Institute For The Study of Insurgent Warfare
Panopticons Then and Now
2014

Retrieved on 26 August 2015 from http://isiw.noblogs.org/post/2014/09/29/two-pieces-on-surveillance/

lib.anarhija.net

Panopticons Then and Now

Institute For The Study of Insurgent Warfare

2014

In his essay *Hope in Common* David Graeber describes the system of social control under capitalism as a "a vast bureaucratic apparatus for the creation and maintenance of hopelessness, a kind of giant machine that is designed, first and foremost, to destroy any sense of possible alternative futures." In their quest the machine's operators are aided by the hopeless themselves, for one simple reason. Being proven wrong is irritating in general, but in the question of hope it would be utterly devastating. What if hope turns out to exist after all, after one had given up on it forever? How miserable would you feel if after abandoning your most cherished dream, you discovered years later it had been within your grasp all along, if you had only had the courage to reach for it? Desperate to avoid such a fate, legions of amateur doom sayers labor tirelessly to convince the rest of us that all revolution is bound to fail and we might as well give up now. Their patron saint is Henry David Thoreau, who in his celebrated work *On Civil Disobedience* made a cogent and brilliantly composed argument for the abolition of government — only to dismiss the idea with a breezy "But *that's* never gonna happen,

so let's just do random minor things the government doesn't like and hope they don't shoot us."

Thoreau's intellectual descendants continue his quest today. Some among them like to point to the massive firepower wielded by the US military as proof that no "alternative future" could ever come to pass. More sophisticated pessimists, perhaps aware that seemingly invincible armies have succumbed to revolution many times throughout history, prefer to focus on the psychological and propaganda weapons of today's ruling class. In any screed from this latter group one will more likely than not run across Jeremy Bentham's infamous[1] Panopticon. This was a prison design in which many inmates could supposedly be controlled by a single guard because, due to the layout of the building, the prisoners could not tell when they were being watched, and would therefore have to assume that they were always under observation. Multiple jeremiads would have us believe that the current infestation of surveillance cameras, databases, smartphones, and NSA monitoring constitute an impassable barrier to uprising through the imposition of Panopticonesque uncertainty on the entire population. The original Panopticon was a complete failure as a prison (a fact the Jeremiahs seldom mention). Yet Bentham's invention still contrives to carry on his mission in a way he could never have imagined, by providing rhetorical ammunition to pretentious armchair theoreticians endeavoring to persuade us that resistance really is futile.

Unfortunately for the theoreticians (not to mention the nation's retailers), most shoplifters have never read Tiqqun. Untroubled by half-baked quasi-philosophical jargon-mongering, these folks manage to pull about $13 billion worth of merch a year, in the US alone, out from under the mall surveillance cameras that are supposed to leave them paralyzed with doubt. This is in spite of warning signage, uniformed guards, and public displays of live surveillance footage – all intended to reinforce the message of deterrence. We should not

[1] Infamous literarily, that is — no actual Panopticon was ever built.

accomplish a Herculean task with laughably inadequate resources. "Eliminating all enemies of the US in three separate countries one explosion at a time" vies with "establishing a real-life Department of Precrime" for the title of most ridiculous government boondoggle ever.

There is good reason to believe then, that the security establishment's surveillance and monitoring plan, to the extent they even have one, not only isn't working, but can't work. If they are running a Panopticon it's only a byproduct of the impossibility of their true goals, and therefore far less effective than it might be. It's not difficult to peek behind the curtain to see the flaws in its inner workings and tailor one's tactics accordingly. That few of us do so is more of a testament to the enormous weight of propaganda and indoctrination imposed by the media and school system than to any actual invulnerability of the surveillance state. When supposedly radical analysts take the propaganda at face value and repeat it the impact is doubled. After all, if one's friends and one's enemies are both telling the same story it must be true, right? Not necessarily. The first step in fighting the hopelessness machine is not believing everything it tells you. Or failing that, at least not repeating it…

be surprised that none of this works very well. Any loss prevention professional will tell you that the cameras are mostly useful only for preserving evidence in those rare cases when someone gets caught, not for preventing attempts. The Panopticon relied not only on the lone watchman, but on close confinement of the prisoners to isolate individuals and ensure that anyone not being watched at a particular moment didn't cause trouble. Absent these strict conditions, the rough equivalent of today's supermax prisons, the Panopticon effect crumbles rapidly. Were Bentham's inmates allowed to congregate in common areas, or even housed two per cell so that one could screen the other from view, his system would break down, while if they were locked alone in their cells 24/7 the Panopticon would be unnecessary. After all, it would hardly matter whether the prisoners were being watched if they couldn't escape no matter what they did.

Out here in minimum security the Panopticon's deficiencies multiply exponentially. The requirements of selling mass surveillance mean that much of it is voluntary. If the government tried to force everyone to carry a monitoring device with them at all times that reported their location and most of their conversations to a central authority, the outcry would be deafening, no one would comply. The only way to pull it off is to throw in Candy Crush, charge 100 bucks a month, and wait for the suckers to roll in. But Iphones can be left at home, cameras can be smashed, communications can be encrypted, Facebook accounts can be closed. Even a relatively small minority who see through the authorities' bluff can make life very difficult for them.

Worse, in any attempt to institute a real-life Panopticon uncertainty works both ways. The prisoners may never know when they're being watched, but neither can the guards ever be certain what the prisoners are getting up to in their unobserved moments. The natural response is to monitor as much activity as possible at all times. In the digital age this urge manifests itself in the massive data harvesting programs carried out by the NSA and other

intelligence and law enforcement agencies. Sadly for them however, while capturing and storing data is easy, data by itself is not information. The NSA's enormous capability to intercept data has not been matched by any corresponding ability to analyze it, much less to act on whatever information is extracted. Data mining has shown some promise in keeping track of known suspects, but has been nearly useless at uncovering new ones. The forces of order are therefore left to wrestle with unmanageable masses of data on people who are little threat to them, while those harboring nefarious intent can slip beneath the radar merely by taking some basic precautions.

Interestingly enough, the history of the Panopticon actually does reveal a useful lesson for insurgents, one which has predictably been lost on the jargon-mongers. Bentham pitched the idea as a money saver, a way to replace a large workforce of guards with a single volunteer (yes, really!) warden. While the the English government ultimately turned him down, modern capitalists have not all shown the same good judgement. Despite that $13 billion, some some retail chains have reportedly been cutting back on loss prevention personnel and relying more on technology in a misguided attempt to reduce expenses. A similar tendency has cropped up in municipal budgets, which have been slashed in many cities to the point that even police departments are coming under the ax. Federal grants for surveillance systems are available to local police, and surplus military equipment under the ax from the Defense Department, but funding for basic policing functions, such as officer salaries and patrol cars, is scarce.

The poster child for this trend is Oakland, CA, where the municipal government is developing a network of high resolution surveillance cameras, combined with various tracking tools such as license plate recognition, aimed at suppressing mass protests. Christened the DDomain Awareness Center, the project is drawing loud squawks from civil libertarians and progressives. Few seem to recall that the city cut its police force to 696 officers the week af-

nating existing enemies without creating more new ones, and indiscriminate killing of random civilians fails on both counts. Yet Scahill and Greenwald make it clear that accuracy is not a major consideration when targeting, that the main focus is on "feeding the beast", *i.e.* keeping the drone operation running at full capacity. It is telling that reviews for civilian deaths occur only *after* strikes occur, not during the planning stages. US drone tactics thus appear to derive more from bureaucratic inertia, extreme resistance to admitting error, and an abiding fascination with the idea of soldier-free warfare than from any deliberate plan. These afflictions are far from unique to the NSA.

The NSA's drone difficulties highlight another aspect of mass surveillance seldom noticed by radicals – the difference between a Panopticon and a failed intelligence operation. It is axiomatic that the value of any intelligence source plummets once the adversary finds out about it. British intelligence in World War II went to great lengths to keep the Germans from realizing that the Enigma code had been cracked, even refusing to share decrypted messages with the Soviet Union lest the Russians' own leaky codes expose the secret. The problem is compounded when the "adversary" is the population of an ostensibly democratic country, since discovery means not only loss of effectiveness but loss of face as well. Unlike Walmart, the NSA has no interest in publicizing their surveillance efforts. Their aim, however clumsily pursued, is to discover useful information without being detected, not to deter resistance by projecting the illusion of omniscience. Yet Snowden's revelations have apparently led many to conclude that NSA surveillance is inescapable, instead of examining them in detail for ways to defeat it.

We can also see parallels between mass data collection and drone strikes. Both projects are carried on because they're technically doable, and appeal strongly to the authoritarian mindset, not because they work particularly well for their ostensible purposes. In both cases public exposure alone threatens to cancel out any minor benefit generated. In both cases government agencies are trying to

point it seems relevant to mention that Yao's company also manufactured *high* resolution surveillance cameras. It is not known how much his sales increased as a result of Klein's article.

Klein's error is representative of more than just technological cluelessness and inexperience of industrial salespeople (which could have easily been cleared up with an email to a digital rights group such as the Electronic Frontier Foundation). Like too many other critics, she rejects the police state's claims of motive, but swallows whole their claims of capability. Countless essays and articles describe various aspects of state repression, but present them, *a la* Klein, as inescapable *faits accompli*. Analysis of strengths and weaknesses with an eye toward resistance is comparatively rare. Perhaps the authors fear that any admission that the state is vulnerable would imply a responsibility to attack it? In any case, cops and critics alike agree that the state's efforts to maintain and extend their control of society are, if not perfect, at least logical and purposeful, that repression is targeted at those who pose the greatest threat, that if you have nothing to hide you have, perhaps not nothing, but at least very little to worry about. It's a highly suspect assumption. Jeremy Scahill and Glen Greenwald's report Death by Metadata reveals that US drone strikes in Pakistan, Somalia, and Yemen and are mostly targeted using phone metadata obtained by the NSA, with very little human intelligence (of either sort) involved. The result is pretty much what one would expect. "Real terrorists" who know they're targets change phones and SIM cards regularly to avoid detection, while victims of strikes often include random bystanders and uninvolved users of the same phone. This situation will only get worse for the NSA as word of Scahill and Greenwald's report spreads and more people start taking appropriate precautions.

One's chances of not being killed by a Hellfire missile in Yemen would therefore seem to depend about as much on luck and knowledge of cell phone security as on abstention from anti-US activity. This is unlikely to be the result of a deliberate strategic choice. The fundamental dilemma of any counter terrorism operation is elimi-

ter the Oscar Grant verdict came down, losing much of their capacity to respond to anything seen in the footage. The department has since declined to 624 officers, a 20 percent reduction from mid-2010. That's not their only problem, either. A recent survey of OPD rank and file cops reveals severe deficiencies in operational logistical capacity, including broken radios, deteriorating patrol cars, and police stations so dilapidated one officer referred to them as "Section 8 housing." Department morale has been eroded by infighting, mandatory overtime, and the withering contempt in which many Oakland residents hold cops, among other factors. Officers are quitting almost as fast as they are recruited, exacerbating the personnel shortage. Oakland's police would be a lot more dangerous if the $12 million being spent annually on the DAC had gone toward addressing these problems, instead of generating countless hours of video footage that no one will have time to view or analyze.

And finally,leading the charge into this technological quagmire we find the Pentagon, who have been putting "toys before boys" for years now, with disastrous (for them) results. Decades of increasing expenditure on fancy weapons systems while cutting back on readiness and personnel have produced a military that has in the last 60 years proven incapable of successfully occupying any country more formidable than Panama.

The true takeaway from the Panopticon then, is that it doesn't work, that clever schemes and high tech gadgets can never effectively replace boots on the ground. The former East Germany, where nearly a sixth of the population had been coerced into informing for the Stasi, gives us an example of a genuinely effective use of uncertainty in social control. Rebellion was nearly impossible, not because one might be recorded on video, but because there was no way to find comrades who could be counted on not to snitch.

The Stasi had an advantage, though. They didn't have to deal with computers. Relying on paper files right up to the day the Berlin Wall came down, their data overload problems never became too unmanageable, their sense of possibilities constrained more or less within

the bounds of feasibility. Today Moore's Law and multi-billion dollar black budgets combine to appeal irresistibly to the most treacherous of authoritarian instincts — the pipe dream of complete control, no uncertainty required, all transgressions seen and punished. Attempting this by recruiting more guards for one's Panopticon only reproduces the original problem at a higher organizational level, as Edward Snowden demonstrated so graphically. But what if you could find guards who never took bathroom breaks, never slept, never decamped to Hong Kong with 58,000 of your most sensitive operational documents? The problem with people is getting them to do exactly what you want and nothing else. Computers, or at least computer salesmen, promise to do away with this annoyance forever.

They can't of course, not really. Any programmer can testify that all programs have bugs, that getting a computer to do precisely what it's supposed to and no more is functionally impossible for any non-trivial task. Cops presented with an opportunity to fulfil their deepest held control fantasies tend to overlook this little inconvenience, which is why they keep spending money on things like facial recognition software. Facial recognition made its public debut at the 2001 Super Bowl in Tampa to the usual chorus of dire warnings by privacy advocates. They needn't have worried — at the time it didn't work well enough to threaten anybody's privacy. But that didn't stop the Tampa police from adopting it that summer to surveil Tampa's Ybor City district, although they abandoned the project after only a few months. It's easy to guess how they were taken in. Some stories are too good to check, and the ability to do instantaneous automatic mug shot look-ups on anybody who turns up in their surveillance footage is near the top of any cop's Christmas list.

Facial recognition doesn't work a lot better now than it did in 2001, even though its adoption has mushroomed. A 2013 article from Ars Technica explains that far from the process being automatic, most images have to be hand tweaked before matching is attempted. Differences in camera angle, lighting, makeup, facial hair, glasses, and other variables also reduce accuracy. The technology is effective in situations like preventing drivers license fraud, where the photographs in the database were taken under the same conditions as the picture to be matched. However, facial recognition in high-profile criminal cases is still mostly done the old fashioned way, by publishing photographs of suspects and waiting for someone to recognize them and rat them out. Both digital and human approaches are far too labor intensive to be useful in large scale tracking efforts (although masking up thoroughly is still highly advisable in certain situations).

Comparatively few radical analysts bother to investigate these sorts of technological underpinnings, even when they're writing about technology. A case in point, Naomi Klein, whose otherwise informative 2008 article for Rolling Stone decrying the rise of state surveillance in China included what amounted to an advertisement for the capabilities of the facial recognition software sold by L-1 Identity Solutions, a US vendor of security technology. Klein's main source on this subject was a salesman named Yao Ruoguang, whose company was peddling L-1's software in China at the time. Yao trotted out what was probably the standard demo he showed prospective customers — taking his own picture with a laptop camera and comparing it to a database of a claimed 600,000 images. Supposedly the search returned several correct matches in about a millisecond. Klein took Yao at his word, even though such a test could easily be faked, and Yao had every incentive to do so. Even if the demo was otherwise legitimate, the conditions under which the sample picture was taken — good light, a closeup frontal shot, and presumably no facial adornment — were far more favorable than those typically found in the field. Klein apparently never asked about any of this. She also accepted Yao's implicit claim that the only technological obstacle in the way of widespread use of facial recognition in China was the low resolution of existing surveillance cameras. As we can see from the Ars article linked above, this is hardly the case. At this