8 Machine learning and artificial intelligence in counterterrorism

The "realities" of security practitioners and technologists

Mark Maguire and David A. Westbrook

Introduction

At approximately 09:24, on 28 February 1997, two armed robbers, Larry Phillips Jr. and Emil Matasareanu exited the North Hollywood branch of Bank of America, leaving terrified customers in their wake. They were confronted by waiting police, but they stood their ground and opened fire with assault rifles. Protected by homemade body armour, the two robbers behaved as if they were invulnerable. Officers ducked for cover behind squad cars only to see their vehicles disintegrate in a hail of bullets. Several officers made for a nearby gun store to plead for heavier weapons. Eventually, at 09:42, help arrived in the form of a rather casual-looking "SWAT" (from "Special Weapons And Tactics") team. The team was called up during a barbecue, and several members arrived in shorts and sneakers. But the SWAT specialists quickly turned the tide. Phillips, wounded, turned his gun on himself. Matasareanu fought on, despite taking several rounds to his body armour. Then a SWAT officer "skipped" bullets beneath a car, striking Matasareanu below his armour, and causing him to bleed to death.

The North Hollywood shooting lasted nearly 45 minutes and was recorded by circling news helicopters. The footage is spectacular, cinematic. It is regularly played on projector screens in counterterrorism training events to stimulate discussion of tactics. The audience is presented with a scene without context. The film is "the" reality on the table, albeit of a particular kind. The North Hollywood shooting speaks to security adepts as they train, learn, and so constitute the discipline of security. The constant replaying of footage of the event exemplifies the curation of an ideal-type reality within the expert domain of counterterrorism, and the closing of the mind to alternative possibilities. Security expertise, like all "disciplines" has an epistemology, which is inherently problematic, given the stakes. But it is not just film that shows, frames, and constrains the way we can think about a problem within a professional world. Today we must also worry about the growing intrusion of experimental technologies into this domain, which tend to add further layers of dangerous abstraction. It is therefore important to attend to the ways that security training and technology innovation are intersecting.

DOI: 10.4324/9781003412908-11

This chapter extends from our larger project on counterterrorism (see Maguire and Westbrook, 2020). We examined public behaviour during terror attacks in the UK, France, Ireland, and Kenya. Here, we will dwell on a specific French example, the foiled 2015 terrorist attack on the Thalys train from Amsterdam to Paris. Because of the paucity of cross-cultural research on emergency management, security bureaucracies welcomed our project, so participation in various meetings and joint training exercises was encouraged. We have already written about the roles of police and military special forces "operators" (see Westbrook and Maguire, 2019; Maguire and Westbrook, 2020, 2021). Such forces are glorified, emulated, and when it comes to equipment, no expense is spared. Indeed, having "the teams" adopt a new technology all but guarantees the commercial success of the product.[1] Though small in number, special forces have an outsized role in technological and material innovation in the security sector.

Elite teams train in secret, but their doors regularly swing open for arms and other technologies companies pushing the latest gadgetry. Training workshops and joint exercises often end with a formal opportunity to view the latest hardware and software. Retired members of elite police or military units are sometimes recruited by companies to sell products and services to their former employers. It is easy to observe the so-called corporate push, but some technologies are adopted while others are not. Solutions, after all, must address specific problems or better "problematizations", challenges that are acknowledged in expert communities of practice. As we shall show, counterterrorism, as bureaucratically organised violence, is converging with a broadly sympathetic style of reasoning coming from technologists. In this emergent space, complex social challenges are often simplified, and difficult moral problems are elided. We use unique data on the 2015 Thalys terror attack and introduce the concept of "boxology" to illuminate the conjuncture between two questionable versions of reality.

The discipline of security

> I simply tried to focus on my three-foot world. My job wasn't to complain; my job was to clear that compound under the orders we were given.
>
> — Navy SEAL Chief Matt Bissonnette

Members of elite military and police teams cultivate extraordinary martial prowess. Reputations – and this is a world in which reputations really do matter – are forged by displays of Olympian athleticism and preternatural mental resilience. But the small psychological literature on special force members also shows selection in favour of problem solvers and, especially, team workers (Stanton, 2011). Teams work together to solve problems using secrecy and surprise, cunning, and, of course, aggression. This is well known.

But there are also more subtle attributes, specific "styles of reason" (Hacking, 1992) that are as effective as any physical weapon.

Special forces, in our ethnographic experience, speak about narrowing their vision when confronted with chaos, imposing a small controllable "reality" onto the chaotic real world. There are a few public statements on this topic. For example, in *No Hero* (2014), quoted in the above epigraph, Navy SEAL Chief Matt Bissonnette, writing under the pen name Mark Owen, popularised the term "three-foot world". In contrast to the 30,000-foot view of strategists and politicians, the operator, he explains, must control chaos by implementing the three-foot world that she or he can affect. Similarly, we spoke to operators who described moments during violent action when they paused, "hit the reset button," and asserted control over their milieu, sorting friends and civilian "sheep" from the evildoers. One individual, an elite police officer involved in the fatal shooting of armed attackers, could recall only the persons and things of that he had been trained to see, a car with armed individuals, innocent civilians. Everything that lacked significance slipped from view. All that remained, at least in his memory, was a "scene" composed of facts, his act of violence, and the expected actions and reactions that followed.

When thinking of the trained actions and responses of elite military and police, one is tempted to reach for Michel Foucault's (1977) work on military "discipline," Marcel Mauss's earlier "Techniques du Corps," or recent ethnographic work on "skill". But Foucault moves gadfly-like across ostensibly different societal domains in order to illustrate general power-knowledge configurations. From Foucault, we learn that the military barracks resemble the school, hospital, and prison, but we learn little about the actual competencies developed in specific barracks. Mauss, for his part, conflates efficiency and effectiveness, a rather elementary misstep.[2] At first blush, "skill" seems to be a spongy term, but anthropologists have recently used the notion of "skilled vision" to illuminate the world of security professionals (Maguire, 2014) and other experts (Grasseni, 2007).

Skilled vision denotes the development of embodied and tacit competence, including acquired assumptions about the world, and biases and preferences, often supported by a formal body of knowledge, a "discipline". As one might suspect, it is hard for members of a community of practice to explain their skilled vision to uninitiated outsiders, to find the right words, and yet similarly competent individuals who have been through the apprenticeship simply "get it". But the realm of skilled vision, at least in counterterrorism, is not permitted to remain elusive, untranslatable. Anthropologists have certainly demonstrated that significant levels of opacity are common in skilled sociality, even in apprenticeships (e.g., Hanks, 2006), but in the example here opacity is punished by practice, and inscrutable fellows are not and cannot be included in elite teams. It is necessary for members of a team to "get it", but a common language with outsiders such as military planners, emergency professionals, and external agencies is also needed. Borrowing

from Gregory Bateson (1972), Erving Goffman (1974) uses the simple term "frame" to articulate how groups stabilise the world to enable the deployment of embodied cognitive resources and in so doing transform the world, making it actionable even if fundamentally uncertain.

We are proposing that the discipline and skill of operators are available in and communicated through purposeful efforts to frame reality. The question becomes: what does such framing look like in practice?

Here we are speaking of elite soldiers who operate in milieus of constant, often frugal innovation, where style and efficiency yield to brutal effectiveness. And because of the high cost of innovation in their world – failure may involve capture, torture, and death, if one is lucky – the elite soldiers' frame, the "three-foot world", has acquired an air of profundity, insight, rather than communicating uncertainty. Indeed, Chief Bissonnette's term names and describes a combat team's emphasis on span of control over an operational field that is composed of facts. A fact here acquires meaning with reference to a known scenario, or it may be new information pressed into a narrow frame. In short, there is a narrowing of vision, such that reality becomes a milieu of knowable actions and reactions, a box.

Footage of the North Hollywood shooting is played in training sessions, while actual operations resemble the North Hollywood shooting. Of course, the creation of cognitive frames – both narrowing and enabling – through the interplay of training and experience is hardly new. Recall Roman historian Josephus said of the legions, "Their training is bloodless battle, their battles are bloody training". But we are not discussing strategy and tactics on the field of Mars here; rather, we are discussing the style of reason that underpins the deployment of kinetic force in a world populated by civilians.

Boxology

> Certain forms of knowledge and control require a narrowing of vision. The great advantage of such tunnel vision is that it brings into sharp focus certain limited aspects of an otherwise far more complex and unwieldy reality. This very simplification, in turn, makes the phenomenon at the centre of the field of vision more legible and hence more susceptible to careful measurement and calculation. Combined with similar observations, an overall, aggregate, synoptic view of a selective reality is achieved, making possible a high degree of schematic knowledge, control, and manipulation.
>
> James Scott, *Seeing like a State*

We carried out our research in Kenya, the UK, Ireland, and France, the latter example being explored in detail further below. Each jurisdiction had specific counterterror forces, the shadowy obverse side of modern bureaucratic order. In any one jurisdiction, a patrol police officer might be the first

to respond to a major incident, but soon an alert travels to, say, Ireland's Emergency Response Unit (ERU) or to London Metropolitan Police's MO-19. A major incident alert would also go to military specialists such as the Irish Army Ranger Wing (ARW) or Britain's 22 Special Air Service (SAS). Such units sometimes train with each other and with other "friendly" forces (for a long time, for example, the ARW and SAS were interoperable, and British forces train Kenya's counterterror Recce Squad). In this small world, an "operator" is expected to deliver kinetic force in a flexible yet highly organised manner, an agile (bureaucratic?) service. French counterterrorism, perhaps unsurprisingly, elevates bureaucratic violence to a quasi-academic level, which merits discussion, and underscores the overall point we make here.

Should there be a major incident in Paris, municipal police will yield control to the Police Nationale's specialist unit, Recherche, Assistance, Intervention, and Dissuasion (RAID) or to their sister unit in the Gendarmerie, Groupe d'Intervention de la Gendarmerie Nationale (GIGN). In 2019, Mark, one of the authors, attended a closed counterterror workshop in the UK. RAID senior staff were guests of honour and presented details of their "methodology". They focused on an infamous incident in Dammartin-en-Goële three years earlier. The incident occurred in the wake of the Charlie Hebdo massacre by, among others, brothers Saïd and Chérif Kouachi. In the days after the massacre, the fugitive Kouachi brothers entered the offices of a signage company by impersonating police officers and proceeded to hold employees hostage at gunpoint. GIGN and RAID officers surrounded the building and established a series of concentric "boxes". In these boxes, persons and things are expected to conform to rigid, scenario-based proformas or be eliminated. The outermost box is the *cordon sanitaire*, protected by snipers. The next, smaller box is the operational milieu of joint forces. The innermost box is the jurisdiction of special forces. A plan is formed, and the plan is displayed as a diagram of and for reality.

The innermost box contains the terrorists and sometimes, unfortunately, their civilian victims. It is, essentially, a kill zone, and its occupants – including the hostages – are categorised as, to quote one senior RAID officer, the "already dead". Humans become facts, "the raw meat of history", to borrow from Albert Camus. This is worrying, not least for liberal democracy. Yet, in Europe, airports and other critical infrastructure sites have played scenarios through and contemplated shuttering off sections of buildings in the event of a major terror incident, effectively locking civilians into boxes with their attackers until armed assistance arrives to "resolve" the situation.

But there is more to worry about than secretive counterterror units operating in the shadows. We must also worry about the rise of AI and X Reality technology, and the intrusion of these technologies into counterterrorism – technologies for control in the search for an imprimatur.

X in a box

We are witnessing today the intrusion of X Reality systems into counterterrorism. X Reality is sometimes referred to as extended reality or simply as XR. The X here commonly denotes distinct but allied technologies: augmented, mixed, assisted, and fully virtual reality systems.

Each of these systems, to varying degrees, uses machine learning and other forms of artificial intelligence. Depending on the generosity of the listener, then, X Reality is either a useful umbrella term for a superset of technologies or an unreadable label for a chaotic collection of incompatible gadgetry.

Of course, some of these technologies have matured over long periods of time. Science fiction writer Stanley Weinbaum's 1935 essay *Pygmalion's Spectacles* fully anticipates virtual reality headsets. In 1961, the famous photographer Charles Wyckoff filed a patent for extended reality film to render nuclear explosions visible. Wyckoff later, allegedly, photographed the Loch Ness monster, a strange detour on the road to the first functioning virtual reality headset in 1991 (see Mann, 2001). Artificial intelligence also has a considerable pedigree. Its theoretical foundations were set by post-WWII Defence Advanced Research Projects Agency (DARPA)-funded projects, and it has been weaponised and used earlier, especially in artillery strikes and air force missions. (One could argue that the USSR's RYaN programme, which scanned US activity for "signs" of a possible nuclear strike, anticipates much of military AI's logic today).[3]

A sample of current AI military capability was available during the summer of 2021 in the US Northern Command's (NORTHCOM) Global Information Dominance Experiments which brought together AI-enabled tools from around the world, especially a cloud-based collaboration tool called Cosmos, a threat alert system called Lattice, and a data-rich "awareness tool" called Gaia. There is much handwringing about the role of Big Tech in air force AI projects, but Algorithmic Warfare is still immature, with the most generous commentators comparing NORTHCOM experiments to building the bicycle while riding it. Nonetheless, AI and X Reality are widely used in visualisation. After all, battlefields are hard to see, and there is an enormous advantage to adopting, essentially, a smart screen with data depth and action alerts. The goal is to replace Napoleon's *coup d'oeil,* the glance of the military genius, with the most relevant and up-to-date information, legible to lesser and more prevalent minds. There are numerous challenges here, not least understanding what's in the "black box" of modern artificial intelligence systems. Today, this challenge is framed as "the opacity problem", or "the problem of explainability" – how can one trust the answer given by the machine if one cannot understand where the answer came from (see also Maguire, 2018)? In military command, explainability is a sincere problem, because command must be exercised over dynamic situations, and multiple overlapping and uncertain three-foot worlds. The crisis commander in an anti-terror incident is also expected to use the latest technology and data,

but, much like the military commander, he will eventually yield to the chaos of conflict, the fog of war, as Clausewitz had it, through which the dogs move.

The US Department of Defence AI Strategy (2019) imagines a future of warfare with artificial intelligence offering enhanced decision-making. But this is just one stream of techno-scientific development. The future of war will also include AI-enabled "symbiotic" man–machine systems, according to the Pentagon. These systems emerge from use, they require use, and thus, perhaps, resolve the "problem of explainability".

So, how are X Reality systems used in counterterrorism? The United Nations Office of Counterterrorism provides a clear statement on this:

> AR and VR technologies have the potential to become effective tools in the global fight against terrorism. AR/VR provides a cost-effective, rapid training solution used globally, and will one day be ubiquitous within training packages. … Moreover, these technologies can increase coordination in post terrorist attacks environments, enabling first responders to have a wholistic understanding of complex terrorist scenes. Such technology is already being tested in border security, emergency management, and criminal investigations.
>
> (UNOCT, 2021: 2)[4]

There is ample evidence that X Reality is making inroads in military command structures, using AI to aggregate and visualise patterns and signals; this is happening coterminous with an AI revolution in logical (cyber) and physical security. But, speaking specifically about the kinetic end of counterterrorism, our experience chimes with the view expressed by the United Nations Office of Counterterrorism: AI-enabled X Reality is intruding into anti-terror training, pre- and post-incident, nesting happily as yet more boxology.

Since 2017, we have attended multiple showcases, demonstrations, and training events where X Reality systems were put on display. During a quasi-academic event in Estonia in 2017, Mark was invited to test one "near-to-reality" system in a hotel. The system was a headset that promised visualisation of data and "terrorist" avatars. After several false starts, frank admissions of failure accompanied by fits of laughter from the commercial operator, the headset brought to life a ghost-like figure on the ground near a sofa. "Is he moving?" the commercial operator asked in response to Mark's description of the figure. "No? Well, you never know with these terrorists! (more laughter)". And, indeed, the most sophisticated bleeding-edge X Reality does have the power to amuse, but the systems are improving, rapidly.

During the same event, and again one year later, Mark met the founder and CEO of a major X Reality company, who was already selling into the counterterrorism and emergency management market. The product he offered was a sleek video-game-like training experience where multiple users could log on from anywhere in the world and play the role of emergency workers,

police, or even anti-terror forces, on the ground or in command, and deal with a terror event or post-event response. For example, one could take on the role of a police officer in an airport who is confronted by a mass casualty event. AI, Mark was told, "scrapes" data from real scenarios and responds to users' actions and decisions to add "layers" of new micro-scenarios, and so the platform "evolves". During a demonstration, a scene unfolded in front of Mark on the platform's screen, and the CEO described how a police officer might make a decision based on what is visible, a drop-down menu of training advice, and new data introduced via "comms". But when asked about the civilian avatars in the visualisation, timing, speed, and several other basic matters, the CEO revealed that the "scenarios" used were in fact news reports read by his software engineers or videos found online. Engineers call this "under-specification". In plain terms, no actual participants in an actual terror incident were ever interviewed. Yet, to be clear, everything in the box felt real.

As explained earlier, this chapter extends from our larger project on counterterrorism (see Maguire and Westbrook, 2020). One of our goals has been to examine public behaviour during terror attacks in Kenya, the UK, Ireland, and, as elaborated in detail here, France. This work involved sitting down with members of the public to understand where they were on a fateful day, what they saw, and what they did. As it happens, we also drew boxes and cognitive maps to help us delimit the specific spaces and understand experiences. Here we indicate what actual terrorism looks like from the perspective of those involved, juxtaposed against the martial order of things and the technological rendering of reality.

Reality unboxed

At 17:45 on 21 August 2015, a young man named Ayoub El Khazzani exited the WC in Carriage 12 of the Thalys train from Amsterdam to Paris. El Khazzani was stripped to the waist and brandishing an assault rifle and a Luger pistol (he carried 900 rounds of ammunition in a backpack). His mission, as he saw it, was to murder as many people as possible, ideally overseas American servicemen and European bureaucrats. We interviewed almost everyone boxed in with the terrorist on Carriage 12 that day, El Khazzani's intended victims.

On seeing him emerge from the WC, a Thalys employee ran away and locked himself in a luggage compartment. But El Khazzani was challenged first by a Frenchman who remains anonymous and then by 51-year-old Mark Moogalian. He overpowered both men, gravely wounding Moogalian. Sixty-two-year-old Christopher Norman instantly recognised the severity of the threat. He had grown up in South Africa and spent time in Kenya. Guns sound the same the world over.

> My first thought was, 'Oh my God, it's happening to me'. … You know I remember the Tunisia thing, immediately before it, where people

> didn't get up and do anything and basically they were all shot down anyway. So, my thinking was you know what do I do, how do I react in relation to this? Is there anything I can do that will basically save our lives? At the same time being very, very scared. So, I was kind of trying to get myself ready to do something but I didn't know whether I was going to do anything or not and then.
>
> (Interview, 2019)

Ten metre further down the carriage, US servicemen Anthony Sadler, Alek Skarlatos, and Spencer Stone sat together. Here is Spencer Stone's account of what happened next:

> So, you know, I was initially woken up by the train employee running past me. … And then I looked at Alek and he was kind of looking towards the back of the train and then he kind of had, like, a shocked, you know, look on his face and then I looked at Anthony and he was just kind of like still looking up and kind of had the same look, like what the heck is going on? I took my headphones and I heard glass breaking, people screaming, and then I turned around and looked behind me and the first thing I see is a guy coming in to our train car bending down picking up the AK and he's trying to load a round in and, you know, I noticed he was kind of like … something was going on with this guy. … So I pretty much took it upon myself, because I just thought our time was running out, that I'd make a move, pretty much, and so I just took off in a full sprint down the aisle towards him and then, you know, I could hear him trying to work the gun again and even more like he actually ended up pulling the trigger on me but there was a bad timer on the bullet so it gave me more time to be able to make it to him, which is like probably the biggest miracle in the whole story.
>
> (Interview, 2019)

Alek Skarlatos takes up the narrative from here:

> Spencer tackled the guy. I caught up to him. We fought with him for a little bit. Then basically Spencer finally got him in a chokehold, and once he got him in a chokehold, the terrorist then pulled out a handgun to try to shoot him with it. I was standing right in front of him, so I pulled the hand gun from out of his hand before he could shoot anything and then put it to his head and told him to stop resisting. He didn't, so I pulled the trigger and the chamber was empty. So, then, I basically just threw it and then I picked up the AK that was on the ground, because I think Spencer was getting stabbed around this time, so I tried to shoot him with the AK but it was on safe so instead of messing with it anymore I just started to hit him in the head with the muzzle.
>
> (Interview, 2019)

Some commentators don't like to hear about "have-a-go heroes". Perhaps it plays to macho illiberal politics. But facts matter. In all of the terror attacks we studied, civilians attempted various interventions, from grappling with armed terrorists to organising medical care. Leviathan, in the form of highly trained counterterror operators, was invariably late to the scene. This is of great significance, then, because even in the box that was Carriage 12 of Thalys train 9364, behaviour was unexpected and full of lessons for public safety. The US servicemen rushed to prevent a terror attack and did so relying on military training, recreational martial arts, and early socialisation in the United States, where the threat of "active shooters" is present, expected even. The US servicemen subdued the terrorist, cleared the carriages in expert fashion, and saved the life of gravely wounded Mark Moogalian using their basic battlefield medical training. By the time counterterror police took charge, the situation was neatly tied up, literally.

Lessons learnt from Thalys included the need to better train frontline staff and the need to have advanced first aid kits onboard trains. But, unsurprisingly, corporations selling X Reality solutions to transport providers, like the global BMT Group, push for investment in "flexible simulation" platforms rather than investments in low cost but effective measures like better first aid kits.[5] And, to continue the juxtaposition, counterterror operators prefer to train to face heavily armed North Hollywood bank robbers rather than face the fact that actual terrorism is dysfunctional, messy, hard to train for, and the kind of thing that will be over before you arrive to save the day.

All of this gestures to a deep problem in the intrusion of X Reality into the boxology of counterterrorism. Our investigations of the Thalys train attack, the 2013 Westgate Mall attack in Nairobi, or the terror incident in London's Borough Market in 2017, and other incidents showed an extraordinary gulf between perceptions about public behaviour and the unboxed realities on the ground. Terrorists struck, the public reacted, from have-a-go-heroes to the selfless individuals who saved others, some froze, others panicked, and yet one could piece together all the stories into an account. One could tell truths about humans, and learn lessons about how to save lives. But counterterror bureaucracies wish to segment reality in order to rationalise expenditures and training, and ultimately the actual deployment of force. For-profit corporations wish to simulate a reality based on guesses that just happen to be addressed by their products, rather than use actual data with all its messy details, contradictions, and uncertainties. The danger in the intrusion of X Reality systems is that it will represent an incorrect version of reality to individuals whose job it is to use deadly force, and to the civilian world in which such force is exercised.

Conclusions

On one level, we have shown that there is a deep problem in contemporary counterterrorism: a limited and limiting style of reasoning that is potentially

dangerous for democratic societies and which lends itself to technological gimmicks. But one cannot simply offer abstract criticism and nothing else in the face of a problem in the world of security. Firstly, because this is a deadly serious context, and, secondly, because today's "bleeding-edge" gimmick is tomorrow's cutting-edge, must-have kit.

Of course, critique is certainly possible and valuable: if one reduces counterterror violence to a series of boxes, one excludes the experiences of those who were there, including the terrorists who created the box. The likely effect of what we are calling boxology is to reduce time, space, and options. Moreover, in order to train, the box reproduces what is known, and therefore what is knowable, closing knowledge in with the expert. One could easily here make reference to Hannah Arendt's comments on bureaucratic "thoughtlessness" and "remoteness from reality" (Arendt, 1963). And yet, some sympathy is required here. What else can one do? Everyone complains about security measures until a white nationalist, Al Shabaab member, or some other unknown person demonstrates that there wasn't enough security. Lives are lost, people are blamed, and careers end. Counterterrorism must engage in reasonable actions with the aim of countering terrorism. X Reality promises something in a context where the most reasonable response is probably to do nothing at all. The question, then, is how to think about an intellectual response beyond critique, one that understands the demands of the day.

Today, scholars and activists are exposing the biases and errors encoded in security technology (e.g., Ferguson, 2017; Sandhu and Fussey, 2021), and some researchers are already looking to a future of interoperable, platform-based technologies that are imbricated with securitarian styles of reason (e.g., Leese and Egbert, 2020). This chapter is a call for more attention to how technologies nest in the security landscape alongside existing and sympathetic frames. When it comes to security, all too often we see only a "sketch of the façade", to borrow from Arthur Schopenhauer (1958: 128), but to understand the adoption of security technology – here AI, and X Reality technology – we must attend to the structures, meanings, and styles of reason behind the façade.

Notes

1 In the United States, the image of the special forces operator is very powerful, and so the endorsement of a product by battle-hardened Teams is a coup for any equipment producer. There is a trickle-down effect within the military, with lower-tier units wishing to emulate their heroes. And there is a trickle-out effect too, as law enforcement becomes, in the USA and elsewhere, ever more reliant on Special Weapons and Tactics (SWAT) teams. In the USA, the FBI alone has over 1,200 SWAT officers, and 85% of all towns with populations between 25,000 and 50,000 persons have their own SWAT team (see Balko, 2013). The "public" special operator equipment market is enormous (the private market is enormous too: today people hunt deer dressed head-to-toe as special forces soldiers, and increasingly operator endorsement is a requisite for success in the Airsoft

equipment market). Moreover, because the so-called Pentagon Pipeline (the 1033 Program, curtailed by the Trump administration) has funnelled $16 billion worth of military equipment to law enforcement since 9-11, there is considerable churn in procurement. This is just the United States. Security is a global industry: from Kabul to Kiev, generic special forces equipment is widely available.

2 On numerous occasions, Mauss conflates terms and offers a suggestive but ultimately specious analysis. For instance:

> The techniques of the body can be classified according to their efficiency, i.e. according to the results of training [*résultats de dressage*]. Training [*le dressage*], like the assembly [*le montage*] of a machine, is the search for, the acquisition of an efficiency. Here it is a human efficiency. These techniques are thus human norms of human training [*dressage humain*]. These procedures that we apply to animals men voluntarily apply to themselves and to their children. … As a result I could to a certain extent compare these techniques, them and their transmission, to training systems [*à des dressages*], and rank them in the order of their effectiveness.
>
> (Mauss, 1973: 77–78 [my emphasis])

In the specific example here of the application of kinetic force, a special forces team may be ranked in terms of efficiency by delivering maximum damage for relatively low cost to the military – think here of a small team of saboteurs delaying an advancing enemy. But extraordinary time, effort, and resources are often committed to special forces because effectiveness, though costly, is worth the expense in a realm that prizes results above all.

3 During the Vietnam War, the US attempted to disrupt the real-and-imagined "Ho Chi Minh Trail" by littering borderland jungles with sensors that could communicate with overflying aircraft and to a data fusion centre for decision-making. Operation Igloo White turned out to be a sophisticated, expensive methodology for murdering trespassing wildlife with aerial bombardments. It was also open to spoofing. The war was lost, eventually, but the model survived to fight another day.

4 The UNOCT also discusses empathy-building for deradicalisation.

5 For examples of BMT products see: https://www.bmt.org/insights/vr-training-inspired-by-gaming/

References

Arendt, H. (1963) *Eichmann in Jerusalem: A Report on the Banality of Evil*. New York: Viking Press.

Balko, R. (2013) *The Rise of the Warrior Cop: The Militarization of America's Police Forces*. New York: Public Affairs.

Bateson, G. (1972) *Steps to an Ecology of Mind*. San Francisco: Chandler.

Department of Defence (2019) Available at: https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

Ferguson, A.G. (2017) *The Rise of Big Data Policing*. New York: NYU Press.

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison,* trans. A. Sheridan. London: Allen Lane, Penguin.

Goffman, E. (1974) *Frame Analysis*. New York: Harper & Row.

Grasseni, C. (ed.) (2007) *Skilled Visions: Between Apprenticeship and Standards*. Oxford: Berghahn.

Hacking, I. (ed.) (1992) *Historical Ontology*. Cambridge, MA: Harvard University Press.

Hanks, W.F. (2006) 'Joint Commitment an Common Ground in a Ritual Event', in N. Enfield and S. Levinson (eds.) *Roots of Human Sociality*. Oxford: Berg, 299–328.
Leese, M. and Egbert, S. (2020) *Criminal Futures: Predictive Policing and Everyday Police Work*. London and New York: Routledge.
Maguire, M. (2014) 'Counterterrorism in European Airports', in M. Maguire, N. Zurawski and C. Frois (eds.) *The Anthropology of Security: Perspectives from the Front Line of Policing, Counterterrorism, and Border Control*. London/New York: Pluto Press, 118–138.
Maguire, M. (2018) 'Policing Future Crime', in M. Maguire, U. Rao and N. Zurawski (eds.) *Bodies as Evidence: Security, Knowledge, and Power*. Durham, NC and London: Duke University Press, 137–158.
Maguire, M. and Westbrook, D.A. (2020) *Getting Through Security: Counterterrorism, Bureaucracy, and a Sense of the Modern*. London/New York: Routledge.
Maguire, M. and Westbrook, D.A. (2021) 'Security By Design: Counterterrorism at the Airport', *Anthropology Now*, 12(3), 122–135.
Mann, S. (2001) *Intelligent Image Processing*. London: John Wiley & Sons.
Mauss, M. (1973), 'Techniques of the Body', trans. Ben Brewster, *Economy and Society,* 2(1), 70–88.
Owen, M. (2014) *No Hero: The Evolution of a Navy SEAL*. New York: Penguin.
Sandhu, A. and Fussey, P. (2021) 'The 'Uberization of Policing'? How Police Negotiate and Operationalise Predictive Policing Technology', *Policing and Society,* 31(1), 66–81.
Schopenhauer, A. (1958) *The World as Will and Representation*. Indian Hills: Falcon's Wing Press.
Scott, J. (1998) *Seeing Like a State: How Certain Schemes to Improve the human Condition Have Failed*. New Haven/London: Yale University Press.
Stanton, N.A. (2011) *Trust in Military Teams*. Wey Court East, England, Ashgate.
UNOCT – United Nations Office of Counterterrorism (2021) 'The Application of Augmented Reality and Virtual Reality Technologies in Countering Terrorism and Preventing Violent Extremism'. Available at: un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20210708_statement_miedico_ar-vr_webinar.pdf.
Weinbaum, S.G. (1935) *Pygmalion's Spectacles*. New York: Simon & Schuster.
Westbrook, D.A. and Maguire, M. (2019) 'Those People [May Yet Be] A Kind of Solution: Late Imperial Thoughts on the Humanization of Officialdom', *Buffalo Law Review,* 67, 889–907.