Sensing evil
Counterterrorism, techno-science, and the cultural reproduction of security

Mark Maguire and Pete Fussey

Abstract: New counterterrorism systems are spreading throughout the world. Many are based on behavior detection by skilled officers; others deploy techno-scientific theories and software-mediated environments. All of these systems raise critical questions about scientific and legal evidence; profiling, costs, and effectiveness. However, much of the recent scholarship on this topic is based on secondhand information and fails to attend to key transformations in security discourses and in practice. Rather than offering just an overview and theoretical critique, this article draws from our ethnographic data on counterterrorism in the UK (with reference to the broader global securityscape) and examines the phantasmagoria of fears and threats, the experimentations, myriad "expert" theories, and productivity in this realm. In doing so, the article examines how, beyond utilitarian notions of efficiency and security, counterterrorism practices perform multiple cultural roles for those charged with its delivery. We discuss particular examples of counterterrorism deployments and explore the production of theories about the human in security discourses and practices.

Keywords: abnormal behavior, counterterrorism, (in)securitization, techno-science

Security and insecurity are keywords in the contemporary moment. A significant body of international scholarship now documents the rise and spread of "amorphous" security discourses and practices in domains ranging from environmental policy to international relations and border control. Anthropologists, who tend to form their ethnographic perspectives alongside populations experiencing insecurity, have been quick to challenge these discourses and practices, calling attention to the vacuousness of the concept and the ramifications of security in everyday lives (e.g., Goldstein 2012). Thus a critical anthropology of security is emerging and contributing to broader debates (see Goldstein 2010). There is great variety in this growing area of research, as security and insecurity take on different content and have different ramifications depending on region and context. That said, some scholars assume the existence of a global archipelago of security spaces that bristle with military technologies seamlessly transported from the martial to the metropolitan realms (e.g., Graham 2010). However, (in)se-

Focaal—Journal of Global and Historical Anthropology 75 (2016): 31–44

doi:10.3167/fcl.2016.750103

curitization remains uneven, experimental, and contested. The ethnographic challenge, then, is to acknowledge broad drivers, trends, and coherencies while also attending to crucial "points of emergence or creativity, unexpected conjunctions or improbable continuums" (Deleuze 1988: 35).

Here we do not aim to develop an overarching theory of security that speaks to all contexts globally. Rather, our arguments emerge from our independent ethnographic projects on counterterrorism. Counterterrorism is but one dimension of the varied global securityscape, though it has consistently been shown to be a significant driver of reasoning and interventions in other domains. During 2011 and early 2012, Mark Maguire (2014) completed a project on counterterrorism in the UK that focused on behavioral assessment in ports of entry and included basic training, deployments, expert literature review, and interviews with key stakeholders in European and US-based agencies. Between 2009 and 2013, Pete Fussey (2013, 2014) undertook a series of projects involving fieldwork alongside security actors in a variety of urban counterterrorism contexts in the UK. This included analysis of active security environments, behavioral detection strategies, and threat analysis, including ethnographic research into policing and security at the London Olympics. Clearly, for both authors a condition of access was an agreement to provide anonymity to the organizations from whom it was granted.

Our separate training in and study of counterterrorism exposed not only local institutional and contextual factors but also the movement of persons, ideas, and ideologues in Euro-American securityscapes, especially vis-à-vis port of entry and aviation security. Strikingly, we noted the ways in which experts and those at the operational end generally cast themselves as professionals combating evildoers. Sometimes jokingly, security operators portrayed themselves as the ones "watching the walls" and "protecting you while you sleep." At other times, they spoke of the "evil" they were trained to combat. Such framings of security and of participants' roles in maintaining it were common. These framings play a vital role in animating and legitimating the work of security actors as well as constructing perceptions and beliefs about those posing a potential threat. However, what is particularly interesting here is the range of approaches developed and deployed to address "evildoers."

At first glance, then, it is not surprising that security professionals would configure themselves as heroically battling the faceless forces of evil. After all, Keith Thomas (1983) famously argued that notions of terror and evil were precisely related to levels of security and control over uncertainty. Moreover, the concept of evil shows sufficient cultural elasticity as to be almost empty (Parkin 1985), thus allowing "the terrorist" to be situated among Nazi war criminals, sadistic murderers, or any who might attack "civilization." Nor is it surprising that security professionals would configure themselves as being engaged in a battle armed with particular knowledge and skills, such as the capacity to make use of sharpened senses. What is surprising, however, is the particular ways in which security is constructing evil today from within professional and expert cultures as well as from within counterterrorist techno-science. The essential core of the argument here is that contemporary security is producing a concept of evil *both* naturalized and politicized through the imbrication of (sometimes paradoxical) expert constructivist subjectivities and techno-science.

As security operators police the high-tech aviation corridors and transportation hubs of the "western" world they deploy combinations of policing techniques and techno-science. We briefly trace the rise of counterterrorism techno-science in the Euro-American security milieu, with its hyper-rationalized and quantified indicators of abnormal behavior. Alongside these means of threat assessment one also finds constructivist subjectivities—for example, hunches and highly intuitive notions of matter out of place. It is the coexistence in one milieu of these seemingly antagonistic styles of reasoning that is of critical importance. The simultaneous operation of multiple, contrasting, and contradic-

tory ways of identifying "evil" points to cultural regimes of verediction that underpin suspicion, evidence, proportionality, and even probable cause. Moreover, we argue that merely by existing, expert theories and expert knowledge articulate a range of performative roles that serve to legitimate action and further reinforce constructed boundaries of good and evil. However, we also argue that one must go beyond accusations of "security theatre" (Schneier 2003) and acknowledge that contemporary securityscapes are not just performative spaces but also sites of creativity and emergence.

Below, we explore the rise of counterterrorism techno-science, focusing on issues of evidence and emergence, experimentation and efficacy. We then discuss the (seemingly antagonistic) "art" of counterterrorism, namely the constructivist subjectivities of security operators, drawing on brief ethnographic moments and observations to illustrate the coexistence of contradictory styles of reasoning and ways of acting. In the third section we analyze a recent theoretical contribution to contemporary counterterrorism studies, a text produced by the originators of the international programs in which we trained and studied. This expert text explores good and evil, the "abnormal" and "emergent," and is illustrative of how techno-scientific approaches and constructivist subjectivities are held together within a cultural regime of verediction. In our analysis, we draw on Foucault (2007) to underscore a shift from security operating as a form of territorial proscription to diverse forms of monitoring mobility. Such arguments make visible the inauguration of new imaginaries and conceptions of security into the complex milieus and environments of security practice.

The rise of counterterrorism techno-science

> Don't you know that … the villains always blink their eyes
>
> —The Velvet Underground: *Sweet Jane*

The concept of terrorism has a long and varied history, and this history reveals that "the terrorist" is a thoroughly cultural figure: definitions of terrorism are vague and often meaningless; and what is or is not counted as a terrorist act is often less of an empirical matter and more of an illustration of political ideology and propaganda (Sluka 2002). Indeed, "Terrorism comes in several varieties. There is 'wholesale terrorism' targeted against large populations, or 'retail terrorism' targeted against individuals. There is state terrorism, individual terrorism, or state-sponsored terrorism, depending on the agency and initiators of the terrorist actions … The most serious issue, of course, is wholesale terrorism, generally state-conducted or state-supported (Chomsky 1988: 701)." Of course, Chomsky's core point, and one animating the recent growth of "critical terrorism studies" (Jackson et al. 2009) is that, while the world reacts with horror to retail terrorism, many parts of the so-called Global South routinely experience state-sponsored terrorism. Too often terrorist attacks in the western world appear magnified, while the death toll from state violence elsewhere continues. Moreover, it should be remembered that the overwhelming majority of "terrorist" incidents in regions such as Europe do not result from actions by international terrorist groups but, rather, are acts by so-called residual terrorists: far-right groups, separatists, dissident republicans in Northern Ireland, among other persons frequently known to the security services, often at address level.

However, the events of 11 September 2001, together with the anthrax attacks and "shoe-bomber" attack by Richard Reid soon thereafter, gave rise to a particular, contemporary problematization of terrorism and to specific responses by security apparatuses. In these and subsequent encounters, terrorists were configured as unknown persons with never-before-seen weapons prepared to die in order to cause the maximum loss of life. Security apparatuses therefore reconfigured to prepare for low frequency but potentially catastrophic events. Consequently, counterterrorism work foregrounded

the imaginaries of experts, mandated to think the impossible and find ways to anticipate and even sense actions before they occur. These transformations are complex and refuse traditional institution-based analyses. Instead, one must look to how broad security apparatuses shape and are shaped by contemporary problematizations and give rise to specific assemblages of governance and action. In this section, we aim to explore the rise of counterterrorism techno-science: the new institutional configurations, forms of expertise, and technology deployments that seek to counter the threat of terrorism. We propose that counterterrorism techno-science focuses on human life itself, building theories and producing evidence, often retrospectively, to counter threats in the near future. In particular, we argue these are drawn from a range of logics seeking to variously identify "abnormality" or "malintent" that become translated as attempts to render the individual legible.

While many of the following examples are drawn from the United States, they are part of a more general global transformation of security techno-science, which had a particularly significant moment in the postwar United States. The most obvious example of all of this is presented by the establishment of the US Department of Homeland Security (DHS) in the wake of the events of 11 September 2001, a development that was part of the most significant reorganization of US government since World War II. Today, the DHS employs a workforce of approximately 230,000 persons and operates with a US$38 billion per annum budget, with well over US$1 billion expenditure on security science and technology (Priest and Arkin 2011). Here, as Masco (2014) notes, one may observe the reconfiguration of the twentieth-century national security state as the contemporary counterterrorist apparatus—anticipatory, affective, boundless, and, we add, besotted with techno-science.

Between the contemporary security apparatuses and the problematization of unknown terrorist evildoers one now finds the extraordinary rise of counterterrorist techno-science. Here we use the term techno-science in the contemporary sense: to elicit the relationality between science, technology, and society, their imbricated processes, undergirding networks and conditions of possibility (Latour 1987). This perspective is especially important here as we are examining the ways in which disciplines such as anthropology, psychology, and primatology have been harnessed to engineering and computer science in order to technologically sense human beings at an emergent level. Clearly then, counterterrorism techno-science is not simply a response to delimited security design challenges in airports or critical infrastructure sites. Rather, to begin to understand counterterrorism techno-science one must realize that a broad convergence of (scientific) disciplinary forms of knowledge and experimental technological work is occurring in the realm of security. The disciplines in play are mined for neo-Darwinian insights and broadly offer the possibility of predictions about human behavior, while the experimental technologies at work are from the digital contemporary and target human life itself.

To further understand security techno-science one must also attend to the complex and transnational web of actors, agencies, institutions, and experts involved, together with the objectivist ontological positions that undergird it.[1] Two examples serve to illustrate. First, after 9/11, the global biometrics industry rapidly expanded to provide imaging and database systems, together with fingerprinting, iris and face recognition security "solutions," among others (Maguire 2012). But the past decade has also witnessed the rise of so-called second-generation biometrics that aim to capture more elusive dimensions of human life, such as basic emotional states, deception cues, and, potentially, emotional signs of hostile intent. Today, in a reimagining of centuries-old criminological positivism, the techno-scientific projects emerging from homeland security include AVATAR—the Automated Virtual Agent for Truth Assessments in Real-time, a physiological-behavioral assessment and face-recognition system encased in an ATM-sized machine. The DHS is also partially responsible for the development of Future At-

tribute Screening Technology (FAST), a mobile security environment that persons pass through in airports or at mega-events. FAST screens persons using an assemblage of sensors that record everything from the skin's electrical resistance to eye movement in order to capture objectivized signs of "malintent," or the intention to cause harm.

The theory of malintent holds that individuals who intend to cause harm will display particular behavioral and/or physiological cues depending on the nature, timing, and consequences of the planned event. And, as we set out further below, because the terrorist suspect is unknown—as is the nature, timing, and consequences of their near-future actions—malintent is a conceptually vacuous yet nonetheless powerful driver of security. The theory of malintent offers a remarkable cultural container that serves to both naturalize and politicize terrorism at one and the same time. It naturalizes the generally political act that is terrorism by attempting to sense an impending action from signals emitted by the human body; at the same time, it allows for those signals to be the result of political motivations, and it holds the door open for interpretations of those signals to be signs of evil—malintent gives evil a face and attempts to read its features.

Important is that AVATAR and FAST are screening technologies for sifting mobile bodies and alerting security operators to potential threats. The DHS insists that the system does not constitute the sole basis for establishing probable cause to conduct a search or make an arrest. Rather, a security operator should decide whether or not to further examine an individual for further scrutiny on the basis of elevated suspicion. But on the ground, one security expert insisted during an interview with Maguire that FAST should "light up like a Christmas tree" (interview 2011) when it encounters malintent. Much technoscientific thinking is embedded in counterterrorist discourses and practices that have spread to Europe and elsewhere along the routes of the global securityscape, and along the way similar or competing systems have emerged. Thus proponents of "scientific" approaches to counterterrorism in the UK echo their US counterparts in holding that many "observable" forms of behavior are predicated on a form of cognitive "leakage" escaping once the load of deception becomes intensified and no longer supportable by its carrier. Particularly notable here is how such knowledge has become codified and reproduced in counterterrorism training, often through recourse to evolutionary psychology, pseudo science, or the legitimating lexicon of medicine. For example, one (now retired) senior police officer, then with responsibility for training colleagues in deception identification explained: "We teach our officers to look at the feet … when someone is nervous, it engages the flight or fight reflex. Either way, the body naturally starts to pump adrenaline, and they will start to shift their weight from foot to foot" (interviewed November 2011). A supposed mimesis of atavistic urges, a return to a state of nature, becomes taken as a universal signifier of deceit. Other "evidence" for deception is drawn from more obvious, retrospectively rationalized material as our ethnographic data of a counterterrorism training session relays, "The trainer plays a video of a clearly uncomfortable Oliver North being cross-examined by a joint congressional committee investigating the Iran-Contra affair in 1987. North is drying up under questioning, padding answers with pauses and hedges. After the clip concludes, the presenter announces that North's evident discomfort constitutes an expression of several key indicators of deception." Yet the degree to which universal properties of deception, or suspicious behavior more generally, can be distilled from an exceptional event such as this—an individual admitting lying to Congress regarding destroying evidence of breaking an arms embargo with Iran to fund atrocities in Central America—is questionable. Retrospective theory-building enterprises such as these raise a number of enduring issues of evidence and epistemology that afflict much research and scholarship around the identification of malintent. First, such examples apply a skewed deduction that draws

a centripetal flow of indicators ("evidence") toward a preordained and already established conclusion ("deception"). Such selective post hoc rationalization merely confirms a known hypothesis, rather than generating a new one (the establishment of whether an individual is being deceptive).

Related is the issue of ecological validity. While the limitations of generalizing from a congressional hearing to interpersonal communication more generally are obvious, other problems of transferability bedevil research in this area. As Vrij (2008) and others recognize, broader problems of ecological validity—particularly centering on the use of small samples, artificial environments, and difficulties in replicating the high stakes of terrorist activity—are consistent in this field, particularly in relation to approaches informed by social psychology. Epistemological and ontological concerns further undermine many claims of scientifically validated techniques for isolating suspicious behavior or "leaked" traits. For example, there is a tendency to assume a shared binary moral universe, of good versus evil, where wrongdoers are cognizant of their supposed turpitude. Notwithstanding self-awareness of deceptive behavior, such perspectives overlook the sense of mission and "just cause" that animate much political violence and, furthermore, do not withstand even basic criminological scrutiny. As many ethnographic exercises have exposed, the boundary between licit and illicit are less easily drawn or perceived by those engaged in transgressive activities. And, as Vrij (2008) notes, the most effective lies are couched and contextualized in truth. More material challenges to these approaches concern issues of efficacy. As Matsumoto et al. (2011) argue, despite the claims of proponents, behavioral detection training based on these principles rarely lead to levels of 50 percent accuracy in identifying deception; thus elevating the availability of coin flipping as a cheaper and more effective alternative.

Nevertheless, crucial here is not level of accuracy in spotting deceptive behavior but an understanding of the roles and tasks this knowledge performs, in terms of positioning in "knowledge brokering" roles (Ericson 1994) as well as a range of legitimating and identity building functions. The objectivist ontological position here instantiates a particular version of the human. Terrorism—commonly spoken of as inhuman, barbarous, or evil—is now reincorporated into the natural order of things as a fundamentally human, albeit abnormal, behavior. It follows that counterterrorism becomes a matter of skilled professionals sensing the abnormal, together with mimetic science and technologies attempting to see malintent objectively. Consequently, controversial fields such as the psychology of deceit detection are required precisely to add the signatures of objective science to theories and practices that do not meet normal evidential criteria. The objectivist ontology of security techno-science insists that such signs simply *must* be available. But the questions posed by the theory of malintent cannot be answered, because the precise theory of malintent is classified. Thus what is at stake here is a secretive regime of verediction in which evidence serves only to legitimize the continued existence of that regime.

Malintent, then, is a theory of human life that emerges from a realm of shadow sovereignty with its own secretive criteria for what counts as evidence. Objectivist ontological positions that include neo-Darwinian theories about all human life and a profound infatuation with contemporary technology suffuse the realm of security today. This is what the philosopher Gros et al. (2008: 5–7) term "a new philosophical anthropology" in the age of security. But to understand the cultural reproduction of (in)security one must also attend to constructivist subjectivities and to good and evil.

Constructivist subjectivities and the art of counterterrorism

Following the Richard Reid attack in late 2001, security experts at Boston's Logan International Airport initiated research that developed into

the passenger screening program operated by the Transportation Security Administration (TSA), which is similar in kind to programs developed simultaneously in Europe and elsewhere. These programs developed, bottom up, as security experts reacted to the problematization of terrorism post-9/11 and flocked to techno-scientific ideas. Such programs are an uneasy social assemblage of deceit detection, crowd behavior analysis, and the strategic deployment of personnel, together with the training of the senses on the basis of experience. The initial screening program, developed in the early 2000s and implemented during later years, was challenged by the American Civil Liberties Union (ACLU) but deemed constitutional on the basis that it targeted "elevated suspicion" in order to deny access to "critical infrastructure" (Robbins and DiDomenica 2013: 195). Another more recent challenge came in 2013, when the US Government Accountability Office (GAO) argued that the $900 million spent on the program since 2007 did not represent value for money, because abnormal behavior detection showed an "absence of scientifically validated evidence" (2013: 1). The GAO's own meta-analytical review of 400 studies conducted over six decades revealed that "the human ability to accurately identify deceptive behavior based on behavioral indicators is the same as or slightly better than chance" (2013: 3). However, these systems continue to operate. The DHS defended its program, as noted above, by suggesting that scholarly research on deceit is extraneous when one's goal is to detect malintent—the scientific basis of which is "not typically published in academic circles for peer review because of various security concerns" (2013: 89). Moreover, they argued that it is likely that terrorists exhibit highly specific emotional signals and thus abnormal behavior detection targets rare terrorists rather than common criminals as part of the "critical security capability to defend against our adversaries" (2013: 88–93).

Thus one might reasonably ask: what do abnormal behavior detection programs look like on the ground? The example below is taken from Maguire's notes on counterterrorism training deployments in the UK within a program developed as a modified version of its US counterpart.

November 2011

> I walked out of the conference room in the bowels of a regional British airport with the twelve other "trainees." This time we were looking at the effects of adjusting a behavioral environment … [i.e., an actual deployment in search for terrorist suspects]. The uniforms took up position; one cradled a sub-machine gun. Five of us fanned out and established a covert pattern. The system is, of course, cognizant of scientific ideas about micro-facial expressions, but after numerous successful interdictions I could safely say that if the suspects were literally faceless they would still have been stopped. All were escorted away for screening interviews by warrant officers and most were subsequently arrested for varying offences, from possession of false documents to smuggling and from possession of suspect material to excessive quantities of cash. Then the call came through. The officers used personal mobile phones rather than radios. The more junior trainer came up to me, pointed at an information screen while saying, "You hear that?" "He's coming up in two minutes." "I don't know where you stand on this, but to me this man is a convicted murderer, and he's walking about like he never saw explosives in his life." "You know there'll be trouble if we stop him—he's a citizen now, it's all in the past. You … you don't even think of staring." Out of habit, however, I looked at the gaze of my opposite number across the hall, and when he redirected his gaze I involuntarily looked at the tall, thin, pale man. Remarkably, he glared at each member of the covert team in turn, smiled at

> us and walked on. No one spoke. We reassembled behind a secure door. "It often happens," said the junior trainer. "They can see you, and you think you're hunting them!" "It's usually an ex-service man or forces … he was a terrorist!"

There were no signs of malintent; rather, this was a case of a common, former terrorist going about his normal business. But in the game of hunting for malintent, in which so much relies on experience and the training of the senses, how are security officers prepared to undertake their tasks, and in what ways do they subjectively construct their roles in the world?

The above vignette describes live operations that were conducted as part of training that also involved workshops on deceit detection. These workshops were composed of numerous operational examples, together with discussions of psychologist Paul Ekman's research on how deceit might be revealed in micro-facial expressions. But little attention was really given to this notion. Actual policing, the program participants understood, required experienced police: the key was to know that there was probably something scientific in all of this, out there among the academic experts, but "we" should recognize and trust the reality of our senses. Participants were reminded that this was not about "the usual suspects"; profiling, it was plainly stated, was a pointless and amateurish activity. Here in the realm of counterterrorism, the person harboring malintent could present themselves in any possible combination of gender or ethnicity: it was underlying states and signs that one had to train oneself to look for.

Across a number of interviews and multiple professional counterterrorism training schemes attended by the authors a recurring theme was the emphasis on subjectively defined notions of what is both "normal" for a particular environment (such as the "normal" pace and direction of crowd flows) and the identification of "matter out of place." It is illustrative that a repeated and highly influential anecdote here is presented by Alfred Herrhausen, then chairman of Deutsche Bank, murdered in 1989 by individuals associated with the dying embers of the Red Army Faction in West Germany.[2] Despite traveling in a 2.8 ton armor-plated limousine following a continually varied course, Herrhausen was killed by a steel projectile concealed and launched in a pannier attached to a bicycle positioned at a "choke point" on his daily route. The attack was made possible by extensive "hostile reconnaissance" involving RAF members posing as construction workers less than 500m from Herrhausen's residence and situating the bicycle (conspicuously less than 100m from permanent cycle racks) six weeks before the attack to normalize its presence and to observe any interference with the device. In counterterrorism circles, learning distilled from this event has condensed into advice to follow hunches, gut feelings, and the "just doesn't look right" principle. And, of course, the same principle extends in modified form to people, or as one senior counterterrorism trainer put it succinctly, it's about "trusting your instincts, knowing when someone is a wee bit odd" (November 2011). This not only works to legitimate and embed subjectivities into the delivery of counterterrorism practice, it also serves to institute heterogeneous enablers of good circulations and pluralize the obstacles to those deemed harmful (see Foucault 2007).

In many programs, counterterrorism training dwells on screening interviews, and several officers will leave the room to prepare truthful daily narratives with one fabricating a bogus narrative to see who among the remaining trainees can spot the cues. The trainees generally fail, but, of course, such training experiments are not "real," and thus failure is no measure of validity. "In reality," of course, counterterrorism operations involved mundane knowledge about what worked and did not, what actions, positions adopted, or environmental intrusions were likely to flush out dangerous individuals or groups. One learns the skills and acquires the needed experiences, and the job means that one uses skills, experiences, and instincts to hunt down those who intend to harm the innocent. Beyond

good and evil, it is understood that the hunter and the hunted share sensibilities. Admiration may even blossom on either side, but so too do cultural imaginaries about specific groups and about what is natural in human life itself. Today, the cultural imaginaries of security experts are based on institutional knowledge and subjective experiences but also suffused by knowledge emanating from new techno-scientific projects.

Theorizing evil and the "emergence of emergence"

> By the pricking of my thumbs, something wicked this way comes.
>
> —*Macbeth,* Act 4, Scene 1

Since 9/11, hundreds of scholarly studies of counterterrorism have been published, and dozens of autobiographies, memoirs, exposés, and intellectual treatises have appeared (e.g., Baer 2003; Pillar 2003; Graham 2008). However, here we are interested in the specific intellectual outputs emanating from counterterrorism. Following Feldman (2013), we take the Foucauldian term "specific intellectual" to denote individuals with "a direct and localised relation to scientific knowledge and institutions" (Foucault 1980: 128), individuals in privileged positions who can navigate apparatuses and processes but who often chafe against power relations and feel solidarity with those outside. Here we extend Feldman's approach by examining work that is both critical and creative, namely Robbins and DiDomenica's *Journey from genesis to genocide* (2013), a remarkable essay on emergence and counterterrorism.

Robbins and DiDomenica's work begins with their reflections on the terrorist attack by Richard Reid on American Airlines flight 63 in December 2001. Robbins was then director of aviation security and DiDomenica was director of security policy at Boston's Logan International Airport, where flight 63 was diverted after the failed attack. The lessons both men learned translated into DiDomenica's key role in developing behavioral assessment screening, later adopted by the TSA, piecemeal by UK counterterrorism, and by transport police across Europe. But this is not a technical manual. Rather, restating the Manichean universe that characterizes the field, the authors set out to explore terrorists' motivations by thinking about the evolutionary dimensions of good and evil. "How could this happen?" they ask. Their search for an answer leads them to consider human nature itself when confronting *the terrorist*:

> [W]e expect to see, literally, at some level of consciousness, an ugly Ogre with grossly distorted features, including horns and a tail. We do this as humans because we can't imagine, even for a moment in time, that one human being like us could commit such an unspeakable act against another. Ultimately, we realise that the answer to the question is even more frightening than an Ogre: It is ourselves. We, as human beings, are capable of the most heinous, despicable acts against our own kind, including genocide. (2013: 63–64)

Their work draws together socio-biology, primatology, psychology, and anthropology. They review numerous examples and psychological experiments and reach the same conclusion as Hannah Arendt: evil is banal. Their recognition of the ordinariness of evil quickly becomes an effort to "naturalize" terrorists. Terrorism, they propose, emerges from hate: a specific emotion emergent in the interfusion of the "primitive survival instincts" of the brain together with neocortical planning and rationality (2013: 61).

But how does one search for unknown persons, possessed by hate but otherwise fundamentally ordinary? Abnormal behavior detection becomes the study of "the emergence of emergence" (Robbins and DiDomenica 2013: 15–21), the contemporary scientific moment's attention to the "emergent rules of collective behavior" and their "fuzzy and probabilistic" qualities (2013: 14–15). Again, populating metaphors with the natural sciences provides a ve-

hicle for conceptual legitimation, "Just as we are confident in walking across a frozen pond based on our understanding of the collective behavior of water molecules, when looking at groups of people, societies, and nations and the interactions between them, understanding the dynamics of behavior and the ability to predict behavior will occur principally through emergent rules dependent on situational and environmental factors" (Robbins and DiDomenica 2013: 21).

In protecting the critical infrastructures and vital systems, counterterrorism deploys behavior detection techno-science and expertise that are shaped by and in turn shape paradoxical ontologies. On the one hand, one finds objectivist techno-science with its universalized indicators of "abnormal" behavior; on the other hand, one finds constructivist subjectivities that range from hunches to professional imaginaries about real and imagined evildoers. But what one also finds are points of connection and creativity in which (in)security is produced and reproduced. Techno-scientific systems, counterterrorist training and operations, and specific intellectual work converge in a naturalization of terrorism that includes discourses on the vital nature of humanity, expert imaginaries, and specific interventions. Discussion of the emergence of emergence may seem lofty and removed from operational practice, but counterterrorism is precisely the kind of problem-space in which multilevel discursive and practical work is occurring. In short, to think in evolutionary terms about the universal dynamics of human behavior and its specific situational and environmental factors may also be to contemplate a modern airport with its woof and warp of human activities. In turn, this means that one must contemplate natural and normal behavior—the idea that crowds have "baseline" behaviors—in order to detect matter out of place, persons who behave abnormally or are "a wee bit odd." Thus, as DiDomenica explained to the US House of Representatives, "a person who is engaged in a serious deception … will suffer mental stress, fear, or anxiety … manifested through involuntary physical and physiological reactions such as an increase in heart rate, facial displays of emotion, and changes in speed and direction of movement" (DiDomenica 2011: 4). But in explaining these mysterious cues, he underscores a crucial point: counterterrorism is not just about arresting terrorists per se; rather, it is about facilitating needed mobility while allowing security apparatuses to protect critical infrastructure. Good and bad circulations become monitored, delineated, and modulated. By elevating the senses and techno-scientifically searching for objective indicators of malintent a new evidential domain emerges around "elevated suspicion" (DiDomenica 2011: 4–9). This is precisely the domain that the US House of Representatives was exploring with DiDomenica and other experts in 2011. At the same time, a report by the US National Research Council (NRC) was also under consideration, a report that argued, "Scientific support for linkages between behavioral and physiological markers and mental state is strongest for elementary states (simple emotions, attentional processes, states of arousal, and cognitive processes), weak for more complex states (deception), and *nonexistent* for highly complex states (terrorist intent and beliefs)" (NRC 2010 [our emphasis]).

A thin red line

Michel Foucault's work suffuses contemporary security research, especially work on biosecurity, risk, and preparedness. However, Foucault attended to security only briefly during his Collège de France lectures, and then only as a staging point for studies of governmentality and biopolitics. Ultimately, security was to remain "a field left fallow" (Bigo 2008: 93–114). Nonetheless, his comments are prescient and further illuminate the diverse registers, *dispositifs,* and approaches that constitute the delivery of "security."

Foucault begins by discussing eighteenth-century urban planning and the problematization of circulation. Apparatuses of security take center stage, he proposes, when cities and towns

are no longer governed by means of enclosure and walls. Faced with the need for liberal government that facilitates the positive circulation of persons and things, planners and thinkers—specific intellectuals of various sorts—encountered potentially "indefinite series" of elements and events (Foucault 2007: 20). Apparatuses therefore constitute "milieus" and manage them in terms of probabilities, in effect naturalizing relations between populations, circulations, and problematizations in a near future. In such milieus, crime will never be entirely rooted out, threats will be ever present; elements that are considered natural cannot be fully suppressed. Life itself is therefore the central preoccupation, and security is about "allowing circulations to take place, of controlling them, sifting the good from the bad, ensuring that things are always in movement, constantly moving around, continually going from one point to another, but in such a way that the inherent dangers of this circulation are cancelled out" (Foucault 2007: 65). Security thus becomes unmoored from traditional (sovereign and disciplinary) preoccupations with territorial control or regimes of prohibition and instead focuses on leaving agents, actors, and flows in situ as their mobilities become monitored and delineated.

Apparatuses of security, then, from a Foucauldian perspective, clearly inaugurate new imaginaries and new concepts, from risk to precaution and from preparedness to prediction. Foucault opens an important challenge: to explore precisely how values like good and evil gain currency in security contexts in which human life itself is naturalized and politicized. The challenge is to understand how contemporary security naturalizes the politics of good versus evil (and uses the "natural" and evolutionary to undergird politics), thus rendering such seemingly archaic values as points of emergence and creativity that animate, legitimate, and give content to security.

A broader reading of Foucault's work on security is instructive here. His last essay, *Life: Experience and science,* is important as a statement on emergence and creativity. Therein he returns to the powerful influence of his teacher Georges Canguilhem and his ideas on the normal and the abnormal. Canguilhem's (1979) project was to explore how truth claims about living beings were constituted in science. He rebelled against positivist scientific treatments of life that rendered deviations as abnormal when situated against a fixed version of what is normal, especially in medical knowledge. For Canguilhem "the basic unit" that specific forms of enlightenment knowledge *normalize* is "a living being in shifting relations with a changing environment" (Rabinow 1998: 195). What is at stake, then, is life that is error-prone, filled with anomalies, and yet caught in the power-knowledge web of normalization. Thus "An anomaly is not an abnormality," Canguilhem reminds us, and "Diversity does not signify sickness" (quoted in Rabinow 1998: 196). Foucault foregrounds Canguilhem's discontinuous history of science by focusing on the importance of errors even from evolutionary perspectives: "life has led to a living being that is never completely in the right place, that is destined to 'err' and be 'wrong'" (Foucault 1994: 15). Moreover, such persistent presence of error leads to its institution into practice. Error becomes "the permanent contingency [aléa] around which the history of life and the development of human beings are coiled," as Foucault (1994: 16) suggests during his reflection on Canguilhem's work.

Paradoxically, although reproduced and integrated into new practices, error is seen to have been effaced. Signals of hostile intent are amplified and the noise of false positives attenuated. Finessed by scientific discourses of humanity's core nature, the deployment of techno-science, and the application of expert imaginaries, new, seemingly more robust forms of knowledge come into being. Yet it is useful here to reflect on the residual presence of error. As Foucault further notes, "Error is eliminated not by the blunt force of a truth that would gradually emerge from the shadows but by the formation of a new way of 'truth telling'" (1994: 471). Thus in this application for identifying suspicious behavior, scientific discourse itself does not generate ob-

jective knowledge that eradicates error through unfalsifiable "truths," but serves to create and scaffold new "truths" that freight and institute extant errors into practice.

What if normalizing scientific knowledge and information systems constantly faced ruptures and disturbances from error-prone life itself? Indeed, building from the data presented above, one of our key arguments is that the increasing presence of intuition and subjectivity in counterterrorism is crucial to the diversification and instantiation of error into such practices.

Foucault establishes the task of exploring "the relationship between life and the understanding (*connaissance*) of life" by tracing and attending to "the thin red line of the presence of value and of the norm" (1994: 14). Amoore (2013: 149) proposes that emergence is therefore central to "security techniques that seek out the emergent threat pre-emptively in the form itself, long before it is actualized." In doing so, this emphasis on futurity performs multiple functions during the present. Adey and Anderson (2011: 1096) note, for example, that "anticipatory action promises to secure a valued life and this makes present a good future of safety, protection, and care." This temporal compression between the present and the future is also recognized by others. But a broader reading of Foucault is also available in Paul Rabinow's work on *the contemporary,* "a moving ratio of modernity, moving through the recent past and near future in a (non-linear) space" (Rabinow 2007: 2), which Rabinow understands as an ontological problem space. Building on this observation, it is the contemporary ontological problem space of counterterrorism, replete with its paradoxical strains, which we have attempted to explore in this article.

Conclusions: Sensing evil and reproducing (in)security

Today, security apparatuses cross nation-state boundaries and blur the lines between institutions and agencies, governments and private corporations. Security may be a new name for long-standing state violence in many parts of the world, but it is also a site of new techno-scientific assemblages and forms of expertise that seek to know and manage the near future. In this article, we have drawn on our ethnographic research on counterterrorism as well as analysis of expert documents and an overview of important trends in counterterrorist techno-science to stake out a number of claims. First, counterterrorism as a contemporary site of (in)securitization includes both objectivist techno-science—which targets universalized indicators of abnormal behavior and terrorist malintent—and constructivist subjectivities that stretch from hunches and suspicions to imaginaries about battles between good and evil. Our goal has been to point to the ways in which techno-science and constructivist subjectivities compete, are paradoxical, yet nest together in the problem-space of contemporary counterterrorism. And in this problem-space one finds the emergence of machines for mimetically acting upon human nature and professional experts theorizing, constructing, and acting upon broadly similar ideas about human life itself. Little if any scientific evidence is available to support the claims of counterterrorism techno-science or the constructivist subjectivities of many experts. Instead, as Foucault (2007) proposed, one sees security constructing milieus and naturalizing processes and patterns therein. However, whereas Foucault glossed the values emergent in security contexts, here we have shown that seemingly archaic values such as good and evil are central to the contemporary naturalization and biopoliticization of security. Today, security experts imagine the potential horrors of the near future and develop technologies and work to heighten senses to protect the innocent against evil. In so doing, evil has become less a philosophical question of the frighteningly normal, to borrow from Hannah Arendt, and more a matter of naturalizing the abnormal such that it becomes knowable through mysterious signs. In the secretive world of counterterrorism, then, one finds in notions like good and evil what Gilles Deleuze terms "points of emergence or creativity" (1988: 35).

Much of this article has explored points of emergence in contemporary realms of (in)security from US techno-science to UK counterterrorism deployments. Many of our arguments point to the importance of evidence or the lack thereof in security discourses and practices. Indeed, it is precisely evidence that threatens the shadowy edifice of counterterrorism. The emergence of emergence in security expertise troubles the very relations of evidence and the world, inaugurating new concepts and a new philosophical anthropology. Just as Gilles Deleuze in his discussion of contemporary societies of control drew on Franz Kafka's *The Trial* to explore the "limitless postponement" characteristic of systems that disregard truth and evidence, one might reflect on how Kafka approached good and evil, in the sense of "stripping all that is becoming to a man except his abstract humanity" (Trilling 1955: 39). It is this Kafkaesque image of evil that is emergent between techno-science and constructivist subjectivities in counterterrorism today. Counterterrorism does not target beasts or ogres but rather abstract, and abstracted, versions of human life itself.

Mark Maguire is head of the Maynooth University Department of Anthropology. He twice held visiting professorships in the Department of Anthropology, Stanford University, California. From 2010 to 2014 he edited the international journal *Social Anthropology* and is co-editor of *The Anthropology of Security: Perspectives from the Frontline of Policing, Counterterrorism, and Border Control* (Pluto, 2014).
Email: Mark.H.Maguire@nuim.ie

Pete Fussey is professor of Sociology at the University of Essex. He has published widely in a number of areas, including terrorism and counterterrorism, critical studies of resilience, major-event security, surveillance and society, organized crime and urban sociology. He is co-author of *Securing and Sustaining the Olympic City* (Ashgate, 2011) and co-editor of *Terrorism and the Olympics* (Routledge, 2010).
Email: pfussey@essex.ac.uk

Notes

1. Here we use "ontology" in a rather straightforward manner that does not directly engage with current disciplinary discussions. Instead, we are simply concerned to unpack the "real" that exists for security operators or the always-constructed realm of human (ethical) action within which they exist, together with its non-human and inhuman actors and actants, from techno-science to terrorists. Moreover we are interested in openness to that which lies beyond, the limits of knowledge, and the penumbral as sources of emergence.
2. The anecdote was relayed to Pete Fussey during separate interviews with senior London-based private-sector security counterterrorism agents (May 2010, August 2011, and February 2012).

References

Adey, Peter, and Ben Anderson. 2011. Affect and security: Exercising emergency in "UK civil contingencies." *Environment and Planning D: Society and Space* 29: 1092–1109.

Amoore, Louise. 2013. *The politics of possibility: Risk and security beyond probability.* Durham: Duke University Press.

Baer, Robert. 2003. *See no evil: The true story of a ground soldier in the CIA's war on terrorism.* New York: Three Rivers Press.

Bigo, Didier. 2008. Security: A field left fallow. In Mitchell Dillon and Andrew Neal, eds., *Foucault on politics, security, and war,* pp. 93–114. London: Palgrave Macmillan.

Canguilhem, Georges. 1979. *Le normal et le pathologique.* Paris: PUE.

Chomsky, Noam. 1988. *Language and politics.* Edinburgh: AK Press.

Deleuze, Gilles. 1988. *Foucault.* Minneapolis: University of Minnesota Press.

DiDomenica, Peter J. 2011. Statement of Detective Lieutenant Peter J. DiDomenica before the US House of Representatives Committee on Science, Space, and Technology, Subcommittee on Investigations and Oversight, The TSA SPOT Programme: A Law Enforcement Perspective, 6 April 2011, https://science.house.gov/sites/republicans.science.house.gov/files/documents/hearings/2011%2003%2031%20DiDomenica%20Testimony.pdf.

Ericson, Richard, V. 1994. The division of expert knowledge in policing and security. *British Journal of Sociology* 45(2): 149–175.

Feldman, Gregory. 2013. The specific intellectual's pivotal position: Action, compassion, and thinking in administrative society, an Arendtian view. *Social Anthropology* 21(2): 135–164.

Foucault, Michel. 1980. Truth and power. In Nikolas Rose, ed., *Power/knowledge: Selected interviews and other writings, 1972–1977,* pp. <page range?>. New York: Pantheon.

Foucault, Michel. 1994. Life: Experience and science. In Paul Rabinow and Nikolas Rose, eds., *The essential Foucault: Selections from essential works of Foucault, 1954–1984,* pp. 6–18. New York: The New Press.

Foucault, Michel. 2007. *Security, territory, population: Lectures at the Collège de France, 1977–1978.* London: Palgrave Macmillan.

Fussey, Pete. 2013. Contested topologies of UK counterterrorist surveillance: The rise and fall of project champion. *Critical Studies on Terrorism* 6(3): 351–370.

Fussey, Pete. 2014. Command, control, and contestation: Negotiating security at the London 2012 Olympics. *The Geographical Journal,* advance publication.

GAO (US Government Accountability Office). 2013. *Report to congressional requesters. AVIATION SECURITY: TSA should limit future funding for behavior detection activities,* http://www.gao.gov/assets/660/658923.pdf.

Goldstein, Daniel M. 2010. Toward a critical anthropology of security. *Current Anthropology* 51(4): 487–517.

Goldstein, Daniel M. 2012. *Outlawed: Between security and rights in a Bolivian city.* Durham: Duke University Press.

Graham, Bob. 2008. *Intelligence matters: The CIA, the FBI, Saudi Arabia, and the failure of America's War on Terror.* Lawrence: University of Kansas Press.

Graham, Stephen. 2010. *Cities under siege: The new military urbanism.* London: Verso.

Gros, Frédéric, Monique Castillo, and Antoine Garapon. 2008. De la sécurité nationale à la sécurité humaine. *Raisons politiques* 4(32): 5–7.

Jackson, Richard, Marie Breen Smyth, and Jeroen Gunning, eds. 2009. *Critical terrorism studies: A new research agenda.* London: Routledge.

Latour, Bruno. 1987. *Science in action: How to follow scientists and engineers through society.* Boston, MA: Harvard University Press.

Maguire, Mark. 2012. Biopower, racialization, and new security technology. *Social Identities: Journal for the Study of Race, Nation, and Culture* 18(5): 593–607.

Maguire, Mark. 2014. Counterterrorism in European airports. In Mark Maguire, Catarina Frois, and Nils Zurawski, eds., *The anthropology of security,* pp. 118–139. London: Pluto.

Masco, Joseph P. 2014. *The theatre of operations: National security affect from the Cold War to the War on Terror.* Durham: Duke University Press.

Matsumoto, D., H. S. Hwang, L. Skinner, and M. Frank. 2011. Evaluating truthfulness and detecting deception. *FBI Law Enforcement Bulletin,* June, http://davidmatsumoto.com/content/Evaluating%20Truthfulness%20and%20Detecting%20Deception.pdf.

NRC (National Research Council of the National Academies). 2010. Workshop summary on field evaluation in the intelligence and counterintelligence context, http://books.nap.edu/openbook.php?record_id=12854&page=R1.

Parkin, David. 1985. *The anthropology of evil.* London: Blackwell.

Pillar, Paul R. 2003. *Terrorism and US foreign policy.* Washington, DC: Brookings Institution Press.

Priest, Dana, and William M. Arkin. 2011. *Top secret America: The rise of the new American security state.* New York: Little, Brown, and Co.

Rabinow, Paul. 1998. French enlightenment: Truth and life. *Economy and Society* 27(2–3): 193–201.

Rabinow, Paul. 2007. *Marking time: On the anthropology of the contemporary.* Princeton: Princeton University Press.

Robbins, Thomas G., and Peter J. DiDomenica. 2013. *Journey from genesis to genocide.* Pittsburgh: Dorrance Publishing.

Schneier, Bruce. 2003. *Beyond fear: Thinking sensibly about security in an uncertain world.* New York: Copernicus Books.

Sluka, Jeffrey. 2002. What anthropologists should know about the concept of terrorism. *Anthropology Today* 18(2): 22–23.

Thomas, Keith. 1983. *Man and the natural world.* London: Allen Lane.

Trilling, Lionel. 1955. *The opposing self.* London: Secker and Warburg.

Vrij, Aldert. 2008. *Detecting lies and deceit: Pitfalls and opportunities.* Chichester: Wiley.