Surveillance Capitalism and Crisis

Kees van der Pijl
Centre for Global Political Economy
University of Sussex
January 2018

What follows was written as a background document for the referendum on the blanket surveillance law in the Netherlands in March 2018 and part of a book project, 'The End of Political Compromise in Capitalism'. I argue that surveillance is part of the 'War on Terror' complex, which in turn evolved as a 'Strategy of Tension' after the model best known from the Italian experience in the 1970s. There it served to prevent the Left, and the Communist Party in particular, from advancing further towards participation in government. After the state capitalist turn of China and the collapse of the Soviet bloc and the USSR, the global wage-dependent but underemployed population grew to around 3 billion people of which one third inhabit fast-growing slums. Controlling this vast human mass became a core issue in managing the post-Cold War global political economy. The United States, profiting from its military pre-eminence, its role as the provider of the world's reserve currency and enjoying the privilege of running permanent budget and current account deficits, from the 1970s worked with the emerging IT industry to establish a global security state grounded in 'Total Information Awareness'. Based on this information advantage, global society is being kept in a state of tension by a range of intelligence activities targeting 'demographic bulges' in the reserve army of labour, even risking or provoking acts of violence against US/Western targets to allow armed control to be imposed. Mass surveillance and a spreading war after 2000 serve to stir the surplus population into activity and a domestic politics of fear has been deployed to win public support The Israeli-US NeoCon project of a War on Terror was revived after the Twin Towers attacks on 9/11, combining the attack on terrorists with pre-emptive war against 'states supporting terror'. Ultimately the doctrine behind the global strategy of tension entails the explicit option and regular practice of targeted assassination of opponents.

Introduction

The global surveillance regime by the United States as part of the 'Five Eyes' (the UK and the Anglophone settler states), revealed to the world by Edward Snowden (cf. Greenwald 2014), here is situated in the context of the 'War on Terror', officially pronounced in response to the 9/11 attacks but much longer in the making. Legislation to make this surveillance regime official also in other NATO countries has meanwhile been introduced. In France, the provisions of the state of emergency, which by definition is temporary, have been turned into a regular law which remains in force until revoked; in the Netherlands, a blanket surveillance law was rushed through parliament in an open vote in July 2017. It will be subject to a consultative referendum in March 2018. What is the background of these developments?

Reporting from a military base in Fort Campbell, Kentucky, the author of a newspaper article titled 'the American era of endless war' (Jaffe 2011), points out that the idea that at some point war would be over, as in the wars against Japan and Nazi Germany, today has been abandoned.

> In previous decades, the military and the American public viewed war as an aberration and peace as the norm. Today, radical religious ideologies, new technologies and cheap, powerful weapons have catapulted the world into "a period of persistent conflict," according to the Pentagon's last major assessment of global security. "No one should harbour the illusion that the developed world can win this conflict in the near future."

Highlighting how as a result of endless war, the military are beginning to lose touch with civilian society, the author also notes that 'The endless conflict…has triggered major changes in the way Americans view war and peace.' 'Peace… has faded from any debate in Washington surrounding the wars… [It] has become something of a dirty word in Washington foreign-policy circles.' 'In the immediate aftermath of 9/11, Americans were willing to bear almost any price for their security. One lesson of today's endless war seems to be that Americans will have to learn to live with a certain amount of insecurity and fear' (Jaffe 2011).

My argument is that the War on Terror, and by implication, the surveillance regime prescribed and legitimated by it, may be understood as a 'Strategy of Tension' after

the model best known from the Italian experience in the 1970s. There it served to prevent the Left, and the Communist Party in particular, from advancing further towards participation in government by provoking and staging violent incidents and chaos. Today the strategy of tension is aimed at the working class, or rather, the semi-urbanised, informally employed reserve army of labour (Davis 2017). Its purpose is to control this human mass through a coercive regime in response to its alleged criminal or terrorist tendencies.

After the state capitalist turn of China and the collapse of the Soviet bloc and the USSR, the wage-dependent but mostly underemployed population grew to around 3 billion people directly exposed to capital. Controlling this vast human mass became a core issue in managing the post-Cold War global political economy. As Raúl Delgado Wise and David Martin write (2015: 75, emphasis added), the neoliberal capitalist economy has no use for such a large workforce and as a result we are witnessing '*a brutal and uncompromising attack on the living and working conditions of the working class on a global scale*.'

> This process, marked by an intensification of asymmetries between countries and regions as well as an unprecedented social polarization, has been the background of, until recently unimaginable, exacerbation of the contradictions of the capitalist system, provoking a profound civilizational crisis affecting the whole of humanity.

Basically were are looking at a reserve army of labour, because owing to the automation of production and the simultaneous application of neoliberal structural adjustment policies, the chances of being regularly employed have been greatly reduced. The formation of the reserve army into a class for itself, a conscious subject of social relations, therefore must be prevented. The new strategy of tension serves to achieve this end. By provoking, intentionally or not, pockets of surplus humanity into violence, it imposes a permanent state of exception, allowing the 'brutal and uncompromising attack' to be sustained and opposition to it silenced. The West, led by the United States and with Israel in the role of a front-line state, has a long history of developing repressive solutions for their own societies to keep the black and Palestinian populations, respectively, in a state of submission. In the War on Terror this experience is applied, for the first time, on a truly global scale. Other rulers and/or oligarchies, such as Russia's or China's, make no secret of wanting to join this War on

Terror, but here another dimension of global political economy, rivalry between imperialist centres, cuts across a potential global coalition against the underclass. This situation resembles World War I, when the great powers clashed but nevertheless shared the common goal of beating down their own working classes.

The United States has sought to turn its historic advantage of hosting the world's key IT industries into a competitive advantage. Profiting from its military pre-eminence, its role as the provider of the world's reserve currency, and enjoying the privilege of running permanent budget, commercial, and current account deficits, the US worked with the IT firms to establish a global security state grounded in 'Total Information Awareness'. This is the link between the surveillance regime (which includes the voluntary deposition of personal data in social media) and the War on Terror. On the basis of its information advantage, the United States keeps global society in a state of tension by a range of military and intelligence activities targeting 'demographic bulges' in the reserve army of labour. In the process, even risking or provoking acts of violence against US/Western targets is part of the scenario *because this allows armed control to be imposed*. A domestic politics of fear has been deployed to win public support.

All this was explicitly discussed as a single project in the Israeli-US NeoCon discussions on a War on Terror. It was originally worked out in the early 1980s and revived after the Twin Towers attacks on 9/11, combining the attack on terrorists with pre-emptive war against 'states supporting terror' as well as imposing the corollary surveillance regime and suspending a range of freedoms on the home front.

Ultimately the doctrine behind the global strategy of tension entails the explicit option and regular practice of targeted assassination of opponents. 'The subliminal purpose of terror tactics,' Douglas Valentine argues in his book on the 'Phoenix' assassination programme in Vietnam, 'was to *drive people into a state of infantile dependence*. In this sense, the CIA psy[chological] war[fare] experts were not exorcists come to heal Vietnam and liberate it from Communist demons; their spells were meant to break up the society and project its repressed homicidal impulses onto the Communists' (Valentine 2000: 63, emphasis added). This insight still today applies to the condition of Western society in the War on Terror. As Dominick Jenkins observes, the Bush administration began the practice of making al-Qaeda a blank screen for the people's fears; the spectacular theatrics of the Twin Towers collapses

was exploited to show ‘the existence of a new kind of terrorist network with the power to threaten civilisation itself’ (Jenkins 2002: 265).

In what follows I first describe how the existence of a ‘Deep State’ with its centre in Anglo-America, was identified in the 1950s and how it evolved into a global spying machine from the Second World War on, able to unseat even its own political leadership when it was deemed necessary to do so. Secondly we turn to the Neo-Conservative project of a War on Terror, which took surveillance to new levels. The background for this were the repressive practices developed by the UK, the US and Israel in dealing with resistance. Thanks to its ability to finance domestic research by running large deficits financed by borrowing, the United States after 1971 began to build up an IT industry under the close watch of its national security state, with which the War on Terror was eventually fought as well.

The Post-Cold War, global intelligence infrastructure that grew out of it was then applied to a key problem big capital faced after the collapse of the USSR triggered a global restructuring of production: the existence of a billion-size surplus population, a reserve army of labour for which no employment was to be expected . This required devising control strategies of various types. After 9/11, the NeoCons revived the War on Terror concept to stir and then repress segments of this vast reserve army of labour, developing the notion of *Total Information Awareness* to allow it to know in advance, not just the intentions of rival states ranged against the West or just insufficiently submissive, but more particularly, the potential systemic opposition to capitalism at home and abroad. Using double agent tactics as well as provocation and targeted assassination, this has created the condition of endless war and a politics of fear sustaining it. Politics and society today operate under a permanent state of exception in which the Internet has been turned into a vast search engine on the lookout for meaningful opposition. Meanwhile in the name of weeding out ‘fake news’, the big Internet companies such as Google have changed their algorithms to prevent Left websites from popping up in searches by the public: the *World Socialist Website, Global Research*, and others, have already experienced sharp declines in numbers of visitors (Tveten 2018: 22). Facebook takes orders from the United States and Israeli governments to remove accounts (Greenwald 2017). Why do these large Internet companies collaborate, and why do they collaborate with these two governments specifically? That is what I intend the clarify in the pages that follow.

As to the method used, when anyone in the current post-modern conjuncture seeks to draw the contours of a larger historical process and identify *agency* in it, the routine dismissal centres on a supposed 'conspiracy theory'. The ultimate consequence of that objection would entail dispatching with the notion of historical structure and process altogether. Yet we may also take it as an injunction to underline the *objective nature* of large-scale historical processes. If what happens before our eyes suggests an inherent, more or less coherent logic, we easily assume, by the nature of how our minds work, *a single intention* behind it. For tens of thousands of years people thought divine will shaped events, and even in the Enlightenment, Immanuel Kant theorised the notion of 'system' as a subjective attribute, brought to bear on an external reality. Only his successor, G.W.F. Hegel, writing in the Napoleonic age, understood the 'systemic' aspect of reality objectively and historically, but he too assumed there was an underlying rationality, ultimately traceable to divine will ('the World Spirit') at work, seeking to realise itself via the action of historical humanity. This was the single intention on its last legs, so to speak.

Marx overcame this final limit by his historical materialist assimilation of Hegel's method. As Antonio Gramsci wrote from his fascist prison cell, from a historical materialist perspective the World Spirit is not the *presupposition* but the *outcome* of concrete historical struggles and consciousness. We are faced with a structure with a certain logic, but there is no 'plan' that can be traced back to a single source (God, 'History', a state, a class, etc.). We understand it as a totality only after the fact, as Hegel already stressed when he spoke about 'the Owl of Minerva spreading its wings at dusk'. There are certainly plans and conspiracies, a multitude of them, but they are developed from different angles; objective connections cut across by contingencies, and the like. The thrust of a given configuration of forces remains for an observer to develop because the consciousness of the agents at work in the larger structure only very rarely is on the scale of the historical process as a totality.

In other words, if we posit a global strategy of tension today that serves to control the vastly expanded popular masses, such a strategy in all probability did not exist before the fact as an abstract, *integral* blueprint. It represents the coming together of separate trajectories, with their accompanying intentional aspects, but formulated from different vantage points in different circumstances at different points in time. As we see below, some aspects of the War on Terror, even including provocation, were

indeed planned; not the ensuing world situation as a whole which was largely an unintended (though not necessary unwelcome) outcome.

1. The Anglo-American Deep State. An Overview

Orwell's Vision of a '1984', War Preparation, and the McCarthy Witch-Hunt

The revelations by Edward Snowden about the global surveillance infrastructure run by the United States National Security Agency (NSA) have led many to repeat the slogan of the ruling party of 'Oceania' in *1984*, 'Big Brother Is Watching You'. In Orwell's nightmarish dystopia, 'the watching is done through ubiquitous telescreens… through which the Party simultaneously broadcasts lying propaganda and has everybody watched all the time for possible heresy' (Fyvel 1982: 197).

Universal submission to the all-pervading state by what his biographer calls, Orwell's 'single mechanical invention for the future' (the 'telescreen') was not just a matter of surveillance. More fundamentally it was ensured by *a perennial state of war and the accompanying state of siege*. Modelled, like *Animal Farm* four years earlier, on the authoritarian turn of Soviet communism under Stalin during forced collectivisation and industrialisation, *1984* actually contains a learned analysis of the *connection between war and repressive surveillance.* Extensively quoted in the novel, its supposed author is Emmanuel Goldstein, the alter ego of Trotsky, the Enemy of the People and target of the daily Two Minutes' Hate. Bronstein/Goldstein's fictional *Theory and Practice of Oligarchical Collectivism* gives Winston Smith (Orwell's tormented protagonist and prototype of today's Snowdens and Mannings), relief from the oppressive reality in which he finds himself.

So what does Goldstein have to say of the mechanisms by which fear is kept alive and turned into submission? Contemporary war, the not-so-fictional Marxist explains, 'if we judge it by the standards of previous wars, is merely an imposture…. It is now a purely internal affair.'

> In the past, the ruling groups of all countries, although they might recognize their common interest and therefore limit the destructiveness of war, did fight against one another, and the victor always plundered the vanquished. In our own day they are not fighting against one another at all. The war is waged by each ruling group against its own subjects, and the object of the war is not to make or prevent conquests of territory, but to keep the structure of society intact. The very word

> "war" therefore, has become misleading. It would probably be accurate to say that by becoming continuous war has ceased to exist (Orwell 1954: 160-61).

The USSR has collapsed but 'Oceania' has not and thanks to Snowden's revelations about the NSA's PRISM and XKeyscore programmes and the publication by *WikiLeaks* of Manning's exposure of US misdeeds in the War on Terror, we can observe in real time something approximating Orwell's nightmare—including, at Guantánamo and elsewhere, the torture practices by which Winston Smith is finally compelled to declare his love of Big Brother.

The War on Terror likewise conforms to Orwell's description. The subjects to be controlled range from the diminishing, regular working class to the fast-growing reserve army of labour inhabiting the proliferating slums of the world's cities and for whom no provision is being made except violent repression (Davis 2017: 7). The surplus population therefore is approached from the perspective of violent excesses and ditto repression, *terrorism*, although it is and certainly began as a marginal phenomenon. Thus Nafeez Ahmed in his monumental study of 9/11 argues that 'al-Qaeda [is] not an "enemy" to be fought and eliminated, but rather an unpredictable intelligence asset to be controlled, manipulated, and co-opted as much as possible to secure covert strategic ends' (Ahmed 2005: 31). These ends blend with traditional imperialist rivalry (US versus Russia and China), but add a qualitatively new element. Mike Davis compares the urbanisation of the world's dispossessed to the Neolithic or Industrial revolution (Davis 2017: 1) and the need for control is certainly perceived to be of that order, too.

Orwell's novel fitted into a pervasive mood during World War II that the liberal West, too, was drifting towards a totalitarian future. James Burnham's *Managerial Revolution* of 1941 (Burnham 1960) or Harold Lasswell's reflections on a society in which the national security apparatus rises to become the dominant force (the 'garrison state', Lasswell 1941) both projected a Spartan future of total regimentation—as had Orwell. Actual steps to bring about such a state of affairs also in the United States (in the name of course of *preventing* it) were taken by J. Edgar Hoover, the FBI director with a long history of spying on the Left. In 1946 Hoover reported to President Harry Truman that there was a Soviet spy ring in Washington including top figures in the State Department such as Dean Acheson and J.J. McCloy (Scott 2015: 143-4). When Truman showed no interest, Hoover turned to the House

Un-American Activities Committee, sharing his files with Richard Nixon of HUAC and the Senate's Internal Security Subcommittee, which established his connection with Senator Joseph McCarthy. The election of Eisenhower, with Nixon as vice-president, strengthened Hoover's powers and with John Foster Dulles' approval he installed an FBI internal security agent in the State Department to weed out supposed leftists. The 'China hands' in the department, in particular, fell victim to a purge (in hindsight many US blunders in Asia have been ascribed to it).

At the time the technological means to be harnessed for the US world position were limited, but in 1946, Eisenhower, then still US Army chief of staff, in a report on 'Scientific and Technological Resources as Military Assets' advocated close association of the army with civilian research and development (Foster and McChesney 2014: 2-3). This in due course would result in the true '1984' as we see it emerging today. Over the period 1947 to 1975 the NSA, under a secret agreement with three US telegraph companies, already collected millions of private telegrams sent to or from the US. 200,000 individuals were indexed on a CIA computer system and in one CIA operation, CHAOS (1967-1973), 7,200 individual US citizens and more than 100 groups were put on file (Greenwald 2014: 185).

Raising the Alarm About a 'Deep State'

In the mid 1950s German exile Hans Morgenthau, renowned as the key International Relations 'power realist' in the United States, raised the alarm about what was happening in the State Department. Morgenthau's argument on the 'dual state', rediscovered by Ola Tunander (2009), was based on his finding that the Department's officers no longer reported to the president and the secretary of state, but to Senator McCarthy. In an essay originally of 1955, dealing with the internal security regime imposed on the State Department, Morgenthau described the dual state as a situation in which,

> the power of making decisions remains with the authorities charged by law with making them while, as a matter of fact, by virtue of their power over life and death, the agents of the secret policy—co-ordinated to, but independent from, the official makers of decisions—at the very least exert an effective veto over the decisions (Morgenthau 1962: 400, cf. 390-1).

The dual state, which Morgenthau saw as a spill-over from totalitarian practice that in the US might still be contained, has in fact remained at the heart of the Western power structure. Today the underground agents of the 'secret policy' are usually referred to as the *Deep State*. Exposed by the *WikiLeaks* disclosures and especially by Snowden's revelations on NSA and GCHQ mass surveillance, understanding its workings requires what Peter Dale Scott calls, 'deep political analysis'. A *deep political system* or process, he claims, is one 'which habitually resorts to decision-making and enforcement procedures outside as well as inside those publicly sanctioned by law and society' (Scott 1996: xiii, xiv). Or in the words of Claude Serfati, the separate existence of the state engenders 'excrescences combining legitimacy and illegal behaviour'. The actions of intelligence services in democratic states reveal that there is always a 'hidden face of the state' (Serfati 2017: 66, citing P. Mazeaux). According to the same author, the state of law has been eroded as a result, notably the rights of minors and the right to strike have been infringed on.

During the post-Watergate, post-Vietnam Senate hearings under the chairmanship Senator Frank Church in 1975, Church stated 'I know the capacity that there is to make tyranny total in America', warning that if the NSA and others operating surveillance technology would not be reined in, the US might 'cross over that abyss… That is the abyss from which there is no return' (cited twice in Scott 2015: 1, 109).

Today we are faced with an invasive, expanding infrastructure of surveillance far beyond what existed in the 1970s and its use to obtain 'total information control' and steer public opinion to support the condition of a state of emergency and the war without end against 'terror'. Obviously 'terror' was never remotely as dangerous as the measures to defend society against it suggest; indeed it primarily serves as a (partly self-fulfilling) justification to impose authoritarian measures under the state of exception in various guises. Clearly the established order is no longer confident it can control society without this safety valve being used. This is based on the theory of the conservative German legal scholar, Carl Schmitt, that 'he who decides on the exception' is the true sovereign (instead of the constitution, the law, or 'the people'). This theory was first formulated in 1922 in *Political Theology* (Schmitt 2005: 5), and when Hitler after his appointment as Chancellor in 1933 destroyed the plebeian SA to placate big business and the army in the 'Night of the Long Knives' in mid 1934, Schmitt hastily declared the theory applicable in this case too (Schmitt 1989).

The Transnational Deep State: UKUSA, ECHELON, and the 'Five Eyes'

The surveillance and spying infrastructure of the dual/Deep State all along was a transnational phenomenon dealing with (potentially) revolutionary forces operating across borders. The US and Britain raised this to a new level in World War II, which was not only a struggle against Nazism and fascism, but also a surreptitious one against the Left. At the time an Anglo-American structure was established for sharing wartime signals intelligence ('SIGINT', decoded military communication) and intelligence gained through communication interception ('COMINT'). This was formalised in the UKUSA agreement of 1947-48 (in fact a series of agreements, exchanges of letters, and memoranda of understanding). Britain brought along its intelligence cooperation with the white Dominions: Canada, Australia and New Zealand, going back to the beginning of the twentieth century. Today's collaboration between the NSA, GCHQ, and similar organizations of Canada, Australia and New Zealand, the 'Five Eyes', remains at the heart of it (Richelson and Ball 1990: 135-44; Greenwald 2014). In the Cold War intelligence cooperation of the Five Eyes was extended to a number of non-UKUSA, 'third party' NATO countries such as West Germany, Denmark and Norway, and outside NATO, to Israel, Japan, and many others (Richelson and Ball 1990: 168-73).

Plans to respond to information gained through these channels with actual repression followed. In the US itself, the tumultuous year of 1968 with its high-profile political murders (of Martin Luther King and Robert Kennedy) led to an emergency plan called Garden Plot that foresaw two army brigades being held at the ready to deal with disturbances (Scott 2015: 148-9, 152). Scandal broke in 1970-71 when it turned out the Army had been collecting files on 7 million US citizens involved in anti-war and civil rights movements, which it transmitted to the NSA via ARPANET (the Pentagon's precursor of the Internet), to be stored in the agency's Fort Meade, Maryland headquarters. The NSA's MINARET programme in combination with the FBI COINTELPRO operations were exposed for having collected information on prominent US citizens including Frank Church, the Senator who would lead the committee investigating these practices. This led to the Foreign Intelligence Surveillance Act of 1978, meant to rule out domestic surveillance but in fact, through the exceptions it allowed, legitimating it (Foster and McChesney 2014: 15). Today,

the counterterrorism/homeland security/intelligence complex in the United States involves1,271 government organisations and 1,931 private companies (Regan 2014: 39).

In the meantime the US jointly with the Five Eyes allies had set up ECHELON to intercept foreign communications. British researchers already in the 1970s found out about this mass collection of intercepts and the data transfer to the NSA, and they were promptly arrested. However, their 'ABC trial' only worked to stimulate further research, which exposed the NSA interception programme of 'most of the world's satellite phone calls, internet, email, faxes and telexes' (Wright 1998: 20). ECHELON was formally established in 1971 (then still under the code-name Shamrock; it was renamed Echelon in 1975). By that time it had expanded into a global surveillance infrastructure targeting all electronic communication, 'primarily non-military targets: governments, organisations and businesses in virtually every country.'

> The ECHELON system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence like Memex, to find key words. Five nations share the results with the US as the senior partner under the UKUSA agreements of 1948. Britain, Canada, New Zealand and Australia are very much acting as subordinate information services (Wright 1998: 19).

As we see below, the ECHELON system actually collected detailed information on the 9/11 attacks well in advance, but this information was not used to prevent them. Today the UKUSA structure continues to operate through the original First-Second-Third Party division (US the First Party, the four others of the Five Eyes the Second Party, other allies the Third Party), sometimes as Tier A/B. Importantly, both for the origin of the concept of a War on Terror and for actual repression, the NSA connection with *Israel* is now as close as between the Five Eyes (Tier A). The NSA supplies Israel with bulk intelligence not yet sifted; legal requirements in that respect are dispensed with. Yet at the same time Israel is recognised as 'one of the most aggressive surveillance services acting against the United States' (Greenwald 2014: 124-5). NATO/EU countries including the Netherlands, but also formal neutrals such as Switzerland, and in Asia and the Middle East, South Korea and Japan, India, Pakistan, Saudi Arabia and UAE countries, constitute 'Tier B' (or Third Party). These

countries are sometimes paid for the surveillance required. Even so, Tier B countries such as Germany, Brazil or India, are also under US surveillance (Greenwald 2014: 90).

The Five Eyes Against Their Own Elected Leaders

Meanwhile the spying operations were not confined to (potential) adversaries but also to set the limits of politics at home. The assassination of president John F. Kennedy in 1963 and the internal spying on Nixon, triggered by the détente policy with the USSR and the president's spectacular visit to China are examples. Kennedy had turned against the CIA over the Bay of Pigs invasion in Cuba, whilst Nixon had antagonised the agency by appointing James Schlesinger to 'clean it out'. The opening to China won Nixon his re-election in 1972 but profoundly antagonised the military-industrial complex and assorted conservative forces. It propelled the Deep State, i.e., concretely, a set of forces within the military, intelligence and the media into action to remove the president (Colodny and Gettlin 1992; on Kennedy, Scott 1996).

In the aftermath of Watergate, the aforementioned Church Committee exposed the illegalities involved in the FBI's counterintelligence operations (COINTELPROs). The aforementioned Foreign Intelligence Surveillance Act (FISA) of 1978 was a compromise effort to limit wiretapping but as noted, worked out differently (Scott 2015: 159). It was based on the 1968 Federal Wiretap Act ('Title III') but the FISA court it established would evolve into the most secret juridical institution in the United States, able to issue orders to telephone companies to hand over data concerning calls within the US and between US and foreign callers (Greenwald 2014: 27). As this legislative programme slowly unfolded, the dialectics of measures intended ostensibly to safeguard democracy but in fact adding up to intensified repression, was also illustrated by the election of Jimmy Carter in 1976. This did not basically change the shift to an international, counterrevolutionary confrontation policy except that the Carter administration added a powerful 'human rights' ideology to the Western armoury.

In 1978, Garden Plot emergency plans for dealing with domestic unrest were resurrected after Samuel Huntington, the advocate of restricting democracy in a joint report to the Trilateral Commission three years earlier (see Crozier, Huntington and Watanuki 1975), had been named Coordinator for Security for the Carter

administration. With his patron, National Security Adviser Zbigniew Brzezinski, Huntington also redesigned the *Continuity in Government* (COG) planning system. The term COG dates from the secret emergency planning for nuclear war in the Eisenhower years: In Annex A of Federal Emergency Plan D, it was used first to refer to measures to keep a government going after a crippling nuclear attack on the US. Under Huntington's supervision, a Federal Emergency Management Agency (FEMA) was created as an infrastructure for an emergency government takeover. In 1979 the emergency communications system originally established by Kennedy in 1963 was tested in the exercise Global Shield (Scott 2015: 148-50).

The FBI meanwhile kept tags on most US lawmakers. At Hoover's death in 1972 it was found he had almost 900 files on senators and more than 700 on congressmen in his possession (McCoy 2014: 74). Carter however followed the Church Committee recommendations and Congress imposed a number of restrictions of clandestine foreign operations. This led to a group of foreign intelligence agencies from the Middle East and France setting up an alternative Far Right intelligence network to fight communism, the 'Safari Club', working with a 'shadow CIA' of disaffected intelligence veterans. Carter's CIA director, Admiral Stansfield Turner, had dismissed key CIA figures, who then began to work with Saudi intelligence and the Safari Club to prevent Carter's re-election. This was achieved by a secret arrangement in July 1980 in which William Casey, Reagan's campaign manager and later CIA director, agreed with Israeli and revolutionary Iranian representatives that the Islamic Republic would keep the hostages in the US embassy (taken in retaliation over the admission of the Shah to the US) until Reagan had been elected, after which the new administration would supply Iran with arms (via Israel), in return for the hostages (Scott 2015: 28).

The domestic spying infrastructure meanwhile was expanded throughout. In 1986 the Electronic Communications Privacy Act was enacted, which in combination with the post-9/11 Patriot Act and the Communications Assistance for Law Enforcement Act (CALEA) tightened surveillance, effectively suspending all privacy. Telecom providers and IT companies and manufacturers under CALEA are obliged to work with law enforcement (Regan 2014: 32-3).

Kennedy, Nixon and Carter were not the only victims of their own Deep State. In the other Anglophone countries, comparable instances of disciplining leaders mistrusted by the Deep State are on record. In the UK, machinations against Labour prime minister Harold Wilson in the 1970s and even strategic assassinations to

prevent the entourage of Margaret Thatcher from reorganising MI5 and MI6; in Australia, the removal of Labour prime minister Gough Whitlam also in the mid 1970s, are cases in point (van der Pijl 2006: 154-6; 166). All along GCHQ snooped on organisations like Amnesty International and Christian Aid. Once computers became available in the 1980s, some 20 million files on dissident organisations in the UK were stored on its Mayfair-based system, 'connected to a growing number of other government data banks' (Wright 1998: 20; Richelson and Ball 1990: 287). In 2011 Australia asked the NSA to intensify surveillance of Australian citizens (Greenwald 2014: 122).

Still today, this Five Eyes connection is at the heart of the Western intelligence network spanning the globe. Within the Five Eyes, GCHQ is the closest NSA ally; the US has paid at least GBP 100 million over the last three years to secure access to its databases and work on joint encryption-breaking programmes. Next is Canada (the Communications Services Establishment Canada, CSEC) (Greenwald 2014: 118-9).

Let me now get to the origins of the NeoConservative (NeoCon) counterrevolution in the 1970s and 80s and how it mobilised the emerging IT industries for its purposes.

2. The NeoCon Project: A War on Terror with Enhanced Surveillance

The 1970s Economic Transformation and the IT Revolution in the US

The successful launch by the Soviet Union of the Sputnik, the first space satellite, in late 1957 was the trigger for stepping up the United States research effort that would lead to the IT revolution. The incoming US secretary of defence, Neil McElroy, within a month after the Soviet success proposed the creation of a single research agency; in January 1958, president Eisenhower proposed to Congress to fund such an agency, the Advanced Research Projects Agency (ARPA) (Foster and McChesney 2014: 11).

Initially ARPA was tasked with space surveillance satellites and orbital weapons, but the creation of NASA later in the year took that away. Before leaving office again McElroy set ARPA on the track of researching anti-ballistic missile defence and what later became GPS, the geo-location system. In the 1960s ARPA also pioneered digital communication technology (ARPANET) on which the Internet is based (Foster and McChesney 2014: 11-2). Renamed DARPA (D for Defence) in 1972, the agency also funded the establishment of academic computer science departments in the United States that would drive forward the IT revolution and enable, eventually, mass surveillance. Thus the personal computer (the first by Apple in 1976) was built on technologies coming out of DARPA-funded research. Indeed it has been argued that the phenomenon of Silicon Valley was the outcome of the collaboration of the American state and industry in the context of 'Cold War defence policy' (Mazzucato 2014: 62, 76).

That the United States was able to take the lead in the IT field had everything to do with the restructuring of the capitalist world economy in that period. The decision to abandon the gold cover of the US dollar in 1971 was an emergency measure meant to avoid a US default on its international obligations, basically caused by the war in Vietnam. At the time most members of the Nixon economic team were still committed to rectifying the trade and budget deficits that led to taking this step, but the secretary of labour (and future secretary of state), George Shultz, and the economist, Charles Kindleberger, already thought along the lines of making US deficits a foreign investment proposition (Bassosi 2006: 34). After the decision to switch to a floating exchange rate regime in 1973, the paper dollar effectively became

the global reserve currency and United States was transformed into a destination for the world's surpluses—especially after Paul Volcker, head of the US Federal Reserve, in 1979 raised real interest rates, terminating a decade of dollar inflation. In the words of Yanis Varoufakis, this turned the United States into the 'Global Minotaur', the monster devouring the world's surpluses of goods and money (Varoufakis 2013).

This gave the beginning IT revolution its American epicentre, financed by borrowing, including from abroad and *without budget constraints*. 'It allowed the United States to spend enormous sums, publicly as well as privately, on information and research, without a corresponding tax take on incomes (including profits) and also on potential domestic capitals' (Boccara 2008: 80, cf. 88). The US massively imported capital through the sale of Treasury Bonds or otherwise, which allowed it to deficit-finance, in large part via its defence establishment, the IT revolution. For whereas the political culture in the United States with its celebration of the free market and competition rules out state support for industry, the Federal government, *via the Pentagon and the defence budget*, did in fact finance the modernization of the industrial apparatus (Junne 1985; Serfati 2017: 121).

This made the IT revolution part of the US military and intelligence posture from the very start. IT research and capital formation, deficit-funded and unburdened by a tax regime that might otherwise have limited its rapid growth, in the specific US context had to fit in with Cold War defence considerations to gain legitimacy. This in turn created a coalition of interests between the military-industrial complex, the IT corporations and university research institutes, and Wall Street. It inflected research and science generally towards military and intelligence purposes with their secrecy requirements, thus threatening democracy itself (Serfati 2017: 117).

This set of connections, involving the structure of the world economy and the composition the post-1970s ruling bloc in the United States, is essential to understand the response to the crisis of 2008—a crisis that began in the late 1960s but of which Western and developed Asian governments could postpone the domestic consequences by inflation and debt until the entire edifice came crashing down (Streeck 2013). In a presentation by an NSA officer revealed by Edward Snowden, it was argued that 'The US was the major player in shaping today's Internet. This resulted in pervasive exportation of American culture as well as technology. It also resulted in a lot of money being made by US entities' (Greenwald 2014: 167). However, even though it was mainly a US preserve originally, the Internet now

threatens to become a global network potentially undermining US influence, hence the need to control all that passes through it (and more) (Greenwald 2014: 169). This control and the defence of this advantage were taken up not just by the US on its own, but jointly with the Five Eyes, and their favourite outsider, Israel. Here the drift towards the political Right labelled Neo-Conservative (NeoCon), the socio-cultural and (geo-)political counterpart to (economic) neoliberalism, played an important role in creating a favourable environment for restoring Western primacy.

The US-Israeli NeoCon Connection

The connection of the US Far Right to the state of Israel, especially after 1967, would come to play a major role in the shaping of a global strategy under the auspices of the US NeoCons. After the Six-Day War of that year, Israel found itself occupying large tracts of Arab land, a situation confirmed after the 1973 Yom Kippur war. The United States at this juncture moved to underwrite the occupation and after 1976 Israel became the largest recipient of US foreign aid, most of it military (Mearsheimer and Walt 2007: 26). Today we can see that the Global War on Terror has evolved out of the US guarantee for the Israeli occupation and that country's need to keep the Palestinians under control, not only in the occupied territories or the open-air prison camp of the Gaza strip, but also in the Palestinian refugee camps in countries like Lebanon. As in Nazi Europe and other cases, resistance to foreign occupation in Israel is called 'terrorism' and to get the West to subscribe to this definition became the goal of a new Far Right tendency in Israeli politics, the Likud Party.

The development of the highly complex set of relationships between the US and Israel and the Arab OPEC countries, notably the Gulf monarchies led by Saudi Arabia (which were also important funders of the US deficit), passed a critical threshold when thanks to growing oil income, the Middle East became a major client of the US arms industry; along with its nominal enemy, Israel (through US aid) and the American military itself. Within the US, this set of interconnections became evident when the 'Senator from Boeing', Henry Jackson, jointly with investment banker and veteran Cold War diplomat Paul Nitze began a campaign for an Anti-Ballistic Missile (ABM) system and restore nuclear superiority over the USSR, in opposition to the détente and arms control policies of Nixon and Kissinger. After the abandoning of the gold cover of the US dollar in 1971, OPEC countries sought to cut their losses due to

dollar inflation by raising the price of crude oil. As Jonathan Nitzan and Shimshon Bichler have demonstrated, kicked off a political business cycle affecting the large US arms producers and 'big oil' in tandem (Nitzan and Bichler 2002: chapter 5). The Jackson-Vanik amendment to the 1973 US trade legislation tied commercial relations with the USSR to its acceptance of Jewish emigration to Israel, mortgaging détente on the Zionist project. The Jackson team led the opposition to ongoing arms control negotiations, undermining the US position on SALT II, the draft treaty covering multiple-warhead ballistic missiles (Kissinger 2000: 1028, cf. 994-5; Colodny and Gettlin 1992: 422). As we can see today, this effectively created the US-Israeli NeoCon bloc that came to dictate Western geopolitical strategy and continues to do so, including the War on Terror.

In the United States the welding together of a new Cold War posture and support for the Israeli occupation received a boost when the influential New York Jewish intelligentsia, formerly liberal and before the war, even Trotskyite Marxists in many cases, threw their media weight behind the military-industrial, pro-Israel campaign (it was they who earned the label 'Neo-Conservative'). They linked up with the Deep State (the shadow CIA and the Safari Club) in the 'Team B' episode in 1976, when the NeoCons convinced CIA director George H.W. Bush, a sympathiser of the shadow CIA and the Safari Club, to upgrade his own agency's estimates of Soviet military outlays (Scheer 1982: 54). The men who would later launch the War on Terror (Vice-President Cheney, Defence Secretary Rumsfeld, and his deputy, Paul Wolfowitz) were protégés of the moving spirit behind Team B at the Pentagon, Andrew Marshall (Ahmed 2015).

In 1977, the victory of the Likud in Israel constituted the first breakthrough of the transnational NeoCon bloc in regular elections. Led by former Zionist terrorist leaders Menachem Begin and Yitzhak Shamir, ruthless military commanders such as Ariel Sharon, and the Netanyahu's (father Benzion, the one-time secretary to the founder of Far Right Zionism, Zeev Jabotinsky, and son Benjamin), this party abandoned the notion of compromise with the Palestinians and opted for repression with Western support. In July 1979, an international conference on terrorism was organised in Jerusalem by the Jonathan Institute, named after Jonathan Netanyahu, who had been killed in a raid to capture a plane hijacked by Palestinian radicals. His brother Benjamin chaired the event, which was opened by Prime Minister Begin. The twin components of a War on Terror, counterattacking an alleged enemy (made up of

terrorists and states supporting them) and rolling back democracy at home by surveillance and a politics of fear, both had a longer history, but they were now combined into a single programme, albeit still in the context of the struggle with Soviet state socialism.

Origin of the NeoCon Concept of a 'War on Terror' (I)

The concept of the War on Terror was launched in the early stages of the new Cold War. Because it was election time in the United States, there were two American delegations at the 1979 Jerusalem conference, representing the two branches of the emerging NeoCon bloc prior to the Reagan victory. One was led by George H.W. Bush, then still a Republican presidential hopeful looking for a cause; the other by Henry Jackson for the Democrats. Richard Pipes, the fiercely anti-Soviet academic who headed the CIA's 'Team B', also participated. The event was a milestone in welding together the emerging NeoCon coalition. Third World national liberation was now baptised 'terrorism' and Moscow was cast as the centre of worldwide terrorist operations (in Israel/Palestine, Central America, Apartheid South Africa, etc.). The War on Terror was to be waged through pre-emptive attacks on 'states supporting terrorism', relying on a dedicated intelligence infrastructure; whilst civil liberties for those connected to 'terror' (formerly national liberation) should be repressed. Warrantless surveillance, preventive detention without charge, and torture were all part of this grand scheme (Ralph 2008: 265; Ahmed 2005: 4-5).

In the election of Margaret Thatcher in the UK in 1979, the weight of finance and the transition to neoliberal capitalism was a more emphatic element than the NeoCon project and the links to the Deep State. Ronald Reagan's victory in November 1980 on the other hand was a straight victory for the NeoCons in every respect. Reagan had shown a keen interest in emergency programmes when still governor of California and now that he was president he built on Nixon-era plans for dealing with domestic opposition whilst creating an operational command structure under a state of emergency. This turned the Deep State into a shadow government that James Mann characterises as 'the permanent, though hidden, national security apparatus of the United States, inhabitants of a world in which presidents may come and go, but America always keeps on fighting' (Mann 2004: 145). A new version of the Continuity of Government (COG) project, an ultra-secret enterprise to impose

surveillance and mass detention of political dissenters, was developed, and military commanders were appointed who would rule under martial law. Donald Rumsfeld and Dick Cheney were recruited as team leaders in exercises preparing for nuclear war management, as were James Woolsey, later CIA director, and others. Supervised by CIA director William Casey and Vice-President Bush, Rumsfeld and Cheney became 'principal figures in one of the most highly classified programs of the Reagan administration', although neither of them held any public office at the time (Mann 2004: 138-9).

Of course the idea that Moscow was the hub of a global terror network was a plain instance of what we now call 'fake news', but the mainstream media demonstrated that they were willing to go along nevertheless. One of the participants of the Jerusalem conference, the journalist, Claire Sterling, in her 1981 book, *The Terror Network*, argued the case for this new reading of world affairs and her claims were promptly taken up by Alexander Haig, Reagan's first secretary of state (van der Pijl 2006: 203, 214 n.153). In May 1981, Sterling took the attempt on the life of Pope John Paul II by a Turkish fascist as evidence that the KGB used terrorism to knock out a pontiff championing the cause of the anti-communist trade union in his native Poland. Based on obviously fabricated evidence produced by the Italian secret service, SISMI, Sterling wrote a piece entitled 'The Plot to Kill the Pope' for the September 1982 issue of *Reader's Digest*. The magazine had hired a former CIA propaganda specialist to investigate the matter and NBC-TV that same month aired a documentary 'The Man Who Shot the Pope—A Study in Terrorism' (Herman and Chomsky 1994: 144-5). SISMI was then led by a member of the Italian P-2 masonic lodge that had been prominently involved in the Strategy of Tension, meant to check the rise of the Italian Communist Party, and had many P-2 members in its ranks who in turn worked with intelligence from the US and NATO countries.

None of this led to hesitations on the part of the mainstream media, which went along with the Bulgarian connection story nevertheless. At the Jerusalem conference George H.W. Bush had still expressed concern that even in a terror emergency, the liberal habits of 'the open society' might frustrate the appropriate government measures (quoted in Ralph 2008: 265), but it now turned out that public opinion could be manipulated into accepting even the most improbable story. In the process, the *New York Times*, *Time*, *Newsweek*, CBS News and others combined forces with the Reagan administration to mobilise public support for a new arms race and

counterrevolutionary operations in Angola, Mozambique, Nicaragua and El Salvador (Herman and Chomsky 1994: 158).

Origin of the NeoCon Concept of a 'War on Terror' (II)

After Reagan's election the NeoCon network convened again to discuss a War on Terror in Washington D.C. in 1984, with Benjamin Netanyahu, then Israel's ambassador at the UN, chairing. In the meantime, Israel had invaded Lebanon in 1981 and Sharon had allowed Lebanese fascist militias to massacre Palestinian civilians in the Chabra and Shatila refugee camps in Beirut. This led a key New York based NeoCon, Norman Podhoretz, to declare criticism of Israel over this operation 'anti-Semitic' in a *Washington Post* piece titled *'J'accuse'* (cited in Landau 1983: 68; the reference is to the 1890s Dreyfus affair manifesto).

The level of the participants in the Washington conference testified to the fact that the NeoCon tendency was now occupying the commanding heights. Participants included top Reagan cabinet members George Schultz, secretary of state after Haig's ouster and Attorney General Ed Meese, as well as Jeane Kirkpatrick, Reagan's UN ambassador, and FBI Director William Webster. From Israel, defence minister Yitzhak Rabin and Netanyahu and his father were the most prominent participants besides a host of journalists and academics. Three main strategic lines emerged from this conference: *first*, forward defence by attacking 'state sponsors of terrorism'. George Shultz actually identified a 'League of Terror' composed of Libya, Syria, Iran, and North Korea, recommending that if intelligence warrants it, pre-emptive attack must be an option (in Netanyahu 1986: 16).

Secondly, getting the media to avoid any investigation into the possible motives of terrorists. This of course was a crucial component when we think of the issue of total information awareness and mind control. The quality press at the time still had a tendency to try and explain the causes of terror, which should be avoided; the example of the tabloids with their lurid descriptions of blood and destruction should be followed instead. As Italian analysts of the 1970s Strategy of Tension already noted, to rally the population requires depicting 'terror' as *absolute evil*; approaching it analytically, in its true proportions, must be avoided (Sanguinetti 1982: 53-5). To ensure that the media fall in line, TV moderator Ted Koppel urged that a War on

Terror had to be really *declared*; only then would 'all kinds of societal pressures, and indeed legal pressures, come to bear on the media' (in Netanyahu 1986: 239).

The *third* component of a War on Terror was the suspension of civil liberties at home by increasing surveillance and preventive detention. The question whether the population would accept all that, already posed by Bush in 1979, was addressed at the Washington conference by Netanyahu Jr himself. After a major terrorist outrage, he argued, the people, united in fear and seeing themselves as 'soldiers in a common battle', would be 'prepared to endure sacrifice and even… immeasurable pain'. Of course, for a comprehensive politics of fear, this or that plane hijack would not do. Only if there would be one mighty blow, the people would follow and then *'a successful war on terrorism*… not just erratic responses to individual terrorist acts', could be launched and the United States would be able to build 'an anti-terrorist alliance … with two or three or possibly more countries… and impel the neutrals to shed their neutrality' (Netanyahu 1986: 225-6, emphasis added).

The existence of the Continuity in Government infrastructure, which would be activated in case of a major terrorist attack and the preventive surveillance of the population were of course still secret at the time. In the hearings on the Iran-Contra scandal in 1987, Oliver North, who handled covert money, weapons and drugs transfers from the White House basement under Bush's responsibility, was asked by a congressman whether he had also worked on 'a contingency plan… that would suspend the American constitution', 'plans for continuity of government in the event of a major disaster'. North declined to answer and the committee chair, Senator Daniel Inouye, ruled that this was a 'highly sensitive and classified' matter and closed the discussion (Scott 2007: 9, 184).

By then, the Soviet bloc was coming apart and after the implosion of the USSR in 1991, given that the alleged hub of global terrorism had capitulated, the whole idea of a War on Terror was shelved—for the moment. The preparations for a COG process and a mass surveillance infrastructure on the other hand continued and the IT revolution would provide it with the social media through which people would voluntarily deposit their private data.

3. Towards a Post-Cold War, Global Surveillance Infrastructure

The Interregnum Between the Cold War and the War on Terror

The collapse of Soviet socialism and the demise of the global Cold War structure led to concern in the United States that this might entail a shift away from a warfare state to rebuilding the social infrastructure at home. Amidst triumphalist pronouncements such as Fukuyama's 'End of History' thesis, the then-Under Secretary of Defence, Paul Wolfowitz, commissioned a report, the *Defence Planning Guidance, FY 1994-1999* to chart the future of US defence policy and rule out a demobilisation as after World Wars I and II. This was not a matter of spending only. Former NATO commander General Wesley Clark reported that in 1991, Wolfowitz told him that the US could now use military power in the Middle East without the Soviets stopping them; there would be an interval of five to ten years to clean out Soviet client regimes in the Middle East before the next major contender state would arise (cited in Scott 2015: 84).

The *Defence Planning Guidance* laid down a doctrine in which the United States enjoys global military supremacy, which it must defend against both contenders to its primacy and against allies seeking to carve out a role for the themselves in the former Soviet space. Hence, the US was advised to ensure a military 'forward presence' (*DPG* 1992: 13). The document states that 'While the United States supports the goal of European integration; we must seek to *prevent the emergence of European-only security arrangements which would undermine NATO*—particularly the Alliance's integrated command structure' (*DPG* 1992: 42, emphasis added).

Importantly, the DPG formulates the express US aim to keep abreast of all other states in critical technologies, and obviously the IT sector would be key among them. During the Clinton administration, which effectively embraced the DPG doctrine in its military posture, Continuity in Government planning was refocused from post-nuclear war management to 'terrorism' and it was under this label that Richard Clarke headed COG exercises in the 1990s (Scott 2015: 32, 39). But how to account for a global terror problem after the alleged centre had collapsed?

The problem that there might be no credible enemy any longer was solved by Samuel Huntington's 'Clash of Civilizations' argument, first in a *Foreign Affairs* piece in 1993 and subsequently in the book of 1998. This notion revived the doctrine

underlying the 1979-1984 War on Terror concept now that Moscow could no longer be credibly pictured as the centre of worldwide terror in the way the USSR had supported national liberation. In hindsight the 'Clash of Civilisations' thesis can be seen as a bridge between the original Netanyahu project of a War on Terror and its revival following 9/11. Fukuyama's End of History argument was too ambivalent about whether full-scale military mobilisation should continue; Huntington's thesis on the other hand identifies China and Islamic terrorism as the twin challenges facing the West. This claim, rather more tenuous of course than the USSR/national liberation connection, is corroborated by the designation of Islam and Confucianism as inherently foreign civilisations. Huntington also takes a leaf from Oswald Spengler's argument on the possible demise of the West, removing any suggestion that the projected confrontation would be one of choice. China, the new contender state after 1991, no longer had a transnational revolutionary network like the Soviet bloc before it. So the Middle East and the Muslim diaspora must fill the void. Islamic terrorism according to Huntington has its roots in a 'demographic explosion in Muslim societies', which turned 'large numbers of often unemployed males' into a 'natural source of instability and violence' (Huntington 1998: 265). I come back to this below because the post-Cold War globalisation of capital doubled the number of 'often unemployed males', raising issues of how to control them.

Atlantic Rivalries over ECHELON

The express provision in the DPG that NATO should remain the sole Atlantic security structure and that no independent European initiatives in the security sphere should emerge, also led to Washington preventing reunified Germany from assuming a leading role in the 1990s dissolution of Yugoslavia. In response to the unilateral German recognition of the Croat and Slovene secessions from the bankrupt federation, the US moved to recognise the independence of the ethnic powder keg of Bosnia and when civil war exploded, pushed for a NATO intervention in 1994 (Woodward 1995: 159-60). The Clinton administration also began the process of enlarging NATO in Central Europe, eventually as far as the borders of Russia proper, mocking solemn declarations not to do so (Sarotte 2014). Richard Holbrooke, entrusted with the Yugoslavia portfolio in the State Department, in a 1995 article

argued that ‘the West must expand to central Europe as fast as possible in fact as well as in spirit, and the United States is ready to lead the way’ (Holbrooke 1995: 42).

In addition, Washington reorganised its surveillance apparatus to cover Western Europe (and other allied countries elsewhere). In December 1991, the NSA division which had spied on the Soviet bloc, Group A, was abolished and its personnel and ‘its massive electronic intelligence systems—including listening posts, satellites, and ships—were added to another group, to bolster the collection of intelligence on all of Europe, including Eastern Europe and traditional U.S. allies in Western Europe’ (Schweizer 1993: 304. Group B, which had spied on Communist Asia, was likewise revamped to cover all of Asia).

A comparable reorganisation was conducted in the CIA and (for counter-espionage) in the FBI. This reorganisation was backed up by a major investment under the Pentagon’s Technology Reinvestment Program (TRP) through which DARPA funded dual-use technologies intended to secure the US edge both in civilian industry and military power (Mazzucato 2014: 97). Crucially, in the 1990s the idea of ‘net-centric warfare’ emerged as well. It included the notion of ISR (Intelligence, Surveillance, and Reconnaissance), which evolved into a key component of what came to be known as the *Revolution in Military Affairs* (RMA) (Cockburn 2015: 47). Rumsfeld and others in the NeoCon bloc that would take over power in Washington with the election of George W. Bush in November 2000, was a forceful proponent of this RMA.

Signals and communication intelligence and surveillance after the collapse of the USSR was also used for commercial and diplomatic purposes, underwriting the US advantage in these domains. Already in 1990 the chairman of the Intelligence Committee of the US senate, David Boren, declared in a press talk that ‘as the arms race is winding down, the spy race is heating up.’ Espionage activity ‘against private commercial targets in the United States’ was on the increase, ‘carried out not by foreign companies, but by foreign governments’ (Boren 1990: 5). This was confirmed by French intelligence director Pierre Marion, who set up a special branch ‘to gather secret technologies and marketing plans of private companies’, US and other (*Newsweek*, 23 September, 1991; cf. Schweizer 1993). ECHELON, too, was put to good use also for commercial rivalry. In 1994 the NSA and CIA passed on intercepts obtained at their UK listening posts that led to Airbus Industries losing important contracts (Foster and McChesney 2014: 16). On the diplomatic front, the NSA

provided US delegations with advance knowledge of the negotiating positions of negotiating partners (Greenwald cites an example of a summit with Latin American countries, 2014: 139).

The evidence of US/Five Eyes exploitation of its Cold War inventory in SIGINT/COMINT for unilateral commercial and political advantage did not fail to cause concern abroad, notably in Europe. In 1998, the consultation version of a report commissioned by the European Parliament's Directorate General for Research and written by Steve Wright of the Omega Foundation in Manchester, for the first time gave a full review of the communications interception by the NSA, among many other instances of foreign operations of doubtful legality (Wright 1998: 19 & passim). The Wright report established that 'within Europe, all email, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland … by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York moors of the UK' (Wright 1998: 20).

The Wright report documents how ISDN protocols allow listening to conversations around a phone without it being taken off the hook, devices to track users of mobile phones, and so on. Its sections on torture practices make for chilling reading, as does detailed information on torture instruments supplied by British and US companies under 'crowd control' and other licences. In its recommendations, the report urges that the 'European Parliament should reject proposals from the United States for making private messages via the [Internet] accessible to US intelligence agencies', and that 'a more detailed report [be commissioned] on the constitutional issues raised by the National Security Agency (NSA) facility to intercept al European telecommunications'. All these concerns were shelved after the 9/11 attacks, which in turn raised communication surveillance to an unprecedented level, made possible by the IT revolution.

Customising the US IT Sector for Military and Intelligence Purposes

Technically, the ability of the US and the Five Eyes and their partners to spy on their populations was greatly enhanced by the information revolution. As we saw, this revolution was deficit-financed, partly from abroad; embedded in the US war machine; and capital formation on the basis of new IT advances was made possible

because the deficit-financing of the US budget absolved existing and aspiring businesses from being taxed for running the US state and its global defence outlays. That is why today, the giants of the IT revolution are American companies. No other states enjoy the luxury of being able to forego tax income, rely on foreign funding and having its national currency serve as world money. Also it explains why the IT giants are so closely integrated with the military-industrial complex, the intelligence services, and the actual repressive apparatus today legitimated by the War on Terror.

As noted, defence-oriented and –financed R&D in the US serves as a 'substitute for industry policy' given the taboo on state support for industry (Junne 1985). It has also been argued that for Washington, defence IT (surveillance and cyber-warfare generally) serves as a (relatively cheap) substitute for the expensive arsenal of 'mailed fists' (McCoy 2014: 70-71). Innovations in the IT field had their origin in the research labs of large corporations; the Pentagon was not itself a source of innovation. It *financed* innovations that were useful to it (Serfati 2017: 120). Thus the integrated circuit was developed by Texas Instruments in 1956, but in the1980s it was Japanese competition and the rapid expansion of IC production capacity there that prompted the Pentagon to subsidise a US capacity through an industry and universities consortium for semiconductor development, SEMATECH. In the early 1970s the touch-screen was already developed by defence-related research in the UK; it was used first in the European Organization for Nuclear Research CERN. The microprocessor (© Intel and Fairchild around 1971) evolved in connection with research work relating to the American intercontinental ballistic missile and the US space programmes. The graphical user interface technology used in Apple and Windows operating systems was developed by Xerox (Mazzucato 2014: 98-9, 101; Serfati 2017: 120).

The Internet grew out of a Pentagon network project (ARPANET) connecting a dozen research centres in the United States (Mazzucato 2014: 63). Nafeez Ahmed cites an investment banker involved in Google and Sun Microsystems to the effect that DARPA funded the Internet, most of the large computer science departments, CAD (computer-aided design) and GPS (Ahmed 2015). However, universities and the National Science Foundation were at least equally important. The NSF created the Computer Science Research Network which combined ARPANET with other networks including PhoneNet for email and in 1985 expanded it to include corporations (Foster and McChesney 2014: 21; Serfati 2017: 121).

In the 1980s DARPA was financing Stanford's artificial intelligence (AI) research with additional funding from the National Science Foundation, NASA, and the Office of Naval Research (ONR). The ONR in particular played an important role in working with Stanford on digital systems for the military (Ahmed 2015). Intelligence needs and military exploitation of such technology were prior to the actual breakthroughs. Thus in the Iran-Contra hearings that unveiled the secret programme of arms sales to Iran via Israel to fund the Nicaraguan Contras, Reagan's National Security Adviser Admiral John Poindexter also was found to have prepared a presidential directive to give the NSA the ability to control all computer databases in the US. After the scandal broke the directive was withdrawn and Poindexter hibernated in a private company working for DARPA (Foster and McChesney 2014: 17). He would later become the head of the Total Information Awareness office at DARPA.

As with Orwell's 'telescreens', US IT advances were intended to work two ways: to collect information and to disseminate propaganda. In 1989, Richard O'Neill, then a US Navy cryptologist, wrote a paper for the US Naval War College, *Toward a methodology for perception management.'* This was seen in the US intelligence command as a breakthrough in developing a strategy for 'perception management' as part of information warfare (IW). O'Neill 'identified three categories of targets for IW: adversaries, so they believe they are vulnerable; potential partners, "so they perceive the cause [of war] as just"; and finally, civilian populations and the political leadership so they "perceive the cost as worth the effort " (cited in Ahmed 2015). Here the logic of the original War on Terror project shines through—if the one mighty blow would come.

In 1994 O'Neill was appointed by defence secretary William J. Perry to set up the Highlands Group as the Pentagon's IW think-tank. In 1999, Ashton Carter, assistant defence secretary, co-authored a study with Perry advocating a new form of 'war by remote control' facilitated by "digital technology and the constant flow of information (Ahmed 2015). This prefigured the drone programme to which we come below. In 1995 SAIC, which O'Neill had been instructed to coordinate with in setting up the Highlands Group, would form its own Center for Information Strategy and Policy, further beefing up the IW infrastructure. Indeed to allow the free circulation of ideas between private companies and the US government, which would otherwise be subject to regulation, the Group was re-baptised the Highlands Forum in 1998 and henceforth operated under the formal cover of O'Neill's private 'Highlands Group

Inc.' consultancy. It developed into the key interface between the Pentagon's most powerful spy agencies including the NSA, the Defense Intelligence Agency (DIA), and others, and Booz Allen (Snowden's employer; James Clapper, Obama's director of national intelligence, was a Booz director), SAIC, RAND, and other private consultancies. At the first meeting the Forum launched the idea 'network-centric warfare', based on total information awareness (Ahmed 2015). Booz Allen Hamilton is majority-owned by the Carlyle group which is close to the Bush family (Foster and McChesney 2014: 26; on Carlyle, Briody 2003). Clearly surveillance to obtain total information awareness is a vital precondition of network-centric warfare.

A Search Engine for Defence Intelligence

The diverse origins of the Internet, DARPA-centred and university/NSF-based, explain why the web was seen *as a tool as well as a challenge* by the national security state (Serfati 2017: 121). Actively surveying it with the aim of control soon became a key objective. In 1994 two Stanford PhD students, Sergey Brin and Larry Page (both meanwhile billionaire founder-owners of Google) made their breakthrough with the first automated web crawling and page ranking application. That application remains the core component of what eventually became Google's search engine. Brin and Page did their research with funding from the Digital Library Initiative (DLI), a multi-agency programme of the National Science Foundation (NSF), NASA and DARPA (Ahmed 2015).

As Nafeez Ahmed has documented in his seminal report, Brin's supervisor at Stanford in the mid 1990s worked under a funding project of DARPA's Intelligent Integration of Information programme; in 1996 he co-chaired DARPA-sponsored meetings on data exchange between multiple systems. Throughout the development of the search engine, Brin reported regularly to the manager of the Massive Digital Data Systems (MDDS) initiative at the MITRE Corporation, a leading US defence contractor (sponsored by the NSA, CIA, and the Director of Central Intelligence, to foster innovative research in information technology) and to the CIA's Office of Research and Development, ORD). It shows again the early imbrication of IT research and the military and intelligence complex. The MITRE project provided information to the NSA, CIA, US Air Force Research Laboratory, as well as the US Navy's Space and Naval Warfare Systems Command (SPAWAR) and

Communications and Electronic Command (CECOM). SAIC handled the MDDS submission process; its manager, Brin's contact, who was among those interviewed by Ahmed, went on to teach courses for US government officials and defence contractors on data-mining for counterterrorism (Ahmed 2015).

Indeed still prior to Google's launch (in 1998), a MITRE board member, University of Virginia computer scientist Dr. Anita K. Jones, was appointed DARPA director and head of research and engineering in the Pentagon in 1993, co-chairing the Highlands Forum during the period of Google's pre-launch development at Stanford under MDSS. When she left the Pentagon four years later a US Senator complimented her for having 'brought the technology and operational military communities together to design detailed plans to sustain US dominance on the battlefield into the next century' (cited in Ahmed 2015). And he concludes: 'Throughout the 1990s, then, DARPA's funding to Stanford, including Google, was explicitly about developing technologies that could augment the Pentagon's military intelligence operations in war theatres'.

Surveillance Capitalism and Security

Brin and Page officially incorporated Google as a company in September 1998, placing the search engine that had come out of the Stanford CIA-NSA-MDDS programme at the disposal of its users, both the public and the original sponsors. In so doing they pioneered what has been called 'surveillance capitalism', in which Google, Facebook, etc. operate by capturing every aspect of people's daily life, often voluntarily submitted through social media. On the one hand it sells these data to advertisers for income and to do this it seeks to collect as many 'surveillance assets' as possible (Zuboff 2015: 79; the special issue of *Monthly Review* of summer 2014 I cite extensively here, in fact was already titled 'surveillance capitalism'). On the other hand it supplies the same data to the national security state, the intelligence services, the military and law enforcement. For whether we speak of Google, the Internet as its terrain of operations, or any other of the whole range of major IT innovations, they were all or mostly products of DARPA or otherwise defence-related public research.

The screen scrolling function used by Apple came out of neuromorphic research at the University of Delaware funded by the NSF and the CIA. Indeed 'Apple's highly comprehensive intellectual property portfolio had benefited… from technology that

was originally underwritten by the [US] state' (Mazzucato 2014: 103). SIRI, developed for the military by Stanford and 19 other US universities as a 'virtual office assistant', was later sold to Apple for use in the iPhone (and for an undisclosed sum) (Mazzucato 2014: 105-6). In turn, the iPhone and other smartphones became trackers of people's movements along with their online behaviour and contacts. Another Stanford Ph D, Andreas Bechtolsheim, pioneered the SUN workstation project, also funded by DARPA and the Stanford computer science department. SUN Microsystems, co-founded by Bechtolsheim (who also invested $100,000 in Google) would be based on it (Ahmed 2015). The LCD screen which was developed at Westinghouse, almost entirely with Pentagon funding after a number of major computer companies turned down its inventor's project for fear they would not be able to competitively produce it (Mazzucato 2014: 107).

The rationale for the CIA-NSA projects in the cyber domain was to kick-start the development of techniques for 'querying, browsing, and filtering; transaction processing; access methods and indexing; metadata management and data modelling; and integrating heterogeneous databases as well as developing appropriate architectures' and to 'provide for the seamless access and fusion of massive amounts of data, information and knowledge in a heterogeneous, real-time environment' for use by the Pentagon, intelligence community and potentially across government (cited in Ahmed 2015). In fact, as a we saw, the rest of the world helped in developing these innovations by accepting and funding US deficits and the world money role of the dollar.

The purpose of COG was to provide for a government function after a nuclear war or comparable emergency. At the RAND Corporation a decentralised communication system was developed that no longer required a central switchboard and would allow post-nuclear *military* functions to be continued. DARPA first approached AT&T and IBM to help with overcoming the technological obstacles to such a decentralised network, but because these companies feared competition, it had to recruit the British Post Office instead. With the Post Office and assistance from the NSF, the communication protocol (TCP/IP), an operating system (UNIX) and an initial e-mail programme was developed successfully. Complementing this DARPA-led enterprise was the work of a British scientist who developed uniform resource locators (URL), a customised language (HTML) and a transfer protocol (HTTP), all first tested out on the computers of CERN in Geneva (Mazzucato 2014: 104-5). When, by 1990, the

World Wide Web was taking shape and as the number of users grew exponentially, a series of new laws led to its deregulation and the monopolisation of the IT and Internet market by Apple, Microsoft and Google and a range of lesser corporations (Foster and McChesney 2014: 22).

This was not just a matter of the Defence Department serving as a substitute for industrial policy, but was meant to create the ability of information warfare. Thus at the Naval Postgraduate School and RAND, John Arquilla developed the concept of *netwar* or *cyberwar* Arquilla was also a founding member of the Highlands Forum, and from his notion that 'it takes a network to defeat a network' emerged a series of tactics relying on mass surveillance and big data mining to support pre-emptive operations to thwart terrorist plots (Cockburn 2015: 48). Concepts running through Arquilla's work include 'networked warfare,' 'networked deterrence,' 'information warfare,' and 'swarming.' Most was produced by the air force think tank, RAND under a Pentagon contract and summed up in Arquilla's 1999 RAND study, *The Emergence of Noopolitik: Toward an American Information Strategy* (Ahmed 2015).

With the global positioning system (GPS), the opportunities for surveillance were greatly enhanced. GPS was developed for the Pentagon to allow the accurate deployment of military assets. Installed on smartphones they today produce permanent location data which are duly stored (Regan 2014: 35). GPS was released for public use in the mid-1990s, but its 24 satellite support system continues to assist military applications (Mazzucato 2014: 105-6). The US Air Force began launching the satellites in 1989 and a year later US troops in Saudi Arabia in the run-up to the First Gulf War were using GPS to find their way in unfamiliar desert surroundings (Cockburn 2015: 56).

Key among military GPS applications was the drone, an invention of the Israeli aerospace engineer Avraham Karem. Karem moved to the US in 1977; there he developed the Predator drone for General Atomic, an offshoot of General Dynamics (Cockburn 2015: 52). The drone, using GPS and connected to a home base far away, would eventually develop into a means of surveillance carrying the ability to target the surveyed objective directly. As I will argue below, targeted assassinations would become the ultimate means of population control, and population control was necessary as the reserve army of labour doubled in size in the 1990s and early 2000s.

4. The War on Terror as Rationale for Mass Surveillance

Exponential Increase of the Reserve Army of Labour

We now come to what I see as the deeper rationale of the War on Terror, the control of the overpopulation of the planet under capitalist conditions, more specifically under the conditions of neoliberal capitalism dominated by speculative finance on the one hand, and with greatly weakened, if not actually superfluous labour on the other. The implosion of the Soviet bloc, coming on top of the opening of China, completed the doubling of the global labour supply from 1.5 to more than 3 billion people in two decades (Delgado Wise and Martin 2015: 70). As the socially protective state withered away around the globe, undermined by debt and ideological corruption, populations came to face transnational capital directly, no longer in a relation mediated by states (Vieille 1988: 247).

In the West and Japan, the problem of tying the growing surplus population to the discipline of the labour market now that the welfare state was being downscaled, was at least partly solved by 'workfare' policies. Instead of keeping workers fed and fit during intervals of joblessness or illness, in the 1990s Clinton and other exponents of the 'radical centre' imposed harsh rules to keep workers in work at all cost. As the number of 'working poor' in the developed part of global capitalism increased as a result, the wage shortfall was covered by debt (Soederberg 2014: 58-61, 88).

In the newly exposed non-Western world, including the former Soviet sphere, the increase in available wage-dependent people was handled differently. One segment is employed in the newly spreading 'global commodity chains' now that the threat of nationalisation was removed (Dzarasov 2014: 26-7). Along these chains, workers living under extremely different social and work circumstances, are nevertheless brought together in a single process. In David Harvey's words, 'peoples possessed of the utmost diversity of historical experience, living in an incredible variety of physical circumstances, have been welded, … often through the exercise of ruthless brute force, *into a complex unity under the international division of labour*' (Harvey 2006: 373; cf. 404, emphasis added).

Jeroen Merk argues that these workers, also those at the lower end of transnational product chains, can yet be seen as part of what Marx called 'the collective worker', whose tasks combine into a complex, geographically dispersed but yet single labour

process (Merk 2009). The brand (mostly in the textile/footwear and electronics sectors) offers a sense of protection because corporations fearing reputational damage may seek to extend certain minimum provisions even for their lowest-paid workers beyond the horizon. Anti-sweatshop campaigns and the self-organisation of local workers thus may turn the objective collective worker in a chain into a militant collective subject with which the company must negotiate (Merk 2015 applies these concepts to Nike; Chan, Pun, and Selden 2015 document the case of Apple in China). Attempts to obtain collective workers' rights such as regional minimum wages are a sign that actually welding together the collective worker into a conscious economic subject is no chimera (Battacharyee and Roy 2015).

However, the workers eligible for trade union mobilisation constitute only a small and diminishing fraction of the entire wage-dependent population. Export-led manufacturing is concentrated in China, Korea and Taiwan; in the remainder of the Third World massive plant closures and tendential de-industrialisation as a result of the neoliberal structural adjustment policies imposed by the West have greatly reduced regular employment, with catastrophic consequences (Davis 2017: 13). As the land is being emptied of its surplus population because only competitive farmers can survive in world-market-oriented agriculture, countries notably in Sub-Saharan Africa are reduced to raw material deposits and conflict in such countries makes life even more hazardous for the surplus population (Halper 2015: 21). However, when people pour into the cities, no regular employment awaits them. It has been estimated that by the time of the financial crisis of 2008, 82 percent of non-agricultural employment in South Asia was 'informal', 66 percent in Sub-Saharan Africa, 65 percent in East and South East Asia, and 51 percent in Latin America (ILO and WTO figures in Taylor and Rioux 2018: 88-9).

But then, what is 'informality'? As the illusions of local 'entrepreneurship' with NGO or micro-credit backing fade, the reality of a one billion strong surplus humanity can no longer be evaded (Davis 2017: 178). Cities grow at a record pace, and employment opportunities dwindle. Mike Davis cites Jan Breman who writes that 'a point of no return is reached when a reserve army waiting to be incorporated into the labour process becomes stigmatized as a permanently redundant mass'… This metamorphosis is… *the real crisis of world capitalism*' (Breman cited in Davis 2017: 199, emphasis added). The question that arises, is to what extent the 'permanently redundant mass', even more than the potential of a collective worker constituting

itself, was the real driver of the eventual War on Terror. In Huntington's 'Clash of Civilisations' argument the human mass for which there is no need, is defined as Muslim. The rise of Islam, all across Asia, North Africa and the Balkans, he argues, is powered by jobless population growth.

> Muslim population growth has *generated large numbers of unemployed and disaffected young people* who become recruits to Islamist causes, exert pressure on neighbouring societies, and *migrate to the West*… The West's simultaneous efforts to universalise its values and institutions, to maintain its military and economic superiority, and to intervene in conflicts in the Muslim world generate intense resentment among Muslims (Huntington 1998: 211, emphasis added).

With the 'Muslim propensity for violent conflict' (Huntington 1998: 258), its 'religion of the sword' (1998: 263), etc. existential conflict is only one step away. Whether these are well- or unfounded assertions, is not important here. What matters is that a key US ideologue presents them in this fashion and links them to terrorism (Huntington 1998: 187-8). But was a coercive, 'Strategy of Tension' approach to the reserve army of labour intentional, formulated ahead of its actual declaration?

Controlling Surplus Humanity

Already in the 1990s, the problems associated with controlling sprawling slums was brought home to the US military when local militias in Mogadishu (Somalia) inflicted casualties in US forces in 1993, forcing them to withdraw ('Black Hawk Down'); the Iraq occupation taught comparable lessons. Four years later a joint training programme was initiated for the different US armed services to prepare for Third World street fighting. The RAND Corporation at that point warned of an 'urbanisation of insurgency' (Davis 2017: 203). As the surplus population seeks to migrate from the local conditions of unemployment, civil conflict over resources, and overpopulation/ecological exhaustion, it further complicates issues associated with controlling labour, even organised labour. A respectable French magazine defines the threat to the country as composed of ISIS (the Islamic State) *and the CGT*, the militant trade union (cited in Serfati 2017: 203). Riots such as the revolt of the *banlieues* in the cities of France in 2005, which led the Villepin government to

proclaim a state of exception (Serfati 2017: 20), the comparable explosion in London in August 2011, spreading to 12 other cities (*Wikipedia*, '2011 England riots') and frequent unrest across the United States, usually triggered by police actions perceived as racist, bring 'Mogadishu'-like situations also to the wealthy West.

As a result, besides the *external* enemy as a concern legitimating defence, the emphasis moves back to the 'internal enemy' (Serfati 2017: 193). From the early 1990s this has led to the emergence of a new concept of security in which strictly military defence is enlarged by border and riot control, also in metropolitan settings (Serfati 2017: 142).

Controlling the globe's surplus humanity and establishing what Jeff Halper calls the 'Global Matrix of Control' to deal with the world's poor and marginalised, relies on the US and Israel. These two outclass all others in terms of experience with militarised securitisation: the United States as the world's policeman protecting the global capitalist economy as well as its own black population, and Israel, 'the predominant authority on securitization and prolonged pacification' (Halper 2015: 71). This applies not only to the actual militants, because in both the cases of US blacks and of the Palestinians, only a tiny fraction is actively resisting ('terrorists'); most people are simply destitute and their desperation is one focused on survival. Indeed an Israeli specialist on population control plays down the priority given to terrorism and stresses instead that criminality and terrorism merge into each other, it is the existence of a restless underclass as such that must be confronted (Halper 2015: 258).

The expansion of the security concept and the business opportunities it offers, has brought a range of large corporations on board who would not immediately be recognised as defence firms. Nafeez Ahmed mentions SAIC, Booz Allen Hamilton, RAND Corp., Cisco, Human Genome Sciences, eBay, PayPal, IBM, Google, Microsoft, AT&T, the BBC, Disney, General Electric and others as examples attracted to the surveillance and next-generation security fields (Ahmed 2015). In Europe the new market opportunities accrue to companies like Thalès, Airbus, or Finmeccanica, but also to Israeli corporations like the defence conglomerate Elbit, which realises 16 percent of its turnover in the EU. According to Claude Serfati, in France alone the defence industries have effectively doubled their market by inclusion of the new security fields (Serfati 2017: 143).

In the relations between native European populations and the newcomers, the attitudes belonging to the colonial relationship persist. The politics of fear, evoked by the association between the 'illegal immigrant', the 'dangerous classes', and the new surplus population packed together in the slums of the big cities, reproduces this relation, especially since the third generation of immigrants from North Africa, Turkey and elsewhere, no longer can hope for improving their lot. Instead of combating this by creating education and job opportunities, governments often encourage mistrust among the mainstream population instead (Serfati 2017: 198-9).

Surveillance is a key asset in controlling the restive suburbs and slums both in the developed and the underdeveloped world. As one aerospace publication puts it, the urban setting creates a 'battlespace environment that is *decreasingly knowable*' (cited in Davis 2017: 204, emphasis added). Incomplete knowledge mixes with the use of double agents and provocation; in the process, the state's opportunistic and authoritarian attitude fosters state terrorism to deal with terrorism. As the Israeli writer, Martin van Creveld, argues, the low-intensity war against domestic enemies undermines state authority to the point where the army degenerates into a collection of armed gangs similar to those in revolt with the inhabitants becoming exposed to both. 'Even in the most stable societies, the least they can expect is to have their identity checked and their persons searched at every turn' (van Creveld 1991: 223). 'The real "War on Terror", writes Mike Davis (2017: 205) is 'the 'low-intensity world war of unlimited duration against criminalized segments of the urban poor.'

The NeoCons Prepare to Launch the 'War on Terror'

Facing the above challenges besides concern over resources, the security of Israel, and others, the NeoCon bloc began to prepare to actually launch the 'War on Terror' that had been temporarily put on ice because of the Soviet collapse. The newly established Project for a New American Century (PNAC, with Cheney, Wolfowitz, Rumsfeld, and others) published *Rebuilding America's Defences,* which rehearsed the themes of the Defence Planning Guidance again, adding the much-cited phrase that the necessary revolution in military affairs, RMA (from Cold-War era air-land battles to global rapid intervention based on 'Intelligence, Surveillance, and Reconnaissance', ISR) would be a protracted transformation, 'absent some catastrophic and catalyzing event—like a new Pearl Harbour' (cited in Ahmed 2005: 343-5). It will be recalled

that Netanyahu too had argued that a War on Terror would only be feasible after a big blow, not this or that hijacking.

Western intelligence had been picking up signals about an impending attack on US soil using 'airplanes as weapons' for more than a year, and even the media had information to that effect for at least six months prior to 9/11 (Ahmed 2005: 167-8). So unless national security figures in the Bush administration did not read reports or even the papers, what they said they feared in terms of a Pearl Harbour was based on at least partial foreknowledge. An 'electronic Pearl Harbour' by the then-CIA director, John Deutch, in 1998. Deutch then co-authored a piece in *Foreign Affairs* with University of Virginia scholar Philip D. Zelikow and former assistant secretary of defence Ashton B. Carter (the aforementioned advocate of 'war by remote control' facilitated by "digital technology and the constant flow of information' and later secretary of defence under Obama) speculating on an impending 'transforming event' that would, 'like Pearl Harbour, … divide our past and future into a before and after'. Taking the World Trade Centre bombing attempt of 1993 as their reference, the authors sum up the Jonathan conference scenario: 'The United States might respond with draconian measures, *scaling back civil liberties*, allowing *wider surveillance of citizens*, detention of suspects, and use of deadly force (Carter, Deutch, and Zelikow 1998: 81, emphasis added).

In 1999 Zelikow in a paper ruminated on how politics is directed by 'public myths' that rest on a 'moulding event' such as Pearl Harbour. That creates 'generational public presumptions … that become etched in the minds of those who live through them.' Not that they need not be 'true'; what matters are beliefs '*thought to be true* (although not necessarily known to be true with certainty)'. Certainly they must be 'shared in common within the relevant political community', hence it is mandatory that consensus is secured by discrediting all dissent (cited in Sacks 2008: 223; ever since the Warren Report on the J.F. Kennedy assassination, dismissing dissent as 'conspiracy theory' had worked well to that effect). Here the War on Terror scenario is approached from the angle of how to institute a politics of fear, Netanyahu's prediction that the people, 'united in fear', would see themselves as 'soldiers in a common battle' (Netanyahu 1986: 225-6).

As the presidential election of 2000 approached, a high-level Aspen Strategy Group worked out a blue-print for the incoming president. Carter, Deutch and Zelikow were among the participants and edited its recommendations. They included

a warning by Ashton Carter of ‘catastrophic terrorism of unprecedented scope and intensity … on U.S. territory’ in addition to the rise of China and other threats (Carter in Zelikow 2001: 37-8). When this report came out Bush Jr had meanwhile assumed the presidency; Zelikow was on the transition team. As PNAC luminaries joined the new administration in key positions (Cheney as vice-president, Rumsfeld at Defence with Wolfowitz as deputy), the Pearl Harbour motif was not laid to rest, on the contrary. Right in January 2001 Rumsfeld, the key RMA advocate, predicted a ‘Space Pearl Harbour’ (cited in Scott 2007: 24), whilst engaging jointly with Cheney and their respective staffs in planning a global war that ‘would extend to the home front with warrantless wiretapping, mass arrests of Arabs, Pakistanis, and Muslim immigrants and a prodigious rollback of the civil liberties of American citizens’ (Scahill 2013: 15).

To prepare for such a vast operation an event at the Carnegie Endowment for International Peace in December 2000 explored ‘the impact of the information revolution, globalization, and the end of the Cold War on the US foreign policy making process.’ With Wolfowitz and John W. Rendon, Jr., whose consultancy had run the State Department’s propaganda campaigns in Iraq and Kosovo under Clinton, taking part, the meeting aimed at building ‘a new model that is optimized to the specific properties of the new global environment’ (cited in Ahmed 2015). Among the issues flagged up in the meeting was the ‘Global Control Revolution’ through which a response to the elusive information revolution was to be developed as the primacy of states and inter-state relations in world affairs was receding. In other words, coercion and war were now conceived as waged against the people directly, which entailed the merging of the military and penal aspects (Paye 2014: 331-2). Above we saw that the ‘people’ here are composed of the home fronts ‘united in fear’ and the surplus population exposed to repression itself.

Through ECHELON the US intelligence community was well informed of the impending attack and surveillance of possible perpetrators or accomplices had been stepped up. This began after the bombing of US embassies in East Africa in 1998, after which Osama bin Laden’s satellite phone calls were being monitored continually. Assuming he was really so central in them, ECHELON surveillance would therefore have picked up hints of the planning of new attacks, which were estimated by US officials to have begun two years prior to 9/11 (Ahmed 2005: 185). Ten weeks prior to 9/11, the ECHELON information was assembled into a detailed prediction of an

impending attack, according to the testimony of the counterterrorism coordinator in the White House, Richard A. Clarke (cited in Ahmed 2005: 168).

I already indicated that in the EU the ECHELON network itself was being questioned. In July 2001 the final report of the European Parliament's inquiry into the system was submitted. It was found that the ECHELON network not only intercepted military communications, but also private and business ones on a world scale: telephone calls, fax, e-mail and other data (*Wikipedia*, 'Echelon'). On 5 September 2001, the Parliament voted to accept the committee's report. But even apart from the fact that EP has no say in these matters, Washington meanwhile was preparing the continuation of ECHELON as part of a War on Terror—but not by investigating the threat: Cheney had been appointed to head a task force on domestic terrorism in May to prevent the possibility of an attack on the US, but the task force was not activated. Instead Wolfowitz delivered a commencement address at West Point in June in which he told cadets that it was sixty years since the Japanese surprise attack on Pearl Harbour, recommending that 'America' prepare for 'the unfamiliar and the unlikely' (cited in Mann 2006: 291).

By then, speculative stock trading (which is also tracked by ECHELON) suggesting foreknowledge of the collapse of the most affected airline stocks, was in evidence. Former Bankers Trust investment banker A.B. Krongard, who was appointed CIA executive director by Bush in March 2001, was among those suspected of having tried to gain from it (Ahmed 2005: 197). Research into financial speculation based on foreknowledge of covert operations and coups over a longer period shows that within days of the authorization of action (before anything was in the open), substantial stock market gains were made relating to the target country. Expensive private newsletters circulating in and around the US government supply the necessary hints in this area and in matters relating to industrial espionage (Price 2014: 50-51). This is a reminder that foreknowledge, like causation, is subject to a particular complexity; in this case, people know to the extent they are involved financially, and others will know of other aspects, without the plot being entirely known by all.

Continuity in Government After the Attacks of 9/11

This is not the place to question the official reading of the attacks of 9/11, although there is no doubt that there was a broad expectation that the 'unfamiliar and the

unlikely' (Wolfowitz) were on the way. The minimum is that 'Cheney and Rumsfeld may not have been able to see 9/11 coming', as Jeremy Scahill puts it, 'but they proved masters at exploiting the attacks' (Scahill 2013: 19). The point here is that *mass surveillance society is premised on a war without end, no longer waged against an enemy that can be defeated, but, as predicted by George Orwell, as a disciplining mechanism on the population*. In particular, it aims at controlling the vast reserve army of labour that has been created as a by-product of neoliberal globalisation and the demise of state socialism. So whatever the details on the actual attacks, its perpetrators and the inexplicable paralysis of US defences in the year leading up to the event and on the fatal day itself, there is no doubt that the War on Terror had been prepared well in advance.

Peter Dale Scott proposes to the call the War on Terror *the Terror War* because it is waged by terrorising civilians from both sides. This is a global trend because regimes opposed to the West are only too eager to join this war.

> Terror war in its global context should perhaps be seen as the latest stage of the age-long secular spread of transurban civilization into areas of mostly rural resistance—areas where conventional forms of warfare, for either geographic or cultural reasons, prove inconclusive (Scott 2015: 81).

On 9/11 itself, before the last plane had crashed, Continuity of Government provisions were introduced. Vice-President Cheney temporarily assumed overall command under COG provisions, whilst billionaire investor Warren Buffett and Brent Scowcroft were among those spending the day at the headquarters of the US Strategic Command, at Offutt airbase in Nebraska. From there the COG exercise 'Global Guardian', one of *fifteen* major military exercises conducted that day, was being directed (Tarpley 2008: xi-xii). 'Doomsday' planes meant to serve as nuclear war-fighting command centres. The exercises allowed the shadow government to become operational even whilst the real attacks were going on (Scott 2015: 34).

The COG plans of Rumsfeld and Cheney that were implemented on 9/11 consisted of 1) warrantless surveillance, 2) warrantless detention, and 3) militarization of domestic security enforcement. Cheney installed a 90-day Shadow Government in his bunker under the East Wing, ordering some 100 mid-level officials to other bunkers and stay there 24 hours a day during 90 days, without rotation, justifying this measure

by intimating that al-Qaeda had nuclear weapons (Scott 2015: 34, cf. 8-9). By-passing several ministers and working through subordinates sympathetic to his views, Cheney introduced the above measures and Project Endgame, a ten-year plan beginning in Sept 2001 to expand detention camps at $400 million for fiscal 2007 alone (Scott 2015: 35).

On 8 October 2001, the Office of Homeland Security was established within the presidential Executive Office. Later it became the Dept of HS, the third largest US cabinet department. Most importantly for domestic purposes was the Patriot Act also of October 25. Congress was given one week to pass this 340 page bill, which had been written long before 11 September. It was passed over the initial objections of two Democratic senators (Daschle and Leahy) only after weapons-grade anthrax letters had been sent to them. As was later established by Glenn Greenwald, the anthrax had been sent from a government laboratory where the false reports that the letters had been sent by Iraq also originated (Scott 2015: 36).

On 14 September Bush declared through Proclamation 7463 a national state of emergency with an Executive Order (13233) to put the reserves on active duty (when it was renewed in 2007 its scope was expanded) A second Executive Order (13224, of 23 September) declared a national emergency with respect to terror suspects. Initially this concerned 27 suspects, in 2014 the list was 158 pages long (Scott 2010: 204-5; 2015: 38). Within 8 weeks of the attacks, more than 1,200 people were arrested, some beaten and abused. Hundreds were locked up under 'hold until cleared' rules established by Attorney General Ashcroft, who also ordered 70 to be detained indefinitely. Four were eventually convicted (Scott 2015: 139).

9/11 made it possible to push through any policy simply by invoking 'terrorism', 'a political technique of framing policy questions in logics of survival with a capacity to mobilize politics of fear' (Elbe 2009: 90-91, citing Jef Huysmans). Thus in 2004 and 2005 the *New York Times* kept a report that the NSA was wiretapping without a warrant under wraps for 15 months because the Bush administration claimed it would play into the hands of terrorism—a further sign that the media had subordinated their critical attitude to government priorities (Greenwald 2014: 54-5). Between 1979 and 2011 almost 40,000 requests for wiretaps were made to the FISA court, only eleven were denied (Regan 2014: 34; cf. Greenwald 2014: 128). In other words, wiretapping was fully covered by this secret, quasi-juridical 'court'. After the NYT scandal of 2008 the FISA surveillance law was amended, but in fact its article 702 only made

wiretapping easier because the NSA was now asked to inform the FISA court once a year of the general principles under which it picks up private communications (Greenwald 2014: 74). Meanwhile the Patriot Act was applied well beyond its purpose: search warrants without prior information were mainly used for drugs and fraud cases, and only a fraction for terrorism-related suspects (Greenwald 2014: 200).

The general trend, in the words of Dominick Jenkins, is that 'the *clear distinction between normal periods of good order and exceptional circumstances is broken down by the repeated depiction of threats*…' This justifies the continued extension of executive power; the executive in turn 'uses its prerogative to alter the very structure of society to decisively shift the balance of power within …government in its favour' (Jenkins 2002: 75, emphasis added). How far the definition of 'terrorism' can be stretched to stifle dissent transpired in the arrest of Glenn Greenwald's partner at Heathrow, on the claim that releasing the Snowden documents was 'designed to influence a government and is made for the purposes of promoting a political or ideological cause. *This therefore falls within the definition of terrorism*' (cited in Greenwald 2014: 186, emphasis added). In fact, several think tanks maintain that the US economy is in danger of being attacked with 'economic jihad' not only by al-Qaeda but also by countries like China or Iran (Edwards 2014: 55). This would imply that another serious recession might be interpreted as a *casus belli*. It certainly shows that the crisis itself is recognised as a driver of military action and/or repression.

The Total Information Control Component of the War on Terror

With the proclamation of the War on Terror, the RMA and its component elements of intelligence, surveillance, and reconnaissance, were propelled into the forefront. An IT company closely involved in the 9/11 terror attacks and their aftermath was Ptech, which provides advanced software and information technology to a number of branches of the US national security establishment and NATO. Two of its financial backers were Saudi investors who had been investigated for terrorist financing, and there were other indisputable links to terrorist networks as well (Ahmed 2005: 313-4). Since its clients included key institutions involved in the command and control of US airspace on 9/11 (the Air Force, the Federal Aviation Authority, and the National Airspace Systems Agency, NAS), of which Ptech possessed critical databases for which it supplied the IT programmes, this makes the company a likely candidate for

one aspect of events on the fatal date of 9/11, viz., the complete paralysis of the US air defence system (Ahmed 2005: 316). This was less likely to have been coordinated from a cave in Afghanistan.

Although commercially speaking, Google is the main force sweeping up data mined from the Internet or otherwise (Zuboff 2015: 77), the largest US corporation in data collection is the marketing firm Acxiom which through is 23,000 servers collects information from social media to compose 'premium proprietary behavioural insights', placing everyone into one of 70 lifestyle clusters. Working closely with FBI, Pentagon and Homeland Security, Acxiom also sells its data to credit card companies, banks and brokerages and insurance companies, retailers, media, and pharmaceutical companies. In 2001 it appointed Wesley Clark, former NATO commander, to its board and through Clark began collaborating with Poindexter's Total Information Awareness office at DARPA (Foster and McChesney 2014: 19).

Other IT firms played a role in upholding the government narrative of 9/11. At a presentation at Harvard, Highlands Forum founding president Richard O'Neill not long after the attacks stated that his job as president was to solicit case studies from private sector companies such as eBay and Human Genome Sciences to figure out the basis of US 'information superiority', how to dominate the information market, and communicate the results the White House and the secretary of defence. To facilitate this the Forum had two co-chairs: Andy Marshall, the Pentagon official behind the Team B episode and godfather of the defence NeoCons; and the director of DARPA, at the time a Rumsfeld appointee and formerly vice president of SAIC's Advanced Technology Sector (Ahmed 2015).

In the case of the invasion of Afghanistan, it was not difficult to retain control of the information environment because the world was still in shock over the spectacular 9/11 attacks. In fact the Bush administration formally agreed on the plan to attack the Taliban on 10 September, one day before 9/11. In the case of the invasion of Iraq, it was a different matter. Here the Bush administration relied on John Rendon and the Rendon Group (TRG) to disseminate the myth of Saddam's weapons of mass destruction. Rendon was key in deploying 'perception management' so that regime change in Iraq would become feasible as far as public opinion was concerned , what we today call 'fake news'. Its master document was *A Clean Break*, a 1996 report for a Jerusalem institute by the NeoCons Richard Perle, Douglas Feith, and Feith's Israeli law partner, Marc Zell. It argued for replacing the Baath regime in Iraq by a Shia one

under a Hashemite monarch and restore, for the benefit of Israel, its influence over the Lebanese Shia (then under the influence of Iran). Israel could then strike a deal with Jordan and Iraq, both Hashemite monarchies again, and be supplied through a direct oil pipeline (Van der Pijl 2006: 365). Targeting Iran's nuclear research programme later, the US and Israel jointly developed the Stuxnet virus that they deployed to sabotage the Islamic Republic's centrifuge programme (Foster and McChesney 2014: 21). The Stuxnet operation was traced to the Israeli Cyber Intelligence Unit, ISNU or Unit 8200 (Price 2014: 47).

Rendon's group developed an information warfare strategy from this starting point and to that end was been given access to the NSA's top-secret surveillance data. This included Sensitive Compartmented Information, data classified higher than Top Secret; besides Special Intelligence, which is highly secret communications intercepted by the NSA. Also Rendon had information from 'Talent/Keyhole', code for imagery from reconnaissance aircraft and spy satellites; Gamma, communications intercepts from extremely sensitive sources, and the Humint Control System information (Ahmed 2015). This gives a sense of the already existing array of information mobilised for information warfare at the time.

According to O'Neill, the formulation of a doctrine of information warfare also required upgrading electronic surveillance and answering the question "what constitutes an act of war in an information environment' (cited in Ahmed 2015). 'Russian hacking' in elections would then be a case of trying to sound out how the public would react to accusations amounting to making claims about 'acts of war' in the information domain. At the RAND Corporation, strategists were meanwhile elaborating how far the goal of 'Information Superiority' should be taken, for instance by surveying and manipulating foreign leaders' communications (Ahmed 2015). From the Snowden revelations we meanwhile know that this was pretty much unlimited.

According to a DARPA official who led the Evidence Extraction and Link Detection (EELD) programme, EELD was meant as one route towards a system of Total Information Awareness that became the main global electronic eavesdropping and data-mining program deployed by the Bush administration after 9/11. It had been set up by the aforementioned Admiral John Poindexter, whom Bush appointed head of DARPA's new Information Awareness Office in 2002. Much of its research was contracted out to Booz Allen Hamilton, Snowden's employer; there the head of the intelligence division was the former NSA director and later director of National

Intelligence (under father and son Bush, respectively), Mike McConnell, a close associate of Poindexter. However, a scandal erupted over the use of Total Information Awareness for an online futures trading market speculating on terrorist attacks (an issue that had come up in the context of 9/11 already, Ahmed 2005: 193-200) and the programme was defunded in 2003 (Foster and McChesney 2014: 17).

DARPA research included 'behaviour-based profiling,' 'automated detection, identification and tracking' of terrorist activity and other data-analyzing projects. As Nafeez Ahmed writes, 'The Pentagon Highlands Forum's intimate link, via Rendon, to the propaganda operations pursued under Bush and Obama in support of the "Long War", demonstrate the integral role of mass surveillance in both irregular warfare and "strategic communications"' (Ahmed 2015).

The Surveillance Infrastructure of the Global Security State

At the centre of the surveillance apparatus, expanded to an unprecedented level, are the NSA and the 16 other US intelligence agencies, their combined budget of around $60 billion (Engelhardt 2014: 15, figure for 2007). The structural advantage enjoyed by the US consists in what Glenn Greenwald calls a 'one-way mirror': 'The US government sees what everyone else in the world does, including its own population, while no one sees its own actions' (Greenwald 2014: 169). The NSA routinely intercepts routers, servers and computer network devices to plant surveillance beacxons and them before repackaging and sending them on as if nothing happened (Greenwald 2014: 148). In 2003, Google began customizing its search engine under special contract with the CIA for its Intelink Management Office, 'overseeing top-secret, secret and sensitive but unclassified intranets for CIA and other IC agencies,' according to *Homeland Security Today.* That year, CIA funding was also being funnelled through the National Science Foundation to projects that might help create 'new capabilities to combat terrorism through advanced technology' (Ahmed 2015).

In addition to communications intercepts, satellite surveillance is organised by the National Geospatial-Intelligence Agency (NGA), which alone has 16,000 employees and an annual budget of $5 billion. It has a $1.8 billion headquarters, the third-largest structure in the Washington area almost as large as the Pentagon. NGA satellites cover the entire globe and constitute 'the nation's primary source for geospatial intelligence, or GEOINT' (Engelhardt 2014: 19-20). Just as defence-funded R&D was

made available to private companies, often at no or negligible cost and under a lightweight tax regime owing to debt-financed budgets, the actual intelligence services have been expanded through private contractors. 70 percent of the US intelligence budget goes to private contractors. Satellite surveillance is not different. It is part-privatised to the *DigitalGlobe* corporation, which had become the monopoly supplier after acquiring its one competitor, *GeoEye*, in 2013. It serves a range of customers including the NGA (*Wikipedia,* 'DigitalGlobe'). Satellite and other remote-sensing information is handled by the National Reconnaisance Office (NRO), the third-largest intelligence office after the CIA and NSA (Engelhardt 2014: 22).

Until the Snowden revelations, few people were aware of the extent of this vast data-mining system, which was entirely geared to cyber-warfare, with commercial and diplomatic spying as a subsidiary activity. In Presidential Policy Directive 20, Obama authorized a list of cyber-targets; all attempts by other states to agree on a cyber-war treaty have been rebuffed by the US (Purkayashta and Bailey 2014: 107). The combination of intelligence agencies and global corporations headquartered in the United States have created large global monopolies on an unprecedented scale and US stewardship of large Internet organisations ensures that attempts to create international regulation stand no chance (Purkayashta and Bailey 2014: 114). At the 2012 international conference on telecom and Internet governance at Dubai, 89 countries signed up to a new regulation structure, but the US and the EU joined forces in rejected it.

The privatisation of the surveillance system also has made it vulnerable to conscientious objectors. Around half a million people work for private contractors in the surveillance business alone. There are nearly 5 million Americans with security clearances and 1.4 million with top security clearances (of which one-third are private contractors) (Engelhardt 2014: 15). In December 2012, the journalist, Glenn Greenwald, was approached by one of them, an anonymous blogger who later turned out to be Edward Snowden, a Booz Allen Hamilton employee working for the NSA. Besides giving unprecedented insight into the extent of the US/Five Eyes global surveillance system, the Snowden revelations also derailed ongoing attempts to tighten the surveillance regime. Thus the exposure dealt a blow to the CISPA law then going through Congress. This cyber data sharing law, adopted by the US House of Representatives in April 2012, prescribes that financial and infrastructure institutions share their data with the military, intelligence and Homeland Security. However, the

Senate did not follow it and the CISPA process began anew, backed by a powerful array of banks, defence industries and the large IT corporations. Snowden's revelations showed it was the US, not foreign powers, that led the world in snooping on others (Edwards 2013: 58-60).

Also following the Snowden revelations, a conference was called by the Brazilian president, Dilma Rousseff, whose private phone was also tapped by the NSA. At this conference agreement was reached on fundamental changes to the governance structure, but ICANN, the California-based private organisation assigning domain names, not only succeeded in largely sidelining the surveillance issue but also to get support for a model that leaves the private sector in charge (Purkayashta and Bailey 2014: 118-9).

Whilst privatisation already means that democratic checks and balances are by-passed, the political system itself is also subject to rolling back democracy. Under the Patriot Act the constitutional rights of US citizens are suspended in key respects, as in the case of the Fourth Amendment prohibiting 'unreasonable searches and seizures'; in addition the government also enrols citizens in the operation of the Deep State under the US Justice Department's Terrorism Information and Prevention System (TIPS). This 'means the US will have a higher percentage of citizen informers than the former East German Stasi secret police' (Jenkins 2002: 266). A $2 billion NSA data repository in Bluffdale, Utah, has been set up to hold an almost unimaginable quantity of intercepted communications (Engelhardt 2014: 15). It has been observed many times that collecting all available information only ensures that real plots are missed (Greenwald 2014: 205), assuming of course that terrorists would indeed sit down behind their laptops to communicate their evil intentions.

IT Corporations in the Service of the US National Security State

Let us now look again at the corporations to which as noted, 70 percent of the estimated $60 billion annual expenditure on US intelligence is outsourced (Scott 2015: 20). The most prominent private partner of the US intelligence community is SAIC (Science Applications International Corporation). SAIC/Leidos (the SAIC holding since 2013) is among the top-10 largest defence contractors in the US and works closely with the NSA in particular (Ahmed 2015). Booz Allen Hamilton is majority owned by Carlyle Group and 99 percent of its business is with the US

government. Booz, employer of Edward Snowden, is also prominent in the COG area as the largest of its 'cleared contractors' and was entwined with the CIA ever since Dulles became CIA director in 1953 (Scott 2015: 21). Its current head office is in McLean, Virginia, near CIA headquarters. Senior personnel from SAIC and Booz Allen Hamilton have been regular participants in the Highland Forum meetings in which new developments in the security field and opportunities for private contractors are discussed. In addition these meetings were attended by eBay, PayPal, Google, Microsoft, and other IT firms (Ahmed 2015).

As Snowden revealed, these IT companies as a matter of routine allow the NSA access to their servers. Under the PRISM agreement Microsoft, Google, Yahoo, Facebook, Paltalk, AOL, Skype, YouTube, and Apple, including their subsidiaries, thus were part of a vast search engine for the US intelligence community and its heartland allies, the 'Five Eyes' (Greenwald 2014: 21). Microsoft gives access to Skydrive with its 250 million users worldwide who store their data online, to Skype (purchased by Microsoft in 2011) with 663 million registered users, and to its Outlook/Hotmail e-mail service. In spite of assurances of privacy, all Skype communications are available to US government, and whilst Microsoft promised encryption to Outlook/Hotmail users, it then worked with the NSA and FBI to circumvent it (Greenwald 2014: 113-5). Telephone companies hand over phone metadata too and actually are under an obligation to do so. Greenwald records that the FISA Court gave an instruction to Verizon to this effect (Greenwald 2014: 27). The phone companies actually earn money this way: AT&T sells its phone metadata to the NSA for over $10 million a year (Foster and McChesney 2014: 24).

Google, the most important private player in the all-round surveillance business, has turned its vast databases into saleable assets too, and Shoshana Zuboff calls this model, in which data are being collected to be sold to advertisers, 'surveillance capitalism' (Zuboff 2015). However, she does not explicitly address the integration with the national security state. Yet here Google is a key player too. Its subsidiary Google Earth is one instance of its involvement with the global surveillance structures. Google Earth goes back to Keyhole, a mapping project originally funded by the CIA venture capital firm, In-Q-Tel. In 2004, Google bought Keyhole and began developing the advanced satellite mapping software behind Google Earth. At the time of its acquisition, Anita Jones, former DARPA director and co-chair of the Highlands Forum, was on the board of In-Q-Tel and when she moved to Google, was

kept on in that role. The director of technical assessment at In-Q-Tel explored ‘new start-up technology firms that were believed to offer tremendous value to the CIA, the National Geospatial-Intelligence Agency, and the Defense Intelligence Agency’ and this included the software later used in Google Earth. After Google also bought In-Q-Tel, Nafeez Ahmed recounts (2015), the said director, a former US Army special operations intelligence officer, also joined Google, one year after this acquisition.

After the invasion of Iraq in 2003, intelligence obtained through Keyhole was used by the NSA to support US operations in the country, tracking down resistance, landmine and IED detection, whilst tracking down people to help fill up the notorious prisons operated by the invaders, such as Abu Ghraib. The Pentagon was already using a version of Google Earth developed in partnership with Lockheed Martin to ‘display information for the military on the ground in Iraq’. In 2010, Google signed a multi-billion dollar contract with the NGA to use Google Earth for visualization services for the agency (Ahmed 2015).

The Snowden revelations on surveillance have compromised every aspect of the Internet: the fiber-optic level (cables of AT&T and others, servers); the NSA’s partner companies Google, Facebook etc.; and software and hardware companies such as Microsoft, and Apple, respectively, to name only a few (Purkayashta and Bailey 2014: 106). However, with the EU in a subservient role as America’s vassal and leaders standing up to the US such as Dilma Rousseff removed in due course, the fears of some of these companies that their competitive position would be harmed by the disclosures has so far proven unfounded.

5. Population Control Under the Permanent State of Exception

Big Data for Surveillance

'For the first time, a great power wants to know, up close and personal, not just what its own citizens are doing but those of distant lands as well, who they are communicating with, and how, and why… None of the twentieth-century totalitarian regimes ever imagined doing the same thing on a genuinely global scale' (Engelhardt 2014: 11). The fact that the vast majority of the world's Internet traffic flows through the US communication infrastructure creates 'choke points', which in turn allow the joint NSA-FBI STORMBREW programme in sweeping up communications (Greenwald 2014: 107). The NSA also has a program to plant surveillance equipment in individual computers and operates its own hacker unit implanting special software, in nearly 100,000 computers around the world (Greenwald 2014: 117). The collection and processing of vast amounts of data was facilitated by another important private company in the IT complex, Palantir.

Palantir was co-founded in 2004 by Facebook board member Peter Thiel (the other two were venture capital tycoon James Breyer and Mark Zuckerberg) and his co-founder Alex Karp after a meeting with John Poindexter hosted by long-standing NeoCon Richard Perle (Biddle 2017). Palantir had its origins in the fraud detection branch of PayPal and initially worked exclusively for the CIA, which had funded it through it In-Q-Tel venture capital subsidiary (Cockburn 2015: 176; Ahmed 2015).

Around 2008 the NSA was resurrecting the Total Information Awareness strategy with a focus on Internet data-mining via comprehensive monitoring of e-mail, text messages, and Web browsing (Ahmed 2015). Facebook and Twitter in particular provide the NSA with a wealth of information on the personal lives of targets; by storing information gained over a period of several days each time the amount of data is increased (Greenwald 2014: 158-9). In this field of large-scale data mining Palantir was to become the dominant supplier. From its initial role working for the CIA it branched out to new clients including Special Forces, US law enforcement, and JP Morgan (Cockburn 2015: 276). It also established contact also with GCHQ, the UK's equivalent of the NSA. At a joint conference Palantir demonstrated how well it could track required information by taking a fictional radical group and identify them through their Wikipedia use.

> Within two years, documents show that at least three members of the "Five Eyes" spy alliance between the United States, the U.K., Australia, New Zealand, and Canada were employing Palantir to help gather and process data from around the world. Palantir excels at making connections between enormous, separate databases, pulling big buckets of information (call records, IP addresses, financial transactions, names, conversations, travel records) into one centralized heap and visualizing them coherently, thus solving one of the persistent problems of modern intelligence gathering: data overload (Biddle 2017)

Thus Palantir provides the US government with 'an unmatched power to sift and exploit information of any kind' (Biddle 2017). Palantir, a company meanwhile worth an estimated $20 billion, calls this 'many analysts working together [to] truly leverage their collective mind'. This collective mind was put at the service of the NSA's global spy network and notably developed its most intrusive surveillance tool, XKEYSCORE, the NSA's 'widest reaching' program, capturing 'nearly everything a typical user does on the internet' (NSA cited by Biddle 2017). XKEYSCORE 'collected communications not only include emails, chats, and web-browsing traffic, but also pictures, documents, voice calls, webcam photos, web searches, advertising analytics traffic, social media traffic, botnet traffic, logged keystrokes, computer network exploitation targeting, intercepted username and password pairs, file uploads to online services, Skype sessions, and more' (Biddle 2017). Every mail address seen in a session, every telephone number, and all address book entries are routinely recorded through XKEYSCORE (Greenwald 2014: 154). As a friend of Donald Trump, co-founder Thiel obviously offers the new president powerful means of resisting attempts to destabilise his presidency (cf. Biddle 2017).

Meanwhile the tactics deployed on the basis of Total Information Awareness continue along the lines already tested out in the 1970s or earlier. A joint NSA-GCHQ 'Mastering the Internet' surveillance program, running Palantir software, thus is able to provide an 'augmented reality' experience (Biddle 2017). In an age of fake news (of which the governments and its institutions and mainstream media are in fact the main providers!), the ability to 'augment' reality is obviously not a mean asset. It widens the field for manipulating not only (passive) public opinion, but also use groups and individuals to act on the basis of 'augmented reality', triggering them into

performing acts deemed useful from the agencies' perspective. This takes us to the role agent-provocateurs in critical situations.

Use of Double Agents under Total Information Awareness (I)

The frequency of so-called terror incidents and their spread notably to countries like France provides ample reason for closer study. This theme, a minefield given the many unknowns surrounding actual incidents, has to be handled with the greatest care and always providing for mistakes and over-interpretation. Even so, the verdict of 'conspiracy theory' hanging over the head of anyone investigating it, should not deter one from questioning the authenticity of certain incidents. For the authorities who want to institute blanket surveillance are also those who handle and as I will argue, occasionally *provoke* terror incidents.

In the United States the military long infiltrated the peace movement, whilst the FBI recruited young women on campuses to spy on and entrap anarchist or environmentalist dates (Regan 2014: 39). The use of provocation by the US in Western Europe has been amply documented and one of its key documents, *US Army Field Manual (FM 30-31),* spells out its rationale. Dating from 1970 and ascribed to the authorship of General William Westmoreland, US Army chief of staff, it recommended penetration of 'insurgent' groups by US agents in case *an allied government proved 'passive and indecisive' in the face of 'communist subversion'*. It was made public first in the Turkish press in 1976 and in 1981, the entire document was found hidden in the luggage of the daughter of Licio Gelli, the Grand Master of the Italian Masonic lodge, Propagada Due (P-2), just after the membership list of the P-2 lodge had been made public (Willan 1991: 209; excerpts were published in Italy by the magazine *Panorama* in July 1981). P-2 effectively was the Deep State in Italy in the 1970s. A full overview of these forces in Europe has been documented by Swiss researcher Daniele Ganser (2005).

How did this capacity for using terrorists to advance the US/NATO agenda evolve *after* the Cold War? In the late 1990s, a British newspaper obtained 10,000 pages of documentation from Egyptian state security showing that al-Qaeda had deployed sleeper cells across the Western world which could be activated into committing terror attacks (Ahmed 2005: 50). If *they* knew, the US too would know because the Mubarak regime was a CIA-run outfit. And after 9/11, US intelligence no longer made a secret

of its readiness to penetrate and manipulate or otherwise exploit the existence of such groups. At an August 2002 briefing, the Pentagon's Defense Science Board proposed the creation of a 'Proactive, Preemptive Operations Group' (P2OG) within the National Security Council. P2OG goes back to the Intelligence Support Activity (ISA) established in 1981 and involved in a range of illegal drugs and counter-terror operations in the Middle East and Latin America. It remained active under the code name, Gray Fox (Ahmed 2005: 325). Building on this legacy, P2OG should 'conduct *clandestine operations to infiltrate and "stimulate reactions" among terrorist networks to provoke them into action*, and thus facilitate targeting them' (Ahmed 2015, emphasis added). Still according to Nafeez Ahmed, at the Pentagon, Rumsfeld set up a new black operations infrastructure under his own supervision, from which CIA and regional US military commanders were to be excluded entirely.

A 2004 US Air Force study on US strategy toward 'non-state armed groups' co-authored by Itamara Lochard, argued that non-state armed groups should be urgently recognized as a 'tier one security priority.' But not only as a threat. The proliferation of armed groups 'provide strategic opportunities that *can be exploited* to help achieve policy goals. There have and will be instances where the United States *may find collaborating with armed group is in its strategic interests*' (cited by Ahmed 2015, emphasis added). To this end a database of 1,700 non-state groups including 'insurgents, militias, terrorists, complex criminal organizations, organized gangs, malicious cyber actors and strategic non-violent actors,' was kept to analyze their 'organizational patterns, areas of cooperation, strategies and tactics.' This clearly was not just a matter of armed groups or terrorists but also 'strategic non-violent actors' engaged in social political activity or campaigning (Ahmed 2015). The UK harboured several key Islamic terrorist leaders recruited by MI5 and MI6 for use against selected targets, and even their incarceration at some point was probably intended to keep them out of the hands of foreign intelligence (Ahmed 2005: 108-16, 144). P2OG too should 'stimulate terrorists' into 'responding or moving operations' (Ahmed 2005: 325).

Clearly the idea of triggering terror events by provocation, penetration and/or direction of 'armed groups' for strategic advantage is not a figment of the imagination of some overheated 'conspiracy theorist'. It can be read from (semi-) official documents. In a way though it is almost a secondary matter to expose individual cases of how double agents are used. Thus David Ray Griffin claims that even the glaring

impossibilities and inconsistencies in the 9/11 attacks should not distract from the basic fact of the role of terrorism for state repression. 'Exposing the truth about 9/11 is also necessary for the sake of preventing further crimes against democracy' (Griffin 2011: 296). These crimes are part of a steady rolling back of democracy since the 1970s, intensified after the collapse of state socialism and the neoliberal globalisation of capital, in order to control the surplus population. To cite Nafeez Ahmed again, 'al-Qaeda terrorism is itself a system, or more precisely, an integral function of the world system under Western hegemony in the post-Cold War era' (Ahmed 2005: 369, emphases deleted).

It is therefore logical that the use of double agents and provocation are part of government armoury. The British GCHQ has a unit which employs these tactics, including 'false flag operations', 'honey-traps', creating computer viruses, and operations aimed at damaging reputations. The dissident hacker network, Anonymous, was one group targeted by this unit (Greenwald 2014: 190). A key political strategist such as former National Security adviser (and David Rockefeller's right-hand man in the establishment of the Trilateral Commission). Zbigniew Brzezinski, in fact did not deny that this set of tactics might be used—for the wrong purposes. When in 2007, Vice-President Cheney, as was later revealed, was pushing for air strikes against Iran (Scott 2010: 208), Brzezinski warned against such a course before the Senate Foreign Relations Committee. For Brzezinski, whose lifelong mission has been to roll back Soviet domination of Eastern Europe and who after 1991 advocated further breaking up the Russian federation, the preoccupation with the Middle East was a fatal distraction. Calling the invasion of Iraq four years earlier 'a historic, strategic, and moral calamity, undertaken under false assumptions… driven by Manichean impulses and imperial hubris', Brzezinski warned against an even more disastrous involvement in Iran and the use of 'false flag' operations to kick-start 'wars of choice'. He specifically alerted the Committee to 'some provocation in Iraq *or a terrorist act in the U.S. blamed on Iran*'.

Asked by a journalist whether he really meant to say that provocation including a false flag operation could in principle be the work of US officials, the following exchange ensued.

> Q: Dr. Brzezinski, who do you think would be carrying out this possible provocation?

A: I have no idea. As I said, these things can never be predicted. It can be spontaneous.

Q: Are you suggesting there is a possibility it could originate within the US government itself?

A: I'm saying the whole situation can get out of hand and all sorts of calculations can produce a circumstance that would be very difficult to trace (Grey 2007).

Such statements by somebody who has certainly been privy to the workings of the Deep State in his time, should encourage us not to join in howling down those who want a murky piece of history such a 9/11, from which more than a decade of war, torture, and human misery have followed, cleared up.

Use of Double Agents under Total Information Awareness (II)

Seymour Hersh in a 2005 investigation actually documented that John Arquilla had worked out a new strategy of 'countering terror' with pseudo-terror on the basis of the thesis that 'It takes a network to fight a network'. The prototype was the British use of Kikuyu tribesmen in Kenya pretending to be Mau Mau terrorists who played a big role in defeating the Mau Mau in the 1950s. Arquilla proposed recruiting pseudo gangs like the ones the British set up, and the Pentagon, which unlike the CIA can keep such actions hidden from Congressional oversight, according to Arquilla was in fact already implementing this strategy. As Hersh relates, 'according to the Pentagon advisers, local citizens could be recruited and asked to join up with guerrillas or terrorists.' This would allow Special Forces to set up 'action teams' in the target countries overseas which can be used to find and eliminate terrorist organizations. This was in fact already tried out in the case of Far Right death squads in El Salvador, which also had been set up and financed by the US, Hersh was told by a former commando officer (Hersh 2005).

The leak of a 2008 US Army special operations field manual, as in the case of FM 30/31 cited earlier, made clear that this strategy was indeed operational.

The US military, the manual said, can conduct irregular and unconventional warfare by using surrogate non-state groups such as "paramilitary forces, individuals, businesses, foreign political organizations, resistant or insurgent

> organizations, expatriates, transnational terrorism adversaries, disillusioned transnational terrorism members, black marketers, and other social or political 'undesirables.'" Shockingly, the manual specifically acknowledged that US special operations can involve both counterterrorism and "Terrorism," as well as: "Transnational criminal activities, including narco-trafficking, illicit arms-dealing, and illegal financial transactions." The purpose of such covert operations is, essentially, population control—they are "specifically focused on leveraging some portion of the indigenous population to accept the status quo," or to accept "whatever political outcome" is being imposed or negotiated (Ahmed 2015).

In his book, Nafeez Ahmed details the use of fake terrorists in acts of provocation or worse and makes clear that what I call the global strategy of tension employs a well-thought out infrastructure for creating chaos and imposed military control. P2OG reveals the depth of thinking and preparation behind that strategy and its ancestry, Ahmed writes, must therefore reach much further back. 'The interlocking web of US-al-Qaeda connections across the globe… provides the most plausible explanation of the facilitation of international terrorism systematically generated by the US national security apparatus over the last decade or so' (Ahmed 2005: 326). Could it be, he asks, that the bogeyman of Osama bin Laden played a functional role 'within the matrix of longstanding plans to increasingly subject world order to US/Western military, political, strategic and economic influence?' (Ahmed 2005: 365).

In March 2004 a train bombing in Madrid killing 191 people and wounding almost 2,000 proved to be the work, not of the Basque ETA as the conservative government maintained, but of a Moroccan al-Qaeda network active in a range of countries including Spain. For years US and European intelligence agencies had been privy to the activities of this network and had a complete insight into its structure and membership. Remarkably, as the London *Times* reported, the man suspected of supplying the dynamite had the telephone number of a Guardia Civil bomb squad officer in his possession whilst two of the suspects were police informants (Ahmed 2005: 327-8).

A comparable overlap between perpetrators and prosecutors played out in France, the historic hard nut to crack for the Western intelligence agencies and their associates. Ever since De Gaulle exposed the structures operating against him in the 50s and 60s, the tradition he spawned has been an obstacle to Atlantic unity. In the

early 90s, Algerian and Afghan operatives committing bomb attacks in France were found having been granted right of residence in London (Ahmed 2005: 73). After his election in 2007 Nicolas Sarkozy attempted to end France's exposure to terror blackmail—by submitting to US-Israeli supervision in this domain. Sarkozy reorganized the French intelligence services, merging General Intelligence (RG) and the Department of Security (DST) into a single General Directorate of Internal Security (DCRI) and placing a close associate at its head; another political ally was made head of the DGSE, foreign intelligence, long the fief of Alexandre de Marenches (a French NeoCon and member of the Safari Club). The new DCRI intensified surveillance of Muslims and raised the level of cooperation with Israel (L. Guyenot in Barrett 2015: 96). After 9/11 Israel had intensified collaboration with NATO, to the point of becoming a NATO member state for all practical purposes except formal membership (Halper 2015: 57-61).

With his re-election due in 2012, the weekly, *L'Expres*s, predicted that Sarkozy would need an 'international, exceptional or traumatizing event' or lose. Two unrelated shootings then took place in the south of France in March: one traceable to neo-Nazis targeting North African soldiers of a parachute regiment, the other a senseless gun attack on a Jewish religious school nearby. Sarkozy compared the two incidents, thrown together as one, to 9/11 and introduced Patriot-style anti-terror laws in parliament, but they were rejected. The intelligence services then identified a single perpetrator of both attacks: an informer of the DCRI of Arab background, who was shot dead in a circus-like siege, unable to contradict a police résumé casting him as a murderous fanatic (L. Guyenot in Barrett 2015: 98-101). This proved almost a blueprint for the *Charlie Hebdo* attacks in 2015.

Charlie Hebdo as a Case of Perception Management

The attack on Libya was initiated by Sarkozy; he previously had engineered a regime change in Ivory Coast, removing Laurent Gbagbo and replacing him with A. Ouattara, nicknamed 'the American'. Libya was turned into a failed state and Africa's surplus population began to trickle across the Mediterranean. The chaos there became part of the US presidential campaign after a crude, Israeli-made anti-Muslim video in September 2012 provoked the attack by Islamists on the American mission in Benghazi that killed the US ambassador and three others. That this was part of an

attempt to prevent the re-election of Obama is suggested by the fact that his opponent, Mitt Romney, obtained the details of the incident before they were made public and used them in a campaign speech (Barrett 2015: 26-7, 44).

Obama won the election but Sarkozy was defeated by François Hollande, who could not be counted on as surely as his predecessor to toe the line. Called to Berlin immediately after his election to be told by Chancellor Merkel that his promise to end austerity was out of the question, Hollande reversed course right away. By 2014, his economy minister had left in protest, to be replaced by Hollande's advisor, the young Rothschild banker, Emmanuel Macron, who wasted no time before writing a neoliberal omnibus bill named after him (Bulard 2015). The bill encountered strong social protests and further political turbulence followed when the parliament in Paris voted in favour of recognising an independent state of Palestine. Then on January 5, 2015, Hollande spoke out against sanctions on Russia over the Ukraine crisis, stuck as he was with two helicopter carriers ordered by Moscow, which could not be delivered under the sanctions. So France faced social unrest but also antagonised both Israel and the US when masked gunmen shot dead 12 people in cold blood and a hostage-taking in a Jewish supermarket caused 4 dead later that month. As in 2012, it seemed as if an anti-Semitic attack was tacked on to an unrelated atrocity.

The Israeli government certainly did not make a secret of its concerns. In August 2014 Netanyahu warned on French TV against recognition of Palestine. 'This is not Israel's battle. It is your battle, it is France's battle. If they succeed here, if Israel is criticized instead of the terrorists, if we do not stand in solidarity, *this plague of terrorism will come to your country*' (cited in Barrett 2015: 113, emphasis added). Whether this was a prediction or a threat, we cannot know for sure, but there were reports that Israel's cyber intelligence unit (ISNU/Unit 8200) had hacked into the Elisée Palace in 2014 (Price 2014: 47) and Avigdor Lieberman, the Far Right foreign minister, visited Paris on the 25th of December, just prior to the *Charlie* massacre, meeting confidentially with Mossad agents (all details from Barrett 2015 and Wisnewski 2015; both combine important if sometimes over-interpreted information).

Charlie Hebdo was a left-over from the 1968 student rebellion but in the meantime had been appropriated by the Sarkozy clique through various connections. Its vulgar and tasteless satire and attacks on religion increasingly focused on Islam in particular; when one cartoonist, Siné, mocked Sarkozy's son's conversion to orthodox Judaism in order to marry, he was fired. The alleged perpetrators of the *Charlie* massacre , two

brothers, were being monitored by French domestic intelligence and the police; both left identity papers in the car and were later shot dead, as was the hostage-taker in the Jewish supermarket. There were many loose ends and odd coincidences in the drama, which Helric Frédou, a police investigator familiar with the two brothers, wanted to report on in spite of having been ordered to let it go. He was found dead with a bullet in the head, allegedly having killed himself whilst working on his report at night.

Meanwhile the mass outpouring of indignation at the brutal massacre was channelled into demonstrations under a single slogan: 'I am Charlie', with political leaders pictured in the media as if leading the march in Paris, but in fact lined up in a side-street photo-op, with Netanyahu in the front row. This after all was the moment the war he had called for at the Jonathan conferences of 1979 and '84 had come to France. The French state as well as various press funds, including one funded by Google, showered money on the presumed bastion of free speech. Netanyahu publicly called on French citizens of Jewish background to emigrate to Israel; Hollande's meeting with Merkel, Putin and Poroshenko, planned for 15 January, was cancelled.

Clearly there is ample room for doubt regarding the *Charlie* massacre, but generally those terror incidents in which 1) perpetrators are known to the police, 2) leave their identity cards in getaway cars or elsewhere, and 3) are shot dead instead of arrested alive, should be looked at more closely for traces of manipulation and the *Charlie Hebdo* attacks are a case in point. The War on Terror as a Strategy of Tension can be used in many ways, also to kick in line an 'ally' seen to be hesitating on key matters.

Placing Surplus Humanity Under Surveillance

As Nafeez Ahmed writes in a chapter 'The Grand Design', 'the new "War on Terror" under US leadership is not, in reality, fundamentally concerned with the elimination of international terrorism.'

> On the contrary, not only does the strategy employed in the new "War on Terror" seem to provoke international terrorism, but an integral dimension of the strategy is the protection of key actors culpable in the financial, logistical, and military-intelligence support of international terrorism. …There is ample evidence from the

historical and contemporary record of wider geostrategic imperatives behind the "War on Terror" (Ahmed 2005: 331).

As Martin Shaw argues, the War on Terror has created a situation in which the West faces 'a sort of extensive (but less intensive) "Israelization": … *immersion in many unending, unwinnable, if low-level wars and the corresponding brutalization of state and society*' (Shaw 2005: 140, emphasis added).

This leads to a situation in which 'Occupied Territories' proliferate, from the *banlieues* of French cities to the home countries from which 'Palestinians' hail and where many of them remain. Whilst politicians call for the 'defence of the nation' against 'terrorism' in order to legitimate surveillance and other control measures (cf. Serfati 2017: 188-9), the idea of isolating and removing the 'alien' element in society will harden mutual attitudes. The need to have Total Information Awareness in the circumstances has to be met by continuous innovation. Whilst domestic restrictions of the Patriot type are slowly undermining the political liberalism and spreading a '1984' atmosphere of disinformation and demonisation, opportunities for controlling people's mindsets increase. Importantly, penal law in this circumstances mutates from a codex aimed at punishing acts to criminalising behaviour ('*comportement*') (Serfati 2017: 191; cf. Paye 2014).

Michele Quaid, an executive in the NGA, National Reconnaissance Office and the Office of the Director of National Intelligence (where she served as Director of the Intelligence, Surveillance, and Reconnaissance Task Force), moved to Google in 2011. Still in the Bush years, this latter Task Force was asked to report to the then-undersecretary of defence for intelligence, James Clapper (who would become Director of National Intelligence under Obama) on the targets of the War on Terror. As Ahmed writes, the Task Force report Ms. Quaid produced identified 24 countries in South and Southeast Asia, North and West Africa, the Middle East and South America that would at some point pose 'possible COIN [counterinsurgency] challenges' for the United State military. Specific countries mentioned were Pakistan, Mexico, Yemen, Nigeria, Guatemala, Gaza/West Bank, Egypt, Saudi Arabia, Lebanon, as well as other 'autocratic regimes' (Ahmed 2015). Many of these countries were already identified by Huntington in his Clash of Civilisations book as harbouring a surplus population of young men inclined to violence. To be prepared for handling possible crises, Total Information Awareness thus was necessary, as were

preparations based on it for manipulating the conflict potential ('population-centric operations').

> US involvement short of military intervention requires *"monitoring the blogosphere and other social media across many different cultures and languages"* to prepare for "population-centric operations," needed in "nascent resource conflicts, whether based on water-crises, agricultural stress, environmental stress, or rents" from mineral resources (Ahmed 2015).

Ultimately this would involve targeted assassination as in the Phoenix programme in Vietnam. In 2004, a top US counterinsurgency expert argued that this programme had been unfairly maligned and that surveillance made it possible to develop what he called 'a "disaggregating strategy" *targeting insurgent networks on a global scale*' in the way Phoenix had done in Vietnam (Cockburn 2015: 88, emphasis added).

Entire populations, especially political activists, would have to be watched to identify threats and (citing Ahmed again) 'to be vigilant against hypothetical populist insurgencies both at home and abroad'. One wrong or misunderstood Twitter or Facebook post and could make one end up on a secret terrorism watch-list, and potentially on a kill list (Ahmed 2015). DARPA's Total Information Awareness programme, apparently grounded by Congress in 2003 over its being used for internet futures speculation in relation to terrorist attacks, was in fact continued privately by Booz Allen Hamilton and SAIC (Foster and McChesney 2014: 25).

To fine-tune the ability to manipulate public opinion under the doctrine of perception management, the Highlands Forum in 2011 hosted two DARPA-funded scientists working on a 'Neurobiology of Narrative Framing' project at the University of Southern California. Its aim is to detect the structure of strong, sacred values that can allow the evocation of emotional responses in people. Because this varies in different cultures, the project investigates linguistic and neuropsychological mechanisms through which these responses come about, based on extracting narratives from millions of American, Iranian and Chinese weblogs, and subjecting them to automated discourse analysis to compare them quantitatively across the three languages. This is then corroborated by MRI scans (Ahmed 2015).

Whilst such in-depth analytical tools are being developed, leaders are being wiretapped on a routine basis. Dilma Rousseff, meanwhile deposed by a soft coup in

2013, was under surveillance from the NSA, as were, in 2011, Mexican presidential candidate, elected in 2012, Enrique Peña Nieto and his entourage (Greenwald 2014: 139-40). In all, it was reported in 2013 that as far as global elites go, US and British intelligence were targeting more than 1,000 people (McCoy 2014: 76). The personal cell phone of German Chancellor Angela Merkel was targeted for many years (Greenwald 2014: 141). In preparation for the invasion of Iraq, Kofi Annan and the 'Middle Six' on the Security Council were all under surveillance (McCoy 2014: 77). Companies such as Brazilian Petrobras, and energy firms in Mexico and Venezuela, as well as Russia's Gazprom and Aeroflot, are all under surveillance (Greenwald 2014: 135).

Google's Continuing Intelligence Role

Google remains the single largest, comprehensively innovative force in the surveillance capitalist universe. Shoshana Zuboff infers far-reaching conclusions of this new stage of capitalism from the Google experience. Thus she notes how Hayek's claim that an economy cannot be planned because of the unknowability of so many of its inner workings, is completely superseded by the integral knowledge that Google and its equivalent IT giants are obtaining and continually updating—knowledge eagerly supplied with them by customers hooked on the Web.

> Google's new investments in machine learning, drones, wearables, self-driving cars, nano particles that "patrol" the body for signs of disease, and smart devices for the home are each essential components of this growing network of smart sensors and Internet-enabled devices intended as a new intelligent infrastructure for objects and bodies (Zuboff 2015: 78).

However, she refrains from venturing into speculation about a shift away from capitalism altogether and towards a democratic planned economy—the Soviet-type planned economy was still subject to an information and democracy shortfall, but a new one might overcome this. Zuboff also plays down the defence intelligence connections of Google. Yet the company employs a special 'government affairs director', who meets on a regular basis with officials of the National Security Council and other branches of the US national security state. In parallel to the coming of

Surveillance Capitalism, in October 2014 a major Strategic Multi-Layer Assessment conference sponsored by the US Department of Defense and the Joint Chiefs of Staff was convened under the title, *A New Information Paradigm? From Genes to "Big Data" and Instagram to Persistent Surveillance… Implications for National Security* (Ahmed 2015).

Indeed as Nafeez Ahmed writes, the 'global surveillance apparatus and the classified tools used by agencies like the NSA to administer it' have been entirely produced by companies like Google, formally outside the structures of the US national security state and then were made available to it. The data Google collects from private WiFi networks identifying so-called 'geolocations' are supplied to the NSA. In fact the NSA, in the name of cyber security, has concluded such sharing agreements with 'hundreds of telecoms CEOs around the country' (Ahmed 2015).

DARPA director Regina Dugan, who was responsible for focusing a growing part of DARPA's work 'on the investigation of offensive capabilities to address military-specific needs' and was able to net half a billion dollars for DARPA cyber research in 2012, in that very year moved to Google (Ahmed 2015). On Dugan's watch DARPA also pioneered drone research; her move to Google was related to its interest in developing high-altitude drones with WiFi capabilities. She was also under investigation for awarding contracts to RedX, a bomb-detection corporation which she co-founded (Foster and McChesney 2014: 24). The nature of the Pentagon-Google connection transpires from e-mail correspondence between NSA chief Gen. Keith Alexander and Google's founding executive Sergey Brin in which the NSA head calls the company a 'key member of [the US military's] Defense Industrial Base' (cited in Ahmed 2015).

Big Data information gathering is important in light of the vast amount of intercepts. In mid 2012 the NSA was processing more than 20 billion communications events (Internet and telephone) a day worldwide (Greenwald 2014: 98). In one month, March 2013, one NSA department under the BOUNDLESS INFORMANT programme collected 3 billion telephone calls from the US. Across the world, 97 billion emails and 124 billion telephone calls were collected in the same period (500 million emails and calls from Germany, 2.3 billion from Brazil, 13.4 billion from India; and in association with their respective governments, 70 million from France, 1.8 million from the Netherlands, and so on (Greenwald 2014: 92-3).

In the case of the *Charlie Hebdo* attacks, all responses were geared to framing the incidents to the supposedly Muslim, terrorist attack on 'free speech' dear to Western civilization, and the simultaneous anti-Semitic outrage. All with a supporting narrative that the jihadists are somehow consumed by envy towards our 'freedoms' or a version of that theme. In combination this highlights the intrinsic relationship between two aspects of the aesthetic of the West's civilisational struggle against violent Islam, as originally argued already by Huntington in his 'Clash of Civilisations' argument in 1993/1998.

However, the ferocity behind the project of a global strategy of tension has a much longer history behind it. How the British defeated the Mau Mau in Kenya was mentioned but in 1965 the Indonesian generals who seized power with Anglo-US support launched a death squad and targeted assassination campaign on a vast scale, aimed at progressive movements or just neutral 'weak links'. CIA veteran Ralph McGehee has described the Indonesian operation as a 'model' for a similar campaign, Operation Phoenix in Vietnam, also noting how the CIA in Chile would forge a document purporting the existence of a plot to murder Chilean generals (cited in Pilger 2003: 39). In a conversation about Indonesia with the US ambassador, incoming president Nixon expressed interest in applying such methods in Southeast Asia and perhaps also in the Western Hemisphere. Citing this, Peter Dale Scott mentions the overthrow of Sihanouk in Cambodia in 1970, the 'Jakarta' scenario in Chile in 1973 and the US sponsorship of Central American death squads as examples of the further evolution of the Indonesian model (Scott 1985: 264).

The success of the anti-communist terror campaign in Indonesia then led the Americans to launch Phoenix (Phung Hoang in Vietnamese), a programme targeting the civilian infrastructure of the insurrection. Phoenix (it got this particular name only in 1967 and existed under different labels before) had its origins in the CIA's adoption of the Lansdale package of capture, interrogation and torture, and assassination, combined with psychological warfare using false flag operations and an admixture of local superstition. The basis for it was laid when OSS veteran and future CIA director William Colby arrived in Saigon as CIA deputy chief of station in 1959. Masquerading as anthropologists, CIA agents toured the country with Vietnamese

secret police and began to organise Vietnamese police units into quasi-military formations. Packaged as intended 'to protect the people from terrorism', Phoenix developed into the prototype of parafascist, counterrevolutionary violence of the entire subsequent era including the War on Terror (Valentine 2000). As journalist Bernard Fall would write in 1965, 'What we're really doing in Vietnam is killing the *cause* of "wars of liberation." It's a testing ground—like Germany in Spain. It's an example to Central America and other guerrilla prone areas' (cited in Valentine 2000: 89).

When Israel after the 1967 and 1973 wars persisted in holding on to the occupied territories, its confrontation with the Palestinians led the country's leadership to develop tactics along the lines tested out in Indonesia and Vietnam. Israel's Likud leadership had a background in the terror squads that attacked British targets in Palestine and also assassinated UN mediator Folke Bernadotte in 1948 (Cockburn 2015: 116). Their concept of a War on Terror, modelled how they handled their own Palestinian resistance, included targeted assassination of its leaders. When asked whether he was not burdened by the idea that the state claims the right to execute people at will, the retiring head of Israel's internal security service Shabak declared in 2005 that

> Foreign delegations come here on a weekly basis to learn from us, not just the Americans. It has become the sexiest trend in counterterrorism. Its effectiveness is amazing… the state of Israel had turned targeted preventions into an art form…. The leaders with experience will die and the others will be without experience and finally the "barrel of terror" … will be drained (cited in Cockburn 2015: 116-7, last sentence added from another Israeli intelligence spokesperson)

Based on its vast experience in terrorising the Palestinian population within its own 1948 state and in the Occupied Territories, Israel has developed expertise no ruling class can afford not to have in reserve for an emergency. Tel Aviv has diplomatic relations with 157 countries and almost all agreements and protocols contain military and security components (Halper 2015: 3). In combination with Total Information Awareness obtained by US-style mass surveillance, this turns existing capitalist society into an impenetrable fortress—as long as the economic engine continues to function.

The Drone War: Shortening the 'Kill Chain'

'The occupation of Iraq and Afghanistan have, since 2001, served as the catalyst for fusing aerospace, cyberspace, and biometrics into a robotic information regime of extraordinary power,' writes Alfred McCoy (2014: 79). The unmanned drone is the epitome of this power. It evolved as a cheap and effective means of short-circuiting surveillance and targeting. Whereas separate reconnaissance requires feedback loop to a command centre, a missile-armed drone can survey a target and attack it in one go, reducing what is called 'the kill chain' to almost zero (Cockburn 2015: 138).

Barack Obama, whose election in November 2008 was widely seen as a rejection of the Bush regime, in fact embraced the targeted assassination programme wholeheartedly, despite its cost in civilian human life. Already under Bush-Cheney, the Joint Special Operations Command (JSOC) had been judged to be out of control. It was operating in 134 countries or more and authorized to kill without a separate mandate (Cockburn 2015: 245). In December 2009, two weeks after Obama had received that year's Nobel Peace Prize, forty people, including fourteen women and twenty-one children, were killed by an American air attack on the remote village of al Majalah in Yemen, a spot identified by US intelligence as an 'al-Qaeda training centre'. Unexploded cluster bombs littering the place killed four more in the days that followed. In mid-2010, Yemeni reporter Abdulelah Shaye, who was pursuing the story, was arrested, apparently at the request of the US authorities. Convicted of 'terrorism-related activities' and condemned to a five years' prison term on concocted charges, Shaye's tribal leaders pressured president Saleh for a pardon in February 2011, but Obama personally intervened with his colleague in Sanaa (meanwhile killed) to rescind it (Scahill 2013: 305-6, 398-9; Baron 2013).

After the 2008 financial crash ushered in an era of deepening uncertainty and growing global instability, the West has moved to wall itself of against the pressure of large masses of people seeking a better life as their own societies are collapsing under the combined strains of social, political and ecological crisis. The global strategy of tension has very much run out of control after the NATO regime change in Libya and the assassination of its leader, Colonel Gaddafi, in 2011, which has removed a

repressive but stabilising factor on the other side of the Mediterranean and set on fire Sahel countries such as Mali.

After a decade of costly ground warfare in Afghanistan in Iraq (cost of the latter, $ 3 trillion), Obama in 2012 switched to reducing infantry and stepping up cyber infrastructure and special operations (McCoy 2014: 79). Drones, JSOC, and targeted assassination, all dependent on US surveillance capacities, were central to this. John Brennan, who became White House counter-terrrorism assistant to Obama (he had from 2005 headed a private corporation preparing terror watch list for the US government), shared the new president's ideas about targeted assassination, 'the need to target the metastasizing disease without destroying the surrounding tissue' (Brennan cited in Cockburn 2015: 214). In that capacity he was, in the words of Alexander Cockburn, the custodian of Obama's kill list. In 2012 Brennan would become CIA director, and in the meantime the agency had morphed into a killing machine. Drone strikes multiplied under Obama and it was now widely accepted that the CIA's 'principal occupation had become assassination' (Cockburn 2015: 219). Not 'destroying the surrounding tissue' had meanwhile turned into a bitter farce. In the case of the Afghan-Pakistan border area, where Obama's war of choice continued to be fought without tangible results other than destruction (Cockburn 2015: 227).

In November 2012 Obama signed an order to the Pentagon and other branches of government to start a programme of aggressive cyber operations across the world (Greenwald 2014: 81). One month later Glenn Greenwald was approached by Edward Snowden, who would expose it all. Yet in 2014 the JCOS commander, Lt. General Joseph Votel, stated, 'We want to be everywhere, know everything, and we want to predict what happens next' (cited in Cockburn 2015: 244). This is what Total Information Awareness is about, why mass surveillance is also being enacted in allied countries such as the Netherlands, and why targeted assassination ('predict what happens next') is part and parcel of the TIA strategy. 'Pacifying humanity', that is, controlling populations before they can rise in revolt 'spawns a manner of global rule shaped by an inherent commitment to war and constant preparedness for war' writes Jeff Halper, but avoiding that endeavour itself becomes a violent, never-ending, totalitarian project' (Halper 2015: 29; Paye 2014: 131).

In *1984*, Winston Smith could still enjoy a moment reading the Goldstein book, without being watched via a telescreen. But as Shoshana Zuboff writes, this model, or the one she discusses, Bentham's Panopticon (the all-seeing warden's eye at the

centre of the concentric prison corridors, which was apposite for the 1980s) is no longer valid. ‘Unlike the centralized power of mass society, there is no escape from Big Other. There is no place to be where the Other is not’ (Zuboff 2015: 82). Power is ensured by ‘a form of unilateral declaration that most closely resembles the social relations of a pre-modern absolutist authority’ and as such constitutes a mortal threat to democracy. This threat is backed up by a surveillance regime not just of capitalism in the economic sense, but as an integral machinery of deceit and violence managed by states. However, if ‘the empire can deploy Orwellian technologies of repression, its outcasts have the gods of chaos on their side’ (Davis 2017: 206). To break out of this infernal dilemma, fighting the technologies of repression such as surveillance and the other attributes of the Revolution in Military Affairs is as important as containing the chaos produced by an economic system degenerated into plunder.

References

Ahmed, Nafeez Mossadeq. 2005. *The War on Truth. 9/11, Disinformation, and the Anatomy of Terrorism*. Northampton, Mss.: Olive Branch Press.

Ahmed, Nafeez Mossadeq. 2015. **'**How the CIA made Google. Inside the secret network behind mass surveillance, endless war, and Skynet.' *Insurge Intelligence*, 22 January. https://medium.com/insurge-intelligence/how-the-cia-made-google-e836451a959e (last accessed 29 November 2017).

Baron, Adam. 2013. 'Yemenis call U.S. drone strikes an overreaction to al Qaida threat'. *McClatchy DC Bureau*, 9 August. http://www.mcclatchydc.com/news/nation-world/world/article24751933.html#.UgicCm1N5Ng#storylink=cpy (last accessed 4 January 2018).

Barrett, Kevin. J., ed. 2015. *We Are NOT Charlie Hebdo. Free Thinkers Question the French 9/11*. Lone Rock, Wisconsin: Sifting & Winnowing Books.

Bassosi, Duccio. 2006. *Il governo del dollaro. Interdipendenza economica e potere statunitense negli anni di Richard Nixon (1969-1973)*. Firenze: Edizioni Polistampa.

Battacharyee, Anannya, and Roy, Ashim. 'Bargaining in the global commodity chain: the Asian Floor Wage Alliance'. In Kees van der Pijl, ed. *Handbook of the International Political Economy of Production*. Cheltenham: Edward Elgar.

Boccara, Paul. 2008. *Transformations et crise du capitalisme mondialisé. Quelle alternative ?* Pantin: Le Temps des Cérises.

Biddle, Sam. 2017. 'How Peter Thiel's Palantir Helped the NSA Spy on the Whole World'. *The Intercept*, 22 February. https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/ (last accessed 14 August 2017).

Boren, David. 1990. 'Remarks by Senator David L. Boren', *National Press Club*, April 3 (mimeo of the transcript).

Briody, Dan. 2003. *The Iron Triangle. Inside the Secret World of the Carlyle Group* [forword C. Byron]. Hoboken, N.J.: John Wiley.

Bulard, Martine. 2015 'Pour amadouer Bruxelles. Loi Macron, le choix du "toujours moins"'. *Le Monde Diplomatique*, April, pp. 1, 4-5.

Burnham, James. 1960 [1941]. *The Managerial Revolution*. Bloomington, Ind.: Indiana University Press.

Carter, Ashton B.; Deutch, John and Zelikow, Philip. 1998. 'Catastrophic Terrorism. Tackling the New Danger'. *Foreign Affairs*, 77 (6)

Chan, Jenny; Pun Ngai, and Selden, Mark. 2015. 'Apple's iPad City: subcontracting exploitation to China.' In Kees van der Pijl, ed. *Handbook of the International Political Economy of Production*. Cheltenham: Edward Elgar.

Chesnais, François. 2011. *Les dettes illégitimes. Quand les banques font main basse sur les politiques publiques*. Paris : Raisons d'agir.

Cockburn, Andrew. 2015. *Kill Chain. The Rise of the High-Tech Assassins*. New York: Henry Holt & Co.

Colodny, Len and Gettlin, Robert . 1992. *Silent Coup. The Removal of a President*. New York: St. Martin's Press.

Crozier, Michel; Huntington, Samuel P., and Watanuki, Joji. 1975. *The Crisis of Democracy. Report on the Governability of Democracies to the Trilateral Commission*. New York: New York University Press.

Davis, Mike. 2017 [2006]. *Planet of Slums*. London: Verso.

Delgado Wise, Raúl, and Martin, David T. 2015. 'The political economy of global labour arbitrage'. In K. van der Pijl (Ed.), *Handbook of the International Political Economy of Production*. Cheltenham: Edward Elgar.

DPG 1992: *Defence Planning Guidance, FY 1994-1999* (16 April 1992, declassified 2008). Original photocopy.

Dzarasov, Ruslan. 2014. *The Conundrum of Russian Capitalism. The Post-Soviet Economy in the World System*. London: Pluto.

Edwards, Beatrice. 2014. 'The Zombie Bill. The Corporate Security Campaign That Would Not Die'. *Monthly Review*, 66 (3) 54-69.

Elbe, Stefan. 2009. *Virus Alert. Security, Governmentality, and the AIDS Pandemic*. New York: Columbia University Press.

Engelhardt, Tom. 2014. *Shadow Government. Surveillance, Secret Wars and a Global Security State in a Single-Superpower World* [foreword G. Greenwald]. Chicago: Haymarket.

Foster, John B., and McChesney, Robert W. 2014. 'Monopoly-Finance Capital, the Military-Industrial Complex, & the Digital Age'. *Monthly Review*, 66 (3) 1-31.

Fyvel, T.R. 1982. *George Orwell, a personal memoir*. London: Weidenfeld & Nicolson.

Ganser, Daniele. 2005. *NATO's Secret Armies. Operation Gladio and Terrorism in Western Europe*. London: Frank Cass.

Greenwald, Glenn. 2014. *No Place to Hide. Edward Snowden, the NSA and the Surveillance State*. London: Hamish Hamilton.

Greenwald, Glenn. 2017. 'Facebook Says It Is Deleting Accounts at the Direction of the U.S. and Israeli Governments'. *The Intercept*, 30 December. https://theintercept.com/2017/12/30/facebook-says-it-is-deleting-accounts-at-the-direction-of-the-u-s-and-israeli-governments/ (last accessed 8 January 2018).

Grey, Barry. 2007. 'A political bombshell from Zbigniew Brzezinski. Ex-national security adviser warns that Bush is seeking a pretext to attack Iran' (2 February. 2007) www.wsws.org/articles/2007/feb2007/brze-f02.shtml (accessed 18 November 2011).

Griffin, David Ray. 2011. *9/11 Ten Years Later. When State Crimes Against Democracy Succeed*. London: Haus.

Halper, Jeff. 2015. *War Against the People. Israel, the Palestinians and Global Pacification*. London: Pluto.

Harvey, David. 2006 [1982]. *The Limits to Capital*, rev. ed. London: Verso.

Herman, Edward S. and Chomsky, Noam. 1994 [1988]. *Manufacturing Consent. The Political Economy of the Mass Media*. London: Vintage Books.

Hersh, Seymour M. 2005. 'The Coming Wars. What the Pentagon can now do in secret'. *The New Yorker*, 24 January. https://www.newyorker.com/magazine/2005/01/24/the-coming-wars (last accessed 8 January 2018)

Holbrooke, Richard. 1995. 'America, A European Power', Foreign Affairs, 74 (2) 38-51.

Huntington, Samuel P. 1998. *The Clash of Civilizations and the Remaking of World Order*. London: Touchstone.

Jaffe, Greg. 2011. 'A decade after the 9/11 attacks, Americans live in an era of endless war', *The Washington Post*, 4 September.

Jenkins, Dominick. 2002. *The Final Frontier. America, Science, and Terror*. London: Verso.

Junne, Gerd. 1985. 'Das amerikanische Rüstungsprogramm: Ein Substitut für Industriepolitik'. *Leviathan. Zeitschrift für Sozialwissenschaft*, 13 (1) 23-37.

Kissinger, Henry A. 2000 [1982]. *Years of Upheaval*. London: Phoenix Press.

Landau, Saul. 1983. *Nieuw Rechts in Amerika* [trans. C. van Splunteren]. Amsterdam: Van Gennep.

Lasswell, Harold D. 1941. 'The Garrison State'. *American Journal of Sociology*, 46 (4) 455-468.

Lipschutz, Ronnie D. 1999. 'Terror in the Suites: Narratives of Fear and the Global Political Economy of Danger'. *Global Society*, 13 (4) 411-439.

Magee, John, ed. 2014. 'Surveillance Capitalism'. Special Issue, *Monthly Review*, 66 (3)

Mann, James. 2004. *Rise of the Vulcans. The History of Bush's War Cabinet*. New York: Penguin.

Mayer, Jane. 2016. *Dark Money. The Hidden History of the Billionaires Behind the Rise of the Radical Right*. New York: Doubleday.

Mazzucato, Mariana. 2014. *The Entrepreneurial State. Debunking Public vs. Private Sector Myths*. London: Anthem Press.

McCoy, Alfred W. 2014. 'Surveillance and Scandal. Weapons in an Emerging Array for U.S. Global Power'. *Monthly Review*, 66 (3) 70-81.

Mearsheimer, John J., and Walt, Stephen M. 2007. *The Israel Lobby and U.S. Foreign Policy*. New York: Farrar, Straus and Giroux.

Merk, Jeroen. 2009. 'Jumping Scale and Bridging Space in the Era of Corporate Responsibility: cross-border labour struggles in the global garment industry'. *Third World Quarterly*, 30 (3) 599-615.

Merk, Jeroen. 2015. 'Global outsourcing and socialization of labour: the case of Nike'. In K. van der Pijl, ed., *Handbook of the International Political Economy of Production*. Cheltenham: Edward Elgar.

Morgenthau Hans J. 1962 [1940-1960]. *The Decline of Democratic Politics* [vol. I of *Politics in the Twentieth Century*, 3 vols.]. Chicago: University of Chicago Press.

Netanyahu, Benjamin, ed. 1986. *Terrorism. How the West Can Win*. London: Weidenfeld & Nicolson.

Nitzan, Jonathan and Bichler, Shimshon. 2002. *The Global Political Economy of Israel*. London: Pluto Press.

Observer, The. 2017. 'Robert Mercer: the big data billionaire waging war on mainstream media'. 26 February. https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage (last accessed 14 August 2017).

Orwell, George. 1954 [1949]. *Nineteen Eighty-Four. A Novel*. Harmondsworth: Penguin.

Paye, Jean-Claude. 2014. 'Merging the Law of War with Criminal Law. France and the United States'. *Monthly Review*, 66 (3) 128-135.

Pilger, John. 2003 [2002]. *The New Rulers of the World*, rev. ed.. London: Verso.

Price, David H. 2014. 'The New Surveillance Normal. NSA and Corporate Surveillance in the Age of Global Capitalism'. *Monthly Review*, 66 (3) 43-53.

Purkayashta, Prabir, and Bailey, Rishab. 2014. 'U.S. Control of the Internet. Problems Facing the Movement to International Governance'. *Monthly Review*, 66 (3) 103-127.

Ralph, Diana. 2008 [2006]. 'Islamophobia and the "War on Terror": The Continuing Pretext for U.S. Imperial Conquest', in Paul Zarembka, ed. *The Hidden History of 9-11*, 2nd ed. New York: Seven Stories Press.

Rasmus, Jack. 2016. *Systemic Fragility in the Global Economy*. Atlanta, Georgia: Clarity Press.

Regan, Lauren. 2014. 'Electronic Communication Surveillance'. *Monthly Review*, 66 (3) 32-42.

Richelson, Jeffrey T. and Ball, Desmond. 1990 [1985]. *The Ties That Bind. Intelligence Cooperation between the UKUSA Countries—The United Kingdom, the United States of America, Canada, Australia and New Zealand*, 2nd ed. Boston: Unwin Hyman.

Sacks, Bryan. 2008 [2006]. 'Making History: The Compromised 9-11 Commission', Paul Zarembka, ed. *The Hidden History of 9-11*, 2nd ed. New York: Seven Stories Press.

Sanguinetti, Gianfranco. 1982 [1979]. *Over het terrorisme en de staat* [trans. from the French]. Bussum: Wereldvenster.

Sarotte, Marie Elise. 2014. 'A Broken Promise? What the West Really Told Moscow About NATO Expansion'. *Foreign Affairs*, 93 (5) 90-97.

Scahill, Jeremy. 2013. *Dirty Wars. The World is a Battlefield*. London: Serpent's Tail.

Scheer, Robert. 1982. *With Enough Shovels. Reagan, Bush, and Nuclear War*. New York: Random House.

Schmitt, Carl. 1989 [1940]. 'Zum 30. Juni 1934' in Léon Poliakov and Joseph Wulf, eds.. *Das Dritte Reich und seine Denker* [1959]. Wiesbaden: Fourier.

Schmitt, Carl. 2005 [1934, 1922]. *Political Theology. Four Chapters on the Concept of Sovereignty*, 2nd ed. [trans. and intro G. Schwab, foreword T.B. Strong]. Chicago: University of Chicago Press.

Schweizer, Peter. 1993. *Friendly Spies. How America's Allies are Using Economic Espionage to Steal our Secrets*. New York: Atlantic Monthly Press.

Scott, Peter Dale. 1985. 'The United States and the Overthrow of Sukarno, 1965-1967'. *Pacific Affairs*, 58 (2) 239-264.

Scott, Peter Dale. 1996 [1993]. *Deep Politics and the Death of JFK* [with a new preface]. Berkeley, Cal.: University of California Press.

Scott, Peter Dale. 2007. *The Road to 9/11. Wealth, Empire, and the Future of America*. Berkeley, Cal.: University of California Press.

Scott, Peter Dale. 2010. *American War Machine. Deep Politics, the CIA Global Drug Connection, and the Road to Afghanistan*. Lanham, Maryland: Rowman & Littlefield.

Scott, Peter Dale. 2015. *The American Deep State. Wall Street, Big Oil, and the Attack on U.S. Democracy*. Lanham, Maryland: Rowman & Littlefield.

Serfati, Claude. 2017. *Le militaire. Une histoire française*. Paris: Éditions Amsterdam.

Shaw, Martin. 2005. *The New Western Way of War. Risk-Transfer War and its Crisis in Iraq*. Cambridge: Polity.

Soederberg, Susanne. 2014. *Debtfare states and the poverty industry. Money, discipline and the surplus population*. London: Routledge.

Streeck, Wolfgang. 2013. *Gekaufte Zeit. Die vertagte Krise des demokratischen Kapitalismus* [Frankfurter Adorno-Vorlesungen 2012]. Frankfurt: Suhrkamp.

Tarpley, Webster G. , 2008 [2005]. *9/11. Synthetic Terror Made in USA*, 4th ed. Joshua Tree, Cal.: Progressive Press

Taylor, Marcus, and Rioux, Sébastien. 2018. *Global Labour Studies*. Cambridge: Polity Press.

Tunander, Ola. 2009. 'Democratic State vs. Deep State. Approaching the Dual State of the West,' in Eric Wilson, ed. *Government of the Shadows. Parapolitics and Criminal Sovereignty*. London: Pluto Press.

Tveten, Julianne. 2018. 'Hoe de angst for "Fake Nieuws" links marginaliseert' [trans. T. Reininga]. *Vredesmagazine*, 11 (1) 22-23.

Valentine, Douglas. 2000 [1990]. *The Phoenix Program*. New York: William Morrow & Co [Authors Guild Backinprint.com Ed.].

Van Creveld, Martin. 1991. *The Transformation of War*. New York: The Free Press.

Van der Pijl, Kees. 2006. *Global Rivalries from the Cold War to Iraq*. London: Pluto; New Delhi: Sage Vistaar.

Varoufakis, Yanis. 2013 [2011]. The Global Minotaur. America, Europe and the Future of the Global Economy [rev. ed]. London: Zed Books.

Vieille, Paul. 1988. 'The World's Chaos and the New Paradigms of the Social Movement' in Lelio Basso Foundation, eds. *Theory and Practice of Liberation at the End of the Twentieth Century*. Brussels: Bruylant.

Willan, Philip. 1991. *Puppet Masters. The Political Use of Terrorism in Italy*. London: Constable.

Wisnewski, Gerhard. 2015. *Die Wahrheit über das Attentat auf Charlie Hebdo. Gründungsakt eines totalitären Europa*. Rottenburg: Kopp.

Woodward, Susan L. 1995. *Balkan Tragedy. Chaos and Dissolution After the Cold War*. Washington, D.C.: The Brookings Institution.

Wright, Steve. 1998. *An Appraisal of Technologies of Political Control.* [working document, consultation version]. Luxemburg: European Parliament., Directorate General for Research.

Zelikow, Philip D. ed., 2001. *American Military Strategy. Memos to a President*. New York: W.W. Norton.

Zuboff, Shoshana. 2015. 'Big other: surveillance capitalism and the prospects of an information civilization'. *Journal of Information Technology*, 30, 75–89.