Enacting the state through security assemblages

Materiality, technology and political subjectification in Nairobi

Colona, F.

Publication date
2019

Document Version
Other version

License
Other

Chapter 4

Security Technologies, Spaces and Political Subjects

During my fieldwork, I attended two major security fairs and a congress organized by a German delegation aimed at boosting commercial ties between the Kenyan security sector and German industry. The first fair was held at the Kenyatta International Conference Centre in July 2015. This event, *SecProTec East Africa*, targeted the security industry of the eastern part of the continent and beyond. It was considered the leading event for the security and protection business and was supported by the East African Community, the Kenyan Ministry for East African affairs, and the KSIA. It hosted international companies whose businesses intersected with security and protection work at large. The second fair I attended was *Securexpo East Africa*, which took place in September 2015 in Forestgrounds, Nairobi, at the Visa Oshwal Centre. While the latter seemed to take a more local branding, its organizers promoted similar events in South Africa and West Africa. It was part of a series of commercial exhibitions on security that run parallel to conference sessions hosting local and national security stakeholders. The German-organized congress aimed to bring together Kenyan state and German industry representatives, providing the latter with a direct platform to market their products.

In all these venues, the exhibitors primarily marketed recent and cutting-edge security solutions. As I entered the hall where the SecProTec fair was held, the number of electronic devices immediately caught my attention (see Figure 2). From small buzzers with in-built cameras to extremely sophisticated systems, access control seemed to be the main concern. Among the items I found most intriguing at this fair were fingerprint or iris-scan activated door locks. I was surprised that with an estimated number of over 400,000 private security guards in Kenya, only one company was sell-

ing safety equipment for the security officers themselves, like helmet and other protective gear – and only from a catalogue, as they did not have any showpieces on site. Rather than CCTV system, which only records videos on a memory drive, the majority of exhibitors were selling Internet Protocol CCTV systems. These provided a live feed to a smartphone, tablet, or computer anywhere with an Internet connection so that, for example, house or store owners could watch their own property from afar. Cameras took the main stage in these fairs. Some of them were able to record details hundreds of meters away while others were able to detect movement and start recording automatically. Their overwhelming presence suggested to me that these devices were the norm.

Figure 2: Various security cameras at Securexpo East Africa.
Source: https://www.securexpoeastafrica.com/2015-gallery.

In Nairobi the ever-growing market for such technological devices is associated with two main concerns. The most ubiquitous is everyday crime like home robberies, muggings and thefts. Terror attacks are the second concern. Since the involvement of the Kenyan military in Somalia in 2011, repeated terror attacks have been carried out in Nairobi. Before the Westgate events, hand grenade attacks terrorized the residents and patrons of various commercial spaces and nightclubs in Nairobi and other urban centers. These series of events bolstered the practices of technological securitization in various commercial and institutional buildings that had already started few years earlier. However, since September 2013, metal detectors and cameras, to name only two, increasingly marked the entrances of malls and other large buildings, and epitomized the technological response to various forms of insecurity.

Contrary to such eye-catching technologies, in wealthy neighborhoods such as Forestgrounds and Greenwoods, everyday security practices are dependent on rather mundane and low-tech devices. The most widespread security technologies through the streets of Forestgrounds are often concerned with access control. But rather than cutting-edge cameras, these are barbed or razor wire and metal bars blocking windows and doors. By driving or walking on these streets, those unfamiliar with the city cannot help but notice the amount of barbed wire spiraling on top of perimeter walls of small or large compounds, single villas or commercial buildings. In Forestgrounds, where I conducted most of my fieldwork, many perimeter walls were topped with broken glass as well. It warned unwanted visitors that getting into the compound would require dealing with its sharp bits. In a somewhat remote corner of Forestgrounds, a four-story apartment block stood behind a three-meter-tall wall rimmed with barbed wire and electric fences. On each floor a small, dark balcony looked out onto the road. They seemed carved out of the bare and grey brick building, their smallness enhanced by the iron bar grids that closed them off. While they prevented any climber or anyone with a sufficient ladder to get onto the balcony and inside the houses, they also made the building look like a fortress, and its apartments prison cells.

Figure 3: My neighbors' wall with barbed wire and an old electric fence. Photo by the author.

Examples of this type abound. My own neighbors fenced their apartment block with a wall about five to six meters tall (see Figure 3). The wall was covered in rusty barbed wire and electric fences. Given the amount of green vegetation growing on and through it, the electric fence was definitely out of order. Whether as an unintended consequence of their imposing and omnipresent materiality or due to the development of my research sensibilities as I mentioned in Chapter 1, I often found myself imagining what it would take to get through these security structures and break into buildings and properties. For instance, I noticed that the weak wooden door of the first house I lived in had a metal grate that made a possible robbery only slightly more labor intensive, because its hinges could be pulled away and the grate would come off easily.

While all these different types of security technologies – from cameras to barbed wire to metal grates – are deployed to protect the lives and property of middle- and upper-class residents, they also do political work. In

the security practices that enroll these devices, residents, business owners, and the security companies can opt for different technological devices. The threat that each device aims to protect against, through its deployment, is embodied in specific subjects. These are often assumed to be dangerous, unwanted within a specific space, and they are enacted as non-belonging. Similarly, whom these devices are supposed to protect is also inscribed in their deployment: by specifying *how* security technologies keep someone out, they also define *who* they are trying to keep out and away from *whom*. In this chapter I ask: *What type of threatening and non-threatening subjects are enacted through various security technologies, and how?*

In conversation with STS debates, I seek to explore how objects and technologies do political work, and how they contribute to including and excluding different categories of people. In so doing, I focus on the centrality of objects and technologies in processes of political subjectification and state enactments. To answer my questions I attend to a number of artifacts that are enrolled in Nairobi's security assemblages. In relation with guards, residents and clients, objects and technologies enable specific ways of recognizing (non-)dangerous people, and thus contribute to the political subjectification of entire categories of people as othered subjects. In this chapter I outline four specific types of subjects: the "dangerous other," the "distrusted security guards," the "residents looking for peace of mind," and the "mediating professionals." They are enacted through the deployment and use of security technologies as more or less belonging to different spaces.

The work of security technologies also produces another type of differentiation: they help to enact very concrete boundaries. Irrespective of the fact that these boundaries can be visible to varying degrees, they partition and differentiate space. These differentiated spaces are enacted either as safe or dangerous, or as worthy of protection and in need of surveillance. The deployment of security objects and technologies changes spaces and redraws boundaries. In this process, spaces become security technologies that are themselves enrolled in security practices of the residential and commercial areas of Nairobi. Belonging or not belonging to one of these differentiated spaces mediates processes of subjectification. Who belongs to the interior

spaces of an apartment block are the subjects to be protected, while not belonging to it contributes to enacting people as potentially dangerous, and as subjects to be protected against. The mobilization of security technologies, which often require professional and skilled expertise to be operated and installed, entails other less defined subjects, such as the mediating professionals, who elude the dangerous versus non-dangerous dichotomy. In the concluding section of the chapter I show how the various subjects (and the processes of subjectification that enact them) are related to each other, and I specifically highlight the critical role of spatiality in processes of subjectification.

Technologies, Subjects, and Space

Unpacking the political work carried out by security technologies can start from looking at what types of threats technological artifacts are designed to neutralize and what types of people they are designed to protect. In this respect, in Nairobi the political consequences of security technologies become evident in the way different categories of people are made to interact with them, and in the way the city is fragmented in different spaces. While all technologies (help to) do political work, it is important to emphasize that security technologies produce differentiations that are often dramatic and palpable. This is especially the case for the ways entire categories of people are made to belong to certain spaces and not to others, how some are considered worthy of protection and others are criminalized and distrusted altogether.

The relation between politics and technology has been a long-standing and foundational issue in STS analysis. In his article *Do Artifacts Have Politics?*, Winner (1980) argues that some technologies, like nuclear plants, are inherently political because, for security reasons, they become entangled with "authoritarian" modes of governance. Winner tends to locate the politics in essential qualities of artifacts and identifies political relations in institutional and state-sanctioned modes of governance. A very different political analysis of technology is in Latour's (1992) discussion of "automated door closers," which are hydraulic engineered artifacts that use the energy stored

in opening a door to close it back again. Notwithstanding the differences between these two types of technologies, they can both be analyzed in political terms, because specific kinds of subjects are enacted through their implementation. Both technologies include and exclude people in different ways. For instance, nuclear plant workers, acknowledging the legitimate power of techno-scientific-industrial-military elite to make binding decisions, could be forced into "covert surveillance, wiretapping, informers, and even emergency measures under martial law" (Winner, 1980: 134). Quite differently from these ways of being political, hydraulic automatic door closers "*discriminate* against very little and very old persons" or against working class employees who often need to pass through doors with large packages (Latour, 1992: 234, emphasis in the original). These two different examples point towards the underlining analytical concern of this chapter: it is not just about whether security technologies are political, but about *how* they are political and, in particular, *what kinds of subjects* are constituted through their deployment.

Winner's (1980) distinction between (inherently) political and (inherently) non-political artifacts might become more tempting when it comes to technologies of security. This is because security often becomes the frame that allows for various issues to be removed from political debate, and arguably made *a*political (cf. Buzan et al., 1998). As such, instead of highlighting how security for one category of people is insecurity for another, it comes to be construed as a homogeneous good for everyone's benefit. Similarly, and as some of my interlocutors suggest in this chapter, security technologies often conflate imaginaries of efficiency and neutrality, and are considered impartial tools of apolitical practices. However, an analysis of mundane and seemingly neutral devices in their contexts of deployment, like the automated door closer (cf. Latour, 1992), or a guard's nightstick, productively interferes with such understandings. It shows how objects do political work once mobilized in various (security) practices and beyond a deliberation about their inherent (political) qualities. It simultaneously opens avenues to link the specific political work of security artifacts in relation to processes of state enactments and political subjectification.

Technologies are always situated in specific contexts. While security devices enact specific subjects, they do not work by themselves: they need to be *made to* work. Akrich argues that technologies go beyond defining actors and their relationships. Instead, "technical objects and people are brought into being in a process of reciprocal definition in which objects are defined by subjects and subjects by objects" (1992: 222). She reminds us that technologies are never disentangled from larger networks of people, imaginaries and institutions. Thus, politics does not "swirl around" (Woolgar & Neyland, 2013: 14) objects, as an interpretation of Winner's suggestion (1980) about some essentially and inherently political technologies might imply. Security technologies, in Nairobi as elsewhere, are entangled in wide socio-material assemblages of security governance that enroll residents, guards, security companies and their managers, technicians, house workers, imaginaries of dangerous people, and artifacts. It is through these reciprocal relations that specific political subjects are enacted as more or less belonging, as subjects to be protected or as criminal ones.

While the artifacts enrolled in these assemblages may be more or less high-tech, they remain unexceptionally ordinary and everyday. The keypad of an alarm system or the nightstick that guards are supposed to carry at all times in Nairobi might be described as high or low tech respectively, but in their everyday use in security practices they are mundane objects with political consequences. Such political consequences emerge tied up with objects in the process of "the ontological constitution of a multitude of people and things" (Woolgar & Neyland, 2013: 250). From such reciprocal constitution of people and things, I will foreground a specific kind of politics whereby some categories of people are enacted as unequally (non-)belonging to various spaces.

Objects are not defining subjects in a deterministic way. Nor, vice versa, do unconstrained subjects define objects. Instead, "like a film script, technical objects define a framework of action together with the actors and the space in which they are supposed to act" (Akrich, 1992: 208), and in this "framework of action" the political emerges highlighting the consequences of how different categories of people are enacted. The kind of action that is afford-

ed is not unfettered; it is constrained and differentiated in relation to who and what is involved. Rather than saying objects liberally (en)act or have agency, as out of an intentional will of some "isolated individual actors," the political work of subjectification is constituted through "*how* they are involved" (Abrahamsson et al., 2015: 16, emphasis in the original). It is in this sense that the subjects that are enacted are relational achievements.

In his political history of barbed wire, Razac's analysis (2002) is particularly helpful in highlighting the tensions that emerge in the reciprocal co-constitution of subjects, objects, and different spaces. Barbed wire may seem like a straightforward and rather uninteresting technology, but it carries its own socio-political genealogies. Razac describes how only after several not-so-successful versions barbed wire came to be manufactured as-we-know-it. It was designed as a lightweight solution for long-distance fencing in the settlers' westward expansion and the conquest of the North American continent. After its massive implementation, it quickly created the "conditions for the physical and cultural disappearance of the Indian" (2002: 22). While barbed wire was created for the use of ranchers, it became the tool that simultaneously enacted private property on the one hand, and the Indians as unwanted and dangerous others who threatened private property on the other. It also simultaneously created two polarized spaces, an exterior and an interior (2002: 73). The case of the barbed wire shows the specific and active work this technology did, a work of inclusion and exclusion, a work of separation and discrimination, a work that facilitates stasis and prevents (freer) movement through the differentiation of spaces.

Artifacts, technologies, and objects in general carry with them specific conditions of possibility, inscribed in their design and production (Akrich & Latour, 1992). Their work depends on such conditions, which have consequences for the type of subjects that are enacted. A fork, for example, is effective for its designed use only if what needs to be forked is soft enough; razor wire does its intended job as long as someone or something can be potentially hurt by the sharp razors; IP CCTV camera systems need a fast internet connection to work; and a city-wide CCTV system needs monetary resources and institutional governance to manage it. In short, any specific

tool or technology has inscribed in its design the social, physical, institutional, or financial circumstances that are necessary to effectively carry out its functions according to design.

The conditions of possibility for the technologies on display in the fairs I visited were not made explicit, though they were nonetheless crucial to the type of (political) work these devices do. The existence of any condition of possibility opens these technologies to the risk of failure because not meeting these conditions faults the work technologies were designed to do. However, when these conditions are not met technologies can be used in unexpected ways (or unintended from a design standpoint). Most importantly, conditions of possibility are never fully present or fully absent. They change and morph in relation to the context where the technologies are deployed. And when the context changes, so does the political work that these technologies do, although they remain constrained by the social relations that "make up the machine" (Grint & Woolgar, 1997: 93). Razac's (2002) case of the barbed wire shows this clearly when he tells how the wire, which was invented in and for the North American prairie, was transferred to the European battlegrounds of the First World War, where the conditions for its use changed dramatically. There were no cattle to contain and no vast plots to be fenced, but rather enemies to keep at bay and slow down in their attacks. The wire became an obstacle that made crossing certain lines perilous and deadly. As the conditions changed, the work of the wire morphed into something else, and in the process, the subjects that were enacted changed too. While in the American prairie ranch-farmers as landowners and Native Americans as dangerous others were the subjects that the wire contributed to enacting, in the European battlegrounds, another subject came to the fore, that of the enemy of war and its corpse entangled by the wire. While the Native Americans were different subjects than the First World War enemies, they are similar in that the wire helped enacting them as someone to be contained and kept from crossing certain lines. Likewise, when residents of wealthy neighborhoods in Nairobi install in their own homes security technologies like CCTV, that were designed for crowd surveillance and public spaces, their conditions of possibility change together with the subjects that are enacted. Danger does not come any longer from large numbers of

unknown people that need to be surveilled, identified as dangerous, and eventually prevented from action. Rather, home CCTV suggests that danger comes from known employees who are already suspected to be dangerous.

In Nairobi's residential neighborhoods, barbed wire, metal grates over doors and windows, and tall walls appear alongside more high-tech solutions. Among the latter there are alarm systems that integrate different sensors of movement, heat, light, temperature and cameras into one "smart building solution," as one of my interlocutors marketed his company's product. The operations manager at a large security company in Kenya considered "smart cameras" more objective, fair, and efficient because of their technological innovations. However, as I will expand upon later in relation to this specific example, the political consequences in terms of discrimination and differentiation do not disappear based on the higher technological sophistication of such devices (cf. Woolgar & Neyland, 2013). According to Latour, the difference between an "ancient" and "modern" technology is not in the objectivity or neutrality. Instead, a more modern or "advanced" technology "translates, crosses over, enrolls, and mobilizes *more* elements, *more* intimately connected, with a *more* finely woven social fabric" than the ancient or more "primitive" one does (Latour, 1994: 47, emphasis added). Both types of technologies mediate inclusion and exclusion, differentiation, and the enactment of subjects.

The deployment of security technologies, as epitomized by the barbed wire, is entangled with the production of specific spaces, another important aspect of their political work. The enactment of political subjects and their differences that I emphasize in this chapter brings to mind what, in her ethnography of Caribbean cities, Jaffe calls "spatial process of categorization" (Jaffe, 2016: 47), a tool to understand when and how differences translate into inequalities and are entangled with the social production of space. Spaces and subjects are, as much as subjects and technologies, in a relation of "reciprocal definition" (Akrich, 1992). In the everyday security practices of residential and commercial compounds in Nairobi, differentiated spaces are both the condition and the context where these subjects and their relations are enacted. Simultaneously, however, these spaces be-

come the outcome of the same relations. Differentiated spaces, while they are a product of the deployment of several technologies, do similar work and become security technologies themselves. They enact what Jaffe and de Koning call "everyday spatial regimes" (2016), that is, those shared norms of who belongs where. These norms are not necessarily antecedent to the implementation of certain security technologies, as this relation is reciprocal as well. They are enacted, reproduced, and reinforced through security practices that mobilize objects and technologies.

In this chapter I discuss the contribution of security artifacts particularly to the processes of political subjectification. As I already mentioned, state enactments and political subjectification are entangled in the same empirical instances. In approaching political subjectification as a "state effect," it is important to keep in mind that they do not unfold necessarily in relation to formal state or governmental institutions (Trouillot, 2001), but through the diffuse work of the assemblages and their elements: private security companies, private guards, residents, alarms, barbed wire, etc.

As I privilege the role of non-human entities in processes of political subjectification, I foreground the relevance of various spaces in Nairobi and how they shift from a context for security practices into security technologies themselves. I show how some categories of people are *made* (not) to belong, and *enacted* as dangerous or in need of protection, in practices where people, artifacts and spaces are at work together. As I framed in the first chapter, technologies are not an outcome or a pre-existing condition, as neither are subjects. Instead, objects and technologies change meaning and do different work in relation to the socio-material security assemblage they are part of. As such, they contribute to specifying and materializing the differences of various political subjects, and to categorizing individuals in terms of danger and safety. The people that technologies are meant to protect, most of the time the residents and patrons of commercial spaces, are reminiscent of the citizens who Isin (2002) identifies as belonging to the historically diverse types of cities. Those who threaten to breach through such technologies are the dangerous subjects. Yet other subjects emerge as mediating professionals in the processes of selling, designing and installing security tech-

nologies. Others still, like security guards, shift between being enacted as subjects who provide security and subjects who are themselves dangerous.

The identification of (non-)danger through technologies

While any object or technology does political work, the specific tasks they are expected to carry out specify the type of political work. Barbed wire, for instance, keeps all bodies out of a specific space, while facial recognition technologies are geared towards the identification of (dangerous) people. Grint and Woolgar suggest that the emergence and the design of new types of microcomputers in the late 80s and early 90s "configure the user" (1997: 71) by setting the parameters for the user's action. It reminds us of Akrich's (1992) point, as subject-users and object-microcomputers are reciprocally defined. Similarly the use of technologies for the identification of danger, does not simply recognize dangerous people as if they were roaming the streets of Nairobi with an identifying tag. It is the way in which technologies are deployed that enacts some as dangerous subjects while others as non-dangerous ones. These types of technologies, therefore, are not the same independently of where they are and how they are used. Depending on the context in which technologies are brought in, their own workings change too.

Let us take for example the "Underbelly Vehicle Scanner" installations, which are a rising technology in the commercial spaces of Nairobi. They are often installed at the entrance of shopping malls or other parking lots. They are quite inconspicuous devices; so much so that I started noticing them only halfway through my fieldwork after Timothy, a security technology sales manager, pointed them out to me during a round of inspections of his technicians in a shopping mall. They are buried under the ground at the level of the tarmac and scan the undercarriage of vehicles for explosives. Other examples are the very sensitive walkthrough metal detectors, the same kind that were ubiquitous in any airport before X-ray scanners were introduced. Both devices are subject to manipulations by their operators, and the identification of danger does not rely solely on either of the two: the human or the machine. The identification of a person as more or

less dangerous is achieved together. It is in this process that the political work that technological artifacts afford changes as well.

As I briefly sketched in the first chapter, in the Westgate mall events the attacker entered the building through the parking lot with a carload of explosives. In the aftermath of the attack these sorts of devices spread exponentially. They assisted the management of shopping malls in Nairobi in showing how they took the concern with terror attacks seriously. Such devices contribute to an image of malls as secure places, safe for consumers and customers, and, depending on the neighborhood, safe for upper-class residents and expats to enjoy shopping and late breakfasts on the terraces of various cafes and restaurants. Though there were many times I was let through without a thorough search, it is still true that driving into any shopping mall in these neighborhoods after the Westgate attack meant undergoing a bit more thorough security checks. Security guards started asking every driver to at least open the trunk of their vehicle and maybe search the underside of the car, either with Underbelly Vehicle Scanner especially designed for the task, or with a simple mirror on three caster wheels and a long handle. Often guards asked drivers to open the doors of the vehicle so they could check the glove compartment and make sure – by what seemed more like caressing the interiors than searching them – no explosives were stuffed in the seats. Sometimes drivers and passengers were asked to get out of the car to complete a more thorough check. Vehicle checkpoints are probably second in numbers only to walkthrough metal detectors erected at pedestrian entrances of malls and large buildings. While I never stopped noticing the sizable presence of private security personnel and the technologies they operated, they slowly became a usual sight.

One particularly revealing episode showed the enactment of both dangerous subjects on the one hand and non-threatening subjects on the other. Towards the end of my first eight months of fieldwork, two colleagues from my research team came to visit Nairobi. One morning we left my house and drove to a shopping mall for breakfast. We headed towards the back-entrance gate for the underground parking lot underneath the mall. As we approached the security check for the vehicle, our car was stopped between

two boom gates that opened only one at the time, to prevent uncooperative drivers from driving through and skipping the security check. Two security guards (from one of the companies that in Kenya are referred to as "the Big 5s") manned this post and they opened the car doors, asking us to get out. They casually looked into our car and then we were let through. After we parked the car, we walked towards the staircase that brings one from the center of the parking lot to the main floor of the shopping mall. From there we could finally access a café for breakfast, but not quite yet. A circular glass wall, whose only door forced clients and visitors through a specific path, fenced the lobby's staircase. The door opened in front of a walkthrough metal detector manned by two security guards. As usual, next to the detector a small table allowed visitors to deposit metallic objects and bags, which were then looked into by the security guards. Like the arrangements of military vehicles and barbed wire during Operation Anvil (see Chapter 2), this material arrangement created an obligatory path for accessing the mall.

One of my colleagues was the first to go in. She deposited her bag on the table on her right-hand side. As she went through, the metal detector made that usual sound announcing to everyone around that she was carrying something metallic, and thus possibly dangerous, on her body. As I walked through the machine behind her, she realized that the annoying beep was singling her out so she immediately turned around to go back. Facing each other I nonchalantly urged her to keep walking. "But … I beeped!" she said in alarm, her eyes showing her anticipation of having to go through the loop several times like in an airport, offering all of her possibly dangerous objects one after the other, until the machine would have silently announced her metal-free. "I know," I told her while we kept walking ahead, suggesting that it did not matter. The guard also signaled with his hand that she could walk in. Security companies usually follow the policy that only female guards can search a female guest, and there was not a female guard to search her. We collected our belongings from the side table and let the guards peek into our bags. When this was over we walked to the terrace and enjoyed our breakfast, discussing the possibilities of someone coming in carrying some serious explosives.

The metallic objects I myself accidentally brought into several shopping malls often went unchecked. The same happened to the gun belonging to Frank, a friend and colleague of a private security company manager whom I sometimes saw after-work hours. I met Frank one night in a bar. He – a former soldier – regularly entered several shopping malls with concealed firearms, by "just walk[ing] in." When he recalled some of these moments for his colleagues, and me especially, on the rooftop lounge, I realized that everyone in that crowd was probably armed and had somehow sneaked through security. Similar stories circulate among the managers of the Nairobi security industry, a source of amusement for those who recount them. Arshad, the instructor of a Hostile Environment Awareness Training (HEAT)[1] I took in Forestgrounds, a middle-class Kenyan of Asian descent, admitted to me several times that he was able to "intimidate" security guards at shopping malls into not checking him. On the other hand, Ashan, who works as a security guard in Forestgrounds, told me of the painstaking checks that he has to go through when entering a shopping mall, by the hands of his own colleagues. He thought that his private security guard uniform alongside his appearance did not help smooth the process of getting into a shopping mall, and actually marked him as potentially more dangerous than my colleague, Arshad (the HEAT trainer), or myself.

The small Swiss army knife that I sometimes brought into shopping malls in order to experience the searching and negotiation of my own access in these spaces was rarely found or considered dangerous. However, it would have taken on a different meaning and sparked different reactions altogether if it had been on Ahsan's body. For once, since Ashan was checked more thoroughly, the knife could have been found more easily and frequently, and the guards would have considered it a dangerous object. Although the metal detectors are designed to detect metallic objects, they need an operator to work together with this device – to react to the beeps – much like the case of the use of visual technologies in telling civilians and combatants apart in Afghanistan, as suggested by Wilke (2017). The beeping of a metal

1 In April 2015 I attended a three-day HEAT course, especially tailored to the residents of the neighborhoods where I conducted my fieldwork.

detector can take different meanings in relation to what sets it off, where, and who is manning the metal detector. The (non-)reaction of the security guards to the beeping of my colleague changed the sound from a signal saying "metal passing through" to one saying "someone who certainly belongs in this mall-space passing through." The security guards' reactions to Ashan's beeps, on the other hand, mark him as a person who could be bringing in potentially dangerous objects, and as someone who is not welcome and non-belonging in the consumption space of a shopping mall.

It would be misleading, however, to think that this specific political categorization of myself, my colleagues, and Ashan fully rests in the hands of the guards. The metal detectors are crucial elements in the relation between customers and guards, as it is their beeping that affords a certain range of actions. That the device does not decide who goes in or out *by itself* does not mean it is not active in the security work of which it is part. The work of object and technologies is not about intentions but rather about making a difference, engendering a change, and thus mediating the enactment of political subjects (see note 6, Chapter 1). Once the device beeps, the guard is allowed and legitimized to search the customers more thoroughly or let them through. The beeping becomes the audible sign that the guards are allowed or even required to ask more of the person passing through. While those wanting to pass might resist these practices, the metal detectors effectively legitimize the guard in being more invasive. In some cases, like for instance the boom gates between which my car was blocked for the search, the presence of certain objects makes some situations less negotiable.

Though metal detector technologies might be designed to reveal the impersonal threat of a piece of metal, this changes once these technologies are installed and placed in security assemblages in which they cannot work without an operator. While they are very effective and efficient in telling whether any metal has passed through the detector device, they do not recognize specific threats that may be attached to such objects. Objects – and in fact bombs too – do not enter a shopping mall on their own. They are necessarily brought in. It is at the gates of shopping malls and other large buildings in Nairobi that *who* brings something in becomes as relevant as *what* is brought in.

Subjects of Security Technology

In this section, by foregrounding the active work of technologies, I detail how four specific political subjects are enacted: the "dangerous others," the "distrusted security guards," the "residents looking for peace of mind" and the "mediating professionals." As I just discussed, the identification of danger never happens on its own; it is always negotiated between the technology, its user and its target. These four subject categories, and the relations between them, highlight the ways in which different groups of people are included or excluded to varying degrees through security practices that enroll the same objects and technologies. The dangerous others, and to a slightly lesser extent the distrusted security guards, tie closely to the specific imaginaries of danger that I analyze in the next chapter. The dangerous others resonate with the thug and al-Shabaab, while the distrusted security guards connect to the inside job.

The Dangerous Others

During an interview with a manager of a major international security company in Nairobi, he introduced me to alarms that can be partitioned. He turned around behind his desk, pulled up a clean sheet of A4 paper from an outdated inkjet printer and started drawing on it. Humanlike figures and an imagined floor plan of a house were drawn together with key words to remember: "code," "kitchen," "sensors." These types of alarm can have more than one code to be deactivated differentially, depending on the time of the day or the area of the house. He suggested that the residents of the house would have the master codes, which could completely arm or disarm the system. Possibly, they could also have a code for the night that would fully arm the alarm in the living area and only partially in the sleeping quarters. Most interestingly, he suggested that the residents could also be provided with what he called a "maid's code," which could be given to the domestic workers. This particular code would disarm – in the manager's example – only the kitchen and living room, allowing the maid to prepare breakfast while the residents slept in, or do her chores while the owners were away. This solution could also work when the residents were away for longer pe-

riods and wanted their domestic workers to keep to their daily tasks, but only within designated spaces. This type of alarm, with different zones and a "maid's code," creates invisible boundaries within a private residence. While some areas are made more accessible to everyone in the house, like the kitchen for both residents and workers, other parts are made less accessible. Simultaneously the domestic workers, by way of not breaching these boundaries, also participate in making them palpable.

This particular function of alarms addresses an assumed worry on the residents' part about a possible inside job. As I will discuss more in detail in the next chapter, within a collective criminalization process of domestic workers, uncertainty about the specific identity of dangerous types and inter-personal relationships between employees and employers produce some exceptions: Jan, a European national who works for an international organization, trusts his security guard to the point that he showed him how to get to the safe room, where he and his wife would hide "in case something bad happens…" Though not inevitable, of course, the collective criminalization of domestic workers in the example of the alarm is inscribed in the "maid's code." While the untrustworthiness that is often attached to domestic workers is "made durable" (Latour, 1990) in technological devices, such durability cannot mean fixity and inflexibility because in the deployment of diverse artifacts, frictions with other security practices and failures are more than common.

CCTV cameras, probably the most representative example of large-scale anonymous surveillance, offer instead an opportunity for analyzing how only some specific people are enacted as dangerous. CCTV installations come with a specific assumption about their effectiveness, or as I discussed earlier, they come with conditions of possibility. While they cannot prevent something from happening, at the very least they are instrumental in discovering who did what – "post mortem," as Arshad, the HEAT trainer in Forestgrounds, often dismissed the worth of these cameras. For instance, expectations for facial recognition technologies – to name but one – depends on an infrastructure that in Nairobi is mostly unavailable. Besides the technology, with its software and hardware, such a system requires a

large database of "faces" to be associated to names. This option, in turn, would meet some standard of efficiency and effectiveness if each name were linked to a reliable address where this person could be found. This is virtually impossible in a city with more than three million inhabitants where obtaining a regular ID card requires interminable long queues and a process riddled with papers, stamps, and bribes; and where the postal system works on a PO box basis.

In Nairobi's residential and commercial premises, then, cameras often become a surveillance system geared towards people that are already known – such as maids, house help, laborers in general and, last but not least, security guards. One brand of such systems indeed markets itself as "nanny cameras." On the company's website it says that such cameras respond to the several parents that have shared "their personal experiences with nannies 'gone bad'" and who, "unfortunately since they have to work, [...] are forced to leave their innocent babies with them."[2] Cameras in this situation become the instruments to surveil someone already seen as likely to commit misdeeds. However, diligent employers in Nairobi – many interlocutors suggested – are expected to collect copies of IDs from their employees, pictures, reference letters from former employers and, crucially, a reference from the chief of the village where the employee's family comes from or lives. While similar practices are widespread in different contexts due to bureaucratic reasons, the collection of personal data and documents (and at times the original ID cards)[3] of employees in Nairobi is regularly justified by a context of suspicion and mistrust.

The trend towards increasingly sophisticated technologies reflects what many members of a WhatsApp group named "Crime Alert" often posted in

2 http://nannycameraskenya.com/about-us/.

3 In 2016 a particular case involving a private security company made the front page as the management kept in a safe all the original copies of ID and other documents of the security guards it employed. Besides being it illegal and showing profound distrust (see sub-section on security guards), it also made the employees subject to blackmail. Furthermore, it became impossible for them to be hired by another employer or to apply for any other vacancy in a different company without an identification document.

the chat:[4] "thugs are getting smarter." A sort of mantra uttered by Nairobians as a commentary on both the believed ubiquity of thugs (see Chapter 5), and on the creative ways in which crimes are often carried out. High-tech artifacts suggest that the protection they are able to afford is against a specific kind of threat: a danger that is vaguely embodied in someone very crafty or a sophisticated villain able to circumvent such security devices. Thugs are getting so smart in their criminal activities that only equally sophisticated systems or counter-actions can decrease the danger that he or she poses. Between thugs getting smarter, and residents installing increasingly more sophisticated technologies, finding where this circular process of reciprocal definition started (Akrich, 1992: 220) seems to be an evasive quest. What it instead points towards is the specificity of the type of danger that such technologies are geared against, especially if compared with other types of security provision practices.

The residents of wealthier areas, besides being able to access highly sophisticated (and expensive) technology, can resort to a vast supply of cheap and relatively unskilled labor to protect their gates and their premises. While this might mitigate the need to invest in expensive security devices, both often go hand in hand. Mobilizing security guards introduces other protective devices and tools in the security assemblage. One among many is the ever-present nightstick of the security officers who stand guard behind gates and in the patrol cars. Even more ubiquitous are the guards' own bodies, which in the world of security labor is laden with meaning and symbolism (Diphoorn, 2015c; Larkins, 2017). The presence of a guard at almost every gate of residential neighborhoods in Nairobi is possibly the most widespread and yet the least trusted way of providing security in Nairobi.

The deployment of technologies like nightsticks and barbed wire, and the security guards themselves suggest other characteristics of the threat, and possibly another kind of danger than the crafty and sophisticated villain. Danger here resembles an opportunistic thief, an unskilled swindler, prob-

4 A resident of Forestgrounds, whom I frequently met when I joined night patrols in his neighborhood, invited me in this WhatsApp chat group.

ably the occasional thug, who can be easily dissuaded from his or her criminal intentions by barbed wire, a poorly designed metal-bar gate like the one I had in my own apartment, and the often-frail bodies of security guards, whose physical fitness usually diverges from worldwide images of well-built security workers. While the villain with sophisticated criminal skills seems to be staged in the security fairs and salons (and the few high-end buildings in Nairobi where more recent security measures are actually installed), the threat enacted by less recent security technologies comes with a more tangible physicality. While CCTV cameras rely on the presence of identifying features on bodies, walls, iron bars, nightsticks, and private security guards are deployed against someone who needs to be kept out of a perimeter beyond and before his or her identification. The conditions of possibility for the effectiveness of these devices lies in the fact that the body that they are trying to keep out can be hurt and cut by razor-sharp barbed wire, or that it could be either dissuaded to enter or – eventually – beaten up by security guards.

The physicality of a tall fence-wall, especially when it is rimmed with coil of razor wire, goes hand in hand with the physicality of a thuggish body that needs to be kept away from a compounded space and instead relegated to the outside. The boundaries enforced through zoned alarms with a "maid's code" are not as physical and visible as barbed wires and baton-armed security guards, yet they remain particularly effective since they are geared to specific and already known domestic workers. However, both are stringent boundaries between a bounded and an open space (Jaffe, 2016), one enacted by a wall and the other by a code. Dangerous types are, and need to be, kept in open and unprotected space, while safe and bounded spaces belong to the residents. Spaces and subjects are thus enacted simultaneously.

Distrusted Security Guards

Security artifacts and technologies in Nairobi do not only contribute to the enactment of subjects as either criminals or deserving of protection. Their political work extends to their operators as well, or, alternatively, to the security workers they aim to replace. In Nairobi, private security guards are

regularly distrusted or considered incompetent, malicious, or ineffective. In a sort of technological solutionism more and more technological devices are geared to reduce, to some extent, the human influence in security provision. This often translates into replacing security guards with alarm systems, automated gates and the like. Other technologies, instead, employ devices to surveil the work of the guards themselves.

During my time in Nairobi, one particular type of camera seemed, at first, to fit the description of a technology that eliminates human influence. I was sitting in the back of a pickup truck with Jack, a former British military officer and the operation manager at a security company, on our way to a training facility where guards were being prepared for mobile response duty. He was excited that his company started to promote "smart cameras," or so he called them. Smart cameras are considered smart – he explained – because they "remember" recurring and non-threatening scenes. The smart bit of it, he clarified, is the software that controls these cameras. It accepts the inputs of many cameras at the same time and all of these feeds are shown as a mosaic on a screen. When a camera detects an unusual scene, the software zooms in to its specific feed and an operator (in the example my interlocutor was telling me about, this operator would be sitting in a "bunker in London") flags it as safe or threatening. If the same kind of scene presents itself again in front of a camera plugged into the same system, it will be ignored if it had been previously flagged as safe; otherwise, an alarm will be activated.

The way he described these devices highlights their credited ability of eliminating human decision-making, usually believed to be a positive improvement. However, smart cameras rely on human operators, as much as the metal detectors of the previous examples. They flag, as Jack put it, some scenes as dangerous and some as not. In his example, the operator was sitting in a bunker in London. For him, seemingly oblivious to the British colonial legacies of ethno-racial classifications in Kenya, this was a solution to "avoid tribalism," which he apparently assumed to be the standard in the Kenyan context. Yet the physical distance cannot be equated with a reduction of the intricate relationships between humans and technological devices, from their design to their daily operation. Assuming for a moment

that this solution could potentially "avoid tribalism" because decisions are taken outside the context where "tribes" matter, it does not mean the system avoided discrimination altogether. According to the way Jack described it, the system's design relied on the presence of a person whose task is to actually discriminate between different types of scenes and people on a screen.

In the transfer of this technology from one of the several technology companies in Europe, the US, or China,[5] something changed and made it specific to Nairobi and its context. In this example, the desiderata of a human-bias-free solution seems to be specified by specific distrust towards Kenyan security guards and CCTV operators. It assumes that the Kenyan security workforce (or African in general, since the example suggested London and not Kampala or Dar el Salam) would be profiling scenes and people based on a "tribal" bias. On the contrary, for my interlocutor, the placing of the control room in a bunker in London brings an aura of fairness and neutrality due to physical and cultural distance.

This, along with other efforts to promote technologies that control, surveil, or substitute security guards at residential or commercial gates and other locations, confirms that the human influence to eliminate is that of low-skilled security laborers. This was made particularly clear during a conversation with two residents in the large driveway of a gated community in Forestgrounds. I was strolling and having a chat with one of them, in the hope that he would invite me (or help me get an invitation) to the neighborhood policing organization of which he was a member. Instead, in our conversation he focused critical attention on the guards, who he said never took responsibility for their mistakes. In the mean time another resident came out of his house and joined us in the conversation, generally agreeing with his neighbor. He added that the security committee of their gated community looked into the possibility of installing an access control system with intercoms and automated gates. To him this solution was more reliable, safe, and, most importantly, it circumvented the incompetence of the guards. On

5 Most of the security technology in Kenya is imported from Europe, the US, and China.

the other hand, he also stressed that the costs of this project, albeit not prohibitive, would substantially dent the community's budget and some members were not keen to pay. They therefore shelved the project and opted for keeping the guards on duty at the entrance gate of their compound. Given the little labor protection that security guards enjoy, this was much cheaper for the members of the gated community, though they considered the guards themselves to be unreliable, and at times a security risk themselves because of their poor performances.

In some contexts, however, the presence of security guards is a necessity and replacing human labor is not possible. Instead of replacing the guards altogether, large gated communities and commercial compounds in Nairobi installed specific devices to surveil and control the guards themselves. Among the most diffuse ones are different types of checkpoints, especially for guards on night duty. These checkpoint technologies are of several types. Some involve fingerprint scanning, others dialing a code, others just coupling a magnetic key to a receiver. Some of them are controlled remotely through wireless connection, while others only memorize the time of the check in. Independent of type, most of these systems require some action to be taken by the guards at pre-determined intervals. When these systems are designed to make sure that guards are patrolling their assigned territories, and not sleeping, several checkpoint receivers are installed in different locations. If the system is controlled remotely, the control room staff expects to receive a signal from each of these locations in a specific sequence. In more recent systems, the guard is given the next location to check-in in a (seemingly) random order. If some of these procedures fail, the staff in the control room would send a MRT to check in with the guard and patrol the premises. In a surveillance spiral, these surveillers are thus also surveilled (Diphoorn, 2016b), since the vehicles of the MRTs are also equipped with similar receivers, to make sure that the area supervisors of a security company actually check on the work and location of the MRTs.

The drive to eliminate or reduce the influence of security guards seems to be deeply seated in the distrust they are regarded with, both by residents and their own managers. The implementations of specific technologies that

can be used to substitute security guards or surveil them inscribe such attitudes in hardware systems that require guards to prove that they are awake and patrolling. The political work of these specific technologies is multifaceted. First of all, rather than as security providers, security guards are enacted as a security risk, as potentially dangerous people, who albeit are not necessarily malicious, cannot be trusted. Furthermore, the guards subjected to these surveillance systems are not trusted as honest employees at all. Asking them to check in every few minutes (sometimes more or less frequently, depending on the distance they need to patrol) assumes that they would not care enough or be honest enough to faithfully execute the tasks with which they are mandated.

The security technologies and the objects that are deployed in Nairobi do not contribute to the enactment of guards only as subject of surveillance or as the human influence to be substituted by machines. Objects such as nightsticks, for example, which are the most diffuse tool that security guards are provided with, contribute to putting the guard in a position of ineffectiveness, highlighting how defenseless they are in the face of better-armed attackers. Most guards considered the nightstick a useless tool. Over the course of my fieldwork I got acquainted with and close to those guards who were harshly criticized by the residents just above. Their nightsticks were most of the time hidden or jammed between the sheet metal roof and the wall of their shed, a location that did not communicate preparedness. One day, when I questioned them on the reasons why they abandoned them, they picked them up, looking reluctantly compelled to make up for seemingly unprofessional behavior. Yet they seemed mostly uncomfortable with those objects. At first, remembering the training of the MRT guards I participated in, I assumed it was because of the little time companies usually dedicated to training their guards on baton combat skills. Later, however, one of the two guards plucked up the courage and sarcastically asked me: "What should I do with this? What can I do when someone comes with a gun?" He looked at me raising his eyebrows almost as if waiting for a definitive answer while I only nodded acknowledging his not-so-hidden argument. Continuing his play, he ostensibly held the nightstick far away from his body with only two fingers, and dropped it to the ground, signaling surrender to a hy-

pothetical robber armed with a gun.

While this last episode ties in well with the discussion in the previous chapter on the ban prohibiting private security companies from carrying firearms, it also signals how the value of the nightstick remains uncertain. On the one hand, it is the most diffuse weapon with which the more professional companies kit their guards. It is part of their uniform. It also comes with the expectation, by companies and residents alike, that such a tool needs to be handy and ready for deterring criminals in a close combat and provides some protection to the guards. On the other hand, the training that guards usually receive on how to handle this tool and how to use it as a defensive or offensive weapon is poor at best. This might be one of the reasons why the two security guards seemed very uncomfortable with handling them. While not all robberies involve firearms, the guard miming being held at gunpoint implied that these are a very likely occurrence. In such situations, the disparity of weaponry seems obvious and the guard's argument convincing. In a robbery where the criminals would not be armed with guns, however, it is the training and confidence in the use of the nightstick that should give the upper hand to the guards, but instead seems to be lacking. Thus, guards who are untrained in the use of a weapon that is often already considered ineffective, are enacted as unready for the job, and consequentially are met with criticism and distrust, and relegated to the task of opening and closing a gate.

Residents Looking for Peace of Mind

In this sub-section I discuss how the residents of the upper-middle class neighborhoods where I conducted my fieldwork are enacted as the subjects to be protected. I show how objects and technologies contribute to this goal, which is articulated by my interlocutors as looking for peace of mind in their own private homes. For many residents this is a state of being to which they continuously aspire. It is never obtained once and for all, and it always necessitates continuous laboring and tinkering, especially in relation to security objects and technologies.

This aspiration of achieving "peace of mind" came up multiple times during my fieldwork. Lisa, a middle-aged European woman, had spent most of her life in Nairobi and was now living in Highsprings. I met her several times, and I could not help but notice that she had very strong opinions about guards and security technologies. She felt that many people placed high value on having a guard because this gave them "peace of mind" – like Jan, Lisa's neighbor, who showed his guard how to access his safe room. Lisa's own peace of mind came from having installed an alarm system that she had personally "invented" and designed. She was particularly confident about the system's effectiveness because she made it "basically independent from human beings." If someone touched the electrified wires that fence her garden, an alarm signal would be sent directly to a private security company, which would then quickly send an MRT. This, she explained, dramatically shortened the response-time, because the system was no longer dependent on a panic button activated by security guards, who were likely to be either asleep or to have colluded with intruders. The automatic alarm signal was also much faster than activating the panic button by herself, as she would most likely wake up only too late should robbers attack at night: "The advantage is that I can open my electric gate from inside the house. I don't need a human being who is probably already bundled in a corner, or has, maybe, collaborated with the intruders anyway…" The way she handled her private home security resembled the policies of her own residents' association in this upscale neighborhood. The association had privately financed the installation of CCTV cameras, street lighting, highly regimented procedures of garbage collection, and boom-gates at the few entrances of the neighborhood. These measures of "self-protection" – she said – helped her move towards peace of mind.

For her, thus, peace of mind came directly from relying on technological artifacts and a system that she had personally designed to match her own needs and wants. Furthermore, the elimination of guards, or the reduction of human influence in general, simultaneously decreased her perceived risk of having other unwanted people in her house and neighborhood. When I went to visit her for coffee, for instance, I was only allowed in through her gate because we had previously been in touch via SMS. Once in front of

her gate, there was no way for me to communicate with her, except through my own mobile phone. Seeking independence from other human beings in their own personal security practices not only enacts residents as subjects seeking peace of mind, but simultaneously enacts the guards as a security risk, as dangerous subjects who threaten such peace.

While one might think the peace of mind Lisa is looking for is reached once various technological artifacts have been installed, it actually requires laboring, tinkering and constant alertness. This was clarified by Arshad, the HEAT trainer in Forestgrounds. Lisa's strategy of relying less on guards and more on objects and self-designed hardware systems resonated with Arshad's own approach. During the HEAT course, he tried to show us how mundane and everyday objects could actually be used as a security technology and increase the chance of not becoming a victim, or of surviving a difficult situation. His personal preference was, for instance, to live in an apartment on a higher floor because it was much easier to defend it from intruders in comparison to a detached house. He had countless suggestions, which took into account his clients' lifestyle, the layout of their house and the type of car they drove. Among others things, he promoted the use of manually activated loud sirens, water bottles and spare mobile phones stocked in the boot of cars, first aid drugs and kits, valuables ready to be handed over to robbers, and a safety door between a designated safe room and the rest of the house. Such reliance on objects is not exclusively dependent, however, on the initial installation of an item in the right place. It requires work. It requires maintenance and routine checks. Is the mobile phone battery charged? Are the drugs past their expiration date? Do the sirens work? Is the list of emergency phone numbers up to date? It shows how, for the HEAT trainer, this was a process that needed continuous adaptation.

These examples point towards two distinct yet interconnected points. First, it shows how technologies or objects are not defined a priori with respect to their functions. In a socio-material assemblage they are defined reciprocally in relation to their users, and together they afford specific modes of interactions. For instance, I had to message or call Lisa in order to be allowed in her house instead of buzzing a doorbell or asking a guard to open the gate.

It became apparent how the material security arrangements she had opted for mediated her interactions with potential visitors or people outside her house. Second, the work that objects and technologies do in these security practices contribute to the formation of specific political subjects. The approach behind Lisa and Arshad's way of handling objects and technologies in their security practices holds together three subject categories at once: the residents to be protected who are looking for peace of mind within the private space of their own homes; the dangerous types to be kept outside that same space; and, finally, the distrusted security guards who have been altogether replaced by hardware systems, which are made "basically independent from human beings."

Mediating Professionals

Residents, however, are not alone in their search for peace of mind while they tinker with technological artifacts and other objects. Teams of sales managers and security technicians promote, sell and install security solutions for the residents as well. Through their various tasks they are enacted as subjects mediating the residents' efforts towards acheiving their peace of mind. Together with the distrusted guards, they become another subject category of security workers that emerges in relation to security technologies and objects.

During an interview, Timothy, the same sales manager who made me aware of Underbelly Vehicle Scanner devices, often repeated that his company did not sell a product, or a technology. They sold a service. While he broadly identified this service with "security," he specified it as "peace of mind:" "I don't sell an alarm, I sell peace of mind to my clients." Differently than how residents see peace of mind however, as something that requires continuous work, the way Timothy and a web commercial for nannycameraskenya.com[6] put it, "peace of mind" here seems to be a good that can be acquired, once and for all, through the purchase of some security artifact, a camera or an alarm system.

6 https://www.youtube.com/watch?v=f3y41mvII7Q&feature=youtu.be.

Timothy is also certain that his job is that of a mediator. He was adamant in making a difference between residents being able to "financially afford" a specific type of CCTV and "understanding" the same system. Similarly Mark, the owner of a renowned company focusing exclusively on electric fences, stressed this type of difference. He said that sometimes clients "don't want to get personally involved with the installation because they feel that is cheap enough to outsource the job [...]. And therefore there's a risk, because they don't understand the system. Though, it is not rocket science, you know!" Mark said that he always tried to actively involve his clients in the process of mediating between what they initially wanted and what he thought they needed.

One day Timothy invited me to go with one of his sales team's members. Johnson, a very ambitious salesman, was to carry out a survey at a client's factory just outside Nairobi. During the survey Johnson seemed very attentive and politely nodded to everything the client asked: alarm, CCTV and two security guards at the gate for eight hours a day and five days a week. While in his notebook he sketched the layout of the warehouse and of the offices precisely drawing the location of doors, windows, staircases and big machinery, he never penciled down what the client specifically asked for. Once back in the car I inquired why he did not seem to care about it. He told me that all his clients always ask for the same things. Some sort of alarm; cameras to deter their own personnel from stealing supplies during the work hours (which was in fact the client's main concern); and "guards and a security company to blame" and against whom they could vent their frustrations when things went wrong. His task now, as he saw it, was to provide his client with the kind of alarm that he actually needed, one with movement sensors for the office rooms and workfloor, and vibration sensors for the big sliding metal doors of his wearhouse and the many windows. This would have protect the client from what Johnson considered the most likely risk, that of a robbery during off-hours. He would also have provided the client with the cameras that he wanted for the surveillance of his personnel but also with the alarm Johnson believed was approrpriate. He was confident that his solution would mitigate the risk of having to manage a dissatisfied and angry client after a robbery.

While sales personnel and technicians might see their mediating work as circumscribed in the time of sale and installation, they become entangled in a dynamic and changing assemblage, because peace of mind requires continuous work. Many times while I was on patrol with MRTs in different neighborhoods, residents would press the panic button to test their alarms and response times. At times they would give advises to the security guards how to approach their own compunds and what telltale signs they should look for, in case an actual robbery was underway. Most often however, they would be unsatisfied with the service. Chakur, with whom I got close over time, was part of the latter group. He constantly involved the managers of the security company in his many tests and finetuning of his alarm system, in an never-ending quest to find peace of mind.

Like the mediating professionals, the technologies and artifacts sold and installed do not do security work in and of themselves, detached and independently from anything else. They become part of a socio-material assemblage together with residents, professionals, guards, and dangerous types. Some buy the technologies that become part of a continuous laboring process; some fix them and tinker with them; some manage them; and others try to get through them. Techniques that materialize different knowledge and expertise are necessary alongside technologies for the unfolding of these processes[7] in which different people are enacted as subjects belonging (or not) to different spaces: the dangerous ones on the street, outside, and the ones to be protected inside private spaces and often (ironically) behind metal bars. It is through these diffuse and heterogeneous processes that the work of security technologies emerges in its political consequences.

The mediating professionals and, as we saw in the previous section, the residents, show how the political work of security technologies lies not only in their relation to dangerous or potentially dangerous subjects; the technol-

7 In her analysis of a crime control pilot study at a bus stop in Amsterdam, Grommé (2015) shows how the "detection of aggression" through artificial intelligence technology required continuous "tinkering" that involved the companies developing the aggression-detection technology, the police, bus drivers and other stakeholders.

ogies that the mediating professionals sell and install, and the systems the residents tinker with, do just as much, though in different ways, in enacting safe spaces and the subjects who belong to them as in need of protection while they are concerned with finding peace of mind.

Conclusion

In this chapter I have detailed how different political subjects are enacted through the deployment of technological devices in security practices. The enactment of these subjects and the differentiations between them highlight the political work that objects and technologies *do*. Some subjects are made to belong to the safe interior spaces of houses and malls, while others are made to belong to the outside, and are simultaneously enacted as potentially dangerous. The rather general category of "dangerous others" resembles other types of subjects that I introduce in the next chapter, like the thug, al-Shabaab, or the inside job. The residents in the process of protecting themselves are enacted as citizens deserving protection from the same dangerous subjects. These residents are also enacted as looking for their peace of mind often through meddling and tinkering with various security objects and technologies. Other less conspicuous subjects also featured in this chapter. They are afforded by specific technologies, which require professional and skilled expertise to be operated and installed.

The subject categories that I foregrounded in this chapter are not independent from each other, and they stand in a specific type of relation to one another. The dangerous subjects became the primary concern of my work for their political relevance and urgency. They show the inequality of access to various spaces, and highlight how entire categories of people are criminalized collectively and enacted as non-belonging. They are also the primary concern of the other subjects (the residents, the guards, and the mediating professionals), as people to keep out and against whom the security practices are targeted. The guards, the residents, and the professionals are enacted in their specific ways in response to the various dangerous subjects. Together, like people and objects, they too are in a process of reciprocal definition (cf. Akrich, 1992).

Similarly, all these subjects are in a reciprocal relation with the spaces they inhabit and contribute to producing. These political subjects are not only embodied in the specific maid, guard, house resident, or the "suspected thug shot dead" that I discuss in the next chapter, but they are necessarily "emplaced" (Jaffe, 2016). The house workers are enacted as dangerous subjects as long as they are in an area of the house not designated to them, while they are enacted as non-dangerous while they go about their daily tasks in the kitchen. Security guards are considered dangerous because they are, literally and figuratively, the gatekeepers at the border between a safe inside and a dangerous outside. Residents seem to seek peace of mind by continuously tinkering with walls, alarms, fences, and metal grates that enact some spaces as dangerous and others as safe. Residents and the mediating professionals together tinker with spaces, change them, fence them, and otherwise make them work against the dangerous subjects. All the various spaces I foregrounded in this chapter are thus simultaneously a product of security technologies and objects, while they become themselves a security technology towards the peace of mind of residents. Similarly, the deployment of security objects and technologies in different spaces (cameras in the interior of a house, barbed wire on perimeter walls, or metal detectors at the entrance of shopping malls) transforms these spaces. Spaces become security technologies themselves and they also contribute to categorizing specific people as (non-)dangerous subjects. These spaces within the assemblage of technologies and the security practices that put them to work help to identify different subjects as dangerous, as unprofessional and unreliable, as mediators towards peace of mind, or as worthy of protection.

While this chapter emphasizes the use of technological devices in daily security provision practices, these devices should not be analyzed in isolation, but as part of the socio-material security practices in which they are put to work. In the governance of security in Nairobi, objects and persons are, in the words of Woolgar and Neyland, "intimately tied together as a governance pair" (2013: 187). The use of technologies is not deterministic in the enactment of subjects but it requires expertise, techniques and labor, as shown by the interventions of the technicians and the professionals in this chapter. Yet it is tempting, for instance, to uphold the rather simplistic inter-

pretation that residents together with professionals define a security device, which then goes on to enact a specific dangerous subject while, for instance, the maid is left to experience its effect and its political consequences. Since objects and people alike "never act alone" but in relation with each other (Abrahamsson et al., 2015: 15), the enactment of these political subjects is the result of the simultaneous and combined work of each element of the various socio-material security assemblages in Nairobi.