Space Warfare Imminent Threat

by Alfred W. McCoy via lee - TomDispatch *Thursday, Nov 8 2012, 9:23pm*
international / prose / post

> Well, it finally made the media thanks to Al McCoy, his efforts are always welcome.
>
> The hacking community has been following these developments for years with the view to intervene or interrupt remote systems at the most critical time and turn the tables on any aggressor superpower. Never forget that the most radical aspect of space warfare is its fragility and insecurity/vulnerability.

X-37B in launch capsule

The principle upon which asymmetric warfare rests is simple; let the other guy do all the heavy lifting and developing and then take control of the situation via superior skill, speed, stealth and strategy.

Hackers have been compromising systems in this field for years. They have also been rehearsing and gaining proficiency with real game scenarios. Elite groups have not shared all their hacked secrets with other superpowers only enough to maintain balance and stability and prevent any nation from gaining a huge advantage over another. Hackers have kept the best to themselves as a safety valve, so to speak.

While most of what has been said above is the stuff of rumour, these rumours are remarkably persistent, to the point where concerned parties are taking them seriously.

WWII was lost and won in the air -- make no mistake, WWIII will be lost and won in space.

I leave you to update and familiarise yourself with the REAL warfare of tomorrow:

> **Beyond Bayonets and Battleships**
>
> 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.

They are still operating in another age. “Our Navy is smaller now than at any time since 1917,” complained Republican candidate Mitt Romney during the last presidential debate.

With words of withering mockery, President Obama shot back: “Well, Governor, we also have fewer horses and bayonets, because the nature of our military's changed… the question is not a game of Battleship, where we're counting ships. It's what are our capabilities.”

Obama later offered just a hint of what those capabilities might be: “What I did was work with our joint chiefs of staff to think about, what are we going to need in the future to make sure that we are safe?... We need to be thinking about cyber security. We need to be talking about space.”

Amid all the post-debate media chatter, however, not a single commentator seemed to have a clue when it came to the profound strategic changes encoded in the president’s sparse words. Yet for the past four years, working in silence and secrecy, the Obama administration has presided over a technological revolution in defense planning, moving the nation far beyond bayonets and battleships to cyberwarfare and the full-scale weaponization of space. In the face of waning economic influence, this bold new breakthrough in what’s called “information warfare” may prove significantly responsible should U.S. global dominion somehow continue far into the twenty-first century.

While the technological changes involved are nothing less than revolutionary, they have deep historical roots in a distinctive style of American global power. It’s been evident from the moment this nation first stepped onto the world stage with its conquest of the Philippines in 1898. Over the span of a century, plunged into three Asian crucibles of counterinsurgency -- in the Philippines, Vietnam, and Afghanistan -- the U.S. military has repeatedly been pushed to the breaking point. It has repeatedly responded by fusing the nation’s most advanced technologies into new information infrastructures of unprecedented power.

That military first created a manual information regime for Philippine pacification, then a computerized apparatus to fight communist guerrillas in Vietnam. Finally, during its decade-plus in Afghanistan (and its years in Iraq), the Pentagon has begun to fuse biometrics, cyberwarfare, and a potential future triple canopy aerospace shield into a robotic information regime that could produce a platform of unprecedented power for the exercise of global dominion -- or for future military disaster.

America’s First Information Revolution

This distinctive U.S. system of imperial information gathering (and the surveillance and war-making practices that go with it) traces its origins to some brilliant American innovations in the management of textual, statistical, and visual data. Their sum was nothing less than a new information infrastructure with an unprecedented capacity for

mass surveillance.

During two extraordinary decades, American inventions like Thomas Alva Edison's quadruplex telegraph (1874), Philo Remington's commercial typewriter (1874), Melvil Dewey's library decimal system (1876), and Herman Hollerith's patented punch card (1889) created synergies that led to the militarized application of America's first information revolution. To pacify a determined guerrilla resistance that persisted in the Philippines for a decade after 1898, the U.S. colonial regime -- unlike European empires with their cultural studies of "Oriental civilizations" -- used these advanced information technologies to amass detailed empirical data on Philippine society. In this way, they forged an Argus-eyed security apparatus that played a major role in crushing the Filipino nationalist movement. The resulting colonial policing and surveillance system would also leave a lasting institutional imprint on the emerging American state.

When the U.S. entered World War I in 1917, the "father of U.S. military intelligence" Colonel Ralph Van Deman drew upon security methods he had developed years before in the Philippines to found the Army's Military Intelligence Division. He recruited a staff that quickly grew from one (himself) to 1,700, deployed some 300,000 citizen-operatives to compile more than a million pages of surveillance reports on American citizens, and laid the foundations for a permanent domestic surveillance apparatus.

A version of this system rose to unparalleled success during World War II when Washington established the Office of Strategic Services (OSS) as the nation's first worldwide espionage agency. Among its nine branches, Research & Analysis recruited a staff of nearly 2,000 academics who amassed 300,000 photographs, a million maps, and three million file cards, which they deployed in an information system via "indexing, cross-indexing, and counter-indexing" to answer countless tactical questions.

Yet by early 1944, the OSS found itself, in the words of historian Robin Winks, "drowning under the flow of information." Many of the materials it had so carefully collected were left to molder in storage, unread and unprocessed. Despite its ambitious global reach, this first U.S. information regime, absent technological change, might well have collapsed under its own weight, slowing the flow of foreign intelligence that would prove so crucial for America's exercise of global dominion after World War II.

Computerizing Vietnam

Under the pressures of a never-ending war in Vietnam, those running the U.S. information infrastructure turned to computerized data management, launching a second American information regime. Powered by the most advanced IBM mainframe computers, the U.S. military compiled monthly tabulations of security in all of South Vietnam's 12,000 villages and filed the three million enemy documents its soldiers captured annually on giant reels of bar-coded film. At the same time, the CIA collated and computerized diverse data on the communist civilian infrastructure as part of its infamous Phoenix Program. This, in turn, became the basis for its systematic tortures and 41,000 "extra-judicial executions" (which, based on disinformation from petty local grudges and communist counterintelligence, killed many but failed to capture more than a handfull of top communist cadres).

Most ambitiously, the U.S. Air Force spent $800 million a year to lace southern Laos with a network of 20,000 acoustic, seismic, thermal, and ammonia-sensitive sensors to

pinpoint Hanoi's truck convoys coming down the Ho Chi Minh Trail under a heavy jungle canopy. The information these provided was then gathered on computerized systems for the targeting of incessant bombing runs. After 100,000 North Vietnamese troops passed right through this electronic grid undetected with trucks, tanks, and heavy artillery to launch the Nguyen Hue Offensive in 1972, the U.S. Pacific Air Force pronounced this bold attempt to build an "electronic battlefield" an unqualified failure.

In this pressure cooker of what became history's largest air war, the Air Force also accelerated the transformation of a new information system that would rise to significance three decades later: the Firebee target drone. By war's end, it had morphed into an increasingly agile unmanned aircraft that would make 3,500 top-secret surveillance sorties over China, North Vietnam, and Laos. By 1972, the SC/TV drone, with a camera in its nose, was capable of flying 2,400 miles while navigating via a low-resolution television image.

On balance, all this computerized data helped foster the illusion that American "pacification" programs in the countryside were winning over the inhabitants of Vietnam's villages, and the delusion that the air war was successfully destroying North Vietnam's supply effort. Despite a dismal succession of short-term failures that helped deliver a soul-searing blow to American power, all this computerized data-gathering proved a seminal experiment, even if its advances would not become evident for another 30 years until the U.S. began creating a third -- robotic -- information regime.

The Global War on Terror

As it found itself at the edge of defeat in the attempted pacification of two complex societies, Afghanistan and Iraq, Washington responded in part by adapting new technologies of electronic surveillance, biometric identification, and drone warfare -- all of which are now melding into what may become an information regime far more powerful and destructive than anything that has come before.

After six years of a failing counterinsurgency effort in Iraq, the Pentagon discovered the power of biometric identification and electronic surveillance to pacify the country's sprawling cities. It then built a biometric database with more than a million Iraqi fingerprints and iris scans that U.S. patrols on the streets of Baghdad could access instantaneously by satellite link to a computer center in West Virginia.

When President Obama took office and launched his "surge," escalating the U.S. war effort in Afghanistan, that country became a new frontier for testing and perfecting such biometric databases, as well as for full-scale drone war in both that country and the Pakistani tribal borderlands, the latest wrinkle in a technowar already loosed by the Bush administration. This meant accelerating technological developments in drone warfare that had largely been suspended for two decades after the Vietnam War.

Launched as an experimental, unarmed surveillance aircraft in 1994, the Predator drone was first deployed in 2000 for combat surveillance under the CIA's "Operation Afghan Eyes." By 2011, the advanced MQ-9 Reaper drone, with "persistent hunter killer" capabilities, was heavily armed with missiles and bombs as well as sensors that could read disturbed dirt at 5,000 feet and track footprints back to enemy installations. Indicating the torrid pace of drone development, between 2004 and 2010 total flying time for all unmanned vehicles rose from just 71 hours to 250,000 hours.

By 2009, the Air Force and the CIA were already deploying a drone armada of at least 195 Predators and 28 Reapers inside Afghanistan, Iraq, and Pakistan -- and it's only grown since. These collected and transmitted 16,000 hours of video daily, and from 2006-2012 fired hundreds of Hellfire missiles that killed an estimated 2,600 supposed insurgents inside Pakistan's tribal areas. Though the second-generation Reaper drones might seem stunningly sophisticated, one defense analyst has called them "very much Model T Fords." Beyond the battlefield, there are now some 7,000 drones in the U.S. armada of unmanned aircraft, including 800 larger missile-firing drones. By funding its own fleet of 35 drones and borrowing others from the Air Force, the CIA has moved beyond passive intelligence collection to build a permanent robotic paramilitary capacity.

In the same years, another form of information warfare came, quite literally, online. Over two administrations, there has been continuity in the development of a cyberwarfare capability at home and abroad. Starting in 2002, President George W. Bush illegally authorized the National Security Agency to scan countless millions of electronic messages with its top-secret "Pinwale" database. Similarly, the FBI started an Investigative Data Warehouse that, by 2009, held a billion individual records.

Under Presidents Bush and Obama, defensive digital surveillance has grown into an offensive "cyberwarfare" capacity, which has already been deployed against Iran in history's first significant cyberwar. In 2009, the Pentagon formed U.S. Cyber Command (CYBERCOM), with headquarters at Ft. Meade, Maryland, and a cyberwarfare center at Lackland Air Base in Texas, staffed by 7,000 Air Force employees. Two years later, it declared cyberspace an "operational domain" like air, land, or sea, and began putting its energy into developing a cadre of cyber-warriors capable of launching offensive operations, such as a variety of attacks on the computerized centrifuges in Iran's nuclear facilities and Middle Eastern banks handling Iranian money.

A Robotic Information Regime

As with the Philippine Insurrection and the Vietnam War, the occupations of Iraq and Afghanistan have served as the catalyst for a new information regime, fusing aerospace, cyberspace, biometrics, and robotics into an apparatus of potentially unprecedented power. In 2012, after years of ground warfare in both countries and the continuous expansion of the Pentagon budget, the Obama administration announced a leaner future defense strategy. It included a 14% cut in future infantry strength to be compensated for by an increased emphasis on investments in the dominions of outer space and cyberspace, particularly in what the administration calls "critical space-based capabilities."

By 2020, this new defense architecture should theoretically be able to integrate space, cyberspace, and terrestrial combat through robotics for -- so the claims go -- the delivery of seamless information for lethal action. Significantly, both space and cyberspace are new, unregulated domains of military conflict, largely beyond international law. And Washington hopes to use both, without limitation, as Archimedean levers to exercise new forms of global dominion far into the twenty-first century, just as the British Empire once ruled from the seas and the Cold War American imperium exercised its global reach via airpower.

As Washington seeks to surveil the globe from space, the world might well ask: Just how

high is national sovereignty? Absent any international agreement about the vertical extent of sovereign airspace (since a conference on international air law, convened in Paris in 1910, failed), some puckish Pentagon lawyer might reply: only as high as you can enforce it. And Washington has filled this legal void with a secret executive matrix -- operated by the CIA and the clandestine Special Operations Command -- that assigns names arbitrarily, without any judicial oversight, to a classified “kill list” that means silent, sudden death from the sky for terror suspects across the Muslim world.

Although U.S. plans for space warfare remain highly classified, it is possible to assemble the pieces of this aerospace puzzle by trolling the Pentagon’s websites, and finding many of the key components in technical descriptions at the Defense Advanced Research Projects Agency (DARPA). As early as 2020, the Pentagon hopes to patrol the entire globe ceaselessly, relentlessly via a triple canopy space shield reaching from stratosphere to exosphere, driven by drones armed with agile missiles, linked by a resilient modular satellite system, monitored through a telescopic panopticon, and operated by robotic controls.

At the lowest tier of this emerging U.S. aerospace shield, within striking distance of Earth in the lower stratosphere, the Pentagon is building an armada of 99 Global Hawk drones equipped with high-resolution cameras capable of surveilling all terrain within a 100-mile radius, electronic sensors to intercept communications, efficient engines for continuous 24-hour flights, and eventually Triple Terminator missiles to destroy targets below. By late 2011, the Air Force and the CIA had already ringed the Eurasian land mass with a network of 60 bases for drones armed with Hellfire missiles and GBU-30 bombs, allowing air strikes against targets just about anywhere in Europe, Africa, or Asia.

The sophistication of the technology at this level was exposed in December 2011 when one of the CIA’s RQ-170 Sentinels came down in Iran. Revealed was a bat-winged drone equipped with radar-evading stealth capacity, active electronically scanned array radar, and advanced optics “that allow operators to positively identify terror suspects from tens of thousands of feet in the air.”

If things go according to plan, in this same lower tier at altitudes up to 12 miles unmanned aircraft such as the “Vulture,” with solar panels covering its massive 400-foot wingspan, will be patrolling the globe ceaselessly for up to five years at a time with sensors for “unblinking” surveillance, and possibly missiles for lethal strikes. Establishing the viability of this new technology, NASA’s solar-powered aircraft Pathfinder, with a 100-foot wingspan, reached an altitude of 71,500 feet altitude in 1997, and its fourth-generation successor the “Helios” flew at 97,000 feet with a 247-foot wingspan in 2001, two miles higher than any previous aircraft.

For the next tier above the Earth, in the upper stratosphere, DARPA and the Air Force are collaborating in the development of the Falcon Hypersonic Cruise Vehicle. Flying at an altitude of 20 miles, it is expected to “deliver 12,000 pounds of payload at a distance of 9,000 nautical miles from the continental United States in less than two hours.” Although the first test launches in April 2010 and August 2011 crashed midflight, they did reach an amazing 13,000 miles per hour, 22 times the speed of sound, and sent back “unique data” that should help resolve remaining aerodynamic problems.

At the outer level of this triple-tier aerospace canopy, the age of space warfare dawned

in April 2010 when the Pentagon quietly launched the X-37B space drone, an unmanned craft just 29 feet long, into an orbit 250 miles above the Earth. By the time its second prototype landed at Vandenberg Air Force Base in June 2012 after a 15-month flight, this classified mission represented a successful test of “robotically controlled reusable spacecraft” and established the viability of unmanned space drones in the exosphere.

At this apex of the triple canopy, 200 miles above Earth where the space drones will soon roam, orbital satellites are the prime targets, a vulnerability that became obvious in 2007 when China used a ground-to-air missile to shoot down one of its own satellites. In response, the Pentagon is now developing the F-6 satellite system that will “decompose a large monolithic spacecraft into a group of wirelessly linked elements, or nodes [that increases] resistance to... a bad part breaking or an adversary attacking.” And keep in mind that the X-37B has a capacious cargo bay to carry missiles or future laser weaponry to knock out enemy satellites -- in other words, the potential capability to cripple the communications of a future military rival like China, which will have its own global satellite system operational by 2020.

Ultimately, the impact of this third information regime will be shaped by the ability of the U.S. military to integrate its array of global aerospace weaponry into a robotic command structure that would be capable of coordinating operations across all combat domains: space, cyberspace, sky, sea, and land. To manage the surging torrent of information within this delicately balanced triple canopy, the system would, in the end, have to become self-maintaining through “robotic manipulator technologies,” such as the Pentagon’s FREND system that someday could potentially deliver fuel, provide repairs, or reposition satellites.

For a new global optic, DARPA is building the wide-angle Space Surveillance Telescope (SST), which could be sited at bases ringing the globe for a quantum leap in "space surveillance.” The system would allow future space warriors to see the whole sky wrapped around the entire planet while seated before a single screen, making it possible to track every object in Earth orbit.

Operation of this complex worldwide apparatus will require, as one DARPA official explained in 2007, "an integrated collection of space surveillance systems -- an architecture -- that is leak-proof." Thus, by 2010, the National Geospatial-Intelligence Agency had 16,000 employees, a $5 billion budget, and a massive $2 billion headquarters at Fort Belvoir, Virginia, with 8,500 staffers wrapped in electronic security -- all aimed at coordinating the flood of surveillance data pouring in from Predators, Reapers, U-2 spy planes, Global Hawks, X-37B space drones, Google Earth, Space Surveillance Telescopes, and orbiting satellites. By 2020 or thereafter -- such a complex techno-system is unlikely to respect schedules -- this triple canopy should be able to atomize a single “terrorist” with a missile strike after tracking his eyeball, facial image, or heat signature for hundreds of miles through field and favela, or blind an entire army by knocking out all ground communications, avionics, and naval navigation.

Technological Dominion or Techno-Disaster?

Peering into the future, a still uncertain balance of forces offers two competing scenarios for the continuation of U.S. global power. 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.

However, as in Vietnam, history offers some pessimistic parallels when it comes to the U.S. preserving its global hegemony by militarized technology alone. Even if this robotic information regime could somehow check China's growing military power, the U.S. might still have the same chance of controlling wider geopolitical forces with aerospace technology as the Third Reich had of winning World War II with its "super weapons" -- V-2 rockets that rained death on London and Messerschmitt Me-262 jets that blasted allied bombers from Europe's skies. Complicating the future further, the illusion of information omniscience might incline Washington to more military misadventures akin to Vietnam or Iraq, creating the possibility of yet more expensive, draining conflicts, from Iran to the South China Sea.

If the future of America's world power is shaped by actual events rather than long-term economic trends, then its fate might well be determined by which comes first in this century-long cycle: military debacle from the illusion of technological mastery, or a new technological regime powerful enough to perpetuate U.S. global dominion.

http://www.tomdispatch.com/blog/175614/
