensus exists among international scholars of law that preventative

65 Ibid.
66 Ulrich Arnswald, "Präventiv-Krieg oder Präemptiv-Krieg?," der Freitag, August 22, 2003, https://www.freitag.de/autoren/ulrich-arnswald/praventiv-krieg-oder-praemptiv-krieg (accessed 1/8/2024).
67 Christopher Greenwood, "Self-Defence," Oxford Public International Law, (April 2011), https://spacelaw.univie.ac.at/fileadmin/user_upload/p_spacelaw/EPIL_SelfDefence.pdf (accessed 1/8/2024).
68 See Anthony Clark Arend, "International law and the preemptive use of military force," The Washington Quarterly 26, Nr. 2 (2003): 89–103, https://ciaotest.cc.columbia.edu/olj/twq/spr2003/twq_spr2003a.pdf (accessed 1/8/2024).
69 François Campagnola, "La légalité internationale de l'action 'préemptive' et 'préventive,'" défense nationale et sécurité collective (2006), 67.
70 "United Nations Charter" https://www.un.org/en/about-us/un-charter/full-text (accessed 1/8/2024).
71 Scientific Services oft he German Bundestag "Das Konzept der präemptiven Selbstverteidigung aus Sicht der internationalen völkerrechtlichen Literatur," Ausarbeitung WD 2 – 3000-049/07 (2007), https://webarchiv.bundestag.de/archive/2016/0617/blob/414640/44a2b7337d3b8fd94962639cb365c9c8/wd-2-049-07-pdf-data.pdf (accessed 1/8/2024).

defense measures are permissible to a limited extent so long as plausible reasons exist.[72] Regarding the use of early detection and prediction systems, AI researchers Karl-Hans Blaesius and Jörg Siekmann highlight that there are systematic reasons why existing indicators could also be seen as harbingers. If this were to happen, a technical *"system would also be more likely to predict a war (or crisis), potentially exacerbating a situation that is already critical."*[73] Such a hypothetical case clearly illustrates the danger that a military action could be mistakenly carried out to prevent developments by other states that were at an early stage. To address this risk, the internal workings and system properties must be transparent and comprehensible at all levels.

The basis for the interpretation of individual cases are the so-called *Caroline criteria*. These are internationally recognized criteria for the exercising of the *right to self-defense* by states. This right is guaranteed when there is no other choice of means except the use of military force to prevent an attack. This means that every possible avenue of negotiation must have been proven to be exhausted. This is the case – for instance – when an enemy missile attack is imminent, and no time is left to conduct negotiations before the enemy missiles are launched. This means that there would be *no other choice* but to attack to defend oneself. Having no other choice of means therefore implies nothing more than the fact of an imminent threat, albeit a threat that must be substantiated. This is the point at which predictions from technical systems – among other things – are brought into play because plausible reasons must exist to believe that this enemy attack is truly imminent and these reasons must be presented in such a way that an objective observer can understand them. This objective observer is the world public or the UN Security Council. It must be convincingly demonstrated to them that the use of military force was the only remaining means of averting an attack. It must therefore be possible to comprehensibly and plausibly explain under time pressure where and how one arrived at the current discoveries. After the events on September 11, 2001, this clause inevitably led to kind of reinterpretation of the permissibility

72 See Mary Ellen O'Connell, "The Myth of Preemptive Self-Defense," ASIL Task Force Papers (August 2002). P. 8, https://www.comw.org/qdr/fulltext/02oconnell.pdf (accessed 1/8/2024).
73 Karl-Hans Bläsius and Jörg Siekmann, "Computergestützte Frühwarn- und Entscheidungssysteme," Januar 22, 2021, www.fwes.info/fwes-21-1.pdf (accessed 1/8/2024).

of preventative use of force, resulting in the international *"shift in the understanding of immediacy."*[74]

The history of technical systems in supporting the detection of imminent attacks or the history of systems that previously actively defend against them has since its inception faced the challenge that future real-world events must be calculated under unpredictable circumstances. Or, in the words of Norbert Wiener, *"it is exceedingly important to shoot the missile, not at the target, but in such a way that missile and target may come together in space at some time in the future."*[75] In 1948, Wiener was tasked with developing a method to predict the future position of an approaching flying object. He called it the *linear prediction code*. Systems like ICEWS or SCARE apply this predictive function that has an almost 100-year-old history of development to human behavior. The transition from prediction to preemption is inherently ambiguous and poses a considerable challenge for society because these systems also attempt to actively prevent a future continuation before it happens with the aid of their designated predictions. However, within the technical systems, there is a clear disconnect from what they are designed to do, and this is as true of Wiener's air defense system as it is of the aforementioned systems. In both cases, the purely internal modes of functioning are separate from the outside world. For these systems, there's no difference between predictions about missiles, possible terrorist attacks, an imminent wave of refugees, or war. It is only in rare cases where the system's internal decision-making functions can be used to embed their meaning for us in the real world on their own. This often leads to unpredictable errors during operation, which might not always be recognized as such. V.S. Subrahmanian – the developer of the SCARE system that was used to predict suicide attacks in Baghdad, among other things – once stated in an interview that *"I would say the weather guys are far ahead of where we are"*[76] in terms of forecasting. He made this statement to highlight that meteorologists are accused of being wrong as often as they are of being right. In the case documented by Kathleen Carley, the developer of the ORA model (see above), the systemic error in real-world

74 Christophe Eick, "'Präemption,' 'Prävention' und die Weiterentwicklung des Völkerrechts," Zeitschrift für Rechtspolitik 37, Nr. 6 (2004): 200–203.

75 Norbert Wiener, Cybernetics: or Control and Communication in the Animal and the Machine, 2. Edition (Cambridge, MA: MIT Press, 1961). 5.

76 See Sharon Weinberger, "Social Science: Web of War," Nature 471, Nr. 7340 (March 1, 2011). 566–568.

usage was clearly recognizable. *"One of the issues,"* she suggested, *"is that you will get people who are […] part of the networks who aren't alive."*[77] When the ORA model was used in Sudan – for instance – textual analysis of a network revealed that one of the central figures in the network in question was the Islamic prophet Muhammad, who died in 632 AD.

Epilogue

Software systems are referred to as *operationally open systems*. They are not systems isolated from the outer world. Nevertheless, there are differences. Computer simulations or calculations of states of the environs made purely from statistics do not directly lead to changes in the environs. No one would claim that a system like ORA, GOTHAM or SCARE directly intervenes in its surroundings by predicting future attacks or creating a threat index. Nonetheless, when these two systems are directly embedded into intelligent security systems, such as when INDECT launches a drone in the event of danger or a security or moderation system automatically denies access to a flight terminal or the user's account on an internet platform, then the calculations directly entail changes in the system's environs and – in the previously mentioned cases – these have a significant impact on daily lives. It is in this realm that the previously closed system becomes an open one. This is a system that not only exists in its respective surroundings and is thus able to exert influence there but also one that engages in constant exchange with its surroundings and having a direct impact on them. Open systems are therefore systems that react to environmental conditions by absorbing information from the surroundings; they are embedded in the real world and alter it through their own activity. In a sense, they modify a reality that they have modeled.

The technical systems explored in this article increasingly refer people (as users) to this modeled reality – or in systemic theoretical terms – the outside. The extent of this localization depends on the transferring of agency to the system through various forms of interfacing the human-machine interactions. These veritably lead to a fusion of preemption and technical prediction, of open and self-contained, *closed systems*. *"The modification of reality (in this fusion)*

77 Ibid.

does not necessarily have to take place through direct actions, as in robotics, but will typically be indirectly effective by changing the perspectives and workflows of the users."[78]

Our collective experience in this century is shaped by decisions that we make in dealing with digital technologies, and we bear the responsibility of ensuring that these decisions align with our inner and social values, as well as with basic human rights. It is only by maintaining a critical distance that we can collectively shape a future where technologies, which were developed to predict our future from the idea of crises, enrich our lives without jeopardizing our fundamental rights.

78 Georg Trogemann, Jochen Viehoff, CodeArt (Vienna: Springer-Verlag, 2005). 37.