Some Thoughts On The Limits of Surveillance

The Construction of the Narrative of the Panoptic

It has become almost fashionable to dismiss the existence of any political possibility of action, to posit that everything

is determined through the use of force and the sheer breadth of its deployment, but this is a dangerous and partial vision.

Largely this view is being drawn from experiences in partial confrontations, where resistance manifests someplace for a

period of time, such as an Occupy camp or summit demonstration, combined with a completely disproportionate

understanding of the capacity of police logistics to function and monitor movements through space. Born of limited

confrontation, in which police force can be concentrated within a zone of conflict, and paranoia about surveillance

apparatuses like the NSA's, which seems to have unfortunately gotten worse since the Snowden leaks, the idea that the

state is all seeing, completely functional in all space and invincible strategically[1]has begun take root, and has generated

a passive sort of waiting[2]. From positing some form of absolute deployment with the capacity to be maintained

endlessly[3] this argument proceeds to claim that this situation could never be impacted through any action, as if action,

any action, does not cause a change in the dynamics of security, an assumption that every asymmetric campaign

undercuts. All around us we can see this hopelessness taking root, a hopelessness that tends to find currency with the

collapse of "movements" that the naïve had ultimate hope in, in this case Occupy, which was crushed through a

coordinated security operation. Often this hopelessness is counterposed by an equally naïve tendency to hold out hope

rather than to examine the roots of failure, to continue with the same methods in the hope that a breakthrough will

occur, rather than to take a sober, realistic look at the materiality of the adversary. Interestingly, this dynamic tends to

find a common core of analysis in an attempt to approach conflict conceptually, as a game of political rhetoric and

ideas, rather than come to terms with the materiality of conflict, the stakes and risks of fighting, the material

deployments of conflict, the severity of repression, and the limits of police capacity.

---

1   This has been made much worse by the tendency among the radical and insurgent scene to listen to conspiracy theorists, who take dispersed pieces of information and fuse them with a series of paranoid assumptions born out of inflated senses of self importance and a complete lack of strategic understanding to generate a vision of malicious policing structures that exist to target one specifically within some supposedly global vision.
2   This passivity of waiting exists in contrast to an active form of waiting, a process of avoiding direct confrontation, but of working to create a terrain conducive to insurrection, both through infrastructural development and minor forms of subversion.
3   Total control not only means total deployment, but the maintenance of total deployment indefinitely.   This would mean that not only would the streets be completely occupied, all moments watched and all actions repressed, but that this would be maintained into some indefinite future. The sheer logistical capacity this would take would be an impossibility, police and soldiers would have to be housed, fed, equipped, vehicles would require gasoline and so on. This was impossible to maintain in even a partial way in Iraq with 400,000 troops, with this number they physically covered very little space at any one moment; the partiality of coverage generated the space for insurgency to be possible, and the logistical toll of maintaining these operations almost ruptured US military force capacity

Through the medium of poststructuralism, and poor readings of Foucault, this idea of the all powerful state tends to concentrate around the concept of panoptic power, the ability of the state to see all action in all moments. But, this understanding of the Panopticon is fundamentally misinformed, relying on the notion that the concept of the Panopticon can be equated to actual surveillance, and that this forms the basis of mass surveillance initiatives such as bulk metadata collection by the NSA. Foucault draws the concept of the Panopticon back to Jeremy Bentham, an 18th Century British utilitarian, and his designs for prison complexes. The design centers around a tall central guard tower, from which wings of the prison emanate. The purpose is to allow the guard in the tower the ability to see all activities of all prisoners simultaneously, but this generates an important and interesting difficulty. Clearly, it would be impossible for one or a handful of guards to watch all prisoners at the same time, so the design is based around a highly specific feature -- the windows of the guard tower are opaque to the outside observer. Therefore, the structure of surveillance becomes based not on the actual ability to monitor, but rather on the possibility of surveillance; it is not that one is always being watched, but that one could be watched at any one point. The tint in the glass is meant to obscure the actual capacity of the gaze of the guard, if there is even a guard, with the assumption that the outside observer, in this case the prisoner, would have to assume that they could be under this gaze at any moment. In other words, the entire design functions through the deterrent force of possible surveillance, rather than the actual gathering of information. Not only does this fundamentally structure the Panopticon along the lines of what Foucault would go on to call biopower, the structure of power around the normativity of the body under possible gaze, but also around the hypothetical possibility of surveillance.

The central core of the functionality of the Panopticon, which was never actually built in its full form as a prison complex, has become a symbolically descriptive term for a structure of surveillance built around a transparency of surveillance, the generation of a sense in which one knows, or has distinct reason to think, that they are or could be watched at any moment. The distinction to make here is that structures that can be termed panoptic are not based on the actual surveillance of subjects, but rather on the deterrent effect of presenting the possibility of surveillance. We do see elements of this in the structure of private, and to a lesser degree public, surveillance in the United States, specifically in the form of the retail surveillance system, which may be functional, which may actually film activities, but are based largely on the clear presence of countermeasures, anti-shoplifting signs, the open presence of "loss prevention" staff, magnetic tags, clearly visible cameras and so on. What has become interesting is that this structure tends to break down when force is not applied at the point when the deterrent effect fails, or when the deterrent effect is seen as ineffective.

This becomes clear with the prevalence of shoplifting, which conservatively estimated costs $13 billion[4] each year in the US. At the point where it becomes clear that anti-shoplifting measures are not as comprehensive as they pretend to be the mythology dissipates and the practice proliferates (there are whole blogs discussing the problems with anti-shoplifting technologies and ways to avoid their functionality). Panoptic structures rely entirely on "self-policing" within a structure in which the definitions of acceptability are clearly defined, rather than on the actual gathering and use of information. The partiality of this approach is clear in the example of shoplifting, – when the structure of deterrence breaks down, or when it becomes clear that no one is watching the cameras, the entire edifice collapses.

Outside of the retail establishment we are beginning to see this structure come to be relied on more and more in certain ways. Increasingly there has become a reliance on public surveillance cameras by police departments, specifically in "high crime" areas and areas where tourists congregate. But rather than hiding cameras, what we are seeing is a more panoptic structure, with the cameras not only made visible, but a tendency to put flashing lights on them and to publicize their installation as widely as possible. Before anti-convention demonstrations we have witnessed this dynamic play itself out in the media, where the local police chief walks journalists around to the new camera locations, discusses how many have been installed around the city, then shows off their new command center, finally finishing with a warning to "out of town trouble makers." The goal here is not primarily intelligence gathering, although intelligence may result. If that were the case then the cameras would be hidden. The intent is rather to deter action. But hiding behind this is a logistical mythology, one that we can clearly see when we take a look at actual intelligence gathering. For all the cameras that are installed, the footage they generate means essentially nothing without the ability to identify targets, track targets and eliminate targets. The necessity to increase operational capacity exists in a direct relationship with the number of cameras that are installed; if there is only partial response then the mythology of total response, the basis of deterrence, evaporates, and the camera becomes nothing but an aesthetic feature, something that, maybe, minor counter-measures have to be employed to avoid.

From Panoptic Structures to the Weaponization of Information

It is fundamentally important to differentiate panoptic deterrence from actual intelligence gathering, which not only attempts to remain secret, but also attempts to weaponize information operationally. When we are speaking about

---

4   http://www.shopliftingprevention.org/TheIssue.htm

actual intelligence gathering, entrapment operations, undercover work, signals intelligence and so on there is a very different goal in mind, the gathering and use of information through the maintenance of a certain clandestinity, through the ability to monitor without being detected, and this is what we are seeing currently from organizations like the NSA. For example, the purpose of the geolocation of cellular phone SIM cards is not to allow the one being monitored to know that they are being watched, at which point counter-measures can be introduced. Rather the point is to actually gather location data and use it within a structure of increasingly fluid, small force footprint counter terrorism operations, and this necessitates the actual gathering of intelligence to go undetected. In this sense, deterrence becomes a hindrance to the attempt to gather and weaponize information, generating a focus on countermeasures among targets, rather than maintaining clandestinity and operational secrecy. The primary emphasis here is on actual operations, the identification of targets, the locating of targets spatially and the direction of operations on a target, rather than to deter the target to begin with. As such, we cannot analyze the scope of state force capacity merely through the lens of information gathering, but have to analyze it on the basis of information becoming weaponized, or processed and made into the basis of actual material operations. When we add in this plane of analysis the picture of state force capacity changes dramatically.

Weaponization occurs on two levels, whether we are discussing the weaponization of pathogens or information; firstly the material has to be turned into a usable form, then it has to be able to be deployed materially[5]. To begin to understand this idea we have to analyze two separate processes with different logistical requirements and limits, the gathering of information and the processing and weaponization of information, and then discuss this in relation to the capacity of policing and military structures to carry out operations. It is on this this level that the predominant structures of surveillance differ from deterrent based, descriptively panoptic structures that are so often discussed at length, or that we see in some cities and retail spaces. On the level of the weaponization and operational use of information we have to begin to develop an analysis of capacity, the capacity to gather information, the capacity to analyze and weaponize information and the capacity to utilize weaponized information operationally.

To begin this analysis we begin with the first link in the chain. It has become common to assume that the capacity to gather information somehow corresponds to the ability to process information, or that the ability to gather information is, in itself, important. It is not that large amounts of information cannot be gathered, but there is a distinct limitation on the level of processing, which requires the use of limited technological forms of narrowing down the signal spectrum

5   Lockwood, 2008

and the information generated in its monitoring. These forms of narrowing down data, from the use of key words to facial recognition, are necessarily based on known variables, making it impossible to detect new forms of communication, careful choices of words or unknown threats. Without an understanding of the so-called threat spectrum in past moments the structures of filtering cannot be constructed in the present. For example, facial recognition operates based on the matching of facial features and the relation of features to one another among known faces, usually faces that come from police image databases. Long ago it was recognized that clandestine operations were easier to carry out of the operative was someone that was not known, someone that did not have any form of criminal record for example, and someone that was not known to be part of an organization; this, even in times where the technology of surveillance was less comprehensive and technologically advanced, has functioned as a common tactic, along with the use of infiltration, in covert operations.

The capacity to process information is then further limited due to the "human factor," not just human error, but also the interpretive elements of information analysis and the limited capacity to process actual information. When we take a look at a computer system, and the structure of the limits of a computer system, we are still looking at a structure that is based in the limitations of the programmer themselves, and the ways that the architecture of the system is structured, a process that incorporates more contingency and choice than is commonly thought. The limits of the system then interact with the limited capacity of analysts themselves, the limits to the amount of information that can be processed within a period of time. This processing comes into a dynamic with the detail of analysis; to do thorough analysis of a subject and a network of connections, for example, takes more time and resources than to engage in a superficial analysis, even when spread out between numerous analysts. The amount of information gathered, therefore, is not the operative category that has to be analyzed, rather we have to focus the dynamic between the ability to gather information and the operational capacity to process information, and the gathering of information becomes nothing but a stream of information that, of not captured through analysis, becomes irrelevant in itself.

On a level of gathering and processing intelligence distinct limitations are reached relatively quickly, more so as the carrying capacity of the system of intelligence gathering expands. As with operations, which we will discuss later, this is a question of capacity. To the degree that we expand the amount of information that we are gathering we have to expand the capacity to process information, as well as the capacity to keep the very gathering of information secret. This not only implies the training and funding of analysts, but also their hiring, screening and training, a process that is

clearly not without error, the whistle blower is that margin of error. As James Bamford discusses in *Body of Secrets[6]*, even within the NSA this limit is reached and exceeded quickly. Within the NSA there may be 100,000 employees and contractors that are responsible for processing data on any number of levels, of which around 30,000-35,000, at best estimate, are involved in the actual analysis of bulk data that is collected. When this is compared with the amount of data that the NSA gathers[7] the problem here should be clear: there is not nearly enough personnel, and could never be enough personnel, to actually process every piece of information. This necessitates the use of filtering protocols, specifically computerized filtering protocols, but these present a problem in themselves. When one filters information one is necessarily limiting the vision of the so-called threat spectrum, there is necessarily information not being analyzed, and potential information not being analyzed. Coupled with the limitations of actual analysis, the analysis of information by human analysts, the importance of looking into the limits of this link between information gathering and information processing becomes clear.

From Weaponization to Operations

From these distinct limitations we have to then begin to analyze the final process, the movement from processed intelligence to material operations. Here, again we reach another set of distinct numerical and operational limitations. For a full operational capacity to exist, for this assumption of the absolute omnipotence of the state to function, we would have to assume that the capacity of the state is limitless and despatialized. In other words, occupation of space is not a momentary phenomena, but an actually limitless operation, one that has no specific point of termination. As such, it is not only that occupation, the maintenance of the ability to operate in an area in such a dense concentration as to be able to limit the ability for counteractions to occur, requires an immense operational infrastructure in an immediate zone, but requires the supply of these zones of operation and so on. Then, for some form of absolute capacity to exist we would have to then argue that this capacity exists in a total way, across all space evenly and without movement. Without this absolute coverage, without literally operating in all spaces simultaneously, there are always gaps in coverage that can serve as the point of departure for insurgent actions. Clearly, the logistical capacity that this would take would be impossible to imagine, a logistical absurdity. This is why occupation forces tend to concentrate in areas, deploy from safe zones and concentrate force in areas of low intensity conflict, but this far from total occupation, and it is this dynamic that constructs the space that insurgencies exploit operationally. Given that the numerical and logistical

---

6   Bamford, 2002
7   According to a number of articles that resulted from the Snowden leaks the NSA gathers 2 million text messages and 5 billion records of cell phone location data a day, and that does not include monitored phone calls, emails, web surfing information or any other form of data that they gather.

limitations of this are clear, the question then becomes one of force capacity, movement through space and the ability to utilize information to carry out operations.

The limitations of the gathering of information and the processing of information into weaponized intelligence that operations can be based on becomes relevant to the degree that operational capacity can compensate for the distinct limitations that are faced in the attempted operation of space or within the framework of security operations, both of which require a structure of occupation to more or less of a degree, in higher and lower concentrations. The concentration of occupation forces within space exists in a direct relationship to the amount of resistance that is presented within a terrain and the predictability of action within a zone of operations. As we have mentioned in other reports, insurgencies tend to function not on the level of holding space, but rather by amplifying contingency. To the degree insurgent forces become legible, and having to defend a space makes one very easily located, allows occupying forces to concentrate force at a specific location where they can contain areas and leverage their firepower advantage[8]. However, to the degree that insurgent forces can prevent being located, contained and eliminated a distinct limitation on the ability to gather intelligence begins to set in, as well as the need to concentrate occupation forces in the attempt to move through space. Though numerous technologies have come to amplify the amount of space that can be operated within and through, such as the use of cars, radios and firearms, at the end of the day, the amount of space that can be physically occupied at any one moment is incredibly limited, a space that becomes more limited when friction, resistance, is added into this movement, at which point police forces have to concentrate to move through space, covering less space.

There are two dynamics to keep in mind here. The first dynamic is the dynamic between the breadth of the terrain of conflict and the concentration of force in a space. As terrain spreads out, as more space has to be covered, the concentration of finite forces has to dissipate in order to cover space. This is a simple mathematical calculation, if we take the number of finite forces and divide this by the space that has to be covered we can come to some understanding of how quickly this dispersal of force occurs. Often, this is compensated for by protecting major lines of movement and communication as well as vital infrastructure; this limits the amount of space that is secured, but not the actual terrain of conflict. As we see in the example of American occupation forces in Iraq, roads and towns could be moved through and secured for periods of time, along with the vicinity immediately around fire bases, but the space outside of these

---

8   Russian General Staff, trans. Grau, Lester and Gress Michael, 2002; In their reportback from the Afghan War the Russian General Staff clearly documents the use of intelligence to locate insurgent forces, the development of the tactics of the isolation of areas of engagement and the movement through these areas to eliminate the ability of insurgents to operate in an area, but only temporarily.

limited areas was not secured, and it is in these spaces that the insurgency structured its logistical bases, weapons stores and training facilities, if they had any in a local area. Insurgencies function by forcing a choice to be made; in the deployment if asymmetric tactics, in which the goal is not to hold space, but to expand the terrain of possible attack, occupying/policing forces have to choose between securing certain areas or covering more space, either leaving critical infrastructure open to attack or limiting the amount of space secured. This is then combined with the level of conflict mobilized within a certain area in the resistance to occupation force operations. When occupation/police forces find themselves under attack it is common to move into defensive postures, concentrating force to repel attack, and limiting the amount of space covered more.

Though it is clear that this process of gathering, weaponizing and operationalizing information operates as a process that has to be analyzed on a step by step level in order to understand the limitations that are presented, it is also important to get an understanding of how the different aspects of this process can come to reinforce other aspects, or degrade them. As has often been discussed, the limitation of information within a terrain of conflict negatively impacts the ability to operate within that terrain, while recognizing that total information is an impossibility. This is not only due to the limits in processing, but also operational limitations as well. As terrain of conflict functions as a mobile kinetic dynamic of actions and effects that proceeds at such a pace, even in low intensity scenarios, that the ability to gather information is always outpaced by the actual flow of events. As such, surveillance tends to focus on three primary planes, human intelligence (humint), signals intelligence (sigint) and image intelligence (imint), and the various practices incorporated within these spheres of surveillance. Though sigint and imint tend to function at a distance, with the ability to capture images from miles in the sky and communications from almost anywhere on the planet, humint, on the other hand, has to always function within proximity of a target. This proximity is not necessarily spatial, and can function through a social proximity, the informant is a part o that process. But, in situations in which occupation forces have difficulty operating within a terrain for a consistent period of time the ability to gather humint becomes more difficult and the ability to understand sigint and imint becomes more interpretive and less based in information about on the ground situations. At the same time, in areas where occupation forces function smoothly, and can project across space, these forms of intelligence become easier to gather and understand. This dynamic is clear if we take a look at the fate of informants in parts of Afghanistan or even in areas of Northern Ireland where the IRA was highly concentrated in communities. As capacities increase or degrade in one area the process as a whole begins to degrade as well. The material limitations of force, combined with the limitations of information analysis, far from generating an omnipotent force that can police all time and all space, eliminating political possibility entirely, actually can be seen as a

remarkably limited force spatially operating in reference to incredibly partial understandings of terrain based in limited capacities to analyze information.

Conclusion: On Unintentional Panopticism

The combinations of the limitations that we have been speaking about above, along with the tendency of this process to become more or less comprehensive as certain elements increase or decrease their operational capacity should point to the obvious conclusion; the assumption of state omnipotence is one borne of strategic miscalculation, lack of access to specific strategic information and a tendency to allow rhetorical excess overcome operational analysis. Even though the intention of surveillance and intelligence gathering logistics within the United States, for the most part, functions through a non-panoptic lens based in actual information gathering and the weaponization of information gathered covertly, the misunderstandings of the material limitations of intelligence and operational capacity has generated a panoptic effect. In other words, even though surveillance, for the most part, is actually structured to gather actual intelligence and use this intelligence operationally, the awareness of these programs, specifically a non-specific and highly conceptual understanding of these programs combined with a general lack of material analysis of tactical capacity, has generated a deterrent effect that is not necessarily the intention of the logistical formations engaged in intelligence gathering.

We can see this with the Snowden leaks, and their aftermath; in response to a seemingly all-seeing NSA many people have begun to drop Gmail accounts or curtail online activities, at best, and have begun to feed the mentality of a total lack of political possibilities, at worst. The leaks themselves, rather than being approached as information about a limited structure that countermeasures can be developed in relation to, have begun to foster a deterrent effect that is unparalleled, and unintended. To the degree that deterrent effects are intentional surveillance infrastructure, or the image of surveillance infrastructure, becomes visible and openly publicized. This is fundamentally different then what is seen in relation to the NSA and other centers of actual intelligence gathering. For intelligence gathering to function the ability to maintain surveillance becomes imperative, and this surveillance has to function in such a way that the behavior of an intelligence target is modified as little as possible. This form of actual information gathering, weaponization and operationalization functions within an assumption of invisibility, making a focus on a deterrent effect impossible. In exposure the behavior of the target can be modified to counter surveillance, which modifies the intelligence dynamic from one that is structured to gather information to one that becomes deterrent in itself, becomes

panoptic in itself. This has become the unfortunate response to the Snowden leaks, among others, on a mass scale. Rather than taking the Snowden leaks as a partial glimpse into the capabilities and limitations of NSA processing methods, limitations and capabilities, material phenomena that can be responded to, the general sense of the scale of surveillance has been separated from other, more specific, information, and fit into a narrative of state omnipotence which has generated a deterrent effect.

This is not to say that the leaks are qualitatively bad or something like this, rather, we have to acknowledge the complicated effects of these leaks in relation to a material dynamic based in a limited capacity of force mobilization. On the one hand, it is clear that the Snowden leaks have had a deterrent effect that is so profound that it essentially has changed the very function of intelligence gathering. Intelligence gathering only achieves a deterrent effect to the degree that methods and scopes are exposed, but this exposure fundamentally prevents intelligence gathering from functioning; at the point of exposure countermeasures can be developed. After the leaks of sensitive intelligence information, and only a fragment of the documents Snowden copied have been released, the very prospect of intelligence gathering ceases to be secret, and comes into the open. As such, the effect has been to generate a certain sense of the panoptic, a sense of the possibility of being watched; intelligence gathering cannot go on as it did before, in secret, and the use of countermeasures has increased, but at the same time the deterrent effect has become the most profound effect of surveillance itself. In this the very function of an organization of the NSA has changed from signals intelligence organization to symbol of panoptic functionality, the symbol that deterrence concentrates around. This is not to say that they do not still collect intelligence, the building of server farms around the US makes it clear that this is expanding is anything, but their primary security role has become the mass deterrent effect that the exposure of the scale of signals intelligence gathering has had.

But, what we can see from this process is something incredibly important, the function of panoptic structures are not a product of their structure, the actual functionality of surveillance or even the clear visibility of surveillance. Rather, panoptic structures exists through the perception of the deterred, the perception of those that are the supposed, possible, targets of surveillance, rather than the functionality or intention of surveillance itself. It is in this sense that the very mythology of state omnipotence has come to serve the function of the Panopticon, and this is the irony of what has been occurring. It is not that panoptic deterrence is even the goal, or at least was not the goal of the structuring of surveillance techniques in 21st Century America, but it is the over-reaction to the exposure of a portion of the surveillance that is already occurring that has generated a panoptic effect in itself. In order to push past this problem we

have to come to understand the information leaks around surveillance and the material context that they exist in on a localized, immediate and material level.

Rather than taking the Snowden leaks as indication of state omnipotence we have to structure a new framework of analysis that reads the capacity to gather information in relation to the limited ability to process information, and the processing of information in relation to an even more limited capacity to generate material operations from processed intelligence. In other words, just as intelligence gathering means nothing outside of the limited capacity to process and weaponize information in the form of material police operations, we cannot understand information about the NSA, or surveillance and policing in general, on a purely informational level, disconnected from material dynamics, conflicts and limitations. Far from the omnipotent structure that is seen in the partial analyses that have proliferated through the progressive media and radical discourse we are actually getting a glimpse into a fundamentally limited structure that, far from functioning as a spatio-temporal totality, actually functions in incredibly partial ways. It is in these gaps in material coverage that possibilities proliferate, and these gaps in coverage, even in the face of total information gathering, exist everywhere. The task, to the degree that panoptic structures function as a result of the perception of surveillance by those possibly under surveillance, is to shift the plane of analysis, away from exaggerated rhetorical statements of police capacity, and into a sober, clear, intelligence driven analysis of actual police operations and actual operational capacity. It is only at this point that we can take the recognition of gaps in coverage to the next step, the actual identification of where these gaps exist, and how they can be exploited. It is only at this point that the self-imposed deterrent effect of surveillance can give way to an actual material and immediate analysis of where the possibilities of action and resistance exist.

Works Cited

Foucault, Michel (1995). *Discipline and Punish: The Birth of the Prison*. (trans. Sheridan, Alan). New York. Vintage Books

National Association for Shoplifting Prevention. *The Shoplifting Problem in the Nation*. Retrieved from: http://www.shopliftingprevention.org/TheIssue.htm

Lockwood, Jeffery (2008). *Six-Legged Soldiers: Using Insects As Weapons of War.* Oxford. University of Oxford Press

Bamford, James (2002). *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency from the Cold War Through the Dawn of the New Century*. New York. Anchor Books

Russian General Staff (2002). *The Soviet-Afghan War: How A Superpower Fought and Lost.* (trans. Grau, Lester and Gress, Michael). Lawrence, KS. University of Kansas Press