Published as **TechnoSecuritySociety: Catastrophic Futures, Pre-emptive Security & Mass Surveillance (2020). In: Maasen, Sabine / Dickel, Sascha / Schneider, Christoph: TechnoScienceSociety - Technological Reconfigurations of Science and Society. Springer 2020 (forthcoming)**

TechnoSecuritySociety:
Catastrophic Futures, Pre-Emptive Security & Mass Surveillance

Michael Nagenborg (University of Twente)
Jutta Weber (University of Paderborn)

From Technopolis to TechnoScienceSociety

"[T]echnology itself is a political phenomenon. A crucial turning point comes when one is able to acknowledge that modern technics, …, now legislates the conditions of human experience. New technologies are institutional structures within an evolving constitution that gives shape to a new polity, the technopolis in which we do increasingly live. For the most part, this constitution still evolves with little public scrutiny or debate. Shielded by the conviction that technology is neutral and tool-like a whole new order is built … " (Winner 1978²: 323f.)

In 1977, Langdon Winner sketched a rough picture of society being reconfigured into a technopolis respectively TechnoScienceSociety which is increasingly driven by radical sociotechnical changes and the reconfiguration of science and technology themselves; this conversion of society continues to proceed, even 40 years later, with little public awareness. In 1985, STS scholar Donna Haraway described the new character of an emerging 'high-tech culture' explicitly as "an emerging system of world order analogous in its novelty and scope to that created by industrial capitalism; we are living through a movement from an organic, industrial society to a polymorphous, information system – from all work to all play, a deadly game." (Haraway 1985/1991: 161). In 1987, Bruno Latour popularized the term 'technoscience' to indicate the fusion of science and technology as well as the messy networks linking research and development, industry and society[1].

[1] "I will use the word technoscience from now on, to describe all the elements tied to the scientific contents no matter how dirty unexpected or foreign they seem" (Latour 1987: 174)

However, until the end of the 20th century, few scholars in the humanities or social sciences engaged with and analysed the close intermingling of science, technology and society. It was the emerging interdisciplinary field of (cultural studies of) science and technology studies that noted from the early 1980s onwards that (techno)‘science *is* culture’ (Franklin and McNeil 1991; Haraway 1985).

Despite manifold ethical, STS or technology assessment discourses, the understanding of technology as a force that formats society, as a decisive life form and as a pervading medium in everyday life is still rarely recognized, as dominant neoliberal thought repeatedly suggests the autonomy and responsibility of the human subject. Only in short historical moments, such as the Fukushima nuclear disaster in March 2011, does a discussion arise on the character of contemporary sociotechnologies.

The disclosure of mass surveillance by data analyst Edward Snowden in 2013 could have served as another starting point to open a broader debate on the nexus of society and technology, especially since Snowden revealed the degree to which state agencies tapped into the constant data streams within the private sector. The possibilities of ubiquitous digital interconnectivity, big data storage, and enhanced data mining tools – a part of the ‘polymorphous, information system’ (Haraway 1991/1985) – make the political character of technology more than obvious. We are actively involved in many public debates on how to ‘tame’ data monopolists like Google or control our intelligence agencies but are rarely involved in public debates about digital ‘technology as culture’,[2] or this phenomenon’s intrinsic logic and consequences.

The epochal claim of technoscience includes a profound sociopolitical, economic, and biopolitical reconfiguration of society or a “New World Order” (Haraway 1985/1991) that comes, beneath others, with the dismantling of the welfare state, neoliberalization, ‘turbocapitalism’, globalization, and the massive deregulation of many societal realms. These developments began in the second half of the 20th century and are accompanied by profound epistemological and ontological changes as well as the transformation of norms and values in the age of technosciences (including computer science, robotics, biomedicine, nano- and neuroscience). The ‘ontological politics’ of technoscience(s) as well as knowledge/power relations get thoroughly reconfigured and accompanied by an extensive production of hybrids (Haraway 1985/1991; Latour 1993, etc.). Concepts such as ‘nature’, ‘body’, ‘technology’ or ‘subjectivity’ gain new meanings. Today, science is no longer a valuable project of knowledge

[2] See Cultural Studies of Technoscience: i.a. Franklin and McNeal (1991); Haraway (1985, 1997); Reid and Traweek (2000); Suchman (1987)

acquisition that is inherent to progress by applying technological insights towards practical solutions but rather an entrepreneurial and pragmatic project wherein technology is the main driver in developing 'innovations' for new markets and (sometimes) specific societal problems. Until the 1980s, theory-based science was understood as the precondition for engineering to turn scientific insights into technical artefacts, to design technical systems and to develop useful applications. In the age of technoscience (Weber 2003; Nordmann 2004; 2010; Forman 2007), science and technology have indiscriminately fused, and the dominant narrative is no longer the one of knowledge and progress but rather of application and innovation.

In this chapter, we will demonstrate the need to take this transformation seriously in studying security and surveillance architectures in contemporary (post-)democracies. It is astonishing that few STS scholars have studied the role of security respectively technosecurity (Weber 2011) in our TechnoScienceSociety.[3] How do the digital interception of mass communications, smart CCTV, body scanners, biometric passports, electronic border systems, etc., shape our technopolis? How do these elements reconfigure our understanding of our polity? What do the extensive implementation and ubiquity of surveillance architectures with increasingly opaque and presumably autonomous security technologies mean for democracy?

A Post-Newtonian Rationality

One of the outstanding features of technosecurity is its 'Post-Newtonian' rationality, its interest in unpredictability, chance, emergence, processes of becoming, and accordingly delimiting forms of behaviour and thought (Hagner and Hörl 2008; Hempel et al. 2010, etc.). This rationality builds on the exploitation of contingent processes to make complex, non-deterministic systems controllable and to find new solutions to problems 'we do not (yet) really understand' (Holland 1992). Thus, contemporary technosecurity practices, such as preventive and pre-emptive risk management, need to be understood in the context of contemporary technoscience, where unpredictability and the unknown are turned into an integral factor of control by the systematized exploitation of processes of trial and error (Weber 2010, 2015). Technosciences no longer focus on the intrinsic properties of organisms or the objective description of universal laws. Evolution via tinkering, the processes of trial and error, search heuristics and post-processing have become important tools for constructing complex, dynamic and adaptive systems. This post-Newtonian techno-rationality uses

[3] There are, of course, notable exceptions besides the scholars mentioned in the text, for example, Monahan (2006, 2010). Still, it is fair to claim that (techno-)security remains an underresearched topic in STS.

processes of imitation and imagination to resource the unpredictable and to find possibilities for exploiting surplus processes in a technical way (Haraway 1985, 1997; Hayles 2003; Weber 2003, 2010). It is not a mere coincidence that technosecurity follows the same ‘Post-Newtonian’ rationale.

The background to this development is the feeling of being at risk that has become frequently manifested in Western societies. Ulrich Beck already described in 1986 the rise of the ‘risk society’ (1986) in which potential threats, such as nuclear disasters or global warming, induced by accelerated technoscientific processes, become no longer calculable, quantifiable and predictable. Anthony Giddens pointed to the growing preoccupation of Western societies with their future(s), thereby generating the feeling of risk (1999): the future is perceived as catastrophic (Aradau and van Munster 2007; Horn 2014), which might not be too surprising a perception in a world in which societies are becoming progressively heterogeneous while personal and social relations and controls are weakened (Knorr-Cetina 1997). Consequently, risk discourses are increasingly enlarged: “… the structural demand for knowledge relating to risk becomes insatiable. As well because the accumulation of such knowledge adds awareness to new sources of risk, the risk-knowledge process gains its own internal momentum” (O’Malley 1999: 139). Risk discourses not only address health, natural, and technological disasters but also terrorism, organized crime, and illegal immigration. While security was traditionally achieved primarily via the empirical identification and assessment of threats framed by a TBC causal logic (Aradau et al. 2008), it is now reconfigured in the logic of a predictive maximum technosecurity based on a hyper pro-activity. As risks are increasingly experienced as limitless, demands for pre-emptive technosecurity measures are spreading (Aradau and van Munster 2007; Kaufmann 2011): Security has become governed by a precautionary logic warning of the “dangerousness of the future” (Aradau et al. 2008: 148) and by attempts to manage contingency and unpredictability. As risks are increasingly experienced as limitless, demands for pre-emptive technosecurity measures as well as social media networks are spreading (Amoore and De Goede 2008; Grusin 2010; Kaufmann 2011).

Technosecurity as Culture

Technosecurity is highly technology-oriented and driven by the Post-Newtonian rationality that is genuine to contemporary technoscience culture. Security today is less regarded as a social, political or ecological issue and more conceptualized as maximum security “obtainable by high-tech, total surveillance” (Brown 2006: 24). Technology becomes the silver bullet for security issues (Aas et al. 2009; Marx 2001). Security and surveillance technologies converge and are used to monitor, track, search and profile almost every realm of society – from the economy, politics, and the military to everyday life. CCTV, RFID chips, drones or scanners are used to search for ‘terrorists’, monitor sport events, grant access to ATMs, and control employees.

Simultaneously, social media has made monitoring an everyday event: millions of people are using Facebook, as well as locative media such as Foursquare, jogging trackers, and apps, to track the cell phone of a partner (Andrejevic 2007; Kaplan 2006). In parallel, huge amounts of data are collected, sorted and processed not only by state authorities (military, police, intelligence agencies) but also by private companies, such as Google and Facebook, for predictive and future analysis. The hope is to gather new information, discover hidden patterns and ‘connect the dots’ in the hope of pre-empting future political and economic risks. Meanwhile, online users are sharing data, tracking the movements of others, or being tracked themselves. Some seem to enjoy the comforting gaze of the other or the self-reflective loops of social monitoring. Surveillance technologies are not only operated top-down by state authorities but also used in diverse interactive ways.

Emphasizing the ‘globalization of surveillance’ in the aftermath of 9/11 and the techno-fetishism of recent military theory, Armand Mattelart coined the term ‘techno-security’ to signify “(t)he exclusively technological approach to intelligence gathering, at the expense of human intelligence” (Mattelart 2010: 138). We suggest expanding the concept of technosecurity, because Mattelart works primarily with a predominantly top-down, institutional approach with a focus on military technology. Hence, his particular perspective does not allow him to make a stronger connection to everyday practices and thus culture.

In this context, culture in general and technosecurity culture in particular are understood as multifaceted, dynamic sociopolitical practices with a broad variety of agents and actors. Technosecurity culture is conceptualized as a heterogeneous, embodied and complex process in which not only states and other authorities but also software, concepts, machines, and humans participate in the production of meanings, standards, categories and norms. Christopher Daase highlighted the fruitfulness of the concept of “security culture” (Daase 2012). Traditionally used with regard to safety issues in technology assessment, this concept was redefined by him as a framework to understand the reconfiguration of security in the course of the profound sociopolitical changes of the last few decades. Framing security as culture makes it possible to focus not only on institutional actors, such as the military or the police, but also to enable a deeper understanding of how security governs policy and everyday life. We share Daase's interest in everyday culture, but we also need to acknowledge and overcome his neglect of the central role of technology in security discourses and practices. As we noted earlier, it is crucial to analyse technology as an integral part of politics and to understand it as culture. Framing a theory of technosecurity culture will allow us to develop a more encompassing understanding of how security governs our lives.

The hyper-pro-activity of security

If we had to single out a decisive characteristic of the understanding of ”security” in the age of technoscience that differs from the understanding of “security” in earlier times, the move from reactive to proactive ways of producing security would be a good candidate.

Currently, security is about “doing something” (Molotch 2012). Whenever something bad or evil has occurred, the questions arise, “How could we let this happen? Why didn't we do something to prevent this?” Hence, whoever takes (or has to take) responsibility for the perceived failure of providing and maintaining security has a strong preference to say that she or he actually did *something*. This points to the larger context of a culture in which we find it hard to accept that we are not in control of everything, for example (Capital-N) “Nature” (Böhme 2012; Shaklar 1990). Earthquakes are the prime example here: Seneca was one of the most prominent authors writing on *securitas* in the ancient world. However, in *Naturales quaestiones* (book 4), he asked, “But if the earth itself stirs up destruction, what refuge or help can we look for?” Ever since the 1755 Lisbon earthquake, Western societies have seemed to be less and less inclined to accept this stoic stance. Since security currently “is about preventing adverse consequences from the intentional and unwarranted actions of others” (Schneier 2003: 11), we are confronted with hyper-pro-activity due to uncertainty about the seemingly unlimited number of potential threats that the future holds.

Technologies play an important part in this line of thinking. They are perceived as the means to address those threats by rendering the future actionable (Anderson 2010a, 2010b) and providing safeguards against potential threats. At the same time, technologies are seen as potential threats themselves, as well as targets that need to be protected. As Langdon Winner (2010) has put it: “The horror of the World Trade Centre attack was that the power of two wonders of modern technology—the skyscraper and the jet airliner—came crashing together causing the carefully contained power of both systems to be released in catastrophic explosion, inferno and collapse.” (Winner 2010: 166) However, “… the ultimate fear driving public and private policies in the post–9/11 era, is an awareness that seemingly secure, reliable structures of contemporary civilization are, taken together, an elaborate house of cards. The collapse of the Twin Towers foreshadows other techno-social disasters too numerous to list, and perhaps the collapse of society as a whole, possibilities that now seem to justify the most urgent, ultimately violent measures.” (Winner 2010: 167)

While we will not focus on the vulnerabilities created by our dependency on technological systems, it is worth noting that Winner, towards the end of the lengthy quote, engages in what Grusin (2010) refers to as *premediation* by actively contributing to mapping out potential — and in this case undesirable — futures. This premediation is especially prominent when he describes how the airplanes that were crashed into the Twin Towers were flying over his home and speculates about how the pilots could have maximized the damage by aiming for the “nuclear reactors at the Indian Point electrical power plant approximately 60 miles south. Since these facilities were not designed to withstand a direct hit by an airliner, targeting them might have caused catastrophic failure, and possibly a core melt down as the fuel sank into the mud and water of the Hudson River.” (Winner 2010: 157). Here, Winner (2010) clearly follows a model that has been a prominent feature of mass media since 9/11: even when confronted with a horrific attack, there is still the tendency to think about even something more horrifying that we need to prevent. One more example of a “journalistic celebration of premediation” from van Goede’s paper is as follows: “Imagine your most unthinkable nightmare of the next terrorist attack. Now try to imagine something even worse.” (Goede 2008: 156). The role of imagination in both critical and journalistic writings is revealing in that it points to the degree to which future is made present (Anderson 2010a) in contemporary security discourses. However, before we turn towards the link between security and futurity, let us briefly explore the general trend from re-active towards pro-active security.

To a certain degree, security has always been about taking certain measures to prevent future acts. For example, Thomas Hobbes in *De Cive* (first published in 1642) provides his readers with the following list of practices that point to the preventive nature of different security measures: “We see that all commonwealths, even if they are at peace with their neighbours, still defend their borders with garrisons of soldiers, their cities with walls, gates and guards. What would be the point if they had nothing to fear from their neighbours? Even within commonwealths, where there are laws and penalties set against wrongdoers, individual citizens do not travel without a weapon to defend themselves or go to bed without barring their doors against their fellow citizens and even locking their chests and boxes against their servants in the house.“ (Hobbes 1998: 10) Countries and towns guard themselves against *potential* attacks, laws are enforced to punish *potential* offenders, and individuals arm themselves and use locks and keys to protect what they regard as their own property against *potential* intruders and perpetrators. In this light, it is tempting to say that security technologies (such as locks and keys) have also been thought of as the means to prevent future acts.

We also need to account for at least two more recent developments in liberal societies: the idea of the state’s monopoly on the legitimate use of physical force and the idea of the security of the individual. Both developments lead to a re-active style of policing, where on the one hand the state is thought of as the sole actor who may use force to protect its citizens and their properties, while on the other hand the liberal state has to ensure the individual’s security by limiting its own power. A relevant example of this line of reasoning can be found in the ruling of the U.S. Supreme Court in Wheaton v. Peters (33 U.S. 591, 634 (1834)), which states the following: “The defendant asks nothing - wants nothing, but to be let alone until it can be shown that he has violated the rights of others.” This is the first time that the “right to be alone” was introduced, and this concept later famously provided the basis for Warren and Brandeis to call for a “right to privacy.” (Standler 1997). There is a recognizable practical challenge in upholding the “right to be let alone”: after all, how can the state show that the rights of others have been violated, if the state is not allowed to search for the evidence? However, the idea is to limit the power of the state by allowing the state and its agents to act only *after* obtaining evidence of something that already has occurred. The contemporary shift from re-active to pro-active forms of policing is thus a clear departure from the traditional liberal understanding of the state, where the state’s power is limited (in theory, at least) to reacting to crimes and offenses already committed.

The break with the traditional liberal understanding of the state is less obvious when we account for the emergence of *social security* in the 19th century, which needs to be understood, at least in part, as a *prophylactic* measure to prevent individuals from becoming criminals (and to decrease the risk of social unrest and political opposition). However, Tobias Singelnstein and Peer Stolle noted in their monograph on the “Sicherheitsgesellschaft” (Security Society) (2011) that we need to make a clear distinction between the *prophylactic* approach to crime in the past and the *pre-emptive* approach of today: the former aimed at preventing individuals from becoming criminals, while the latter aims at preventing crimes before they are committed. This pre-emptive approach can be achieved through the use of legal instruments by labelling as criminal activities those that are perceived to be steps taken in preparation for a crime, such as joining certain organizations, travelling to suspicious locations, looking for dangerous information on the Internet, etc. However, technologies also contribute to the shift from re-active to pro-active security.

A prominent example of this shift is *predictive policing*: "The innovative predictive-policing model moves law enforcement from focusing on what occurred to focusing on what will occur and how to effectively deploy resources in front of crime, thereby changing outcomes. With new technology, new business processes, and new algorithms, predictive policing is based on directed, information-based patrol; rapid response, supported by fact-based prepositioning of assets; and proactive, intelligence-based tactics, strategy, and policy. The analytic methods used in the predictive-policing model surface particular times and locations predicted to be associated with an increased likelihood of crime." (Beck and McCue 2009). While it is not surprising that in the current age of digitalization, policing has become data-driven and "intelligence led" (Ratcliffe 2012), we need to be aware of the fundamental shift from re-active to pro-active policing, wherein police officers are assigned to tasks based on the probability of future crimes.

A concrete example of "Predictive Crime Fighting" is IBM's "Blue CRUSH," where "CRUSH" stands for "Criminal Reduction Utilizing Statistical History" (IBM 2011). According to IBM's promotional material, "a predictive model that incorporates fresh crime data from sources that range from the [police department's] records management system to video cameras monitoring events on the street" is at core of this system that allows the department, in the words of the Director of Police Services in Memphis, "to shift officers to a particular ward, on a particular day, right down to the shift level. It's a bit like a chess match and it's enabling us to make arrests we never could have before." (IBM 2011). The reference to playing a game of chess nicely illustrates the role of a playful attitude in providing technosecurity.

It's worth noting that the full name of the IBM system points to the long-standing use of statistics in modern policing. Indeed, as Ian Hacking (1990) has shown in great detail, the emergence of the modern understanding of policing went hand in hand with the rise of statistics in the 19th century. However, we also need to note the incorporation of multiple data sources into one unifying platform, which is presented as a tool to enable decision-making based on real time data. Therefore, predictive policing systems also need to be understood as the offspring of the "Semi-Automatic Ground Environment" (SAGE) air defence project and other real-time virtual control systems that were developed in the 1950s. According to Patrick Crogan (2011), “the success (however imagined) of the system rested on the effectiveness of its advance mapping of the real environment’s potential eventuality … and the execution of a controlling, pre-emptive gesture based on that mapping.” (Crogan 2011: 11). Works like Crogan’s historical account on the emergence of technoculture highlight the need to closely study the role of technology in what, at first glance, might be perceived as an epistemological shift in which the border between factual knowledge about past events and the probability of future events has become blurred. Staying with the example of the SAGE system, what we see here is the representation of factual knowledge (the mapping of the environment) and predicted events (“potential eventuality”) on one flat screen, where no distinction between the ontological differences (actual/potential) is being made. Thus, we would argue that the rise of the idea of predictive policing does not indicate that police agencies all over the world have suddenly started to believe in predicting the future. Rather, the discussion on the feasibility of predictive policing needs to be taken as an indication of the role of technology in shaping our everyday security practices.

Predictive policing turns into an imminent part of technosecurity culture because not only is it increasingly embedded into policing systems all around the world, from the US to China, but its underlying technologies are also increasingly becoming part of everyday culture. Predictive policing is no longer only a subject of popular culture, as was paradigmatically portrayed in Steven Spielberg's *Minority Report*.

Jordan Crandall (2005) provides us with an elaborated account of the internal logic of media technologies and argues that the ideas of real-time tracking of behaviour, scenario-techniques, and distributed, interactive simulations (of behaviour) are grounded in the cybernetic conception of today's surveillance (and more generally information) technologies. These new technologies of tracking and simulation enable, at least partially, the impression that it is possible to control future actions—or even the future as a whole—via a ubiquitous panoptical system (Crandall 2005).

This new epistemic culture of data-processing, planning and control is no longer based on representation, causality and objectivity (Haraway 1985; Weber 2016) but rather on recombination, correlation and resourcing the unpredictable, thereby using systematized and automatized processes of trial and error and tinkering. One example of this new orientation is data mining, which is central to predictive policing (but also to so-called counter-terrorism operations). Data mining is conducted based on flexible databases with structured and unstructured data that can be searched systematically using advanced data mining algorithms. Huge piles of data are searched and clustered to produce patterns of correlations between data and thus to ‘discover knowledge in databases’ (Hildebrandt and Gutwirth 2008; Kitchin 2014). The discovery approach does not rest on the idea of correlations based on causal relationships but rather assumes that a (possible) past correlation will appear again at some point in the future. “With smart applications ... the target is to collect and aggregate as much data as possible, in order to mine them for relevant patterns that allow the profiler to anticipate future behaviours. The hiding of data in fact diminishes the (so-called) ‘intelligence’ of the applications” (Gutwirth and Hildebrandt 2010: 7). Data mining is a tinkering approach that is set in place to produce endless re-/combinations in the hope of pre-empting unwanted future actions. It is only within this epistemic framework that tracking and simulation have become key in our technoscience and technosecurity culture. We experience a shift in focus from the traditional measurement of humans and nature towards the projection and control of behaviour in organic, technical and social systems.

Another kind of technology that embodies the move towards pro-active security are so-called “Smart CCTV systems” that aim to recognize so-called ‘abnormal’ behaviour. Again, the novel quality of the technology seems to be obvious at first glance. At the same time, the emergence of “Smart CCTV” is unsurprising if we consider “Smart CCTV” to be the logical next step in the development from classic CCTV systems to automated systems, which began with plate recognition systems and led to face recognition systems in the 2000s (Brey 2004; Introna and Wood 2004). Such face recognition systems can be broadly connected to the history and ideology of biometric measurements in the 19th century (Lyon 2008; Hacking 1990) as well as the history of biometrical devices developed since the 1950s (Wayman 2007). However, Smart CCTV systems for abnormal behaviour detection no longer operate on a given representation of a specific person but come with the promise of identifying what does not belong and is at odds with everyday activities. They are no longer designed to re-identify and re-discover what is known (e.g., by matching the biometrical data captured by the camera with those stored in a database) but are designed to detect what is not known yet. Smart CCTV systems of this kind are no longer looking for previously registered offenders but are watching out for ‘suspicious’ behaviour. This phenomenon in turn increases the pressure on everybody under surveillance to behave in 'non-suspicious' ways. This phenomenon might lead into truly Kafkaesque situations because there is no way to distinguish between regular and Smart CCTV systems, no way to know how the data is being processed, and hence, no way to know what kind of behaviour is considered to be 'non-suspicious'.[4]

Both predictive policing and smart CCTV technologies are therefore good examples of the move towards proactive security measures. Additionally, both technologies offer a historical reading that allows them to be framed as the next logical step in an ongoing development. However, we should not allow ourselves to be misled by the continuation of the technological development. We also need to note and analyse the frictions embodied in these technologies.

The necessity of continual analysis also holds true for other security practices, which we may refer to as *anticipatory actions* (Anderson 2010a): "In relation to terrorism, climate change and trans-species epidemics, acting in advance of the future is an integral, yet taken-for-granted, part of liberal-democratic life. … [Bombs] are dropped, birds are tracked, and carbon is traded on the basis of what has not and may never happen: the future" (Anderson 2010a: 777). Anderson (2010a, 2010b) offers two noteworthy examples of how the future is rendered actionable in technoscientific practices: the "Infectious Disease Catastrophe Model" (2010a) and RAND's TableTop strategic games (Anderson 2010b). According to Anderson (2010a), Risk Management Solutions' 'Infectious Disease Catastrophe Model' "generates a stochastic event set of, approximately, 2000 possible pandemics. The possible geographies of the pandemics vary from one another on the basis of infectiousness and lethality of a virus, spatial and temporal location of an outbreak, pandemic lifecycle, and countermeasures. Each 'possible pandemic' is generated through standard metrics for counting and tracking the geographies of actually existing pandemics. These include virology, epidemiology, case studies of past epidemics, and diagnostic pandemic surveillance data" (Anderson 2010a: 784).

Again, it is very tempting to focus on historical continuation in the reasoning behind the design and employment of such models, which are currently employed to predict various kinds of "low probability-high impact" events, "including hurricanes, flooding, infectious diseases and terrorism" (Anderson 2010a: 784). After all, epidemics have been studied using probabilistic means since the 17th century (Hacking 2006). However, what sets the 'Infectious Disease Catastrophe Model' and other modelling solutions apart from other established forms of risk management (Power 2004) is the shift from *probability* to *possibility*. The models can also be understood as a kind of premediation in that they follow the same logic of imagining something even worse when confronted with already existing threats, only in this case it is

[4] One may take some relief in the fact that the providers of security are very much interested in minimizing the number of false-positives. However, for a person marked as suspicious, the basic uncertainty remains. The individual may even not be aware that she is being confronted by security providers because of an alarm triggered by a technological system.

numbers being used rather than the text that newspapers use to premediate events and identify the next, even more dangerous threat.

Anderson’s second example of how the future is rendered actionable in technoscientific practices is the tabletop strategic games ‘played’ in 2004, in which participants acted out their response to the detonation of a nuclear weapon at the Port of Long Beach: “The advent of the event is imagined to disrupt the connections and circulations that make up life in the Los Angeles basin. People die and are injured from flash burns, radiation poisoning, flying debris, and traffic accidents. Infrastructure is damaged, causing power outages, and the loss of telecommunications. Global equity markets plummet. All commercial air traffic is halted. Millions flee the LA basin. What else will occur after the advent of event is, however, unpredictable” (Anderson 2010b: 227). However, the organizers ask, “In the weeks and months after the attack, what would the longer-term economic implications be?” (RAND, quoted by Anderson 2010b: 227). Neither exercises as such these nor the use of tabletop games are new developments. However, in comparison to, for example, the original *Kriegsspiel* used to train Prussian military officers in the 19th century, contemporary tabletop exercises serve multiple purposes: they continue to be training sessions and “drills for habituated response” but are also “tests of existing response capability; audits of emergency plans … as well as laboratories to generate knowledge of future disruptive events” (Anderson 2010b: 230). Thus, tabletop exercises also need to be understood as a means of knowledge production. The question is not whether the participants make the correct moves. Rather, the participants’ creative engagement in the course of the fictional events contributes to establishing knowledge about a potential event, which is considered to be “unpredictable”.

Technosecurity Technologies

While societies are preoccupied with their possible catastrophic futures and trying to gather knowledge about possible future events to pre-empt and manage possible risks, technosciences, such as computer science and Artificial Intelligence, are inventing ways to exploit the unpredictable and the processes of inventing new solutions to tame the unpredictable.

Accordingly, contemporary security technologies in civil security (as well as warfare discourses and practices) build on systematized practices of imagination, playing/tinkering, and mining of (often highly unlikely) possibilities, practices in which the unpredictable becomes a central resource for the management and control of open, dynamic systems that are made productive in the arenas of policing and killing. The new approach also rests on an ontology that turns the suspect/enemy into a possibilistic system that can—most prominently in the military context—be found, fixed, (finished), exploited and analysed (F3EA) with the help of information superiority based on real-time tracking, data mining, and an omnipotent sensoric control that is tested not only in warfare simulations and games but also in computational counterinsurgency and law enforcement (see Belcher 2013; González 2015; Mayer and Weber *under review*). This ontology perfectly demonstrates the idea and logic of post-processing and is driven by the hope of "finding, tracking, and targeting virtually in real time any significant element moving on the face of the earth" (Crandall 2005).

At the same time, security, surveillance, and killing technologies configure a "regime of technologically enhanced identification techniques" (Ruppert 2009: 4) and build on data collections of huge populations "not only to monitor certain targets in real time but also to be able to retrace any individual's itinerary of relations if in the meantime this has become of interest" (Chamayou 2015: 7). Ideally, any person in a war/riot/mega-event zone[5] who is categorized as a possibilistic risk (not only a concrete threat) to the dominant order is eliminated, disposed or excluded. Elsewhere, so-called risk populations are identified and registered. Social unrest is hoped to be pre-empted by taking suspects in custody. Technologies of identification, such as data mining, profiling, biometrics, and big data analytics, are governed by a productive technorationality that generates non-representational and non-objective but highly productive knowledge on the basis of imagination (Salter 2008; Amoore and de Goede 2008), speculation and an epistemology of (semi-)automated tinkering (Weber 2015). Predictions are produced and profiles constructed, creating a new reality by projecting past 'reality' into the future using parameters and values that prefer specific categories and especially highlight specific correlations and not others.

The precondition for this new knowledge/epistemic regime of information processing, planning and control is not only a new ontology but an epistemological shift from the representational (Haraway 1985; Pickering 2002) towards an optimized logic of control that exploits the unpredictable with the help of systematized tinkering. Only then can virtuality, real-time tracking and simulation take over the command. The traditional measurement of

[5] One example of the application of these techniques would be the arrests of peaceful demonstrators at the Olympic Games in London and their ban from the Olympic arena, which implies a suspension of their civil rights.

humans and nature is substituted by the projection and control of human and non-human behaviour in organic, technological and social systems.

Conclusion

What seems to be the crucial epistemological and ontological difference between contemporary technosecurity compared to modern forms of security is the focus of the former on the possibilistic. Contemporary technosecurity seeks to premediate any possible future event, even highly unlikely ones, in the fear that they might turn catastrophic. This approach fits into an epistemic regime, a post-Newtonian rationality that builds on the exploitation of the unpredictable, on the unknown, on automatized practices of tinkering, and on mapping our world as completely as possible by collecting and mining any available data.

Our findings demonstrate the need to build a stronger connection between current technosecurity discourses and practices and the phenomena of technosciences at large. To do so means, on the one hand, to avoid focusing on the role of specific technologies within a specific institutional setting alone (as Mattelart’s 2010 study on the military did) and to take seriously the role of technology within the contemporary “security culture” (Daase 2012) on the other hand. We need to take seriously the idea of technosecurity *as* Culture. Therefore, our contribution should be understood as an invitation for scholars of techno-science to bring their knowledge and skills to the study of security and surveillance architectures.

Bibliography:

Aas, K. F., H. O. Gundhus, and H. M. Lomell (eds.), (2009), *Technologies of InSecurity: the Surveillance of Everyday Life,* Abingdon: Routledge-Cavendish.

Amoore, L. and M. de Goede (eds.), (2008), *Risk and the War on Terror*, New York, NY: Routledge.

Anderson, B. (2010a), ‘Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies’, *Progress in Human Geography* 34(6): 777–798.

Anderson, B. (2010b), ‘Security and the Future: Anticipating the Event of Terror’, *Geoforum* 41(2): 227–235.

Andrejevic, M. (2007), *ISpy: Surveillance and Power in the Interactive Era*, Lawrence, KS: University Press of Kansas.

Aradau, C. and R. Van Munster (2007), ‘Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future’, *European Journal of International Relations* 13(1): 89–115.

Aradau, C., L. Lobo-Guerrero, and R. van Munster (2008), ‘Security, Technologies of Risk, and the Political: Guest Editors' Introduction,’ *Security Dialogue* 39: 147–154.

Beck, C. and C. McCue (2009), ‘Predictive Policing: What Can We Learn from Wal-Mart and Amazon about Fighting Crime in a Recession?’, *Police Chief*, 76(11): 18.

Beck, U. (1986), *Risikogesellschaft: Auf dem Weg in eine andere Moderne*, Frankfurt am Main: Suhrkamp.

Belcher, O. (2013), *The Afterlives of Counterinsurgency: Postcolonialism, Military Social Science, and Afghanistan 2006-2012. PhD Thesis.* https://circle.ubc.ca/bitstream/handle/2429/45520/ubc_2014_spring_belcher_oliver.pdf?sequence=5 (accessed December 30, 2015).

Boehme, G. (2012), *Invasive Technification*, C. Shingleton (trans.), London: Bloomsbury.

Brey, P. (2004), 'Ethical Aspects of Facial Recognition Systems in Public Places,' *Journal of Information, Communication and Ethics in Society* 2(2): 97–109.

Brown, F. (2006), *Rethinking the Role of Surveillance Studies in the Critical Political Economy of Communication. IAMCR Prize in Memory of Dallas W. Smythe.* http://www.msu.ac.zw/elearning/material/1330622850Curran%20and%20Gurevitch.pdf (accessed on February 17, 2013).

Chamayou, G. (2015), *A Theory of the Drone*, Janet Lloyd (trans), New York, NY: New Press.

Crandall, J. (2005), *Operational Media*. http://www.ctheory.net/articles.aspx?id=441 (accessed on February 17, 2013).

Crogan, P. (2011), *Gameplay Mode. War, Simulation, and Technoculture*, Minneapolis - London: University of Minnesota Press.

Daase, C. (2012), 'Sicherheitskultur als interdisziplinäres Forschungsprogramm' in C. Daase, P. Offermann, and V. Rauer (eds.), *Sicherheitskultur. Soziale und Politische Praktiken der Gefahrenabwehr*, Frankfurt am Main / New York, NY: Campus: 23–44.

De Goede, M. (2008), 'Beyond Risk: Premediation and the post-9/11 Security Imagination,' *Security Dialogue* 39(2–3): 155–176.

Forman, P. (2007), 'The Primacy of Science in Modernity, of Technology in Postmodernity, and of Ideology in the History of Technology,' *History and Technology* 23(1–2): 1–152.

Franklin, S. and M. McNeil (1991), 'Science and Technology: Questions for Cultural Studies and Feminism' in S. Franklin, C. Lury, and J. Stacey (eds.), *Off-Centre. Feminsm and Cultural Studies*, London / New York, NY: HarperCollins: 129-146.

Giddens, A. (1999), 'Risk and Responsibility,' *Modern Law Review* 62(1): 1–10.

González, R. J. (2015), 'Seeing into Hearts and Minds: Part 2. 'Big Data', Algorithms, and Computational Counterinsurgency,' *Anthropology Today* 31(4): 13–18.

Grusin, R. (2010), *Premediation: Affect and Mediality After 9/11*, New York, NY: Palgrave Macmillan.

Gutwirth, S. and M. Hildebrandt (2010), 'Some Caveats on Profiling' in S. Gutwirth, Y. Poullet, and P. de Hert, (eds.), *Data Protection in a Profiled World*, Dordrecht: Springer: 31-41.

Hacking, I. (1990), *The Taming of Chance*, Cambridge, UK: Cambridge University Press.

Hacking, I. (2006), *The Emergence of Probability*, Cambridge, UK: Cambridge University Press.

Hagner, M. and E. Hörl (eds.), (2008), *Die Transformation des Humanen. Zur Kulturgeschichte der Kybernetik*, Frankfurt am Main: Suhrkamp.

Haraway, D. (1985/1991), 'A Cyborg Manifest: Science, Technology, and Socialist-Feminism in the Late Twentieth Century' in D. Haraway, *Simians, Cyborgs, and Women: the Reinvention of Nature*, London: Routledge: 149-182.

Haraway, D. (1997), *Modest Witness@Second Millenium. FemaleMan Meets Oncomouse: Feminism and Technoscience*, New York, NY: Routledge Chapman & Hall.

Haraway, D. (1985), ‘Manifesto for Cyborgs: Science, Technology, and Socialist Feminism in the 1980s’, *Socialist Review* 80: 65-108.

Hayles, N. K. (2003), ‘Computing the Human’ in J. Weber and C. Bath (eds.), *Turbulente Körper, Soziale Maschinen: Feministische Studien zur Technowissenschaftskultur,* Wiesbaden: VS Verlag für Sozialwissenschaften: 99–118.

Hempel, L., S. Krasman, and U. Bröckling (eds.), (2010), *Sichtbarkeitsregime: Überwachung, Sicherheit und Privatheit im 21 Jahrhundert. Leviathan Sonderheft 25/2010*, Wiesbaden: VS Verlag für Sozialwissenschaften.

Hildebrandt, M. and S. Gutwirth (2008), *Profiling the European Citizen. Cross Disciplinary Perspectives*, Dordrecht: Springer.

Hobbes, T. (1998), *On the Citizen*, edited and translated by R. Tuck and M. Silverthrone, Cambridge: Cambridge University Press.

Holland, J. H. (1992), ‘Genetic Algorithms Computer Programs That ‘Evolve’ in Ways That Resemble Natural Selection Can Solve Complex Problems Even Their Creators do Not Fully Understand,’ *Scientific American* 267: 66-72.

Horn, E. (2014), *Zukunft als Katastrophe*, Frankfurt am Main: Fischer Verlag.

IBM (2011), *Memphis PD: Keeping Ahead of Criminals by Finding the Hot Spots.* https://www.ibm.com/smarterplanet/us/en/leadership/memphispd/assets/pdf/IBM_MemphisPD.pdf (accessed on July 23, 2015).

Introna, L. D. and D. Wood (2004), ‘Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems’, *Surveillance and Society* 2(2–3): 177–198.

Kaplan, C. (2006), ‘Precision Targets: GPS and the Militarization of U.S. Consumer Identity,’ *American Quarterly* 58(3): 693–714.

Kaufmann, S. (2011), ‘Zivile Sicherheit: Vom Aufstieg eines Topos’ in: L. Hempel, S. Krasmann, and U. Bröckling (eds.), *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert*, Wiesbaden: VS Verlag für Sozialwissenschaften: 101–123.

Kitchin, R. (2014), *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*, Los Angeles: Sage.

Knorr-Cetina, K. (1997), ‘Sociality with Objects: Social Relations in Postsocial Knowledge Societies,’ *Theory, Culture & Society* 14(4): 1-30.

Latour, B. (1987), *Science in Action*, Milton Keynes: Open University Press.

Latour, B. (1993), *We Have Never Been Modern*, Harvard University Press.

Lyon, D. (2008), ‘Biometrics, Identification and Surveillance’, *Bioethics* 22(9): 499–508.

Marx, G. T. (2001), ‘Technology and Social Control: The Search for the Illusive Silver Bullet’, *International Encyclopedia of the Social and Behavioral Sciences*. http://web.mit.edu/gtmarx/www/techandsocial.html (accessed on February 17, 2013).

Mattelart, A. (2010), *The Globalization of Surveillance: the Origin of the Securitarian Order*, Cambridge: Polity Press.

Mayer, K. and J. Weber [Under review], ‘From Optimizing Military Operations to Targeting Terrorist Networks: Social Network Analysis in Data-Driven Warfare’, *Science, Technology and Human Values.*

Molotch, H. (2012), *Against Security: How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger*, Princeton, NJ: Princeton University Press.

Monahan, T. (2006), *Surveillance and Security. Technological Politics and Power in Everyday Life*, New York, NY / London: Routledge.

Monahan, T. (2010), *Surveillance in the Time of Insecurity*, New Brunswick, NJ: Rutgers University Press

Nordmann, A. (2004), 'Was ist TechnoWissenschaft - Zum Wandel der Wissenschaftskultur am Beispiel von Nanoforschung und Bionik' in: T. Rossmann and C. Tropea (eds.), *Bionik - Neue Forschungsergebnisse aus Natur-, Ingenieur- und Geisteswissenschaften*, Berlin: Springer.

O'Malley, P. (1999), 'Governmentality and the Risk Society', *Economy and Society* 28(1): 138–148.

Pickering, A. (2002), 'Cybernetics and the Mangle: Ashby, Beer and Pask', *Social Studies of Science* 32(3): 413-437.

Power, M. (2004), *The Risk Management of Everything. Rethinking the Politics of Uncertainty*, London: Demos Publications.

Ratcliffe, J. H. (2012), *Intelligence-Led Policing*, London: Routledge.

Reid, R. and S. Traweek (eds.), (2000), *Doing Science and Culture. How Cultural and Interdisciplinary Studies Are Changing the Way We Look at Science and Medicine*, New York, NY / London: Routledge.

Ruppert, E. S. (2009), 'Number Regimes. From Census to Metrics. Cresc Working Paper Series' [Working paper No. 68]. http://hummedia.manchester.ac.uk/institutes/cresc/workingpapers/wp68.pdf (accessed on September 19, 2017).

Salter, M. (2008), 'Risk and Imagination in the War on Terror' in L. Amoore and M. de Goede (eds.), *Risk and the War on Terror*, New York, NY / London: Routledge: 233–246.

Schneier, B. (2003), *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York, NY: Copernicus Books.

Shklar, J. N. (1990), *The Faces of Injustice*, New Haven: Yale University Press.

Singelnstein, T. and P. Stolle (2011), *Die Sicherheitsgesellschaft: Soziale Kontrolle im 21. Jahrhundert*, Wiesbaden: VS Verlag.

Standler, R. B. (1997), *Privacy Law in the USA*. http://www.rbs2.com/privacy.htm (accessed on December 30, 2016).

Suchman, L. (1987), *Plans and Situated Actions: the Problem of Human-Machine Communication*, Cambridge, MA: Cambridge University Press.

Wayman, J. L. (2007), 'The Scientific Development of Biometrics over the Last 40 Years' in K. de Leeuw and J. Bergstra (eds.), *The History of Information Security: A Comprehensive Handbook*, Amsterdam: Elsevier: 263–276.

Weber, J. (2003), *Umkämpfte Bedeutungen: Naturkonzepte im Zeitalter der Technoscience*, Frankfurt am Main / New York, NY: Campus.

Weber, J. (2010), 'Making Worlds: Epistemological, Ontological and Political Dimensions of Technoscience', *Poiesis und Praxis* 7(1–2): 17–36.

Weber, J. (2011), 'Techno-Security, Risk and the Militarization of Everyday Life' in C. Ess and R. Hagengruber (eds.), *The Computational Turn: Past, Presents, Futures?* Proceedings of the International Association for Computing and Philosophy, *MV Wissenschaft*, Münster: Aarhus University: 193–200.

Weber, J. (2016), ‘Keep Adding. On Kill Lists, Drone Warfare and the Politics of Databases,’ *Environment and Planning D: Society and Space* 34(1): 107-125.

Winner, L. (1978), *Autonomous Technology. Technics-Out-Of-Control as a Theme in Political Thought*, Cambridge, MA / London: MIT Press.

Winner, L. (2010), ‘Trust and terror: the vulnerability of complex socio-technical systems,’ *Science as Culture* 13(2): 155-172.