# Predictive Surveillance Systems and the *Dispositif* of Precautionary Risk: An Approach on Big Data Technologies in United States' Armed Drones and Policing Activity

Alcides Eduardo dos Reis Peron*

## *Introduction*

Over the past twenty years, a significant number of new data-oriented technological ventures have been introduced in US military and police circles with the tacit objective of streamlining procedures for tracking and identifying the various hazards that these institutions deals with. In general, these sophisticated surveillance devices (such as cameras) are embedded with software for facial recognition, imagery analysis and crime mapping. These instruments involve a compendium of data collection, correlation, and large data profiling technologies based on algorithms, and often involve machine learning techniques to make these procedures even more fast and refined.

There are several examples of such endeavours in the US military, such as the Predictive Battlespace Awareness Program, the recently developed Skynet Program, and the 'Project Maven'. It is no different in the police milieu, as we see the profusion of tools like Predpol, from the Los Angeles Police Department, and the Domain Awareness System (DAS), developed by Microsoft for the New York Police Department. All these programs and technologies were developed in the context of Global War on Terror as an effort to amplify the means of surveillance, production of knowledge, and precision in targeting in the cities and in military operations. They are 'intelligent' and automated monitoring systems which register imagery and collect several forms of data, allowing the users to identify (suspicious) patterns of behaviour and to recognise faces.

* The author would like to thank the FAPESP for its support and engagement in this research.

These military and police systems have been responsible for rendering surveillance and automated data processes increasingly central to operational practices, mainly after the attacks of 11 September 2001.[1] However, rather than guaranteeing greater capacity of surveillance, these instruments and programs provide their users with proactive and preemptive capabilities for action, allowing the identification of zones with greater potential of occurrences of crimes, and the identification of suspects based on their relational and behavioural profile.

Predictive Surveillance systems are registered in a context in which police and military practices, discourses, technologies, and operational concepts interact in the promotion of security policies and the fight against terrorism, in which the measurement of risk becomes a determinant for the establishment of proactive or preemptive actions. Not only are the risks of a terrorist plot and criminal actions perceived as part of the same semantic continuum, these potential incidences also become classifiable, measured and actualised through statistics and data from past occurrences. This knowledge, that sustains and guides the measurement of risk, therefore grants a rationality to governments, which we call statistical-predictive knowledge. It is based on algorithmic readings and correlations about past experiences (static and opaque evidence), in order to turn hypothetical risks into 'solid' evidence of the future, which supports immediate discourses and actions, and preemptive interventions. However, this 'statistical' authority of the risk appears to conform exceptional practices ranging from extrajudicial killings by US drones in Pakistan, Yemen, and Somalia, to internal police abuses such as reports and illegal detention in the United States.

In view of this, we follow the approach by of Claudia Aradau and Rens Van Munster2 who characterise risk as a dispositif, a

[1] At the time of the attacks, New York was already one of the most monitored cities of the world, analogue cameras and some informatised systems were at the core of its security apparatus. Since then, drone systems, agencies like Homeland Security and the National Security Agency were created or enforced to deal with security issues. See Cora Currier, 'A Walking Tour of New York's Massive Surveillance Network', in *The Intercept*, 24 September 2016, online at https://theintercept.com/2016/09/24/a-walking-tour-of-new-yorks-massive-surveillance-network (Here and subsequently, all internet links were last accessed on 12 May 2019.)

[2] Claudia Aradau & Rens Van Munster 'Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future', in *European Journal of International Relations*, Vol. 13, No. 1 (2007), p. 91.

heterogeneous assemblage of material and discursive elements oriented to the governance of social problems. In particular, the authors point to the emergence of a form of precautionary risk, whose discourses around catastrophes and their eminence coexist with the imprecision and uncertainty of futures calculated by predictive algorithms, ordering reality and legitimising discretionary actions of the authorities. Here, this dispositif responds to the urgency of a governmentality model of terrorism that continues to this day, since, as Didier Bigo explore, it is still capable of structuring an (in)security continuum which ensures that the struggle against certain social groups can be framed as a fight against terror. As Bigo puts it:

> The (in)security continuum is therefore a move that aims to transfer the legitimacy of the fight against a certain type of identified enemy against suspected ones, against collateral victims of security operations reframed as helping the potential enemy, against minorities identified as potential supporters of clandestine actions'.[3]

Thus, from the framework of Critical Security Studies and more specifically the works of Claudia Aradau and Didier Bigo, our objective in this article is to explore how these instruments of 'predictive surveillance' contributes to the production of a continuum of (in)security, by composing statistical knowledge with precautionary discourses and practices, in order to legitimise, or at least naturalise, arbitrary police and military practices. If, as Ulrich Beck4 puts it, risk would be a systematic way of dealing with the dangers and insecurities of modernity, which are not perceptible to human sensibility but detectable only through the 'sensorial organs of science', to what extent does this process border on exceptionality? In other words, to what extent is the materialisation of risk not also the materialisation of bias, as well as its elevation to the category of truth and reality?

In doing so, we will focus on exploring how this precautionary risk *dispositif*, in particular the technologies and operational concepts that constitute it, evolve from the common base

---

[3] Didier Bigo 'Rethinking Security at the Crossroad of International Relations and Criminology', in *British Journal of Criminology*, Vol. 56, No. 5 (2016), p. 12.

4 Ulrich Beck, *A Sociedade de Risco: Rumo a uma outra Modernidade* (Editora 34, 2010), p. 32.

of the so-called Revolution in Military Affairs (RMA), which would also be responsible for a deepening of relations between the military and police forces in the United States. Next, we will focus on exploring how these predictive surveillance tools have been adopted by the US Air Force in armed drones (the Skynet and Maven projects), debating their more latent limits and controversies. Finally, we will analyse the proliferation of predictive surveillance software in the U.S., discussing the main concerns and debates that have arisen from its deployment, especially regarding its use as a way of subjecting vulnerable communities. In our final remarks we point to the notion that this statistical-predictive knowledge is problematic not only in the assumption that it provides a clear view of future probabilities, once it relies on narrow databases or structuring the algorithm, but also because it elevates bias, prejudice to the status of proof, strengthening and perpetuating the governmentality of terrorism and other crimes.

### *RMA: The Material basis for the Dispositive of Precautionary Risk*

For Ulrich Beck, the idea of risk is inherent to the modernising process, marked by deep and radical uncertainties that may undermine social stability. In this process, paradigmatically, the modernity that produces the risks is the same one that has to create mechanisms capable of governing them and avoiding their spread. As he points out, 'The promise of security progresses with the risks and, in face of an attentive and critical public sphere, need to be continuously reinforced through cosmetic or effective interventions in the technical-economical development'.[5]

However, this perspective becomes flawed, as Aradau and van Munster[6] argue, because it does not succeed in making risk identification and management a way of organising reality and disciplining the future. Moreover, it understands risk as a macro-historical construct, given *a priori*, and not a construction. In contrast, Aradau and Van Munster focus on the notion of governmentality and *dispositifs* in Michel Foucault to characterise the idea of risk more critically and to properly insert it in the efforts of the United States in its fight against terrorism. Then, governmentality in Foucault's sense,

[5] Ibid., p. 24.
[6] Aradau & Van Munster, 'Governing Terrorism through Risk', p. 95.

is seen as a technique of government that relies on the population and instrumentalises economic knowledge as a way of producing and conducting acceptable behaviour. It presupposes a permanent administration of fear[7], since it demands the constant production and reproduction of threats to freedom as means of expanding the available instruments to combat and manage these same threats. It comes from the articulation between a Pastoral Power, which is anchored in the idea of salvation of the 'flock', as a justification for – to quote Foucault – 'conducting its conduct', and the emergence of the liberal art of governing, which conceives the government as a reactive technique to the demands of a social body with an apparent economic-utilitarian rationality.[8]

In Foucault's view, *dispositifs* are the set of relationships established between heterogeneous elements within society with strategic functions including discourses (pronounced and non-pronounced), institutions, architectures and regulations, whose composition aims to respond to an urgency, and to sustain the dynamics and rationality of governmentality.[9] In this context, as Thomas Lemke[10] points out, *dispositifs* can be understood as technologies of government, which through consensus and coercion operate to systematise, regulate and stabilise social and power relations, avoiding both the dissolution of individual freedoms and the imposition of sovereign power and domination. Thus, 'governmental technologies bring together scientific knowledge, technical devices, anthropological hypotheses and architectural forms in strategic ways of forming relations of conduct'[11]. Moreover, as Aradau[12] points out, the process of securitisation, and the development of security processes can be understood as a process of

[7]According to Thomas Lemke, fear becomes instrumental, cultivating a permanent sense of susceptibility and vulnerability, which does not necessarily lead to a mere expansion of the means of security, but to the breaking of the covenant of security between State and population, allowing the transgression of the limits defined for the state action. See Thomas Lemke, *Foucault, Governamentalidade e Crítica* (Politéia, 2017), p. 69.

[8] Michel Foucault, *Segurança, Território e População: Curso dado no Collège de France (1977-1978)* (Martins Fontes, 2008), p. 298.

[9] Edgardo Castro, *Vocabulário de Foucault* (Autêntica, 2016), p. 194.

[10] Lemke, *Foucault, Governamentalidade e Crítica*, p. 27.

[11] Sven Opitz, 'Governo Não-Ilimitado: o Dispositivo de Segurança da Governamentalidade Não-Liberal', in *Ecopolítica*, Vol 2 (2011), p. 22.

[12] Claudia Aradau, 'Security that Matters: Critical Infrastructure and Objects of Protection', in *Security Dialogue*, Vol 41, No. 5 (2010), p. 509.

materialisation that emerges out of the interaction and intra-action between material-discursive practices.

In this sense, Aradau and Van Munster[13] understand that since Global War on Terror demands an insatiable amount of knowledge, population-profiling, vigilance, intelligence and knowledge about catastrophe management and prevention, it can be understood as a form of governmentality. Because it involves knowledge and decision-making based on this knowledge, strategies for wars and surveillance, injunctions for integration, and drastic policies against antisocial behaviour, all of these are activated and operationalised by the *dispositif* of precautionary risk. According to the authors, due to the rise of a neoliberal rationality, and the terrorist threat (uncertain and catastrophic risk), the idea of precautionary risk emerged. This *dispositif* encourages that no precautions be taken on the conditions of knowledge and available technologies but rather recommends action even under conditions of casual and scientific uncertainty, given the catastrophic contingency of the future on terrorism. In short, these technical instruments are not entirely precise, and just give a glimpse of knowledge about future conducts and actions of the monitored ones. Even under this 'limited' information's condition, this *dispositif* authorises the use of force. Where there is uncertainty and statistical predictive models are not able to anticipate the future, the precautionary *dispositif* complements it with discourses, technologies based on algorithmic profiling and prediction and constant, broad and permanent vigilance.[14]

Therefore, the precautionary risk involves the study of the discourses of authorities regarding the eminence of catastrophic attacks, discourses of networks private expert networks, associated with information tools of risk management, surveillance, reports and other documents that points to the constant possibility of attacks, and the correlation between common crimes and terrorism. However, the precautionary risk *dispositif* has a material and technological dimension that goes beyond the institutions and organisations created for governing terrorism, involving technical artefacts, information systems, discourses on these instruments, and a wide range of military doctrines that support the operation of these technologies.

---

[13] Aradau & Van Munster, 'Governing Terrorism through Risk', p. 91.
[14] Ibid., p. 104.

In this sense, the technical and discursive bases of this *dispositif* is being managed since the mid-1990s, with the Revolution in Military Affairs (RMA). There, new technologies were developed and dual operational concepts were defined that would be deployed both for armed conflicts and for the management of public safety. These technologies gain prominence thanks to a series of economic and political problems, such as the military budget cuts during the Reagan, Bush and Clinton administrations (1981-1989, 1989-1993 and 1993-2001) and the so-called Vietnam Syndrome – a collective fear by certain political actors in getting involved in military operations with great risk of losing people's lives and political support – among other issues.[15] In that time, the Pentagon and the entire military bureaucracy were encouraged to modify the current operational concepts, combat models and operations of the Armed Forces, and the technologies available to them. The principles guiding these changes were those of 'surgical wars,', low-intensity warfare, informational warfare, and preventive-preemptive actions, all oriented by a new operative concept called 'situational awareness' – understood as a regime of broad visibility of the operational field, in which the monitoring information from different channels can contribute to the strategic and tactical management of the operations.[16] That is to say, the conflicts that the United States would henceforth confront, would be marked by the intensive use of surveillance and monitoring technologies, such as satellites and surveillance drones. The employment of these new technologies would not only be used over battlefields, but also across cities, allowing wide recognition and awareness of the theatres of operations.

The imaginary of this type of conflict has been summarised in a series of military doctrines, such as the well-known Shock and Awe (1996), that understands the information management apparatus as a determinant element for the operations, a kind of 'network-centric warfare'. According to Albert and Hayes,[17] the idea of situational domain awareness, or situational awareness, develops from the

[15] Alcides Eduardo dos Reis Peron, 'No Boots on the Ground: Reflections on the US Drone Campaign through Virtuous War and STS Theories', in *Contexto Internacional*, Vol. 40, No. 1 (2018), p. 64.

[16] Ken Oscar, 'Can Revolutions be Managed?', in R. Matthews & J. Treddenick (eds.), *Managing the Revolution in Military Affairs* (Palgrave Macmillan, 2001), p. 128.

[17] David Alberts & Richard Hayes, *Power to the Edge: Comand… Control… in the Information Age* (CCRP Publication Series, 2003), p. 16.

vigilance and production of information about the enemy, which would guarantee an advantage for the 'surgical' action on the targets. The idea of Shock and Awe as applied in the Iraq War (2003-2010) was to conduct military operations of rapid and powerful domination, incapacitating or discouraging the opponent from reacting.[18]

In the mid-2000s, this information management apparatus would be reinforced by the most sophisticated technologies for massive data collection and management. This development happened mainly through a greater participation of the Central Intelligence Agency (CIA) and the Security Agency (NSA) in the sorting of information and data. In addition, with the attacks of September 11 and the following 'Global War on Terror', increasingly the orientation of the armed forces and police came to be on preventing the occurrence of attacks through intensive surveillance and monitoring of citizens and suspects around the globe. In the meantime, various institutions have been created to face the alleged proliferation of internal threats, such as the US Department of Homeland Security, as well as doctrines that guide decision-making about international conflicts such as preemptive war, and 'predictive battlespace awareness'.[19]

In this case, the doctrine of 'predictive battlefield awareness' developed under the Total Information Awareness Program (TIA), managed by the Defense Advanced Research Projects Agency (DARPA), aimed at collecting massive travel data and financial activities from private sources, to predict and act on terrorist threats.[20]Although the TIA was discontinued in 2003, the doctrine of predictive battlefield consciousness continued to be instrumental, by example, for the equipment of armed drones in US 'counterinsurgency' operations ever since.[21] At the heart of the

[18] Harlan K. Ullman & James P. Wade, *Shock and Awe: Achieving Rapid Dominance* (The National Defense University, 1996), p. 88.

[19] Robert A. Piccerillo, & David A. Brumbaugh, *Predictive Battlespace Awareness: Linking Inteligence, Surveillance and Recoinnassance Operations to Effects Based Operations* (The Pentagon, 2004), p. iii.

[20] G. Mack, *Total Information Awareness Program (TIA)*. (System Description Document, 2002), p. 24.

[21] These Counterinsurgecy operations begun during George W. Bush's administration, and were joint operations with intelligence agents and military, seeking to disrupt terrorist networks and plots. The majority of these drone strikes have been taking place in Somalia, Yemen and Pakistan. See Peron, 'No Boots on the Ground', p. 59.

doctrine was the integration of several data collection systems, with the aim of constructing a specific domain of the predictive future, that is, of the possibilities of acting in response to the predictions about the behaviour of targets, as presented in its general lines: 'the knowledge of the operating environment that enables the commander and his or her personnel to correctly anticipate future conditions, access changing conditions, prioritize, and explore emerging opportunities while mitigating the impact of unexpected, unexpected actions.'[22]

In face of the closure of TIA activities in the USA, the use of these instruments and techniques was primarily carried out overseas, under the tutelage of the armed forces, which would verify their effectiveness in combat, and their adaptability in adverse territories. As Stephen Graham[23] argues, this process was envisaged and intended by the RMA, in order to use foreign urban and 'wild' spaces as testing laboratories for surveillance, tracking and monitoring systems for the management of public safety. He suggests that the RMA sets that urbanisation processes in the global south have been imagined and represented by US military theorists as processes that significantly undermine US interests and their techno-scientific hegemony, since cities are perceived as blockages to military strategies of global surveillance and power projection.[24] However, according to him, these techniques applied in countries from the Global South would be transported back to their country of origin as innovative security solutions, proven in battle by corporate coalitions that connect businesses and governments.[25] Thus, algorithmic surveillance devices widely used both for international military operations and policing in the cities, make up a wide range of instruments available to the government of the 'Global War on Terror'.

### *Skynet and Maven: Pushing the 'predictiveness' to the limit*

By the mid of the 1980s, with the so-called Revolution in Military Affairs promoted by the Reagan Administration, a discourse of

[22] Piccerillo & Brumbaugh, *Predictive Battlespace Awareness*, p. iii.
[23] Stephen Graham, 'Surveillance, Urbanization and the US "Revolution in Military Affairs"', in David Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond* (Willan, 2006), p. 250.
[24] Ibid., p. 255.
[25] Stephen Graham, *Cidades Sitiadas: o novo urbanismo militar* (Boitempo, 2016), p. 32.

surgical and fast warfare became increasingly common inside the barracks as well as in the corridors of the Pentagon. This discourse, made up by the new doctrines of 'Network Centric Warfare' and in the mid 1990s, 'Shock and Awe', stated that it would be possible for the US Armed Forces to conduct low-intensity conflicts, with just a few 'collateral effects'. These doctrines hold that thanks to new information and communication technologies, such as links with satellites, and radio links with drones, war would become less destructive, because it would be more precise, and more combatant lives would be preserved, once they would be displaced from the conflicts. This reordering views drones, such as the Predator MQ-1,[26] as important vehicles of surveillance and intelligence-gathering for optimising military operations.

Armed drones fall in the category of remote-controlled weaponry mediated by graphic and/or manual interfaces, similar to other stand-off weapons, such as smart bombs, which came to be ostensibly used since the Gulf War (August 1990 – February 1991). The use of armed drones has been an important element of recent American military operations at the border between Afghanistan and Pakistan. According to data provided by the New America Foundation platform,[27] since 2004 there have been over 400 drone strikes in the region, leading to more than 3.5 thousand deaths, of which 17% were civilian and unknown casualties. The remaining were alleged militants with terrorist ties, indicated by the 'pattern of life' analyses of the victims[28]. This, however, remains a controversial topic, since the actual identity of the bulk of airstrike victims is hard to determine, not only because of the destruction caused, but due to the lack of information made available by the Pentagon. Only about fifty-two of them were confirmed leaders[29] of terrorist organisations marked as priority targets by the US government.

Extrajudicial killings with drones are organised in two ways.

---

[26] The Predator MQ-1 was developed in the end of the 1990's by the General Atomics. It was firstly equipped with hellfire infrared missiles, and it has flight autonomy of 1.2 thousand kilometers. See Peron, 'No Boots on the Ground', p. 65.

[27] New America Foundation, 'Drone Strikes: Pakistan', in *New America*, undated, online at https://www.newamerica.org/in-depth/americas-counterterrorism-wars/pakistan.

[28] Nina Franz, 'Targeted Killing and Pattern-of-Life Analysis: Weaponised Media', in *Media, Culture & Society*, Vol. 39, No. 1 (2016), p. 112.

[29] Examples of high-profile targets are Zuib al-Zahibi, a well-known commander of al Quaeda in Pakistan, and Sheik Mansoor, an al Quaeda leader in Egypt. See New America Foundation, 'Drone Strikes: Pakistan'.

First, through targeted killing, where the operations are geared towards eliminating very specific targets based on the work of intelligence officers in the field (known as human intelligence, HUMINT), as well as data collected from the screening of images (known as imagery intelligence, IMINT) performed by drones. Another method would be signature killing which is, as Gregoire Chamayou[30] puts it, based on the visualisation of 'targets' through infrared cameras, identifying heat signals as bodies and creating an archive of images. This material is cross-referenced with information about geolocation and telephone data from the suspects, building what is called patterns of life.[31]

Since 2012, however, the US Air Force and the NSA are developing a system for crossing data obtained by the drones, a program called *Skynet.* [32] This program should be able to garner data for building dynamic and relational communication patterns, through intelligence gathering, and connect this information to social networks, cross-checking it both with the images and records about patterns that are considered suspicious.[33] Thus, drones integrate an extensive communication chain, made up of people, instruments and institutions which operators call the 'Kill Chain'.[34] The adoption of data mining and profiling techniques allows a new way of visualising the targets focusing on the flow of data and metadata produced by them.

Also, since 2017, the Pentagon has been investing in public-private partnerships to carry out projects such as the 'Maven', which attempts to incorporate deep learning algorithms for automatic detection and recognition of suspects in military drone video-feed. This has raised many questions, both by human rights organisations

---

[30] Grégoire Chamayou, *Théorie du Drone* (La Fabrique, 2013), p. 72-73.

[31] Both Nina Franz and Grégoire Chamayou use this term as a 'native concept', once it is widely employed by US military to describe their activities.

[32] Cora Currier, Glenn Greenwald & Andrew Fishman, 'U.S. Government Designated Prominent Al Jazeera Journalist as "Member of Al Qaeda"', in *The Intercept,* 8 May 2015, online at https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list.

[33] The Pentagon or the CIA do not clarify how the algorithm works, and which patterns could be considered suspicious, what makes really difficult to understand whether a strike can be considered legal or illegal.

[34] Derek Gregory 'From a View to a Kill: Drones and Late Modern War', in *Theory Culture Society*, Vol. 28, Nos. 7-8 (2011), p. 193.

and academics.[35] The most common point of criticism is the fear that this process of automation will become increasingly opaque, and unable to guarantee the basic rules of engagement in armed conflicts, including discrimination and proportionality.

These processes, based on algorithms for correlation and prediction, invoke data from the past as concrete evidence for the establishment of predictions about future behaviour. It forms the device of precautionary risk, which from a statistic-predictive knowledge is duly anchored and supported by speeches of just war, and the eminence of terrorist attacks, thereby authorising preemptive attacks against targets in other countries. More than that, by making patterns of behaviour, connections and associations (not always stable and definitive) visible through data mining and profiling, this procedure is responsible for building up a visible network of enemies, insurgents, and terrorists where there was only an invisible dynamic of relationships (neither characterised nor profiled). In Beck's perspective, the gaze of science begins to make the risk visible and eminent.[36]

Nevertheless, as several analyses and investigative news articles have exposed, this system has been responsible for errors and illegalities. One example is the fact that in 2015, this system was responsible for labeling Ahmad Muaffaq Zaidan, an Al Jazeera journalist, a member of Al Qaeda, since the program mapped his pattern of behaviour (movement and relational) and telephone communications, cross-checking it with data from other suspects.[37] Although this seems to be a case of 'false positive',[38] it demonstrates the difficulties of tracking and classifying such systems based on predictive algorithms, which, as Aradau and Blanke point out, 'are

---

[35] Colin Clark & Paul McLeary, 'Legal Scholars, Software Engineers Revolt against War Robots', in *Breaking Defense,* 5 April 2018, online at https://breakingdefense.com/2018/04/a-treaty-to-ban-autonomous-intelligence-weapons.

[36] Beck, *A Sociedade de Risco*, p. 32.

[37] Currier, Greenwald & Fishman 'U.S. Government Designated'.

[38] A false positive can be defined as a test result that incorrectly indicates that a particular condition is present. This means that a 'false' event alert may be triggered even if it has matched the conditions for it. See Martin Robbins, 'Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan?', in *The Guardian,* 18 February 2016, online at https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan.

designed to substantiate the suspicion the security analyst already has, rather than predict new suspects or suspected behavior'.[39]

*DAS, Predpol and the actualisation of the offence*

Between 1970 and 1990, several American cities began to observe an increase in crime, whether in terms of violent crimes or minor robberies and patrimonial robberies.[40] According to Loic Wacquant,[41] this increase in crime would be related to a greater economic weakness and bankruptcy of a social state, as well as a greater legal punitivism whose focus was on a type of crime practiced by the poorest of the social strata, and in areas where these groups live together.[42]

Since the 1990s, David Garland[43] has been pointing to the emergence of a 'new culture of control' in the United States, where surveillance and monitoring practices are no longer focused on suspects only but is widened in scope to potentially include all citizens, looking for signs of future disturbances such as suspicious behavioural patterns, monitored all over the city, with emphasis one zones of decay and deprivation. In other words, the governance mechanisms of conduct are crucial, modulating them throughout the social spectrum in order to stimulate practices considered healthy and normal, which facilitate the process of identification and sanctioning of 'deviations'. Security ceases to be a disciplinary function, becoming a function of the guiding the disorder, which calls for directly engaging any form of invisibility that may cloud perspectives on circulating people in the city.

During this period, there was a growing militarisation of police activity in the United States, which implies that police has assumed attributes that are traditionally part of the toolkit for the

[39] Claudia Aradau & Tobias Blanke, 'The (Big) Data-security assemblage: Knowledge and Critique', in *Big Data & Society*, unnumbered (2015), p. 08.

[40] United States Department of Justice. 'Uniform Crime Rate Statistics', online at https://www.ucrdatatool.gov/Search/Crime/Crime.cfm.

[41] Loic Wacquant, *Punir os Pobres: A Nova Gestão da Miséria nos Estados Unidos*. (Revan, 2003), p. 09.

[42] Loic Wacquant suggests that along the 1970's and 1980's, the legal punitive system in the United States was conformed in a way to criminalize several aspects of the poorer classes, in an attempt to promote segregation and exclusion. See Ibid., p. 09.

[43] David Garland, *A Nova Cultura do Controle: Crime e Ordem Social na Sociedade Contemporânea* (Revan, 2008), p. 367.

armed forces, especially in regards to their commitment to the adoption of high technology, and their movement to other areas.[44] This environment, whose production of information is extremely broad, requires the adoption of doctrines, devices and structures that allow greater capacity for 'situational awareness' to the police. This process intensified after the attacks of September 11, with a greater circulation of technologies, speeches and operational concepts coming from the RAM in the U.S. police milieu. This would be the result of an intense mediation between the military and police sectors promoted by government agencies, private companies, risk management companies, and consulting firms. This network of 'experts' ensured the production of consensus and discourses that helped to connect internal and international security, thereby merging initiatives to combat crime and terrorism on the same (in)security continuum. In this context, the concept of situational awareness developed by the doctrines of 'Shock and Awe' and enhanced from TIA initiatives, builds on police vocabulary, underpinning hyper-vigilance practices in the fight against crime and terrorism.

Thus, counter-terrorism initiatives will be responsible for the development and application of a range of algorithmic surveillance, profiling and massive data collection technologies, which will spin-off as 'effective' anti-crime practices such as the Predpol system, and the Domain Awareness System (DAS). These initiatives come to translate complex demands of hyper vigilance, identification of enemies and 'suspicious behaviors', as well as the probability of occurrence of crimes, through predictive algorithms.

The DAS is characterised as a technology for tracking and profiling criminal and suspicious conducts from analytical videos, and integrating this information with criminal databases. In practice, it is a system that combines information from diverse databases (police, federal revenue, and traffic department) with camera systems, and peripheral police devices, allowing greater efficiency of the service and dispatch activities, and heatmaps of criminal practices, allowing for proactive police actions to the detriment of merely reactive actions in the fight against crime and terrorism.[45]

---

[44] Kevin D. Haggerty & R.V. Ericson, 'The Militarization of Policing in the Information Age', in *Journal of Political and Military Sociology*, Vol. 27, No. 2 (1999), p. 234.

[45] New York Police Department, *DAS: Public Security Privacy Guidelines* (2009), p. 02.

Predpol (an acronym for Predictive Policing) is a software that, like the DAS and the Skynet systems, operates on the basis of predictive algorithms and is designed to analyse past criminal statistics, integrating various criminal and legal databases to generate probabilities of the occurrence of future crimes in various regions of the city. In this case, the rounds and police activities are guided by this dynamic of actualising the risk of future crimes, and in the case of the DAS, the actualisation of future suspicious conduct.

However, these 'solutions' have been the subject of much doubt and questioning by researchers, authorities, and associations, since they tend to reinforce and legitimise discriminatory police practices, especially on more vulnerable communities. A study by the University of Utah[46], for example, shows that Predpol suffers from the 'Feedback Loop'. That is, these systems based on past data and statistics, tend to punish vulnerable communities, especially when this technology relies on criminal databases that for years have been supplied with data from that same community. We could this phenomenon a 'data ghetto' which generates a perpetual 'loop' in the probability of occurrence of crimes in the same areas.

Essentially, the DAS and Predpol make visible and actualise the risks to which cities would be exposed, mobilising statistics, data, information and images through predictive algorithms or analytical alerts. They compose the device of precautionary risk by producing statistical-predictive knowledge, 'materially' basing the discourses on the risks capable of disturbing the social order. However, rather than attacking the 'invisibility' of risks, these systems seem to guarantee the perpetual replacement of mechanisms of subjection, exclusion and segregation for significant portions of the population. This implies that the biases that characterise the feedback loop – usually manifested in the collection of data from the same territory to form their databases, and the selection of just a few variables – cannot be understood as errors at all, but rather as a manifest of political intentionality in some of the cases of the algorithmic design of this tool.

*Final Remarks*

[46] Danielle Ensign, et al., 'Runaway Feedback Loops in Predictive Policing', in *Proceedings of Machine Learning Research*, Vol. 81 (2018), p. 11.

Strictly, algorithms can be understood as solutions or logical instructions directed to the accomplishment of tasks or solving specific problems, that are later translated into a programming language. These instructions would depend on a data input that can be given in different ways, by the most varied sensors, and from the programming, which allows it to correlate and produce new information. The algorithm, like technology in its broadest expression, is a product of human agency and action, the result of a series of interactions, disputes between values, interests, and programming that, as Bruno Latour[47] asserts, are crystallised in artifacts. In that sense, Joshua Scannell[48] states that predictive algorithms only 'mathematize' a discriminatory police aesthetic, organising the city around unrealistic perceptions, or a 'reorganization of ontology into computing.' The algorithm would, therefore, be a political object, a combination of forces imprinted on the social. On this, the author argues that these algorithms, in their attempt to reduce the 'social context mess in lean computation' in an aesthetic and simplistic decision, end up eliminating the social from sociability – meaning the contempt to the complexity and subjectivity of the social, which begins to be mathematically translated as multiple linear relations and correlations.

Depending on the weights and criteria attributed to the signals and to the past experience that 'trains the algorithm', a particular course of action is pointed out as definitive. It is some form of prediction that eliminates other possible courses of action, crushing the subjectivity of the subjects at the moment they conform the innumerable possibilities of future actions into a small compendium of pre-established ordinances. That which is uncertain and invisible becomes certain, clear, and present, as a will which is realized only by considering its possibility, authorising and legitimising discretionary actions under the preemptive-proactive mantle.

---

[47] Bruno Latour, 'Technology is Society Made Durable', in John Law (ed.), *A Sociology of Monsters: Essays on Power, Technology and Domination* (Routledge, 1991), p. 129.

[48] Josh Scannel, 'What can an Algorithm Do?', in *DIS Magazine* (2016), online at http://dismagazine.com/discussion/72975/josh-scannell-what-can-an-algorithm-do.

As Cathy O'Neil[49] points out, the fact that many programmers or mathematicians who develop algorithms are seldom aware of the end-use and purposes that their products serve, opens room for inconsistencies in the creative process. It is in this context that the author argues that this dynamic of algorithmic governmentality tends to favour a portion of society (which is generally more affluent) which will never be considered a deviation that ought to be normalized, while reaching a significant portion of the underprivileged, producing exclusions and discriminations.[50]

The *dispositif* of precautionary frames risk as a construct that 'tames' the future as a way of authorising and legitimising actions in the present. It is through this mechanism that anticipatory measures are taken as reasonable and necessary to avoid disorder, the emergence of crimes and catastrophes. Strictly speaking, it is through this *dispositif*, in its clear dimension of sociotechnical assemblage, that exceptional measures are naturalised and normalised in daily police and international military activity, producing this continuum of (in)security, where international threats and local crime is treated as being of a similar nature, demanding the interchange of knowledge and practices to assure the expansion of the ways of controlling and mitigating it. This actualises domestically several excessive practices as essential means for guaranteeing order, while targeting vulnerable communities as a way to reinforce the sense of security in other segments of the society.

From a theoretical point of view, this article sought to conciliate Critical Security Studies to an analytic of technology and *dispositifs*, exploring how discourses, artifacts and practices make up government technologies that structure and organise social life. This approach is made possible through authors in the Critical Security Studies, who have progressively inculcated Foucault's vocabulary in security debates, and have established new approaches between technology and society through a critique of the concept of *dispositif*. Moreover, this article demonstrates the urgency of drawing up approximations that take account of this new range of sociotechnical

---

[49] O'Neil, C. *Weapons of Math destruction: How Big Data Increases Inequality and Threatens Democracy*, (Broadway Books, 2017), p. 03.

[50] Ana Torres Menárguez, 'Entrevista com Cathy O'Neil: "Os Privilegiados são analisados por pessoas; as massas por máquinas"', in *El País*, 21 November 2018, online at https://brasil.elpais.com/brasil/2018/11/12/tecnologia/1542018368_035000.html?fbclid=IwAR3AKTfZi9Mma80N1HlvTNBMIlQHqSTaIJTvI4W9qup.

assemblages that have marked the exercise of (in)security in the central countries, in international conflicts, and which has gradually expanded to countries of the Global South as a way of intensifying policies to control and curtail freedoms.

---