10.6094/behemoth.2015.8.2.867

BEHEMOTH A Journal on Civilisation
2015 Volume 8 Issue No. 2

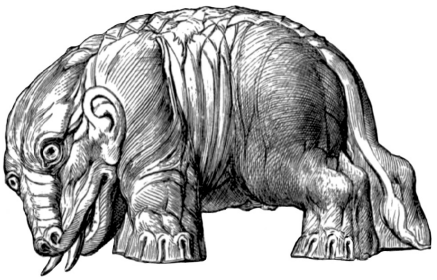
Mass Surveillance, Drones, and Unconventional Warfare

Armin Krishnan

Abstract:

The article argues that armed drones are weapons made for unconventional warfare and have little value for conventional interstate conflict. The rise of armed drones to prominence has to be considered as an indicator for the changed nature of contemporary armed conflict that has now become focused on countering terrorism, insurgencies, transnational organized crime and fighting 'hybrid wars' globally. The US military is preparing for both global counterinsurgency and for civil unrest at home as they are creating a global surveillance architecture reaching from outer space to cyber space, where everything and everybody can be continuously identified, tracked and located. Unmanned systems assist in global surveillance and provide the global reach for intervening in internal conflicts without the need of deploying large ground forces. The new technological capabilities, including drones, biometrics and cyber warfare, are very useful for global manhunts in the context of the ongoing war on terror and for the control of large populations from afar. Western governments are also increasingly concerned about the spread of extremist ideologies and the possibility of mass civil unrest, which means that many of the lessons learned in the counterinsurgency campaigns in Afghanistan and Iraq could be applied within the West.

Keywords: drones, space war, manhunts, mass surveillance, counterinsurgency



Armin Krishnan is Assistant Professor for Security Studies at East Carolina University. His research interests focus on military technology, future warfare and military ethics. **E-mail: KrishnanA@Ecu.Edu**

Drones are a very misunderstood weapon in terms of their role and significance in contemporary warfare. Often drones are praised for their ability to discriminate targets (Strawser 2010, 351f.). Sometimes they are portrayed as 'killer robots' that might indiscriminately target people and that could be weapons "so cruel as to be beyond the pale of human tolerance." (Wardrop 2009) Although it seems absurd to either characterize a weapon as inherently humane or inherently inhumane since it always depends on how exactly the weapon is used, it is true that certain types of weapons have greater suitability for particular uses than for others. It is argued here that drones are most suitable for security applications (surveillance) and for unconventional warfare (targeted killings). Furthermore, it is claimed that there is in terms of technology very little that would make unmanned aircraft a revolutionary or a transformative technology. The first drones flew before the Wright brothers and almost entered mass production during World War I (as the 'Kettering bugs') if the war had not ended sooner. There is nothing new about the concept of the unmanned aircraft or even about arming it with explosives and turning it into a projectile (or now a projectile platform – a minor alteration of the basic idea).

It is thus not unmanned systems such as drones that are transforming war, but rather it is the transformed nature of war that makes unmanned systems technology in conjunction with advanced surveillance technology, satellites for command and control and precision ammunitions so relevant today. Modern armed drones can be integrated into a global military network. It is the overall package of technologies that provides an entirely new capability, which is extremely useful for the kind of wars that the US military expects to fight in the future. According to a study by the US Army's Strategic Studies Institute, "[t]he most compelling future defense-relevant shocks are likely to be unconventional." (Freier 2008, 14) Unconventional warfare has become the focus of contemporary military thinking, both in terms of counterinsurgency (suppressing insurgencies), as well as in providing assistance to irregular proxy forces (hybrid warfare). It is projected that political instability could increase globally as a result of a combination of "contagious un- and under-governance; civil violence; the swift catastrophic onset of consequential natural, environmental, and/or human disaster; a rapidly expanding and uncontrolled transregional epidemic; and the sudden crippling instability or collapse of a large and important state." (Freier 2008, 17)

This means that the new American military approach that has taken shape since 9/11 is to intervene in a large number of internal conflicts to counteract local instability affecting larger regions and to prevent any consolidated bloc of global resistance from forming that could potentially threaten US hegemony in the long term. The US military already has a presence in 134 nations where mostly small teams of Special Operations Forces train local militaries, provide security assistance, and conduct special operations such as long-range reconnaissance or 'kill or capture' missions (Turse 2014). The drones are part of the overall mix of special warfare, cyber warfare, and political warfare that now defines the new American way of

war (Turse 2012). The ongoing 'global war on terror' is therefore not merely a global counterterrorism campaign aimed at disrupting a few terrorist groups operating in loose collaboration, but has to be understood as a long and potentially open-ended global counterinsurgency campaign that has to constantly suppress diverse political movements and ideologies that are opposed to the American vision of a future more integrated world order or 'pax Americana', as is outlined in David Kilcullen's article 'Countering Global Insurgency' (Kilcullen 2007).

This article will describe the emerging military information architecture for the global surveillance of populations in the context of unconventional warfare with a particular focus on unmanned systems technology. It is argued that the ultimate goal of global surveillance is the suppression of resistance to globalization and "total population control" (as NSA whistleblower William Binney phrased it).

The 'Triple Canopy'

The Pentagon has long considered outer space to be the 'ultimate high ground' from which earth can be dominated. The military importance of outer space is grounded less in the possibility of basing weapons there, but rather in its role in global surveillance and global command and control that is deemed critical to the overall goal of 'full spectrum dominance' in future military conflicts on planet earth. Historian Alfred McCoy published an influential article in 2012 where he gives his own interpretation of the US Air Force's plans for future 'space wars':

> "It's 2025 and an American 'triple canopy' of advanced surveillance and armed drones fills the heavens from the lower- to the exo-atmosphere. A wonder of the modern age, it can deliver its weaponry anywhere on the planet with staggering speed, knock out an enemy's satellite communications system, or follow individuals biometrically for great distances. Along with the country's advanced cyberwar capacity, it's also the most sophisticated militarized information system ever created and an insurance policy for U.S. global dominion deep into the twenty-first century. It's the future as the Pentagon imagines it; it's under development; and Americans know nothing about it." (McCoy 2012)

What is emerging is a global "robotic information regime" that is potentially capable of monitoring and tracking everything of military significance on earth. At the moment, many of the technologies for global surveillance are still under development and not yet operational, but might be available within a decade or so. As indicated by McCoy, it is going to be a vertically layered system that has most of its command and control elements in space, its key surveillance elements in the upper stratosphere and most of its 'kinetic' capabilities in the lower atmosphere.

Near Earth Space

Earth observation satellites have become the backbone of global military communications, navigation and targeting (GPS), and intelligence, reconnaissance and surveillance (ISR) capabilities. The most advanced militaries cannot operate globally without spaceborne communications and navigation systems necessary for effective command and control. Earth observation satellites provide important ISR capabilities since they can, with limitations due to their orbits and sensors, remotely monitor activities and also to some extent track vehicles, objects, or devices anywhere on the earth's surface.

Satellites are important enablers for military operations in all other domains of warfare: land, sea, air and cyber. This means that outer space has already become the center of gravity for earth wars and this will be even more so in the future. As a result, space assets may be interfered with through a variety of methods such as jamming, hacking, nuclear EMP, high energy radio frequency weapons, kinetic attack from the earth, as well as the use of dazzling lasers that can blind earth observation satellites (Moore 2008, 47-55). Wars in space thus become a probable scenario and this makes it imperative for the US military to control space through space surveillance, protection of space assets and space negation, including the denial of access to and use of space by hostile powers (US Air Force 1997). The ultimate goal is to dominate earth from space, to protect global commerce of the wealthy states and keep "those 'have-nots' in line" (Grossman 2001, 13).

Stratosphere

Key elements of the emerging global surveillance architecture will be likely located in the upper stratosphere (30 km above the surface), which is already out of the range of all but the most advanced air defense systems. These altitudes are feasible for airships, aerostats and balloons that do not have air-breathing engines. The idea is that airships and aerostats could be not only cheap substitutes for satellites, but would be also in some ways better than satellites since they are not subject to orbital mechanics. They could be easily moved into a target area and hover over it for an extended period of time, which is impossible for a satellite (except in a geosynchronous orbit 36,000 km away from earth). The US Army has already deployed tethered aerostats in Afghanistan, Iraq, and Kosovo as cheap surveillance platforms that can monitor activities on the ground from an altitude of 300 m. Future aerostats and airships could operate at much greater altitudes and thus provide much greater coverage than current systems. On the drawing board is a high-altitude airship that could operate at the edge of space and that could provide persistent surveillance capabilities. A report to Congress from 2006 suggested: "[t]his altitude might enable a small number of airships to surveill the entire United States. The HAA [high altitude airship] program seeks to demonstrate a prototype by 2010 that could fly for 30 days at a time." (Bolkcom 2006, 3) The HAA has since run into trouble as some tests

were unsuccessful and funding has been cut (Matthews 2012).

In addition to developing high-altitude surveillance platforms, the US military also intends to use the stratosphere for a global strike capability. The concept is called *Prompt Global Strike* (PGS) and is currently based on hypersonic cruise vehicle technology, which would make it possible to attack any target worldwide within a few hours (Moore 2008, 87-89). The main rationale of PGS is to engage fleeting targets at the outset of a conflict without the need of having forward deployed forces. The unclassified program associated with PGS is the *X-51 Waverider* hypersonic cruise missile that can reach a maximum speed of Mach 5 and is expected to be ready for deployment in 2020.

Troposphere and Below

The kinetic elements of the "robotic information regime" will be located in the troposphere and below. There will be a mixture of manned and unmanned systems that the US Air Force expects to use in the coming decades. Drones are more suitable for global missions since they are not limited by 'human factors': they can operate for extended periods of time (currently up to 40 hours) and they are expendable. The US Air Force divides its drones into three tiers based on the altitude they operate in (low, medium, high) and a fourth tier for stealth (Fowler 2014, 116). The most sophisticated drone currently operated by the US Air Force is the *Global Hawk*, which has a ceiling of 15 km to 20 km and a range of up to 22,000 km.

The US Air Force has currently a fleet of 32 *Global Hawks* and the US Navy is planning to buy 68 of a special version of the *Global Hawk*. The unarmed drones can do wide area surveillance and can locate targets within 20 meters of probable error (Clark 2011, 68). The *Global Hawks* contribute largely to the global war on terror thanks to their great range and endurance. However, the *Reaper* drones are the current backbone of America's ability to hunt and kill terrorists worldwide. These drones have a range of about 5,000 km, which means that they need to operate out of forward bases, although the pilots and sensor operators can be located anywhere in the world.

Smaller drones that make up the vast majority of the US military drone fleet (only about 400 of the 11,000 US military drones are large) are used for tactical purposes as they typically have little endurance and only a short range. Bird or insect-size drones could be either used in swarms for conducting surveillance in an urban environment or for assassination missions (Bumiller/Shanker 2011). US Special Operations Forces have been equipped with Aeronvironment *Switchblade* assassination drones that can fly 10 km and kill a single person by exploding next to it since 2012.

The main advantage of drones compared to manned aircraft and other methods of ground attack is really their ability to apply limited amounts of force with great precision in situations where the airspace is not contested and the enemy is relatively unsophisticated. This has to do with the slow speed of drones, their high-resolution optical sensors, the involvement of

numerous imagery analysts in the targeting process and the requirement that a higher authority has to approve strikes based on video feeds and other intelligence, which is very different from the use of manned combat aircraft. When a manned jet fighter is used, it is the pilot, who has to make targeting decisions with lesser possibilities for accurate discrimination (Fowler 2014, 110). In other words, armed drones are made for a different type of war than conventional high-intensity conflict.

A New Type of War

The global war on terror that began in 2001 represents a new type of war since it is directed against non-state actors, since it has no geographic limitations and since it emphasizes 'manhunting' as its main tactics. In September 2001 the George W. Bush administration made the decision to hunt down members of al Qaeda wherever they happened to be (Gregory 2011, 240). The early 2000s were a time of a massive expansion of the CIA's extraordinary rendition program, which was based on the idea of capturing suspected terrorists worldwide and transferring them to black sites in third countries, where they could be interrogated to obtain intelligence on al Qaeda and associated groups, which would subsequently generate more targets for manhunting. At the minimum 136 individuals were 'rendered' or disappeared in secret prisons located outside of the US between 2001 and 2005 (Open Society 2013, 30). When the program was publicly revealed in 2005 it became a major international embarrassment to the George W. Bush administration. The rendition program was eventually shut down by President Obama after it had become abundantly clear that extraordinary rendition created a legal nightmare as suspects whose rights had been violated could neither be turned over to the court system nor simply be killed (Mayer 2005). Although the tactics have since somewhat changed, the overall approach of using manhunting as a method of war has not. In fact, the practice of manhunting was much refined during the occupations of Afghanistan and Iraq.

Manhunting in Unconventional Warfare

The main problem in counterterrorism and counterinsurgency operations is to know who the enemy is and to find enemy combatants so that they can be turned, captured or killed. Typically the enemy hides within a population and only attacks when they have an advantage, using hit-and-run tactics. It is extremely difficult for conventional forces to fight such an enemy since it is impossible to secure all conceivable targets that might be attacked. Even in situations where the enemy exposes itself in an attack the military is very much constrained by the amount of force that it can use because of the presence of innocent civilians on the battlefield. This is not merely a legal constraint, but also a strategic constraint. If the use of force is excessive and results in a lot of collateral damage, it will turn the population against counterterrorist and counterinsurgent forces. This means that in

counterterrorism and counterinsurgency campaigns force has to be applied with the greatest possible precision and with careful consideration given to the public perception of the use of force. This is where surveillance technologies and drones come into play.

Unconventional warfare, which has become the focus of the US military since operations in Afghanistan and Iraq, takes place within what the US Army calls the 'human domain'. The human domain deals with all human factors such as leadership, organization, motivation and the 'human terrain', in which the military operates. So it becomes necessary to collect massive amounts of information on populations to map social networks and to understand social organization. This ultimately assists in identifying who is likely to help the counterinsurgents, who is neutral and who is part of the opposition. Unconventional warfare in essence means sorting out who is who, compiling 'kill or capture' lists and trying to deny insurgents support by using psychological operations against populations designed to both intimidate or deter and win support (this is called 'pacification').

Counterinsurgency doctrines can be thus either enemy-centric (focused on the elimination of insurgents) or population-centric (focused on the security of the population). In reality, counterinsurgents always have to do both and it is only a matter of style or circumstances what is emphasized more. Oliver Belcher has made the argument that already in the Vietnam era the US military integrated social science and behavioral science methodologies in its counterinsurgency campaign as part of a population-centric approach. For example, he discovered that statistical methods for predicting insurgent activity were developed in the Civil Operations and Revolutionary Development Support (CORDS) program (Belcher 2012, 261). A component of CORDS was also the infamous enemy-centric Phoenix program, which was a computerized system for managing intelligence on the Vietcong Infrastructure (VCI) to systematically kill or capture individuals believed to be VCI.

As in Vietnam, counterinsurgency in Afghanistan and Iraq thus consisted mainly of hunting down insurgents in night raids by Special Forces and sometimes killing them with drones. These intelligence-driven special operations relied on a combination of human intelligence gained from local agents and the interrogation of prisoners, signals intelligence and overhead imagery intelligence to identify and hunt down opposition forces. The difference to the Vietnam era is the new ability of integrating vast amounts of diverse data from many different sources into one overall operational picture and to rapidly generate missions based on the data and its computerized analysis. An advisor to General Petraeus, John Nagl, commented about the new manhunting capabilities developed in the context of the two campaigns:

> "We're getting so good at various electronic means of identifying, tracking, locating members of the insurgency that we're able to employ this extraordinary machine, an almost industrial-scale counterterrorism killing machine that has been able to pick out and take off the battlefield not just

> the top level al Qaeda-level insurgents, but also increasingly is being used to target mid-level insurgents." (Grey/Edge 2011)

The Role of SIGINT

Typically the targeting is based on information from human agents on the ground and on the collection and analysis of communications, which can work in conjunction. For example, CIA informants are rumored to have placed drone-targeting chips on suspected militants in Pakistan (Stanford Law School; New York University 2012, 38). But HUMINT has lots of pitfalls such as the unreliability of local agents and it is often not sufficiently available in the more remote parts of the world. This means that US intelligence usually has to rely on SIGINT for globally locating individuals. According to journalist Shane Harris, the NSA's ability to exploit SIGINT and to wage offensive cyber warfare played a key role in turning around the war in Iraq during the 2007 surge. He wrote "hacking into the communications network of the senior al-Qaeda leaders in Iraq helped break the terrorist group's hold on the neighborhoods around Baghdad. By one account, it aided US troops in capturing or killing at least ten of those senior leaders from the battlefield." (Harris 2014, 22)

The new NSA cyber capabilities have been also critical in the drone war in Pakistan that expanded in 2009. Important in this respect is the NSA's metadata collection program *Boundless Informant*, which was acknowledged by former NSA and CIA director Michael Hayden, who famously remarked: "We kill people based on metadata." (Cole 2014) The NSA even created a special targeting unit called Counter-terrorism Mission Aligned Cell (CT MAC) specifically tasked with finding and tracking terrorists (Miller; Tate; Gellman 2013). Cell phones and tracking chips are typically used for geolocating targets and for achieving greater precision of drone strikes. Jeremy Scahill and Glenn Greenwald, who publish the Snowden documents on The Intercept website, stated: "In one tactic, the NSA 'geolocates' the SIM card or handset of a suspected terrorist's mobile phone, enabling the CIA and U.S. military to conduct night raids and drone strikes to kill or capture the individual in possession of the device." (Scahill; Greenwald 2014)

Of course, the NSA tracking does not stop with just geolocating SIM cards, but also includes even more sophisticated ways of figuring out where a known terrorist may be located. NSA expert James Bamford recently wrote "that a NSA program known as TREASUREMAP is being developed to continuously map every Internet connection — cellphones, laptops, tablets — of everyone on the planet, including Americans." (Bamford 2015) This means that any wireless device can be tracked and everyone using the device could be located at least approximately anywhere in the world using NSA's SIGINT satellites and cyber capabilities.

'Patterns of Life' Analysis

If other intelligence is not available, drone operators might rely on the persistent monitoring of a target area or of individuals on the ground to detect hostile activities. This so-called 'patterns of life' analysis can combine ground-based intelligence with data gathered from the air to individually identify persons, who are or may be engaged in hostile activity (Pincus 2009). Former drone pilot Matt Martin has explained the practice in his book. Describing one incident when he served as drone pilot in Iraq: "I noticed several men acting suspiciously in the parking lot of a greasy spoon café across the street…the men began loading boxes into the trunk of a faded-red compact car…The driver…looked all around…I decided to follow the car when it pulled into the city traffic." (Martin/Sasser 2010, 81-82) It turned out that the men were indeed insurgents transporting ammunition after Martin had directed ground forces to the vehicle, who searched it. If the potential target had been located within a 'kill box', where the use of force is authorized and further analysis showed that the target 'acts' like a terrorist or militant, then the drone pilot could have decided to attack the target.

This practice of attacking individuals whose identities are not known based on patterns of life analysis has been called 'signature strike', which have been authorized by President Obama for Pakistan's tribal areas and for Yemen. An inherent problem is that there is little public information with respect to what kind of 'signatures' or observed behaviors allow initiating an attack, which raises suspicions about vague criteria inviting wrongful use of force (Stanford Law School/New York University 2012, 12-13). There are also fairly simple countermeasures that terrorists and insurgents can use for avoiding detection from drones, which were outlined in an al Qaeda paper discovered in Timbuktu in 2011. The paper suggested using a Russian 'sky grabber' to intercept drone footage, electromagnetic jamming of drone control signals, maintaining silence of wireless contacts, exploiting natural vegetation and most bizarrely, employing snipers for shooting down drones (AP 2011).

However, the idea of a human pilot observing a scene, then coming to conclusions about potentially hostile activities that are observed, as described by Martin, is already becoming outdated. The US Air Force has recently deployed in Afghanistan a very powerful video capture system called Gorgon Stare. It is designed for wide-area surveillance and can cover over 100 km2 with 368 cameras that take high-resolution images at the rate of 12 images per second (Trimble 2014). The system can generate from the data a 1.8 billion pixel composite image that enables analysts with the help of advanced imaging processing software to detect and track all moving objects in the area of view. The system can also store the massive amounts of imagery that it generates for 30 days for later forensic analysis. In other words, a few drones with *Gorgon Stares* could surveil entire populations across large territories.

Biometrics

The US military has introduced biometrics as a means for identifying friend and foe in their counterinsurgency campaign in Afghanistan and used it also extensively in Iraq, which is a real novelty compared to the Vietnam War. The goal is 'identity dominance'. A US Army Handbook on the use of biometrics explains:

> "Biometrics capabilities on the tactical battlefield enable a wide variety of defensive and offensive operations. Biometrics help ensure enemy personnel, criminals, and other undesirable elements are not allowed access to our facilities, hired to provide services, or awarded contracts. Biometrics is used to vet members of the Afghan government and military with whom our forces interact…Biometrics is a critical COIN nonlethal weapons system." (US Army 2011, 1-3)

In other words, the US military now routinely collects biometrics from populations where it conducts counterinsurgency operations to control access to secure areas and to find the 'bad guys' or to identify them after they have been captured or killed. For this purpose the US military collected the biometrics of 3 million Iraqis, as well as of millions of Afghans using handheld devices (Ackerman 2011). The systematically collected biometrics data includes fingerprints, retinal scans, facial recognition, DNA and more exotic types of biometrics that can uniquely and reliably identify a particular individual (e.g. 'earprints'). Ideally one could collect the biometrics of an entire population, which in combination with other data that is indicative of an individual being a 'bad guy', would make it possible to more easily find these individuals, or at least severely restrict their movements by having people pass through checkpoints and borders with biometric ID systems.

The technology of biometrical identification has become already very advanced. It is no longer critical that an individual cooperates in the collection and use of biometrics since some of it can be done discretely and from distance. Very promising in this respect is facial recognition technology, which has been already tested in London back in 2002 and which could soon be used nationwide in the US. The Russian government has already deployed a facial recognition system across Moscow that can scan 10 million images in less than seven seconds. The developer stated "the face on the photograph is measured using 30 identifiers, and the resulting mathematical matrix is very difficult to fool." (Soldatov/Borogan 2015, 177)

A watchlisted individual whose facial geometry data is available in a database could walk past a surveillance camera and the security forces would be immediately alerted. Such a system has been described by urban warfare researcher Stephen Graham: "DARPA (2003) is developing systems of micro-cameras and sensors that can be scattered discretely across built urban landscapes and that automatically scan millions of vehicles and human faces for 'known targets' and record any event deemed to be 'unusual'." (Graham 2006, 269) The Department of Homeland Security is funding the Biometric Optical Surveillance System (BOSS), which aims to identify people using facial recognition with 80 to 90 percent accuracy at

a distance of 100 m (Savage 2013). In principle, such a future biometric identification system might be placed on drones, high-altitude airships, or even on satellites and could be used for systematically tracking individuals globally.

At the moment, it is still technologically challenging to put biometric sensors on mobile platforms that are remote, moving, and shaky, which affects sensor performance. However, a system that combines various kinds of data from different sensors with different methods of biometric identification could then probabilistically determine whether the individual captured by a drone camera or satellite is potentially a 'bad guy' on a target list (Shachtman 2011). Some of the new methods might include 'human thermal fingerprints' (unique human body heat signatures), 'gait intelligence' (unique walking styles), or maybe remote measurement of individually unique brainwave patterns.

The War Comes Home

In the War on Terror the battlefield is everywhere. Derek Gregory pointed out that in the new geography of war "[v]iolence can erupt in commuter train in Madrid, a house in Gaza City, a poppy field in Helmand or a street in Ciudad Juarez." (Gregory 2011, 239) The logical consequence is that the US homeland or other Western countries are no longer a sanctuary, but part of the global battlefield, where terrorist or insurgent forces may operate and where counterinsurgency tactics used in the "borderlands" may be applied.

The signs are unmistakable that Western governments are incorporating counterinsurgency tactics, technologies and approaches tested in Afghanistan and Iraq into everyday policing and security operations in the homeland. This includes drones and other surveillance systems, the increasing use of 'tagging, tracking and locating' (TTL) technology like 'stingrays' (devices for tracking cell phones and downloading data from them) by the police and the growing outright militarization of the police in terms of their tactics, equipment and culture.

To a lesser extent this disturbing trend can be also seen in Europe. For example, the Statewatch report 'Eurodrones' has documented that over €500 million have been spent by the EU to develop surveillance drones for patrolling European skies in an effort of reinventing European security (Hayes et al. 2014, 7). The report states:

> "Despite the often benign intent behind collaborative European 'research' into integrated land, air, maritime, space and cyber-surveillance systems, the EU's security and R&D policy is coalescing around a high-tech blueprint for a new kind of security. It envisages a future world of red zones and green zones; external borders controlled by military force and internally by a sprawling network of physical and virtual security checkpoints; public spaces, micro-states and 'mega events' policed by high-tech surveillance systems and rapid reaction forces; 'peacekeeping' and 'crisis management' missions that make no operational distinction between the suburbs of Basra or the Banlieue; and the in-

> creasing integration of defence and national security functions at home and abroad." (Hayes et al. 2014, 7)

One can speculate whether it is the technological advances achieved in the process of fighting counterinsurgency campaigns in the third world that is leading to the introduction of these systems in the West as a form of recycling these systems, or whether Western interventions in wars of the third world are mere test laboratories for technology development aimed from the beginning at instituting tighter population control at home. In any case, governments may see more intensive surveillance as a necessary price of globalization and their growing inability to control their borders resulting from it. With a lesser control of borders, people, ideologies and conflicts can easily spill over from one country or region to another, causing a kind of instability that did not exist prior to globalization.

Domestic Surveillance

Western governments have systematically expanded the surveillance of their populations in numerous ways. Governments keep now extensive records on all of their citizens and even of foreigners who travel or transit through their countries, which are now easily searchable and retrievable from online databases that may be 'datamined'. This includes the collection and retention of birth records, education records, medical records, police records, biometrics and so on. Governments also admittedly collect 'open source' information on individuals through social media for the purposes of law enforcement and counterterrorism (Nagashima 2012). This collection may soon become systematic and automated. For example, research sponsored by the Pentagon aims at developing software for examining Twitter posts "to identify individuals mobilized in a social contagion and when they become mobilized." (Ahmed 2014) The apparent fear is that Islamic or other ideological subversion on the Internet could result in 'digital insurgencies' and mass civil unrest.

More controversial is the mass surveillance of private communications, which were once considered to be protected by constitutional safeguards. Documents leaked by NSA whistleblower Edward Snowden have provided solid proof of the existence of NSA domestic surveillance that collects communications metadata of 'US persons' in bulk and that can be queried by NSA analysts to find terrorism connections. It is known that the NSA built for this purpose its own version of *Google* that can query a communications database containing "850 billion records about phone calls, emails, cellphone locations, and internet chats." (Gallagher 2014) Furthermore, there is hard evidence that numerous Western governments participate in the NSA mass surveillance by giving them access to communications data of their respective populations. Internet security expert Bruce Schneier recently wrote in *The Atlantic* that governments are united by their desire to conduct mass surveillance globally, which would create strong incentives

> "to join the most extensive spying network around. And

> that's the United States. This is what's happening right now. U.S. intelligence agencies partner with many countries as part of an extremely close relationship of wealthy, English-speaking nations called the Five Eyes: the U.S., U.K., Canada, Australia, and New Zealand. Other partnerships include the Nine Eyes, which adds Denmark, France, the Netherlands, and Norway; and the Fourteen Eyes, which adds Germany, Belgium, Italy, Spain, and Sweden. And the United States partners with countries that have traditionally been much more standoffish, like India, and even with brutally repressive regimes like Saudi Arabia's." (Schneier 2015)

The collected communications data is then used for identifying and tracking terrorists and terrorist activities across the world, making it more and more difficult for individuals on watchlists to escape the global dragnet of an emerging "global security state", as journalist Tom Engelhardt has called it (Engelhardt 2014, 10f.). According to ACLU, there are already over a million names on the American TIDE terror watchlist (Terrorist Identities Datamart Environment) of which 680,000 names are on the master watchlist that is shared with law enforcement and 22 foreign governments (Handeyside 2013). In addition to the dataveillance of populations, Western governments seem to be keen on introducing ever more intrusive surveillance technology such as high-tech surveillance drones that could persistently monitor their populations from above, follow individuals around their daily lives and if necessary, apply lethal or nonlethal force.

Domestic Surveillance Drones

It seems inevitable that military drones will increasingly operate domestically for the purposes of border security, internal security and law enforcement. The US military has been already authorized to "collect imagery during formal and continuation training missions as long as the collected imagery is not for the purpose of obtaining information about specific US persons and property." (US Air Force 2012) Of course, drone technology has long proliferated into the civilian sphere. There are numerous factors why the domestic drones will grow significantly over the next few decades, most importantly their lower cost, endurance and relative ease of operation compared to manned aircraft.

The Department of Homeland Security operates *Predator* drones since 2006, mainly to patrol the US-Mexico border. The drones can be used for detecting smugglers and other security threats and they can be used for monitoring individuals and activities across the US. Although the use of domestic drones has been recently criticized by the General Accounting Office for its high cost and elusive results, DHS plans to expand its current drone fleet from ten to 24 *Predator* drones, which still needs to pass through Congress. The new *Predators* shall have, according to a DHS requirements sheet for the manufacturer, a sensor capability to determine whether an individual is armed and a SIGINT capability to track individuals by their cell phones, as well as the capability to do direction finding for mobile devices

and two-way radios for precise geolocation (McCullagh 2013).

Many law enforcement agencies in the US and in Europe have shown great interest in drone technology and some have already bought Micro Aerial Vehicles (MAVs) that they use for monitoring protests and tracking individuals. The FBI has reportedly spent $3 million since 2006 to procure a small drone fleet and has on occasion borrowed a *Predator* drone from DHS. The FBI now operates a fleet of surveillance aircraft that can track individuals and have them circle over large cities (Gillum et al. 2015).

Not surprisingly, there is a growing concern that the domestic use of surveillance drones could lead to gross violations of privacy. *The American Civil Liberties Union* (ACLU) has frequently pointed at the threat to privacy resulting from domestic drone use. In a recent article on the drone use during the Baltimore riots ACLU analyst Jay Stanley argued:

> "these are not your parents' surveillance aircraft. Today there are powerful new surveillance technologies that use aircraft to collect mass information about whole populations, potentially reaching far beyond what the police might need to manage unrest."

He further elaborates:

> "Every moving pedestrian and vehicle can be tracked: the beginning and end everyone's journeys, and the route taken in between. This gives the authorities the power to press 'rewind' on anybody's movements, and learn a lot of intrusive things about how they live their life." (Stanley 2015)

It is not just optical sensors that can be paired with drones, but also many other types of sensors. For example, *Predator* and *Global Hawk* type drones can be also outfitted with wall-penetrating imaging radars and thermal imaging that look inside houses and exactly locate individuals. A recent *Congressional Research Service* report expressed the concern:

> "the sophistication of surveillance technology available to drones, such as facial recognition or laser radar which can 'see' through walls, may lead some to question the relevance of prior Fourth Amendment jurisprudence concerning more rudimentary forms of surveillance technology." (Thompson II 2013, 16)

A major issue with drones is that citizens may have their civil rights violated with no possibility for them to prove it or to protect the privacy of their homes. Although there are currently no plans of having armed Predator drones patrol American skies, it remains a likely prospect that some police drones might be armed with more than just sensors in the future.

Armed Police Drones

The *UN Rapporteur for Extrajudicial, Summary, and Arbitrary Executions,* Cristof Hejns, has expressed the concern that drones could be armed with nonlethal weapons and used for domestic law enforcement and riot control,

which could result in human rights violations (Hejns 2014, 14-16). He lists numerous examples of riot control drones that are being marketed to police forces around the world such as a South African drone called *Desert Wolf* that disperses crowds with a malodorant, a US drone named *Chaotic Unmanned Intercept Drone* that can shock intruders with 80,000 V, a US *Shadowhawk* drone that can shoot 37 mm and 40 mm Taser rounds and a German drone that can attack protesters with tear gas. Other police and security drones might be outfitted with guns that shoot rubber bullets or that are equipped with nonlethal directed energy weapons like dazzling lasers, sonic weapons, microwave weapons (pain rays). For special tactical situations like hostage liberation police forces might use drones that carry lethal weapons to kill a dangerous criminal.

Nonlethal weapons should not be automatically considered to be more humane or any less problematic than the use of lethal force. Not only can 'nonlethal weapons' be lethal if used improperly or against vulnerable persons, they also might lead to more frequent use of force by police officers exactly because they are considered less harmful. Pairing nonlethal weapons with drones might lead to an escalation of the use of force against largely innocent civilians, as pointed out by Hejns. It removes, or at least strongly reduces, two factors that have tended to restrain police forces: 1) it creates much greater physical distance between police officers and the population at large thus reducing the psychological restraint for violence; 2) it makes it possible to automate the use of nonlethal force, allowing the security drones to Taser, tear gas, or pain ray individuals and crowds into submission based on preset parameters of threatening behavior.

Up to now, nonlethal police drones remain hypothetical – only in India has a police department introduced a drone armed that can disperse crowds with pepper spray – but both the technology and the interest by law enforcement agencies are there. What has up to now prevented armed police drones is the public controversy that would accompany such an unprecedented move towards 'Robocop'. Even unarmed police drones that are circling cities and are buzzing over crowds would have undoubtedly a huge psychological effect on people – unlike the invisible dataveillance they are a constant reminder that they are being watched and that any misbehavior in the eyes of the watchers could have consequences.

Global Counterinsurgency

It seems that the next world war will be a war of global counterinsurgency conducted by an emerging global security state led by the US and directed against a diverse set of state and nonstate anti-globalization forces. An eye-opening strategy paper of the UK Ministry of Defence claims that within the next two or three decades the "world is *likely* to face the reality of a changing climate, rapid population growth, resource scarcity, resurgence in ideology, and shifts in global power from West to East." The report argues that since no nation will be able to address these issues alone, it will be necessary "to establish an effective system of global governance, capable of

responding to these challenges." (UK MoD 2010, 10) In other words, it is expected that globalization would reach its logical conclusion and eventually unite most nations on earth in order to implement key solutions to global problems. However, the report also suggests that such a new "system of global governance" could be opposed by diverse groupings of individuals, communities and states and may fuel extremism and violence within states (UK MoD 2010, 12). This could increase political instability in the world and may result in more international conflict (UK MoD 2010, 38). Although the report suggests that there is a potential for a great power conflict, it also points out that the US is unlikely to be challenged militarily by new rising powers such as China. State actors may therefore use nonstate proxies to conduct "hybrid wars" (UK Mod 2010, 84). It follows that the West has to be ready to conduct counterinsurgency on a global scale to prevent the enemy from coalescing and from destabilizing critical states or world regions or even from destabilizing the West from within.

Controlling Populations

As political systems fail to address key societal issues such as the widening gap between rich and poor, economic crisis, environmental disaster and poor governance, it can be expected that parts of the world's population become radicalized and that governments around the world will increasingly face civil disorder and rioting. First signs of civil unrest in the West have been seen in the London riots of 2011 or the Ferguson riots of 2014. So when governments expand their surveillance of their populations it is not so much about fighting terrorism, which is for the most part a mere law enforcement issue, but rather about preparing for counterinsurgency which is an entirely different concept. A RAND study explains the difference:

> "Not all insurgencies employ terror, and not all terrorists are insurgents. Insurgencies have an alternative vision of how to organize society, and they use various instruments, ranging from public service to terror, to realize that vision. Terrorism may be embedded in and subordinate to insurgency. But terrorism may also exist outside of insurgency, animated by sheer revulsion toward the status quo, without offering or striving for an alternative." (Gompert/Gordon 2008, 7)

Counterinsurgency is different from counterterrorism as the latter only deals with disrupting relatively small terrorist groups, while the former has to deal with political ideologies that may have mass appeal. Insurgencies are driven by broader political movements that have their military wings that might or might not use terrorist tactics, but that are mostly dangerous because of their ability to subvert larger segments of populations and turn them against the government. As a result, counterinsurgents have to fight the enemy's ideology as much as they need to fight the enemy forces. Mass surveillance is utterly ineffective in finding a few dangerous individuals in a large population (the proverbial needle in the haystack), but it is potentially

very effective in terms of identifying who may be susceptible to 'extremism' and thus needs to be watched more intensely in order to prevent them from organizing into larger resistance movements.

Researcher Nafeez Ahmed has argued that the US and the European governments already prepare for some kind of major future disruption and mass civil unrest (Ahmed 2014). Tremendous amounts of military grade equipment have been transferred to police departments under the '1033 program' that began in 1997 (Balko 2013, 209). For example, from 2006 to 2014 police departments received 600 MRAP 18-ton tanks, 79,288 assault rifles, 205 grenade launchers, 11,959 bayonets, 3,972 combat knives, $124 million worth of night-vision equipment, including night-vision sniper scopes, 479 bomb detonator robots, 50 airplanes, including 27 cargo transport airplanes, 422 helicopters, and $3.6 million worth of camouflage gear (NPR 2014).

Although traditionally barred from operating on US soil, the US military is nevertheless also preparing for domestic contingencies. Nathan Freier from the Army's SSI suggested: "To the extent events like this involve organized violence against local, state, and national authorities and exceed the capacity of the former two to restore public order and protect vulnerable populations, DoD [Department of Defense] would be required to fill the gap." (Freier 2008, 32) The US military has since drawn up a still classified contingency plan for domestic civil unrest, codenamed CONPLAN 3502 (Hudson 2011). An article by Kevin Benson and Jennifer Weber published in the military *Small Wars* journal even develops the scenario of a TEA Party insurrection fuelled by a weakening economy, high taxes on the middle class and an influx of immigrants that increases anti-immigration sentiment in South Carolina in 2016. In this scenario, the governor of the state would request federal law enforcement assistance in the face of riots in Darlington and the US Army are sent in to restore order (Benson; Weber 2012). However, a more likely scenario is the gradual introduction of counterinsurgency policing to get citizens slowly accustomed to police in riot gear, armored vehicles and surveillance drones in the sky.

Americans are already watched from above to track their movements and to make it easier to apprehend dangerous individuals, if necessary. At the periphery of the global security state armed drones can be used to crush local insurgencies and to pacify foreign populations from afar.

Armed Drones and World Order

Drone strikes are not only intended to simply kill dangerous terrorists, but to have psychological effects on the enemy such as intimidate, deter and make them feel powerless. But it is not just terrorist groups that are being intimidated by drone strikes – entire populations might be controlled by the fear of instant death delivered by drones that constantly circle the skies. Military analyst Thomas Barnett claims that this would be a good thing:

> "Trust me, along with drones, these frontier-settling tech-

> nologies will most definitely infiltrate our society in coming years, just like the military's Internet and GPS did before. The results will be similar: that much more capacity for individuals to be identified, tracked and watched, meaning anti-social behavior will become that much harder to pull off…for those of us not interested in committing terror, crimes and mischief, the larger truth is that we'll actually experience more freedom from all of those things…The result will be the same the world over: the end of off-grid locations, nowhere to hide, etc. You will be held responsible for what you do. There will be no frontiers left in which you can disappear. Anti-globalization forces like al-Qaeda will spring up here and there along this historical pathway, and each will have their moments before succumbing."Barnett 2011)

A different perspective of the psychological effects of drone strikes is offered in the Stanford Law School and New York University study *Living Under Drones*. The authors of the study claim that the population in the tribal areas of Pakistan is traumatized and that their normal lives have been seriously disrupted by the constant fear that they might become a victim of drone strike by sheer accident. People stay at home, are afraid to attend public gatherings such as funerals, are reluctant to go to school or work and even start distrusting people in their community, who might plant tracking chips on them (Stanford Law School/New York University 2012, 80-101). From a counterinsurgency perspective, such psychological effects on a population could be considered to be conducive to the overall aim, namely to prevent people from organizing resistance or deter them from joining a resistance group. But drone warfare is hardly any more humanitarian just because it can be much more targeted, especially if merely having the wrong political views (susceptibility to extremism) or the wrong friends (terrorist association) can potentially get a person on a 'kill list'. Furthermore, it may actually achieve an opposite effect and motivate retaliation, result in more widespread radicalization and the destabilization of an ally (Hudson et al. 2011, 126f.).

Conclusion

The Pentagon in collaboration with numerous other governments is creating a world where there is for the average individual nowhere to hide and nowhere to run. People can be constantly tracked and their actions made visible to the authorities using a variety of ground-based and overhead surveillance. Who is identified as a threat will have the own name added to the 'disposition matrix' that will enable US government agencies to figure out how to best neutralize the individual in question, using drone strikes, kill or capture by Special Forces, or maybe a simple arrest by the police, if local authorities are cooperative. The ongoing quest for US global dominance is being turned into a never-ending campaign of global counterinsurgency against 'terrorists', 'extremists', 'rogue states' and really anybody else who may resist the change from the old order of a system of nation states to a

new order of a system of 'global governance', backed by a robotic global surveillance and global enforcement apparatus. The end result of these efforts cannot be predicted. Alfred McCoy contends:

> "If all or much goes according to plan, sometime in the third decade of this century the Pentagon will complete a comprehensive global surveillance system for Earth, sky, and space using robotics to coordinate a veritable flood of data from biometric street-level monitoring, cyber-data mining, a worldwide network of Space Surveillance Telescopes, and triple canopy aeronautic patrols. Through agile data management of exceptional power, this system might allow the United States a veto of global lethality, an equalizer for any further loss of economic strength." (McCoy 2012)

However, he cautions that the dreams of technological omnipotence may just as well result "in military debacle from the illusion of technological mastery."

References

Ackerman, S. (2011) US Holds Onto Biometrics Database of 3 Million Iraqis. In: *Wired Blog*. http://www.wired.com/2011/12/iraq-biometrics-database/ (16/09/2015).

Ahmed, N. (2014) Pentagon Preparing for Mass Civil Breakdown. In: *The Guardian*. http://www.theguardian.com/environment/earth-insight/2014/jun/12/pentagon-mass-civil-breakdown (16/09/2015).

Associated Press (2011) The Al Qaeda Papers –Drones. http://hosted.ap.org/specials/interactives/_international/_pdfs/al-qaida-papers-drones.pdf (19/09/2015).

Bamford, J. (2015) Why NSA's Surveillance Is Worse Than You've Ever Imagined. In: *Reuters*. http://blogs.reuters.com/great-debate/2015/05/11/if-youre-not-outraged-about-the-nsa-surveillance-heres-why-you-should-be/ (16/09/2015).

Barnett, T. (2011) Drones + Biometrics: Weapons That Conquer's Civilization's Frontiers. In: *Time Magazine*. http://nation.time.com/2011/07/14/drones-biometrics-weapons-that-conquer-globalizations-frontiers/ (16/09/2015).

Belcher, O. (2012) The Best-Laid Schemes: Postcolonialism, Military Social Science, and the Making of US Counterinsurgency Doctrine, 1947-2009. In: *Antipode* 44 (1): 258-263.

Benson, K.; Weber, J. (2012) Full Spectrum Operations in the Homeland: A 'Vision' of the Future. In: *Small Wars Journal*, July 25.

Bolkcom, C. (2006) Potential Military Use of Airships and Aerostats. CRS Report for Congress. https://www.fas.org/sgp/crs/weapons/RS21886.pdf (16/09/2015).

Bumiller, E.; Shanker, T. (2011) War Evolves With Drones, Some Tiny as Bugs. In: *The New York Times*. http://www.nytimes.com/2011/06/20/world/20drones.html?_r=0 (16/09/2015).

Clark, R. M. (2011) *The Technical Collection of Intelligence*. Washington, DC: CQ Press.

Engelhard, T. (2014) *Shadow Government: Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World*. Chicago, IL: Haymarket Books.

Fowler, M. (2014) The Strategy of Drone Warfare. In: *Journal of Strategic Security* 7 (4): 108-119.

Freier, N. (2008) Known Unknowns: Unconventional 'Strategic Shocks' in Defense Strategy Development. US Army War College, Strategic Studies Institute. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB890.pdf (16/09/2015).

Gillum, J./Sullivan, E./Tucker, E. (2015) FBI Behind Mysterious Surveillance Aircraft Over US Cities. In: *Associated Press*. http://bigstory.ap.org/article/4b3f220e33b64123a3909c60845da045/fbi-behind-mysterious-surveillance-aircraft-over-us-cities?utm_source=jolt&utm_medium=email&utm_term=Jolt&utm_campaign=New%20Campaign (16/09/2015).

Graham, S. (2006) Cities and the 'War on Terror'. In: *International Journal of Urban and Regional Research* 30 (2): 255-276.

Gregory, D. (2011) The Everywhere War. In: *The Geographical Journal* 177 (3): 238-250.

Grey, S.; Edge, D. (2011) Frontline: Kill/ Capture. PBS Frontline, transcript available at: http://www.pbs.org/wgbh/pages/frontline/afghanistan-pakistan/kill-capture/transcript/ (16/09/2015).

Grossman, K. (2001) *Weapons in Space*. New York: Seven Stories Press.

Handeyside, H. (2013) Numbers Tell the Story of Our Government's Watchlisting Binge. American Civil Liberties Union. https://www.aclu.org/blog/numbers-tell-story-our-governments-watchlisting-binge (16/09/2015).

Hayes, B.; Jones, C.; Töpfer, E. (2014) Eurodrones Inc. Statewatch. http://www.statewatch.org/news/2014/feb/sw-tni-eurodrones-inc-feb-2014.pdf (16/09/2015).

Heath, B. (2015) New Police Radars Can "See" Inside Homes. In: *USA Today*. http://www.usatoday.com/story/news/2015/01/19/police-radar-see-through-walls/22007615/ (16/09/2015).

Hudson, J. (2011) The Military's Plan for London-Like Riots. In: *The Atlantic*. http://www.thewire.com/global/2011/08/us-militarys-plan-london-riots/41101/ (16/09/2015).

Hudson, L.; Owens, C.S.; Flannes, M. (2011) Drone Warfare: Blowback From the New American Way of War. In: *Middle East Policy* 18 (3): 122-132.

Kilcullen, D. (2007) Countering Global Insurgency. In: *The Journal of Strategic Studies* 28 (4): 597-617.

Matthews, W. (2012) Deflated: America's Airship Revolution Is Threatened by Mishaps and Funding Cuts. In: *Defense News*. http://archive.defensenews.com/article/20120501/C4ISR01/305010009/Deflated-America-8217-s-Airship-Revolution-Threatened-by-Mishaps-Delays-Funding-Cuts (16/09/2015).

Mayer, J. (2005) Outsourcing Torture: The Secret History of America's 'Extraordinary Rendition' Program. In: *The New Yorker*. http://www.newyorker.com/magazine/2005/02/14/outsourcing-torture (16/09/2015).

McCoy, A. W. (2012) Beyond Bayonets and Battleships: Space Warfare and the Future of U.S. Global Power. In: *TomDispatch*. http://www.tomdispatch.com/blog/175614/alfred_mccoy_superweapons_and_global_dominion (16/09/2015).

McCullagh, D. (2013) DHS Built Domestic Surveillance Tech into Predator Drones. In: *CNET Magazine*. http://www.cnet.com/news/dhs-built-domestic-surveillance-tech-into-predator-drones/ (16/09/2015).

Miller, G.; Tate, J.; Gellman, B. (2013) Documents Reveal NSA's Extensive Involvement in Targeted Killing Program. In: *The Washington Post*. http://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html (16/09/2015).

Moore, M. (2008) *Twilight War: The Folly of U.S. Space Dominance*. Oakland, CA: The Independent Institute.

Nakashima, E. (2012) DHS Monitoring of Social Media Worries Civil Liberties Advocates. In: *The Washington Post*. http://www.washingtonpost.com/world/national-security/dhs-monitoring-of-social-media-worries-civil-liberties-advocates/2012/01/13/gIQANPO7wP_story.html (16/09/2015).

NPR (2014) MRAPs and Bayonets: What We Know About the Pentagon's 1033 Program. In: *NPR*. http://www.npr.org/2014/09/02/342494225/mraps-and-bayonets-what-we-know-about-the-pentagons-1033-program (16/09/2015).

Open Society (2013) *Globalizing Torture: CIA Secret Detention and Extraordinary Rendition*. Open Society Foundations New York.

Pincus, W. (2009) Airborne Intelligence Playing Greater Role in Irregular Warfare. In: The Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2009/04/27/AR2009042703672.html (16/09/2015).

Richelson, J. T. (2008) *The US Intelligence Community*. Boulder, CO: Westview Press.

Rosenau, W.; Long, A. (2009) *The Phoenix Program and Contemporary Counterinsurgency*. Santa Monica, CA: RAND.

Savage, C. (2013) Facial Scanning Is Making Gains in Surveillance. In: *The New York Times*. http://www.nytimes.com/2013/08/21/us/facial-scanning-is-making-gains-in-surveillance.html?ref=global-home&_r=1 (16/09/2015).

Scahill, J.; Greenwald, G. (2014) The NSA's Secret Role in the U.S. Assassination Program. In: *The Intercept*. https://firstlook.org/theintercept/2014/02/10/the-nsas-secret-role/ (16/09/2015).

Schneier, B. (2015) What Is Next in Government Surveillance. In: *The Atlantic*. http://www.theatlantic.com/international/archive/2015/03/whats-next-in-government-surveillance/385667/ (16/09/2015).

Shachtman, N. (2011) Army Tracking Plan: Drones That Never Forget a Face. In: *Wired Blog*. http://www.wired.com/2011/09/drones-never-forget-a-face/ (16/09/2015).

Soldatov, A.; Borogan, I. (2015) *The Red Web: The Struggle Between Russia's Dictators and the New Online Revolutionaries*. New York: Public Affairs.

Spiegel (2014) Spying Together: Germany's Deep Cooperation with the NSA. In: *Der Spiegel Online*. http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.

html (16/09/2015).
Stanford Law School & New York University School of Law (2012) Living Under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan (September). http://www.livingunderdrones.org/wp-content/uploads/2013/10/Stanford-NYU-Living-Under-Drones.pdf (16/09/2015).
Stanley, J. (2015) Mysterious Planes Over Baltimore Spark Surveillance Suspicions. In: *American Civil Liberties Union*. https://www.aclu.org/blog/free-future/mysterious-planes-over-baltimore-spark-surveillance-suspicions (16/09/2015).
Strawser, B.J. (2010) Moral Predators. The Duty to Employ Uninhabited Aerial Vehicles. In: *Journal of Military Ethics* 9 (4): 342-368.
Trimble, S. (2014) Sierra Nevada Fields ARGIS-IS Upgrade to Gorgon Stare Pod. Flightglobal.com. http://www.flightglobal.com/news/articles/sierra-nevada-fields-argus-is-upgrade-to-gorgon-stare-400978/ (16/09/2015).
Turse, N. (2012) *The Changing Face of Empire. Special Ops, Drones, Spies, Proxy Fighters, Secret Bases, and Cyberwarfare*. Chicago, IL: Haymarket Books.
Turse, N. (2014) The Special Ops Surge. America's Secret War in 134 Countries. In: *TomDispatch.com*. http://www.tomdispatch.com/blog/175794/tomgram%3A_nick_turse,_secret_wars_and_black_ops_blowback/ (16/09/2015).
United Kingdom (2010) Global Strategic Trends – Out to 2040. Ministry of Defence. January 12.
United Nations (2014) Report of the Special Rapporteur for Extrajudicial, Arbitrary, or Summary Executions. General Assembly 69th Session. A/69/265.
United States Department of the Air Force (1990) The Air Force and US National Security: Global Reach – Global Power. White Paper (June). https://secure.afa.org/EdOp/2012/GRGP_Rice_1990.pdf (16/09/2015).
United States Department of the Air Force (1997) Vision for 2020. Petersen, AFB: US Space Command.
United States Department of the Air Force (2012) Air Force Instruction 14-104. Secretary of the Air Force (April 23).
United States Department of the Army (2011) Commander's Guide to Biometrics in Afghanistan. Handbook (11-25). https://publicintelligence.net/call-afghan-biometrics/ (16/09/2015).
Wardrop, M. (2009) Unmanned Drones Could Be Banned, Says Senior Judge. In: *The Telegraph*. http://www.telegraph.co.uk/news/newstopics/politics/defence/5755446/Unmanned-drones-could-be-banned-says-senior-judge.html (16/09/2015).