Published as **Introduction: Technosecurity Cultures. In: Jutta Weber/Katrin M. Kämpf (Eds.) Technosecurity Cultures, Special Issue of "Science as Culture" Vol. 29(1) 2020, pp. 1-10.** Pre-print version.

Technosecurity Cultures: Introduction

Jutta Weber[a] and Katrin M. Kämpf[b]

[a]Media Studies, Paderborn University, Paderborn, Germany; [b]Art and Media Studies, Academy of Media Arts Cologne, Cologne, Germany

During his electoral campaign, Donald Trump proclaimed in a speech on national security, immigration, and terrorism that the development of 'a new screening test for the threats we face today' was long overdue (Trump, 2016). Anybody with 'hostile attitudes' towards the US or 'its principles,' anybody supporting 'bigotry and hatred,' or unlikely to 'flourish in our country' should be screened 'out' (Trump, 2016). As the development of such procedures might take some time, he suggested that the processing of visas from a number of countries should be stopped for an unspecified time until the aforementioned procedures were in place (Trump, 2016). The measure was later realized as Executive Order 13769, the so-called 'Muslim ban' that targeted people from several Muslim majority countries – regardless of their Visa and passport status – from entering the US.

Shortly after his inauguration, in January 2017, he renewed this pledge on Twitter, demanding 'extreme vetting' and 'strong borders' (Trump, 2017). Finally, in August 2017, leaked documents concerning an 'Industry Day' hosted by the US Immigration and Customs Enforcement's Homeland Security Division painted a somewhat clearer picture of the proposed 'screening test' and 'extreme vetting' (Biddle and Woodman, 2017). The ICE had invited technology companies interested in the construction of such an 'extreme vetting' software and had presented its expectations in such a tool: An automated, centralized data-mining software capable of screening, vetting, and reviewing risk profiles in accordance with Executive Orders concerning 'immigration and border protection security and interest' (Biddle and Woodman, 2017).

Furthermore, the would-be machine learning project was meant to 'determine and evaluate an applicant's probability of becoming a positively contributing member of society, as well as their ability to contribute to national interests' and to predict 'whether an applicant intends to commit criminal or terrorist acts after entering the United States' (Biddle and Woodman, 2017; Harwell and Miroff, 2018). Information used for this purpose was meant to encompass all publicly available channels, including Social Media, telephone records, and geospatial databases etc., far beyond visa applications or criminal records (Biddle and Woodman, 2017).

Securitizing Everyday Life

All this may resemble a dystopian plot device similar to 'The Machine' in the series 'Person of Interest,' an A.I. capable of predicting and identifying all sorts of future behaviors. Yet it highlights current society's preoccupation with security, technology, and its futures. In the name of security, the proposed technology was supposed to identify persons posing a risk and to predict, on the basis of risk profiles, what somebody will or will not do in the future. Here, different forms of insecurity and risk are framed as problems to be urgently solved and projected onto people on the move. The purely technological solution conflates accidental and intentional harm to an imagined biopolitical collective, while framing all these threats as issues of risk and insecurity. More than ever, policymakers, politicians, researchers and mass media address a broad range of societal issues – from migration and border control to crime, terrorism or public health – as 'security' problems (Figure 1).

Physical security has become an overall concern in Western societies (Beck, 1986; Giddens, 1999; Mattelart, 2010). Social security – such as protection against poverty, homelessness and precarity, food and job security or equal opportunities in education – has been radically destabilized in the recent neoliberal decades. Technological developments – from nuclear power plants, to recent advances in Artificial Intelligence – have engendered a widespread feeling of being at risk. Warnings of the 'dangerousness of the future' prevail (Aradau et al., 2008, 148) aiming at the management of contingency and unpredictability. While security expectations are permanently rising,

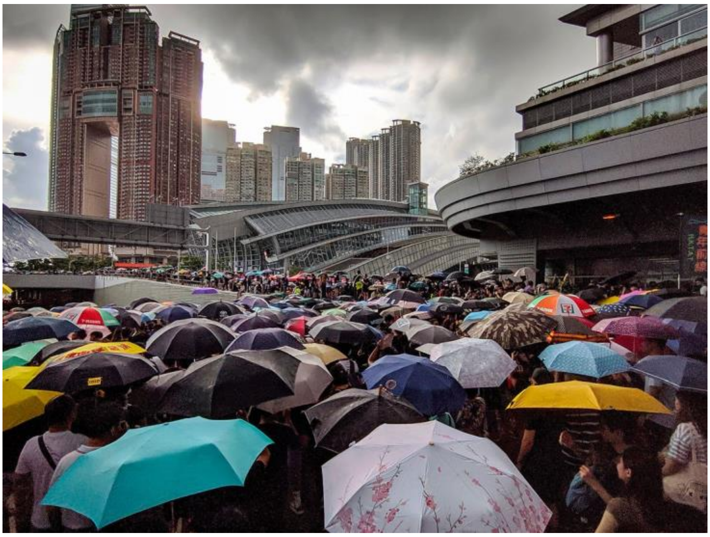

Figure 1. Hong Kong Protesters shielding themselves with umbrellas to evade surveillance (Studio Incendo 2019, https://en.wikipedia.org/wiki/File:190707_HK_Protest_Incendo_17.jpg).

risks are at the same time increasingly experienced as limitless; demands for preemptive security measures have been expanding (Amoore and De Goede, 2008; Kaufmann, 2011). Security is regarded less as a social or ecological issue than as a high-tech maximum security to be achieved by total surveillance. Various technologies are promoted as solutions to this growing demand for security (Marx, 2001; Brown, 2006; Ericson and Haggerty, 2006; Aas et al., 2009; Bröckling et al., 2010; Suchman et al., 2017; Nagenborg and Weber, 2019).

This overall tendency has been analyzed as a securitization process, especially since the end of the Cold War. Governments used new ‘threat’ scenarios to justify ‘defence’ measures, especially the expansion of military forces. Through a broader securitization process, moreover, claims of existential threats to society justify urgent extraordinary measures (Waever, 1995; Buzan et al., 1998, 24–25; Balzacq et al., 2010). As means ‘to manage dangerous irruptions in the future,’ governments, and corporations invest in security architectures and extensive risk-management techniques (Aradau and Van Munster, 2007).

Indeed, ‘risk’ itself has become a governance tool as well as a problem-diagnosis (Aradau et al., 2008; Dillon, 2008). Within risk discourses, there is a strong focus on supposedly ‘systemic characteristics’ of certain groups and less interest in past or current actions, statements, causal assessment of threats, or intentions of certain actors (Aradau et al., 2008, 148), which makes profiling – as for example the risk profiling of the screening software mentioned above or identification technologies such as biometrics – central practices of security culture.

Technosecurity Culture

Current security discourses and practices show a focus on an anticipatory maximum technosecurity (Mattelart, 2010), e.g. by urging the preemption of ‘unknown unknowns’ (Daase and Kessler, 2007). This shift in security – from a proactive to a preemptive mode – coincides with a search for technological superiority (Grusin, 2010). Surveillance technology has been combined with advances in A.I. and computer systems, together handling huge databases on entire populations or specified groups defined as a risk. We understand all this as a shift towards a technosecurity culture (cf. Daase, 2012).

In his book The Globalization of Surveillance, Armand Mattelart coined the term ‘technosecurity paradigm’ (Mattelart, 2010, 137). This signifies

> … a new configuration of power. Integration and interoperability are the passwords for reducing vulnerability and anticipating risk, uncertainty and global threats. Ties have become established and reinforced between industry, the state, the army and the police; between civilians and the military, internal and external (in)security, homeland territory and the space of transnational networks; between economic and socio-political logics, mergingcontroloverbodieswithcontroloverheartsandminds … .(Mattelart,2010,199)

This entails the massive expansion of surveillance systems (such as Echelon) into global immersive surveillance infrastructures; the policing of global flows of people, goods, and messages; the global monitoring of financial transactions in general; the dramatization of criminality and the labeling of a broad variety of incidents and deeds as terrorism by mainstream media as well as the cuttingback of constitutional rights and juridical safeguards.

But at the beginning of the twenty-first century, not only control but also revolts and protests are rising – from Occupy Wall Street and the Arab Spring (s) to Black Lives Matters, Fridays for Future and the refugee movement in the Mediterranean and elsewhere. At the same time, these '(non)citizenactors' (protestors and demonstrators) are increasingly repressed and criminalized. The withdrawal of juridical protection had already started in the 1970s and 1980s with emergency laws, e.g. the 1970s anti-terrorist decrees in Germany, the 1975 Reale Law in Italy, or the 1974 Prevention of Terrorism Act in the UK.

While Mattelart focuses mainly on institutional actors, Christopher Daase has extended the concept 'security culture' (Daase, 2012), which traditionally was used for safety issues in technology assessment. He develops 'security culture' as a framework to highlight the profound sociopolitical changes of the last few decades which led to the redefinition of security in political as well as everyday discourses and practices. From the perspective of cultural studies of technoscience, rethinking security as culture enables a deeper understanding of how security and surveillance increasingly govern policy and everyday life, beyond institutional actors such as the states or corporations.

With the 'ontological turn' in STS (e.g. Cussins, 1996; Mol, 1999), a productive understanding of technology has emerged. Beyond physical artifact (s), and sociotechnical systems, technology is interpreted as specific networks of inter- and intra-actions, processes and things. Interpreting technology as culture has a lengthy tradition in Feminist Cultural Studies of Technoscience (Haraway, 1985; McNeil and Franklin, 1991) and is a widespread concept in STS today. In this tradition, we suggest to understand the current securitytechnology nexus (Van der Ploeg, 2003) as a technosecurity culture which is profoundly shaped by the impact of high-tech surveillance and identification technologies, including their epistemologies and techno-imaginaries. And in turn it shapes technologies, epistemologies, subjects and technoimaginaries.

In this technosecurity culture, the invocation of supposed 'dangers' – such as unregulated migration, terrorism, crime, or epidemics – justifies greater control over everyone's lives. Security has been turned into a multifold, dynamic and complex sociopolitical practice (Holert and

Terkessidis, 2003; Balzacq et al., 2010). Beyond institutions and policy makers, many different agents – not just humans, but also algorithms, concepts, machines, or cyborgs – produce meanings, norms and ways of governing (Weber, 2014). Thus technosecurity cultures are a multi-agential process shaping knowledge, policies, power relations and experience around 'insecurity' problems.

There is a rich body of literature on the changing meaning of security in critical security studies as well as surveillance studies, which offer insights on the sociopolitical constitution and effects of surveillance technologies. Yet few scholars explicitly address the problem of the security-technology nexus (Van der Ploeg, 2003). Often technology is overestimated, reified, made invisible or polarized as the solution, e.g. against crime and terrorism, or as the advent of a 'Big Brother' surveillance society (Mathiesen, 1997; Ericson and Haggerty, 2006). In many cases, technologies are mainly approached from a perspective of institutional or organizational power politics. In others, technology is regarded as a tool used by to solve problems – but not as an agent producing knowledge, shaping experience and inscribing values. In surveillance studies, although 'this general emphasis on institutional or organizational power has been amazingly productive, it also set a trajectory from which it has been difficult to deviate' (Monahan, 2011, 494p.).

The Special Issue

Understanding technosecurity as culture allows us to open up the concept of security and the black box of technology. We reframe security as a complex sociotechnical practice involving many heterogeneous agents – including algorithms, everyday users, police officers and teachers, border control agents or health workers. We analyze how diverse agents inscribe values and produce meanings by reshaping standards, categories and norms.

The idea of a technosecurity culture allows us to grasp security, premediation, and surveillance as multifold, dynamic and complex processes, in which not only institutions, but also concepts, machines, algorithms, technical infrastructures, or subjects participate in the production of meanings, standards, categories, affects, desires and norms. In this special issue, we develop a more comprehensive understanding of how technosecurity culture governs our lives.

Our contributors have analyzed issues such as identification and screening systems, surveillance and bioveillance practices, their sociotechnical imaginations, and the social sorting practices they enable. Profiling and identification technologies play a dominant role in technosecurity culture: Biometrics, brain scanners, algorithmic screening technologies, DNA tests, etc. are being used to identify or profile supposed criminals, illegalized migrants, citizens, trusted travelers, or – as in the proposed extreme vetting tool – 'positively contributing member[s] of society.' In these identification processes, categories, standards, and norms concerning race, ethnicity, sexuality, health, or citizenship can be encoded, reproduced, reshaped or introduced.

As Mattelart pointed out, under the technosecurity paradigm the State's concerns with migration, terrorism, and crime are increasingly entangled. This is reflected in the development of identification systems that depend on the collection and analysis of both data and bodily traces. Race is persistent if sometimes elusive element in this. David Skinner examines three domains of innovation in our technosecurity culture – the management of dispersed borders, the expanding use of DNA in criminal justice, and the sourcing, sharing and analysis of digitized facial images – revealing the complexities of the resulting politics. Across these different domains, there is a varied and ambiguous relationship between explicit race talk and patterns of disadvantage. This can obscure a common underlying pattern: emerging sociotechnical arrangements, directly or indirectly, highlight and discriminate against minorities. The interdependences of security and technology reconfigure the race object as an unstable assemblage of corporeal, digital, and discursive elements. The implementation and management of new identification systems often accommodate to contemporary sensitivities around cultural difference and expression of identity but in ways that do little to address the structured inequalities they reinforce.

Katrin M. Kämpf takes a closer look at the identification of pedophiles, as pedophilia features among the prominent fears of western societies. Sexology defines pedophilia as a sexual preference for prepubescent children, meaning that prior sex offenses are not essential for a diagnosis. The diagnostic criteria have changed little since pedophilia was first described as a psychiatric phenomenon. Although there have been vast changes in how pedophilia is diagnosed, there remains a persistent belief that it is an innate trait of an individual. This makes pedophilia discourses compatible with current risk discourses. Technologically enhanced diagnostics indicate a shift towards a technosecurity logic within the project of seeking physical evidence to demonstrate sexual desire. At the same time, this shift is co-constitutive of current risk discourses regarding child abuse. Attempts along the technosecurity paradigm to identify pedophiles may re-normalize the notion that 'dangerous sub-populations' exist that deserve only limited rights, thus paving the way for the erosion of the legal system and of democratic principles.

In Israel, attempts by the Ministry of Interior to create a national biometric identification program for citizens and residents generated significant political debate. Michelle Spektor presents the debate as a case of a dialectic of two sociotechnical imaginaries of biometric identification that both drew upon aspirations for security, yet offered contrasting visions of the biometric future. Though prioritizations of security and technology are entrenched in both the Israeli social imagination and sociotechnical networks of security and surveillance, these imaginaries differentially connected and disentangled understandings of national security and personal security, as well as the database and ID components of the program, and influenced the technological and political trajectory of the system.

The failures of biometric systems have recently been discussed with a focus on racialized or gendered biases encoded in these systems and were most frequently criticized with regard to their alleged inherent whiteness. Sanneke Kloppenburg and Irma van der Ploeg on the other hand draw attention to the complexity of the interrelations between biometrics and bodily differences. In use as well as during research and design processes of biometric systems, bodily differences are not only reproduced, but also produced and employed. In their analysis of design challenges in engineering research as well as the workarounds and tinkering practices in the daily use of biometrics in border control, they provide more nuanced interpretations of the relation between bodies and biometric systems. They challenge the claim that the main problem with biometrics is the ‘correct’ or ‘incorrect’ recognition of pre-defined categories of gender or ethnicity. Instead, they suggest that biometric technologies are actively involved in the construction and enactment of these categories. Thus, a more nuanced look at the emergent and complex relations between biometry, gender and ethnicity is necessary.

As Darren Ellis describes, state-corporate forms of surveillance are ever more encroaching peoples’ privacy. Yet concerns about this appear to be relatively mute. Why? As technosecurity systems are becoming increasingly complex, multiple, normative, invisible and all encompassing, the psychological effects are largely unconscious. Indeed, we are all uncertain about surveillance technologies and practices in terms of their capabilities, who has access to the data, and of the ways that it affect subjectivity. Rather than being plainly indifferent, apathetic or simply silently consenting to increased technosecuritisation, some participants in Darren Ellis’ study developed a disposition of ‘surveillance-apatheia.’ They tended to say, ‘As there is no avoiding these systems and not much one can do about them, why explicitly worry about them?’ Rather than an apathetic lack of interest, this is a form of suppression for managing associated affects, for example, those that may lead to undesirable emotions and feelings such as helplessness.

Patrick Petit offers a closer look at NSA surveillance infrastructures and their global expansion which is connected to the increasing techno-securitization of societies. Surveillance technologies have become a key technique of government and have made everyone a potential threat and a target of securitizing technologies. We now seem to live under a regime of ‘everywhere surveillance’ where surveillance is carried out basically everywhere and against everyone. Inspired by Gregory’s notion of ‘everywhere war,’ the main characteristics of ‘everywhere surveillance’ seem to lie in its global reach and the heterogeneous geographies of surveillance it produces. Under ‘everywhere surveillance,’ transparency and accountability are on the run and the lines between civilians and combatants/ targets are virtually non-existent.

Biological life has come to be understood at the molecular level as information or code. Rebecca Hester details how in response to this epistemic shift, novel bioinsecurities related to the capacity to transform, modify, edit, re-write, and disseminate biological information have been identified. These bioinsecurities have engendered new practices of biosecurity including collapsing cyber and bio domains such that we now see the emergence of cyberbiosecurity.

Biosecurity technologies mirror the networked life forms they intend to preempt, prevent, and manage. Consequently, a global surveillance system focused on networked biological information, has developed. The term bioveillance is coined to describe this system. The fact that biological life is not a code, a language, or information in any strict sense, even though it is increasingly understood and discussed in these terms, means that efforts to technologically control, manipulate, re-write, and secure it will remain elusive. Yet it is this same elusiveness that will continue to incite security specialists to harness and control it.

Disclosure Statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Jutta Weber is a science & technology studies scholar and professor for media sociology at the University of Paderborn. Her research focuses on computational technoscience culture(s) asking how and for whom the non/human actors work. She has been visiting professor i.a. at the University of Uppsala (S), Vienna (A) and Twente (NL). Some related publications: Tracking and Targeting: Sociotechnologies of (In)security. Special Issue of 'Science, Technology & Human Values' 42:6, 2017 (ed. with Karolina Follis and Lucy Suchman); Keep Adding. Kill Lists, Drone Warfare and the Politics of Databases. In: Environment and Planning D. Society and Space, 2016, Vol. 34(1) 107–125; see also www.juttaweber.eu.

Katrin M. Kämpf holds a degree in Cultural History & Theory and Gender Studies from Humboldt-University, Berlin, where she is also pursuing a PhD in Cultural History & Theory. Her PhD project examines the discourse history of pedophilia. Her research interests include feminist STS, the history of sexuality, and queer theory. She is currently a researcher at Academy of Media Arts Cologne. https://www.khm.de/personen_lehrende/id.29364.katrin-mkaempf/.

References

Aas, K. F., Gundhus, H. O. and Lomell, H. (Eds) (2009) Technologies of In Security. The Surveillance of Everyday Life (Abingdon: Routledge-Cavendish).

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

Aradau, C., Lobo-Guerrero, L. and Van Munster, R. (Eds) (2008) Security, technologies of risk, and the political: Guest editors' introduction, Security Dialogue, 39, pp. 147–154.

Aradau, C. and Van Munster, R. (2007) Governing terrorism through risk: Taking precautions, (un)knowing the future, European Journal of International Relations, 13(1), pp. 89–115.

Balzacq, T., Basaran, T., Bigo, D., Guittet, E. and Olsson, C. (2010) Security practices, International Studies Encyclopedia Online. Available at http://oxfordre.com/internationalstudies/abstract/10.1093/acrefore/9780190846626.001.0001/acrefore9780190846626-e-475?rskey=plY82Q&result=1 (accessed 11 January 2019).

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

Biddle, S. and Woodman, S. (2017) These are the technology firms lining up to build Trump's "extreme vetting" program, The Intercept. Available at https://theintercept.com/2017/08/ 07/these-are-the-technology-firms-lining-up-to-build-trumps-extreme-vetting-program/ (accessed 9 August 2017).

Brown, F. (2006) Rethinking the role of surveillance studies in the critical political economy of communication, IAMCR Prize in Memory of Dallas W. Smythe. Available at http:// www.msu.ac.zw/elearning/material/1330622850Curran%20and%20 Gurevitch.pdf (accessed 17 February 2013).

Bröckling, U., Hempel, L., Krasmann, S. and Bröckling, U. (Eds) (2010) Sichtbarkeitsregime: Ueberwachung, Sicherheit und Privatheit im 21. Jahrhundert (Wiesbaden: VS Verl. für Sozialwissenschaften).

Buzan, B., Wæver, O. and de Wilde, J. (1998) Security a New Framework for Analysis (Boulder: Lynne Rienner).

Cussins, C. (1996) Ontological choreography: Agency through objectification in infertility clinics, Social Studies of Science, 26(3), pp. 575–610.

Daase, C. (2012) Sicherheitskultur Als Interdisziplinäres Forschungsprogramm, in: C. Daase, P. Offermann and V. Rauer (Eds) Sicherheitskultur. Soziale Und Politische Praktiken Der Gefahrenabwehr, pp. 23–44 (Frankfurt a.M.: Campus).

Daase, C. and Kessler, O. (2007) Knowns and unknowns in the 'war on terror': Uncertainty and the political construction of danger, Security Dialogue, 38(4), pp. 411–434.

Dillon, M. (2008) Underwriting security, Security Dialogue, 39(2–3), pp. 309–332.

Ericson, R. V. and Haggerty, K. D. (Eds) (2006) The New Politics of Surveillance and Visibility. Green College Thematic Lecture Series (Toronto: University of Toronto Press).

Giddens, A. (1999) Risk and responsibility, Modern Law Review, 62(1), pp. 1–10.

Grusin, R. (2010) Premediation: Affect and mediality after 9/11 (New York: Palgrave Macmillan).

Haraway, D. (1985) A manifesto for cyborgs: Science, technology, and socialist feminism in the 1980s, Socialist Review, 80, pp. 65–108.

Harwell, D. and Miroff, N. (2018) ICE just abandoned its dream of 'extreme vetting' software that could predict whether a foreign visitor would become a terrorist, Washington Post. Available at https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-justabandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-aforeign-visitor-would-become-a-terrorist (accessed 11 January 2019).

Holert, T. and Terkessidis, M. (2003) Entsichert. Krieg als Massenkultur im 21.Jahrhundert (Köln: Kiepenheuer & Witsch).

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, pp. 101–123 (Wiesbaden: VS Verlag für Sozialwissenschaften).

Marx, G. T. (2001) Technology and social control: The search for the illusive silver bullet, International Encyclopedia of the Social and Behavioral Sciences. Available at http://web. mit.edu/gtmarx/www/techandsocial.html (accessed 17 February 2013).

Mathiesen, T. (1997) The viewer society: Michel Foucault's 'panopticon' revisited, Theoretical Criminology, 1(2), pp. 215–234.

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

McNeil, M. and Franklin, S. (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, pp. 129–146 (London: HarperCollins).

Mol, A. (1999) Ontological politics: A word and some questions, in: J. Law and J. Lassard (Eds) Actor Network Theory and After, pp. 74–89 (Malden, MA: Blackwell).

Monahan, T. (2011) Surveillance as cultural practice, The Sociological Quarterly, 52(4), pp. 495–508.

Nagenborg, M. and Weber, J. (2019) Technosecuritysociety: Catastrophic futures, preemptive security & mass surveillance, in: Sabine Maasen, Sascha Dickel and Christoph Schneider (Eds) TechnoScienceSociety – Technological Reconfigurations of Science and Society (Berlin: Springer).

Trump, D. (2016) Immigration and terrorism, reprinted in: White, D.: Read Donald Trump's Ohio speech on immigration and terrorism, Time, August 15. Available at http://time. com/4453110/donald-trump-national-security-immigration-terrorism-speech/ (accessed 11 January 2019).

Trump, D. (2017) https://twitter.com/realDonaldTrump/status/825692045532618753 (accessed 29 January 2017).

Suchman, L., Follis, K. and Weber, J. (2017) Tracking and targeting: Sociotechnologies of (in)security. Science, Technology, & Human Values, 42(6), pp. 983–1002.

Van der Ploeg, I. (2003) Biometrics and privacy a note on the politics of theorizing technology, Information, Communication & Society, 6(1), pp. 85–104.

Waever, O. (1995) Securitization and desecuritization, in: R. Lipschutz (Ed) On Security, pp. 44–86 (New York: Columbia University Press).

Weber, J. (2014) Wild cards. Techno-security und die systematische imagination unwahrscheinlicher Katastrophen, Zeitschrift für Kulturwissenschaft, 8(2), pp. 83–97.