Oceanic enemy

A brief philosophical history of the NSA

Grégoire Chamayou

6 July 1962, NAVFAC base, Barbados.

A grey building stands at the foot of a stone lighthouse overlooking the Caribbean Sea. Inside, a military serviceman is examining the lines being recorded on an enormous roll of paper by the stylus of a sort of gigantic electrocardiogram. We are in one of the secret bases of the Sound Surveillance System (SOSUS) network, established by the US Navy in the 1950s. Among the clutter of zigzags, from which he has learnt to read the sound of the oceans, the man is looking for a 'signature'. Today, for the first time, he spots the signal of a Soviet nuclear submarine.[1]

The problem with submarine warfare was that enemy vessels were hidden from view. But what one could not see, one could nonetheless hear: the water in which the submarines hid carried the sound of their engines far into the distance. This is how the sea was put under surveillance. The sound waves could be captured by hydrophones and transmitted by cables to coastal stations where machines transcribed them into graphs. The 'ocean technicians' who deciphered them were able to 'discern subtle nuances in sound signals via intensity, colour, shape, and shade that often made the difference between seeing a school of fish or a submarine on a Lofargram'.[2] They listened with their eyes. Typical patterns corresponding to known entities were called 'signatures'. The metaphor spoke for itself: there, like elsewhere, an identity would be certified by some lines inscribed on a piece of paper.

Yet all this met with a very unexpected fate. A model that had combined a global listening system, the mass collection of signals, and remote sensing via signature recognition, a few decades later would provide the conceptual basis for an altogether different kind of surveillance apparatus.

At the end of the 1990s, the National Security Agency (NSA) understood that something new was in the offing that promised, excepting the need to overcome certain obstacles, an unheard-of extension of its empire. Historically, the agency had been charged with the task of intercepting electromagnetic signals for external intelligence – diplomatic cables, military communications, satellite beams, and so on. But with the close of the millennium, civil populations were themselves becoming signal transmitters. The whole world was becoming connected, and creating one in which each of us would soon produce more data than any Soviet embassy of the past.

Recalling the reigning zeitgeist of this era, the ex-director of the NSA Michael Hayden today admits:

> prior to 9/11, when we were looking at modern telecommunications, … we said we had the problem of what we would call … V cubed – volume, variety and velocity – that the modern telecommunications were just exploding in variety and in size.… But also, we knew that our species was putting more of its knowledge out there in ones and zeroes than it ever had at

any time in its existence. In other words, we were putting human knowledge out there in a form that was susceptible to signals intelligence. So to be very candid, I mean, our view even before 9/11 was if we could be even half good at mastering this global telecommunications revolution, this would be the golden age of signals intelligence. And candidly, that's what NSA set out to do.[3]

The utopia of anti-terrorist data mining

The logo depicts a pyramid topped by an all-seeing eye, Illuminati-style, floating in space and bombarding Earth with luminous rays. This was the emblem of a research programme launched by the Defense Advanced Research Projects Agency (DARPA), an electronic surveillance project entitled Total Information Awareness. This idiotic design, which seemed deliberately created to stoke crazy conspiracy theories, was emblazoned with a Latin motto which, in a sense, rescued the entire design: *scientia est potentia*, knowledge is power. That was, effectively, what it was all about.

In August 2002, the programme director John Poindexter presented it with great pomp at the DARPATech conference that was being held at Anaheim in California. What is at stake, he began, is 'somewhat analogous to the anti-submarine warfare problem of finding submarines in an ocean of noise – we must find the terrorists in a world of noise.' The oceanic analogy was not by accident. The admiral had begun his career in the Navy at the end of the 1950s in a unit tasked with the tracking of Soviet submarines. He added, referring to the 'terrorists', that 'they will leave signatures in this information space.'[4]

The parallel was clear: what had once been done in the ocean was now going to be done in an 'ocean of information'. Instead of the old lofargrams, computers would now be used to sieve through an immense mass of heterogeneous data – telecommunications, bank details, administrative files, and so on – searching for 'signatures of terrorist behaviour'. A 'red team' would be charged with the task of enumerating potential scenarios of terrorist attack and coming up with the necessary preparative measures: 'These transactions would form a pattern that may be discernible in certain databases.'[5]

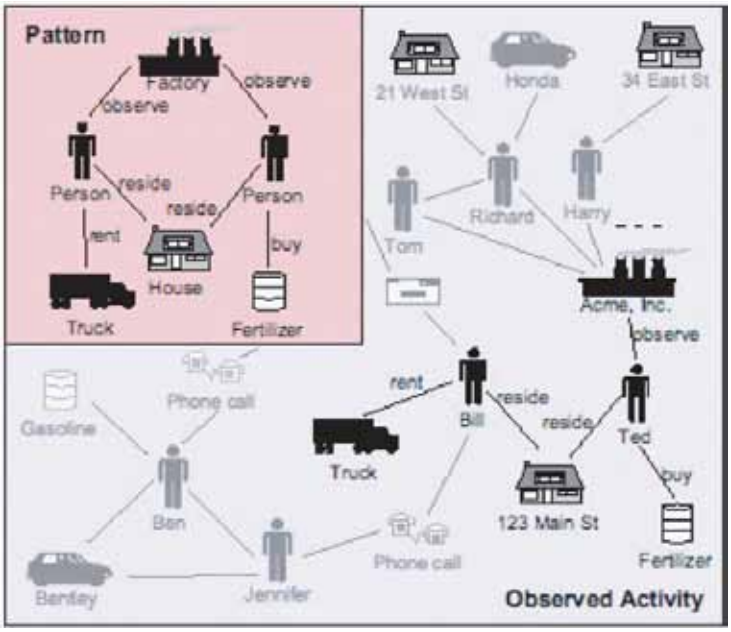


Diagram of a 'terrorist pattern' in an activity graph[6]

For example, if Bill and Ted live at the same address, rent a truck, visit a sensitive location and buy some ammonium nitrate fertilizer (known to be used for growing potatoes but also for the production of home-made bombs), they would exhibit

a behavioural pattern that corresponds to that of a terrorist signature, and the algorithm designed to process this data would then sound the alarm. However, as one sceptical expert has remarked during a hearing, one of the worries is that by defining a terroristic profile in this manner those who would suddenly find themselves on a list of suspects would not only be potential Timothy McVeighs, but also the majority of farmers in Nebraska, who also very often live on the same farm, buy fertilizer and rent trucks.[7] Even supposing that 'terrorism' is detectable through signatures that could be spotted through data mining – which is a risky hypothesis to say the least – such a system would inevitably throw up a plethora of suspects, with an overwhelming majority of false leads – with the latter, it has been estimated, in the millions.[8]

The other fundamental problem concerns the very notion of 'terrorism', which is too vague to be given a satisfactory operational definition. What is terrorism? Let's assume the following official definition: all illegal and calculated use or threat of violence aimed at producing a feeling of terror for political ends.[9] This conception is not defined by certain operational modes, but by an intention whose objective is to produce a subjective effect, an emotion – fear. What algorithm would be capable of detecting behavioural indices that could unmask this kind of intentionality? There are a million and one ways to *want* to terrorize.

Brains that had been trained during the Cold War enacted a false analogy as they sought to graft a mechanistic model (the signal of a submarine engine, necessary and constant) back onto the realm of the living (a political intentionality, polymorphous and adaptive). The entire project rested on the premiss that 'terrorist signatures' actually existed. Yet this premiss did not hold up. The conclusion was inevitable: 'The one thing predictable about predictive data mining for terrorism is that it would be consistently wrong.'[10]

To the critics who pointed out the epistemological limits of such a programme, its creators responded with procedures designed to mitigate its excesses. Confronted with the problem of exploding numbers of 'false positives', itself linked to the low frequency of the phenomenon in question within a considered totality, they borrowed their solutions from the methods of medical screening: by isolating from a general population subgroups at risk. As some of Poindexter's collaborators explained, the idea was to combine the approaches of 'propositional data mining' (based on requests of the type: 'search for all entities exhibiting *properties* x and y') and 'relational data mining' (based on requests of the type: 'search for all entities *related* to entity A').[11] Groups of individuals would thus be targeted on the basis of their relationships, a bit like in a medical screening, which starts by tracking family histories in the hope of flushing out a rare illness.

One implication of this 'solution' barely emerged in the debates, even though it was politically crucial: in the prevailing context, the so-called 'populations at risk' seriously risked being defined according to a thinly veiled logic of racial profiling. For instance, the preferential targeting of individuals with regular connections to persons living in the Near and Middle East meant constituting the Arab-American population as a target group. Under the apparent colour blindness of computational analysis, an old racist vision did not fail to resurface. In some NSA documents, the target type has a revealing sobriquet: 'Mohammed Raghead'.[12]

By admission of its own creators, this 'relational data mining' model entailed another 'obvious flaw' at the tactical level:

> Some types of relational data are clearly not resistant to adversarial conduct. For example, an individual terrorist could refrain from initiating or receiving email messages, telephone calls, or financial transactions with other terrorists. Alternatively, an individual could purposively attempt to reduce his or her homophily, intentionally generating records that constitute 'noise'.[13]

Now, if such systems can be thwarted via precautions of this type, available to any well-informed group, then, quite paradoxically, and contrary to their declared aim, these same systems could only be mobilized against individuals or groups whose activities, in order to be partly private or discrete, would not for that matter be actively clandestine.

Poindexter's project was a political failure. In November 2002, an inflammatory column drew the public's attention to the programme. The logo was shown. People got scared. Pressure mounted, and so much so that on 13 February 2003 Congress withdrew the funds. However, this was nothing but a smokescreen. The programme continued its life elsewhere under the seal of secrecy.[14] It should be pointed out that during the same period other characters were already courting similar ambitions.

'Collect it all'

At the height of the polemic, Keith Alexander and James Heath, who two years later would become director and scientific adviser to the NSA respectively, openly sided with the turn towards Big Data in the intelligence field:

> Many may argue that we suffer from the effects of collecting too much information, and that the answer to more accurate situational awareness is to reduce or filter the data we already collect. We believe the opposite to be true… The solution is to continue to collect as much information as possible, and concurrently revolutionize how we receive, tag, link, analyse, store and share that information.[15]

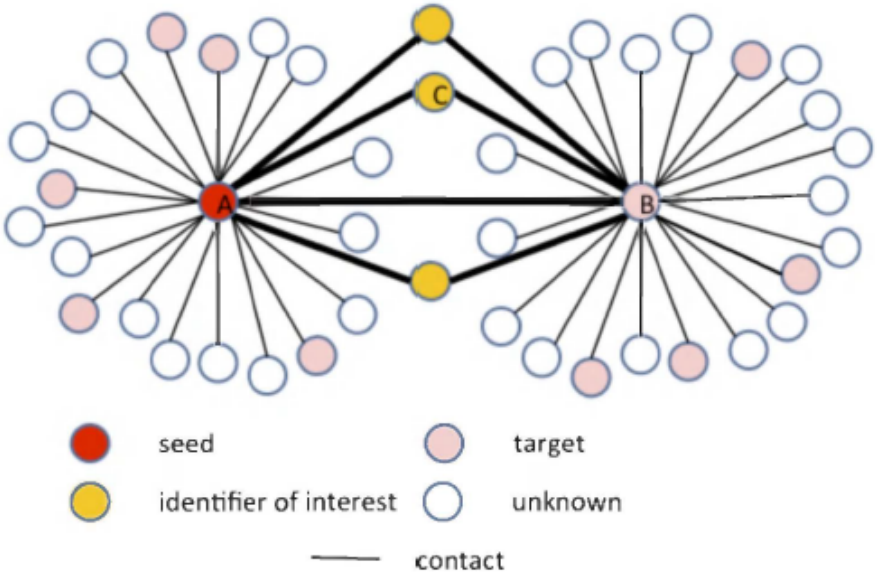
When Alexander assumed directorship of the NSA in 2005, his position had not changed one iota: 'Rather than look for a single needle in the haystack, his approach was, "Let's collect the whole haystack", said one former senior U.S. intelligence official who tracked the plan's implementation. "Collect it all, tag it, store it".'[16] This approach was summed up in one principle: 'total collection'. But what should also be noted is the way such a principle ends up biting its own tail: to ensure that nothing is missed in the analysis, more and more data must be collected, except that the more one has of it the less capacity one has to analyse it. This is the fundamental contradiction between increased capacities in data collection and limited capacities for analysis. Mass collection does not, however, imply that everything be analysed, read or heard. Hence the crucial difference between 'passive surveillance' and 'active surveillance'.

Collection can be carried out in bulk or in targeted fashion. Bulk collection gathers data without sorting it. This was the case with the Telephone Record Program, conducted under the auspices of section 15 of the Patriot Act, where the NSA was able to 'collect nearly all call detail records generated by certain telephone companies in the United States'.[17] Targeted collection, on the other hand, focuses on 'strong selectors' (telephone numbers, email addresses, IP addresses, etc.). But being 'targeted' does not stop the collection being very wide in scope: 89,138 identifiers were tracked by the NSA in 2013 in this way and under legal cover from section 702 of the Foreign Intelligence Surveillance Act (FISA), within whose ambit the Internet data collection program PRISM, alongside others, also operated.[18] 'Targeted collection' – just like a 'targeted strike', in fact – can result in 'collateral damage': certain modes of interception can thus 'accidentally' or 'inadvertently' – but in reality in an entirely foreseeable manner – suck up all the data packets transiting in the vicinity of the officially targeted selectors.[19]

Since the American debate is polarized in a nationalist vein, almost exclusively on the question of domestic espionage and the private life of the citizens *of the United States*, these first two programs (metadata and PRISM) have been subject to extensive media coverage. But this focus tends to distort the bigger picture, because a large proportion of the mining of data is carried out, as far as one could know, in the shadow of yet another legal finesse, executive order 12333, inherited from the Reagan

administration.[20] It covers, among others, the DANCINGOASIS program, which siphons the fibre-optic cables that run between Europe and the Middle East, constituting one of the most important resources of this kind, with more than 57 billion records collected in a single month at the end of 2012.[21]

In order to analyse the collected data, two main types of method are deployed. In the first category, XKEYSCORE functions like a search engine through 'weak selectors', namely keywords or requests of the type 'show me all individuals who speak German in Pakistan'.[22] If one discovers, through this skew or another, an interesting individual, one can run a second type of method: the analysis of contacts. The 'contact chaining' procedure consists in 'building a network graph that models the communication (e-mail, telephony, etc.) patterns of targeted entities'.[23] One begins with an identifier, called a 'seed', and then follows the stems that begin to sprout one by one. As the network of connections starts to form, a sort of blossoming tree-like dandelion structure emerges. The target here is conceived fundamentally as a reticular individuality. What is being sought, through the hacking of an individual's private life, is their *social life*.



'Contact chaining'[24]

Once again, though, being 'targeted' does not prevent this sort of analysis from exceeding its stated target. In the case of telephone metadata, given the so-called 'three degrees of separation' rule, 'If a seed number has seventy-five direct contacts, for instance, and each of these first-hop contacts has seventy-five new contacts of its own, then each query would provide the government with the complete calling records of 5,625 telephone numbers. And if each of those second-hop numbers has seventy-five new contacts of its own, a single query would result in a batch of calling records involving over 420,000 telephone numbers.'[25]

Programmatic surveillance and time machines

In the wake of the Snowden revelations, it was often suggested that the NSA programmes were presiding over a form of 'total surveillance' – a kind of Big Brother scenario or panopticon. But this diagnosis needs to be corrected. The notion that the NSA was capable of *collecting and analysing everything*, other than being empirically false, is also politically counterproductive because it conveys the debilitating image of

an all-encompassing power. These programmes have in fact neither the capacity nor the desire to *actively monitor the whole world*. This of course does not mean that they are not dangerous.

In order to portray the matter more clearly, one can turn to the concept of *programmatic surveillance*. This notion refers to a specific legal expression: the 'programmatic approval' granted to the NSA by the secret court that oversees a part of its activities.[26] Traditionally, the wiretapping of this or that suspect was authorized *individually* by judicial warrant. The special powers secured after September 11 opened the floodgates, perhaps already half-open: the court has since authorized a number of surveillance *programmes* outright, thereby surrendering to the NSA the power to choose its targets. Questioned over what comes under the criterion of 'Reasonable Articulable Suspicion', which was supposed to internally restrict the exercise of this prerogative, the general counsel to the NSA once remarked, in full official hearing: 'It's effectively the same standard as stop and frisk.'[27]

Describing these programmes in terms of 'programmatic surveillance' *in a broad sense* reveals the following: it matters less to the NSA to actively monitor the entire world than to endow itself with the powers to target *anyone* – or, rather, *whomever it wishes*. The surveillance targets will be defined according to the priorities of the day; that is to say, according to the needs of the 'programme', this time understood as the totality of 'actions that it aims to accomplish'. This programme, it should be made clear, is nothing but one of Reason of State.

MYSTIC is a 'surveillance system capable of recording "100 percent" of a foreign country's telephone calls.' It has been tested by the NSA in the Bahamas and deployed in another non-identified country, in all likelihood Afghanistan. The related storage device, SOMALGET, is today capable of storing an entire month's worth of recorded conversations.[28] It is thus possible to 'replay the voices from any call without requiring that a person be identified in advance for surveillance.' Total collection and targeted collection are not opposed: they combine perfectly through the double mode of provisional archiving and retrospective analysis. What has been built here is welcomed as a little 'time machine'.[29]

This capacity for 'retrospective retrieval' – here still in embryonic stage, and so far only available for a limited period – is essential for grasping the longer-term aims of the Agency. The objective is not only to monitor certain targets in real time, but also to be able to retrace any individual's itinerary of relations if in the meantime this has become of interest. The dream is to put together sleeper dossiers for every person through an automated data collection system. Such an archival apparatus would constitute the instrument of a *biographical power* founded on the generalized informational capture of the micro-histories of individual lives.

While the ambition of predictive data mining was to detect the traces of the future in the present, here the perspective is inverted: to gather in the present the archives of a future past. Since anyone could become a target one day, the possibility of this becoming-target must be anticipated by archiving everyone's lives. Having as its object the indeterminacy of the future, this rationality itself tends to become, under its own dynamic, unlimited.

A question of power

In June 2013, Alexander claimed that the NSA's surveillance programmes had made possible the thwarting of dozens of 'terrorist plots'. In October of the same year, the general downgraded his estimate, evoking thirteen 'events' on American soil before admitting that the number of threats foiled by the telephone metadata collection program actually amounted to one or perhaps two.[30] When all was said and done, only a single 'plot' had been foiled by more than ten years of mass collection of telephone

records in the United States: an inhabitant of San Diego had been arrested for sending 8,500 dollars to a Somali militant group.[31]

While people had been racking their brains to expatiate, like lousy philosophers, upon the least unjust compromise between security and liberty, what happened in practice never corresponded to the theories, which turned out to be wholly irrelevant to the real problem at hand. A portion of liberty was not being exchanged for a dose of security. Rather, a portion of liberty was being exchanged for nothing. But this way of putting things is still incorrect. What one lost, through the pretext of a gain in security, was actually another portion of *safety* [*sûreté*], in the classical sense covered by this concept since the Enlightenment, namely protection against the arbitrariness of state power, and in particular police power.

Contrary to the official discourse that has served to legitimate them, these instruments have shown themselves to be mediocre means of anti-terrorist detection. It is in this light that the following words, uttered by the ex-director of the NSA Michael Hayden in a briefing at a Washington think-tank, should be read: 'I think folks in my government have attempted to justify NSA activities far too much on a narrow counterterrorism platform. And that's just simply inadequate to justify what the United States is doing. And we have lots of motivations that are … consistent with state sovereignty.'[32] Edward Snowden, for his part, has said precisely the same thing: 'These programs were never about terrorism: they're about economic spying, social control, and diplomatic manipulation. They're about power.'[33]

Anti-terrorism is but one of the NSA's multiple missions, a panoply comprising concerns as varied as the surveillance of the internal political activities of countries whose regime one wants to protect, such as Saudi Arabia, the monitoring of political processes representing a danger to American interests, such as 'Latin American Bolivarian developments',[34] or the spying of the technological activities of foreign powers. This explains, for example, the bugging of Chancellor Merkel, Dilma Rousseff and Chinese industrialists. But the NSA is meant, above all, for waging war.

The eyes and ears of the war machine

The battlefields of Afghanistan and Iraq have served as great laboratories, vast zones of open-air experimentation for new weapons. There, American intelligence agencies have developed a new model of Intelligence, Surveillance and Reconnaissance (ISR). The first problem in a counter-insurgency war is how to spot a 'low contrast enemy' – an enemy blending into a landscape that no longer emits 'Soviet style military signatures'.[35] Now, if your opponent 'can no longer be identified by what they are', the theory goes that they may still be recognized 'by what they are doing'.[36] One monitors activity in order to induce its identity.

To this end, the decisive technological device was the drone. This type of aircraft, which is capable of remaining in the air for hours, finally makes 'persistent surveillance' possible. One speaks of an eye that never blinks. Traditionally, geographical intelligence had been focused on the more or less static elements of the terrain. The persistent gaze of the camera changed things: the imagery could now capture the movements of entire populations. Through high-tech means, analysts took the classical policing techniques of undercover tailing and converted them to a military context. Drones had not only cameras on board, but also other types of sensors, such as small boxes capable of intercepting mobile phone signals from below. This was a crucial element: combining video imaging and signal interception constituted an overhaul in the fundamental aspects of armed surveillance.

Parallel to this, the NSA, with Alexander at the helm, applied its principle of total collection to counter-insurgency warfare. In 2007 in Iraq, the agency deployed a new data-processing tool called Real Time Regional Gateway. It enabled the agency 'to

capture all the data, store it, and make it instantly available to intelligence analysts.'[37] But the crucial contribution of this network technology, stressed Peter Rustan, was its 'ability to integrate the signals [for] geolocation'. At stake was nothing less than the ability of 'turning meta-data into actionable Intelligence' – that is, into targets.[38]

This work was entrusted to special teams. Their badge shows a spy character that looks as if it has been taken straight from a *MAD Magazine* comic strip, armed with a magnifying glass aimed at blood-red footprints leading to the top of a dune. The slogan makes things plain: 'We track 'em. You whack 'em.'

This was the slogan of the Geocell teams, which were born out of a novel collaboration at the beginning of the 2000s between the NSA and its Siamese twin, the then still obscure National Geospatial Agency (NGA). The purpose of these 'geolocalization cells' was, through the combined analysis of both signals and images, 'to track people, geographically, in real time'.[39]

This partnership between the NGA and the NSA has been described as constituting a 'critical shift'.[40] The revolution consisted in a perceptual synthesis: seeing what one listened to and watching what one heard. This synthesis was achieved by joining 'the eyes and ears' of the war machine; that is, by fusing what in the jargon might be called two 'phenomenologies'. In the process, the two agencies created a hybrid model that combined their respective know-hows. The outcome was a new discipline, 'SIGINT Geospatial Analysis'. In order to train analysts in this emerging discipline a special course was put in place, the Geocell bootcamp on Goodfellow base in Texas. Various data-processing tools were also developed, such as the Analyst Notebook software, which, as the IBM instruction manual underlines, allows for the conversion of nearly all the available data into 'one analytical picture that combines geospatial, association and temporal analysis'.[41] Derek Gregory has explained that, equipped with these kinds of visualization interfaces, the analysts' job was 'to track multiple individuals through different social networks to establish a "pattern of life" consistent with the paradigm of activity-based intelligence that forms the core of contemporary counterinsurgency'.[42]

Traditionally, intelligence mainly intervened during the preparatory stages of reconnaissance. It is now incorporated in real time during the operational stage: 'Today, intelligence *is* operations', writes Michael Flynn.[43] This displacement is linked to a profound reform of the 'targeting cycle' driven by the Join Special Operations Command (JSOC) in Iraq. The idea, general McChrystal has revealed, 'was to combine analysts who found the enemy, … drone operators who fixed the target; combat teams who finished the target …, specialists who exploited the intelligence the raid yielded, such as cell phones… By doing this, we speeded up the cycle.'[44] Whereas at the start of the war, analysing intelligence collected during an operation could take weeks, the implementation of this aggressive cycle now allowed the 'kill chain' to be set in motion at full throttle, increasing the number of night raids, with each new operation generating new suspects, who would be tracked by contact chaining and then targeted on the field, a process that gradually led all the way to 'people we didn't even know existed at the beginning of the night'. The shift was from 18 raids per month in August 2004 to 300 raids per month in 2006 – 'ten a night', boasted McChrystal.[45] Joint director of the NSA John Inglis was ecstatic: Geocell was 'something near miraculous'. John Nagl greeted the implementation of an 'industrial strength counterterrorism killing machine' with similar enthusiasm.[46]

The journalist Gareth Porter has offered another version of the facts: 'the application of the new intelligence methodology developed by McChrystal and Flynn was that anyone who visited a location under surveillance or who communicated with a mobile phone associated with that location could be considered to be part of the insurgent network.'[47] The instruments of reticular suspicion developed by the NSA were mobilized to provide the basis for life-and-death decisions, and all this while pretending not to remember the fact that they had always been 'investigative', not 'evidentiary' tools. The authorities had built themselves a theatre of shadows in which bloody scenes began to unfold at an accelerated rhythm: 'The result, way too often, is firing blind based on "pattern of life" indicators without direct confirmation that the targets are, in fact, who we think they are.'[48] This was the same kind of methodology behind so-called 'signature strikes' in which drones kill 'without knowing precisely the identity of the individuals targeted. Instead, the individuals match a pre-identified "signature" of behaviour that the US links to militant activity or association.'[49]

Beyond the killings, the desolation and the destabilization of entire regions, what is the outcome of nearly fifteen years of the 'war on terror'? How many aspiring jihadis were there in 2001 and how many are there today? One of the few tangible results of these policies has been to amplify the very threat one had claimed to be eradicating, if not to make it proliferate on an industrial scale.

Fish story

For the NSA and the NGA, however, this new geospatial surveillance model seemed like a brilliant innovation that needed to be extended and generalized. The question was, then, as Gregory Treverton has put it, how 'can we expand it beyond counterterrorism and manhunting and the fight against terror?'[50]

> Today, intelligence-gathering is like looking in a global ocean for an object that might or might not be a fish. It might be anything and it might be important, but at first, we are not sure it even exists. … They might make up an organized school of fish or they might not be related at all. But we do know that we need to find it, identify what it is, and figure out how it relates to all the other objects – whether fish or sea fowl – we either know or think might be important.[51]

What Letitia Long was trying to put forward through these extended marine metaphors (though it should be noted that, well before becoming director of the NGA,

she had already cut her teeth in acoustic submarine detection) was a new philosophy, a new paradigm that since 2010 has been pursued by one of the highest authorities in the US intelligence services.

This was the doctrine of 'Activity Based Intelligence' (ABI): 'we used to know what we're looking for, and we're not looking for things but rather activities.'[52] The premiss is the same as before: 'in environments where there is no visual difference between friend and enemy, it is by their actions that enemies are visible.'[53] Today the task of establishing a distinction between friend and enemy is once again to be entrusted to algorithms.

Translated by Giovanni Menegalle

Notes

1. Owen Cote, *The Third Battle: Innovation in the U.S. Navy's Silent Cold War Struggle with Soviet Submarine*, Naval War College Newport Papers 16, Naval War College Press, Newport RI, 2003, p. 39.
2. The lofargram is the graph recorded by these machines, called LOFAR – Low Frequency Analysis and Recording. Citation from Gary E. Weir, 'The American Sound Surveillance System: Using the Ocean to Hunt Soviet Submarines, 1950–1961', *International Journal of Naval History*, vol. 5, no. 2, August 2006.
3. Declaration at the panel 'Stabilizing Transatlantic Relations after the NSA Revelations', Atlantic Council, Washington DC, 8 November 2013.
4. Remarks as prepared for delivery by Dr John Poindexter, Director, Information Awareness Office of DARPA, at DARPATech 2002 Conference, Anaheim, California, 2 August 2002.
5. John Poindexter, *Report to Congress Regarding the Terrorism Information Awareness Program*, Washington DC, 20 May 2003, p. 14.
6. Seth Greenblatt, Thayne Coffman and Sherry Marcus, 'Behavioral Network Analysis for Terrorist Detection', in Robert L. Popp and John Yen, *Emergent Information Technologies and Enabling Policies for Counter-Terrorism*, Wiley–IEEE Press, Hoboken NJ, 2006, pp. 331–48, p. 334.
7. Timothy James McVeigh is the well-known architect of the truck bomb exploded in front of a federal building in Oklahoma City on 19 April 1995. The remark was by Paul Rosenzweig. See House Hearing, 108th Congress, 'Can the Use of Factual Data Strengthen National Security ?', part II, serial no. 108–98, 20 May 2003, p. 85. This scene is recounted by Shane Harris, who outlines in great detail the twists and turns of the Poindexter programme. See Shane Harris, *The Watchers: The Rise of America's Surveillance State*, Penguin, New York, 2010.
8. If 'the system has a one in 100 false-positive rate (99 percent accurate)', and, '1 trillion possible indicators to sift through: that's about 10 events – e-mails, phone calls, purchases, web destinations, whatever – per person in the United States per day', then, 'This unrealistically accurate system will generate 1 billion false alarms for every real terrorist plot it uncovers. Every day of every year, the police will have to investigate 27 million potential plots in order to find the one real terrorist plot per month.' Bruce Schneier, 'Why Data Mining Won't Stop Terror', *Wired*, 3 September 2006.
9. This definition captures in summary form that given by the Department of Defense. See *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, p. 472.
10. Jeff Jonas and Jim Harper, 'Effective Counterterrorism and the Limited Role of Predictive Data Mining', *Policy Analysis* 584, Cato Institute, 11 December 2006, p. 8. See also Jeffrey Rosen, *The Naked Crowd*, Random House, New York, 2004.
11. See D. Jensen, M. Rattigen and H. Blau, 'Information Awareness: A Prospective Technical Assessment', *Proceedings of the 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Association for Computing Machinery, New York, 2003.
12. Glenn Greenwald and Murtaza Hussain, 'Meet the Muslim-American Leaders the FBI and the NSA Have Been Spying on', *The Intercept*, 7 September 2014.
13. Jensen, Rattigen and Blau, 'Information Awareness: A Prospective Technical Assessment', p. 9.
14. William Safire, 'You Are a Suspect', *New York Times*, 14 November 2002. Several features of the programme were transferred to the NSA. See Shane Harris, 'TIA lives on', *National Journal*, 23 February 2006.
15. See Keith Alexander, Mike Ennis, Robert L. Grossman, James Heath, Russ Richardson, Glenn Tarbox and Eric Sumner, 'Automating Markup of Intelligence Community Data: A Primer', *Defense Intelligence Journal*, vol. 12, no. 2, 2003, pp. 83–96, p. 84.
16. Ellen Nakashima and Joby Warrick, 'For NSA Chief, Terrorist Threat Drives Passion to "collect it all"', *Washington Post*, 14 July 2013.
17. Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, 23 January 2014, p. 8.
18. Office of the Director of National Intelligence, *Statistical Transparency. Report Regarding use of National Security Authorities*, 26 June 2014, p. 2.
19. In 'upstream collection', the siphoning of data packets, the data collection is larger than the selectors it targets. See Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program. Operated Pursuant to Sec on702 of the Foreign Intelligence Surveillance Act*, 2 July 2014, p. 124.
20. See John Napier Tye, 'Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans', *Washington Post*, 18 July 2014, and in particular the excellent article by Axel Arnbak and Sharon Goldberg, 'Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad', *Michigan Telecommunications and Technology Law Review*, May 2015.
21. See 'NSA's Largest Cable Tapping Program: DANCINGOASIS', 24 May 2004, on the *Top Level Communications* blog: http://electrospaces.blogspot.nl/2014/05/nsas-largest-cable-tapping-program.html.

22. See Amy Davidson, 'Presenting XKeyscore: What the N.S.A. is Still Hiding', *New Yorker*, 31 July 2013.
23. Office of the Inspector general, National Security Agency Central security Service, *ST-09–000 Working draft*, 24 March 2009, p. 13.
24. *PPD-28 Report: Bulk Collection of Signals Intelligence: Technical Options*, National Academy of Sciences, 2015, 3–3.
25. Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*, p. 29.
26. The 'Foreign Intelligence Surveillance Court' (FISC). See William Banks, 'Programmatic Surveillance and FISA: Of Needles in Haystacks', *Texas Law Review*, vol. 88, no. 7, June 2010, pp. 1633–67.
27. Kate Tummarello, 'Official: NSA's Work Is Like "Stop and Frisk"', *The Hill*, 11 April 2013.
28. Barton Gellman and Ashkan Soltani, 'NSA Surveillance Program Reaches "into the Past" to Retrieve, Replay Phone Calls', *Washington Post*, 18 March 2014. See http://cryptome.org/2014/05/nsa-mystic-identity.pdf. Ryan Devereaux, Glen Greenwald and Laura Poitras, 'Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas', *The Intercept*, 19 May 2014.
29. Gellman and Soltani, 'NSA Surveillance Program Reaches "into the Past" to Retrieve, Replay Phone Calls'.
30. Spencer Ackerman, 'Senators Challenge NSA's Claim to Have Foiled 'Dozens' of Terror Attacks', *Guardian*, 13 June 2013; Shaun Waterman, 'NSA Chief's Admission of Misleading Numbers Adds to Obama Administration Blunders', *Washington Times*, 2 October 2013.
31. See Bruce Schneier, 'How the NSA Threatens National Security', *The Atlantic*, 6 January 2014. See also Ellen Nakashima, 'NSA Cites Case as Success of Phone Data-collection Program', *Washington Post*, 8 August 2013.
32. 'Stabilizing Transatlantic Relations after the NSA Revelations'.
33. Edward Snowden, 'An Open Letter to the People of Brazil', *Folha de S.Paulo*, 16 December 2013.
34. United States SIGINT System January 2007 Strategic Mission Lis, http://cryptome.org/2013/11/nsa-sigint-strategic-mission-2007.pdf.
35. Michael Flynn, Rich Juergens and Thomas Cantrell, 'Employing ISR: SOF Best Practices', *Joint Forces Quarterly*, vol. 50, no. 3, pp. 56–61, p. 57 (see also David M. Houff, 'Antisubmarine Warfare Concepts Offer Promise For Counterterrorism', *Signal*, May 2010); Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, *Report of the Defense Science Board Task Force on Defense Intelligence Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations*, Washington DC, February 2011, p. 28.
36. Rick Wood and Tony McPherson, 'Video Track Screening Using Syntactic Activity-based Methods', Applied Imagery Pattern Recognition Workshop (AIPR), IEEE, 2012.
37. Bob Woodward, *Obama's Wars*, Simon & Schuster, New York, 2010, p. 7.
38. Peter Rustan, 'Change Agent', *Defense News*, 8 October 2010; Tom Lash, 'Integrated Persistent ISR', *Geospatial Intelligence Forum*, vol. 8, no. 4, 2010.
39. Dana Priest, 'NSA Growth Fuelled by Need to Target Terrorists', *Washington Post*, 21 July 2013.
40. Bob Drogin, 'Two Agencies Melding Minds on Intelligence', *Los Angeles Times*, 31 December 2004.
41. See 'Training the Corps', *Military Intelligence* PB 34–05–1, vol. 31, no. 1, January–March 2005, p. 54; www-03.ibm.com/software/products/en/analysts-notebook-family.
42. Derek Gregory, 'Lines of Descent', *Open Democracy*, 8 November 2011. Pattern of life analysis is defined more precisely as 'the fusion of link analysis and geospatial analysis'. See Tony Mason, Suzanne Foss and Vinh Lam, 'Using ArcGIS for Intelligence Analysis', Esri International User Conference, San Diego CA, 2012.
43. Flynn, Juergens and Cantrell, 'Employing ISR: SOF Best Practices', p. 1.
44. Stanley McChrystal, 'It Takes a Network', *Foreign Policy*, 21 February 2011.
45. 'Generation Kill: A Conversation with Stanley McChrystal', *Foreign Affairs*, March–April 2013.
46. John Inglis, *Remarks at GEOINT Symposium 2010*, 4 November 2010, p. 8. www.nsa.gov/public_info/_files/speeches_testimonies/GEOINT2010.pdf; Gareth Porter, 'How McChrystal and Petraeus Built an Indiscriminate "Killing Machine"', *Truthout*, 26 September 2011.
47. Porter, ibid.
48. Joshua Foust, 'Unaccountable Killing Machines: The True Cost of US Drones', *The Atlantic*, 30 December 2011. See also Jeremy Scahill, *Dirty Wars: The World is a Battlefield*, Nation Books, New York, 2013.
49. Human Rights Clinic at Columbia Law School, the Center for Civilians in Conflict, *The Civilian Impact of Drones: Unexamined Costs, Unanswered Questions*, September 2012, p. 8. But, as Derek Gregory has made clear, 'anyone who thinks that so-called "personality strikes" are somehow less deadly needs to read REPRIEVE's latest report': Reprieve, *You Never Die Twice: Multiple Kills in the US Drone Program*, 24 November 2011.
50. Cited by Gabriel Miller, 'Activity-Based Intelligence Uses Metadata to Map Adversary Networks', *Defense News*, 8 July 2013.
51. Letitia Long, 'Activity Based Intelligence Understanding the Unknown', *The Intelligencer: Journal of U.S. Intelligence*, vol. 20, no. 2, Fall/Winter 2013, pp. 7–15, p. 7.
52. Gregory Treverton, 'Creatively Disrupting the Intelligence Paradigm', *ISN*, 13 August 2011. The main foundations of ABI were laid in 2010 in a series of confidential strategic documents edited by Robert Arbetter, an old official of the NSA who became Director for Collection Concepts and Strategies under the Undersecretary of State for Intelligence.
53. Edwin Tse, 'Activity Based Intelligence Challenges', Northrop Grumman, IMSC Spring Retreat, 7 March 2013.