AIR WAR COLLEGE

AIR UNIVERSITY

MINORITY REPORT:

POTENTIAL CHALLENGES IN EMPLOYING GLOBAL STRIKE AGAINST VIOLENT NON-STATE ACTORS IN 2035

by

Timothy D. West, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

13 February 2012

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Timothy D. West is a U.S. Air Force flight test engineer assigned to the Air War College, Air University, Maxwell AFB, AL. Commissioned in 1990 as a Distinguished Graduate of the Air Force Reserve Officer Training Corps, Colonel West has a Bachelor of Science degree in Mechanical Engineering from the University of Kentucky and Master of Science degrees in Aerospace Engineering and Industrial Engineering from the University of Tennessee Space Institute. Colonel West has orchestrated a wide variety of ground and flight test over the course of his career, including evaluations of munitions, avionics, command and control systems, electronic warfare systems, and cyber systems. After completing the U.S. Air Force Test Pilot School's Flight Test Engineering course in 2000, he amassed nearly 400 flying hours in a variety of aircraft, including the T-38, F-15, F-16, C-130, and MH-60. A Distinguished Graduate of Air Command and Staff College, Colonel West has also commanded a test squadron and an acquisition squadron.

Abstract

The computing environment of 2035 is projected to be vastly different from that of today. Assuming processing power continues to double every 18 months in accordance with Moore's Law, computers will be 41,285 times more powerful. Further, the environment will likely be saturated with microchips: in our walls, our furniture, our clothes, and even in our bodies. As a result, many analysts share a common belief that it will be impossible for a clandestine group or individual to hide in such a society – that tomorrow's Osama bin Laden does not have a prayer of staying below the radar for 10 minutes, let alone 10 years.

This "minority report" challenges that belief by first showing that the amount of data available to be analyzed is currently growing faster than processing power, and then discussing the challenges and complexities this creates for employing global strike against a violent non-state actor (VNSA) in the 2035 timeframe. It examines each of the six steps of the kill chain (e.g., Find, Fix, Track, Target, Engage, and Assess) and considers the actions a VNSA might employ to block that step. The paper shows that an enemy who can break even one link in the kill chain can effectively thwart global strike, at least temporarily. Further, the earlier the VNSA breaks the chain, the more likely his survival, with the ideal being to break the chain before the enemy can even find the VNSA.

The author concludes that the key to a successful global strike against a VNSA in 2035 is the intelligence that enables the strike, and not the strike weapon itself. Thus, he recommends the Air Force continue to invest in a full spectrum of intelligence, surveillance, and reconnaissance technologies.

Introduction

General Norman Schwartz, Air Force Chief of Staff, tasked the Air War College's Center for Strategy and Technology (CSAT) to "investigate how the Air Force should posture itself with strategically and operationally relevant capabilities to strike globally on demand and in any domain, in 2035."[1] This paper supports that tasking by assessing the challenges and complexities of employing Global Strike against a violent non-state actor (VNSA) in the 2035 timeframe. It examines each of the six steps of the kill chain (e.g., Find, Fix, Track, Target, Engage, and Assess, collectively known as the F2T2EA process)[2] and considers the actions a VNSA might employ to block that step. The central premise of this paper is that an enemy who can break even one link in the kill chain remains invulnerable to global strike.

To be clear from the outset, the purpose of this paper is not to question whether a global strike capability would be a valuable addition to the Air Force inventory, since such a system would unquestionably provide the President of 2035 with strategic options that President Obama does not currently possess. Instead, the intent of this *Minority Report* is to add a degree of balance to the optimistic tenor expected in the companion papers written my colleagues on the CSAT team. Ideally, the combined body of research will adeptly equip today's Air Force leadership to make long-term, high-dollar acquisition decisions regarding tomorrow's Global Strike capability.

What is Global Strike?

One of the early challenges faced by the CSAT team was to define exactly what we meant by "Global Strike." After much discussion and with considerable assistance from the

[1] Gen. Norman A. Schwartz, *Invitation to Participate in the Blue Horizons Program for Academic Year 2012*, 19 May 2011.
[2] Thomas K. Anderson, et al., *Air Force Doctrine Document (AFDD) 3-60: Targeting* (Montgomery, AL: Lemay Center), 28 Jul 2001, 49-53. http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-60.pdf.

CSAT staff, the following definition emerged: *"a set of capabilities allowing the President of the United States to preempt or respond with an act of war to quickly strike any target anywhere, in any environment, on demand in order to achieve strategic objectives."*

The wording of this definition – which notably describes global strike not as a *weapon*, but rather as a *set of capabilities* – acknowledges two early conclusions by the team. First, a singular weapon would be unlikely to fully satisfy the specified requirement. For instance, a weapon devised to strike an orbiting satellite would likely be very different from one intended to destroy hardened and deeply buried targets. Likewise, neither of these weapons would be very useful for taking out a target in cyberspace whose physical location was unknown.

The definition also reflects the team's second conclusion: a weapon alone is insufficient to accomplish the global strike mission. As *Multi-Service Tactics, Techniques, and Procedures for Targeting Time-Sensitive Targets* confirms, four of these six processes (e.g., Find, Fix, Track, and Assess, but not Target or Engage) rely heavily on intelligence, surveillance, and reconnaissance (ISR) capabilities.[3] In other words, our definition acknowledges that a global strike weapon without the supporting ISR capability is comparable to a lion without sight, hearing, and smell: the gazelle need not fear such a lion despite its razor-sharp teeth and claws.

Violent Non-State Actors – Are They Relevant To Global Strike?

Are VNSAs a viable target for global strike? The scope of the above definition (e.g., *any target*) clearly includes the full spectrum of non-state entities, ranging from large organizations that exhibit state-like behavior such as Hamas and Hezbollah, to large terrorist networks such as al Qaeda and Abu Nidal Organization, to criminal groups such as the Medellín Cartel, to the

[3] Maj Gen Robert W. Mixon, et al., *Multi-Service Tactics, Techniques, and Procedures for Targeting Time-Sensitive Targets* (Ft Monroe, VA: U.S. Army Training and Doctrine Command), April 2004, I-3. http://www.alsa.mil/library/mttps/tst.html.

"evil genius" – an individual empowered through technology with vast destructive capability. The scope also includes VNSAs consisting partially or entirely of American citizens and those composed of citizens of allied nations, in addition to the citizens of America's sworn enemies.

More importantly, such groups have proven to be a threat to U.S. national security, as reflected in President George W. Bush's speech to the U.S. Military Academy on 1 June 2002. In it, Bush stated that "the gravest danger to freedom lies at the crossroads of radicalism and technology" and "even weak states and small groups could attain a catastrophic power to strike great nations."[4] The President's statement reflected the sudden awakening to the dangers posed by the growing global network of VNSAs that the 9/11 terrorist attacks had caused: in a single day, 19 al Qaeda hijackers successfully transformed four civilian airliners into cruise missiles, resulting in 2,996 deaths and the destruction of U.S. infrastructure worth $16.2B.[5]

Although perhaps the most infamous attack, 9/11 hardly qualifies as a singularity. It was not the first such attack conducted against the U.S. by a VNSA (e.g., the 12 October 2000 bombing of the USS Cole in the port of Aden, Yemen that killed 17 U.S. sailors; the 26 February1993 truck bomb at the World Trade Center; the 19 April 1995 bombing of the the Alfred P. Murrah Federal Building in downtown Oklahoma City that killed 168 people, including 19 children; the 25 June 1996 truck bomb in Dhahran, Saudi Arabia, that nearly destroyed the Khubar Towers housing facility and killed 19 U.S. military personnel; and the 7 August 1998 bombing of the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania,

---

[4] George W. Bush, *United States National Security Strategy* (Washington, D.C.: The White House), 2002, 13. http://merln.ndu.edu/whitepapers/USnss2002.pdf.

[5] According to analysis conducted for the Naval Postgraduate School's Center for Contemporary Conflict, the value of physical assets destroyed on 9/11 "was estimated in the national accounts to amount to $14 billion for private businesses, $1.5 billion for state and local government enterprises and $0.7 billion for federal enterprises [totaling $16.2 billion]. Rescue, cleanup and related costs have been estimated to amount to at least $11 billion for a total direct cost of $27.2 billion." Richard Looney, *Strategic Insight: Economic Costs to the United States Stemming From the 9/11 Attacks* (Monterey, CA: Naval Postgraduate School), 5 Aug 2002, 2. http://www.hsdl.org/?view&did=1459.

that killed 301 people, including 12 Americans), nor was it the most recent (e.g., the anthrax letter attacks that followed 9/11, killing two postal workers and putting hundreds at risk through exposure to the deadly virus and costing billions in cleanup and prevention; and sniper attacks in late 2002 that killed 13 people and injured another three in Louisiana, Alabama, Maryland, Virginia, and Washington, D.C.). In fact, the Heritage Foundation reports that at least 40 such attacks have been foiled since 9/11, including attempts to explode a radiological bomb in the U.S.; blow up the Brooklyn Bridge and Sears Tower; destroy inflight airliners; attack financial institutions in New York, New Jersey, and Washington, D.C.; attack petroleum infrastructure in New York, New Jersey, and Wyoming; and attack a variety of shopping malls, Jewish schools, and synagogues.[6]

Further, such groups appear to be growing in numbers and influence in today's globally-interconnected world. One example of their growing dominance is the state-like roles that groups like Hezbollah, Hamas, and the Taliban now play in Lebanon, Palestine, and Afghanistan, respectively. Regarding the bulging numbers, Itamara Lochard, Senior Researcher at the Fletcher School of Law and Diplomacy, has documented over 1,700 active non-state armed groups in existence today with membership exceeding 1,000 members.[7] In a similar study, the Federation of American Scientists identified 387 such organizations capable of challenging the host state's "monopoly on the use of violence within a specified geographical territory."[8]

---

[6] James J. Carafono & Jessica Zuckerman, *40 Terror Plots Foiled Since 9/11: Combating Complacency in the Long War on Terror* (Washington, D.C.: The Heritage Foundation), 2011, 1. http://www.heritage.org/research/reports/2011/09/40-terror-plots-foiled-since-9-11-combating-complacency-in-the-long-war-on-terror.

[7] Itamara Lochard, *About Us – Research.* (Medford, MA: Tufts University's Fletcher School of Law and Diplomacy), 2011. http://fletcher.tufts.edu/ISSP/About_Us/Lochard.

[8] Phil Williams, "Violent Non-State Actors and National and International Security," *International Relations and Security Network*. (Zurich, Switzerland: Swiss Federal Institute of Technology), 2008, 4. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=93880&lng=en.

Furthermore, Dr. Phil Williams, an expert on VNSAs, predicts the number of such groups will continue to grow over the next several decades.[9]

Admittedly, a large percentage of these groups could be excluded from consideration because they are located in faraway countries, they focus on local or regional issues, or they lack the means or motive to execute such a strike against the U.S. homeland. However, as the 19 hijackers demonstrated on 9/11, neither large numbers nor conventional arms are needed to conduct an effective strategic attack against America. Suffice it to say that dozens, perhaps hundreds, of entities – ranging in size from individuals to groups with thousands of members – currently possess the desire, if not the capability, to do grave harm to the U.S.

As nuclear, biological, chemical, computational, electromagnetic and nanometric technologies continue to advance at exponential rates over the next 25 years, even those VNSAs who currently lack the means may well possess the destructive capability of today's nation-states by 2035. Clearly, a capability of this caliber constitutes a viable security threat to the U.S. Thus, any new global strike capability fielded in 2035 should be capable of addressing the full range of NVSAs.

Let's Play Hide & Seek…You're It!

According to *Air Force Doctrine Document (AFDD) 3-60,* The first step in the F2T2EA process is "the Find phase [which] involves ISR detection of an emerging target…[t]he result of the Find phase is a probable target nominated for further investigation and development in the Fix phase."[10] This phase is sensor-intensive, relying on some signal or output from the potential target to exceed a certain threshold or "noise floor."

[9] Ibid.
[10] Anderson, *AFDD 3-60*, 50. See also *Multi-Service Tactics, Techniques, and Procedures for Targeting Time-Sensitive Targets*, I-4, which offers a similar definition.

To illustrate the concept of a noise floor and how to exploit it, consider how a stealth aircraft avoids radar detection. As anyone who has seen a stealthy aircraft knows, the aircraft itself is not invisible to the human eye; nor is it invisible to the pulses of electromagnetic energy emitted by radar trackers. Rather, stealth works by minimizing the energy reflected back to the tracking radar. This is accomplished by a variety of techniques, such as absorbing the energy within carbon composite components of the aircraft and reflecting it in other directions. Nevertheless, some of the energy is reflected back to the tracking radar. Since other things in the vicinity of the radar (e.g., terrain, trees, buildings, cars, etc.) are also reflecting energy back at it, the system ignores signals below a certain threshold; otherwise the display would be littered with dozens of false targets. As long as the reflected energy from the stealthy aircraft remains below that threshold (a.k.a., the "noise floor"), the radar will not establish a track file on the aircraft and the radar operator will not see a blip on his screen where the aircraft should be. However, if the aircraft continues towards the radar, it will eventually reach a "burn-through" range where the reflected energy exceeds the radar's noise floor, causing the system to establish a track file on the aircraft and place a radar blip on the display. Pilots of stealth aircraft plan their missions to stay outside this burn-through range so that their radar signature stays below the tracking radar's noise floor.

Likewise, a VNSA can break the first link of the kill chain by simply staying below the noise floor of the collective ISR system. Osama bin Laden successfully evaded detection by the U.S. intelligence community for over 10 years by altering his tradecraft to minimize his emissions. He carefully avoided the use of cellular or satellite phones, relying instead on letters, videotaped messages, trusted agents, and personal meetings to communicate to other members of his terrorist network. He only associated with a very small circle of individuals that he trusted.

Admittedly, these measures did limit his autonomy and his ability to orchestrate a second 9/11, and America did ultimately find and kill him. Nevertheless, for 10 years, he was able to continue developing dastardly plans to harm our country.

Will such evasion be possible in the globally interconnected environment of 2035? Admittedly, the answer to such a question is highly speculative, but examining recent technological trends, in conjunction with futurist literature, can guide such speculation. One can reasonably assume that computational capability, which has already transformed modern society, will continue to grow for the foreseeable future at similar rates. This means that computational power would continue to double every 18 months, in accordance with Moore's law,[11,12] while the cost of a transistor declines by half in approximately the same timeframe.[13] Based on these growth rates, one futurist, Michio Kaku, predicts that by 2035 much of the world will have entered the era of "ubiquitous computing," where computer chips have become "so cheap and plentiful that they would be scattered throughout the environment – in our clothing, our furniture, the walls, even our bodies. And they would all be connected to the Internet, sharing data."[14] Another futurist, Ray Kurzweil, predicts that scientists will have designed "learning computers" with "intelligence indistinguishable from that of biological humans" prior to 2030.[15] Such computers, which would be capable of mimicking the pattern recognition capabilities of the human brain, will be essential to sort through the mounds of ISR data available in 2035.

---

[11] Michio Kaku, *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100* (New York: Doubleday), 2011, pg 20.

[12] Kurzweil's analysis shows a slightly slower rate of increase, with computational performance – measured in instructions executed per second – doubling every 1.8 years. Ray Kurzweil, *The Singularity is Near: When Humans Transcend Biology* (New York, NY: Penguin), 2005, pg. 64.

[13] Ibid, 59. The average transistor price is halved aver 1.6 years (or 19.2 months). He proposes "microprocessor cost per transistor cycle," which is halved is every 1.1 years, as a "more accurate measure of price-performance because it takes into account both speed and performance" (62).

[14] Kaku, *Physics of the Future*, 20.

[15] Kurzweil, *The Singularity is Near*, 25. The author forecasts the development of software models that can mimic man's brain by the mid-2020s, and computer systems fully capable of emulating human intelligence before 2030.

As computer chips become cheaper, more ubiquitous, and more interconnected, the amount of data available to analysts will continue to grow exponentially. Kurzweil indicates the amount of data traffic on the Internet has "doubled every year" since 1990, which has also required exponential growth in the data transmission speed of the Internet backbone.[16] Even scientific knowledge "is exploding exponentially around us," doubling "every decade or so."[17] With millions – perhaps billions – of interconnected microchips embedded in everything from sofas to socks to skin, with each chip broadcasting to the 2035 equivalent of the Internet, one can easily imagine how such a growth trend in data might be sustained, or even accelerated.

This means that the intelligence community's challenge of sorting through these mounds of data to find a target of interest will be exacerbated by the fact that Internet traffic is increasing at a faster rate than computer processing power. With Internet traffic doubling every 12 months, compared to every 18 months for processor power, this difference may seem small at first glance; however, a more thorough analysis reveals that the mound of Internet data for analysts to sift through will have grown over 200 times more than processing capability by 2035.[18] In other words, although ISR analysts in 2035 will have far more computational horsepower for searching for the proverbial needle in the haystack, the amount of hay to sort through will have grown so much that the net effect may well be a *decreased* capability to find the needle – the challenge of finding VNSAs could be 200 times more difficult in 2035 than it is today.[19]

The VNSA can further decrease his probability of detection through a number of protective actions. The most significant action would be to simply stay off the cyber grid, at

[16] Ibid, 80-81.
[17] Kaku, *Physics of the Future*, 10.
[18] Since the amount of Internet traffic is doubling every year, it will double 23 times between 2012 and 2035. Since processor power is doubling every 18 months instead of 12, it will only double 15.333 times in the same period. That means Internet traffic will be 2^{23} or 8,388,608 times larger than it is today, whereas computational power will only be $2^{15.333}$ or 41,285 times larger. The ratio of increased Internet traffic to increased processor power is 8,388,608/41,285 or 203.2.
[19] See *Appendix A – The Shrinking Haystack Scenario* for additional discussion on this issue.

least for any nefarious activities. This will likely be much harder to do in the ubiquitous computing environment of 2035, but not impossible. To assume that tech-savvy criminals will be incapable of circumventing such chips would be the height of naivety. Such criminals might disable the broadcast capability of the chips, or disable the chips entirely by exposing them to microwaves or other forms of electromagnetic energy. Alternatively, they may physically block or electronically jam the chip's transmitters, preventing a connection to the grid. Another option would be to simply buy certified "chip-free" products, which, ironically, could become the premium products in stores around the world as consumer concerns about privacy grow.[20]

By 2035, video coverage of most urban areas is also likely to be ubiquitous. Video feeds from traffic cameras, ATM machines, private security systems, personal laptops, and cell phones will likely all be interconnected with the grid and made available to ISR analysts for review. These data streams will be augmented by high-resolution global coverage from satellites and air vehicles, creating an environment akin to that seen in many science fiction movies, where the government is able to remotely observe the bad guy's every activity.

However, even in the movies, the first step is determining *who* to track. Today, law enforcement and intelligence specialists do that by surveilling suspects – both visually and electronically – and establishing a network of contacts, which are subsequently investigated to establish further interconnections. By 2035, computers with advanced facial recognition capabilities will be able to assist with building these connections and identifying the members of the various criminal and terror networks. Conceivably, such computers could use the various video streams to autonomously track a suspect, identify any "person of interest" that the suspect comes in contact with, and then track the new person of interest. Using the large volumes of

[20] Although retailers such as Wal-Mart may want to track a consumer's every movement through their store to optimize marketing advertisements to the consumer's tastes, the consumer may not want to be tracked, and may pay extra to avoid it.

historical video stored on the grid, analysts would also be able to work backwards in time to observe behavior and build a contact list for the new suspect. Likewise, analysts could also leverage historical video to work backwards from a significant event to determine who might have been in the area prior to the event and to identify places that these individuals frequented. Analysts have already leveraged similar "point of origin" capabilities – albeit on a far more rudimentary level – in support of counterinsurgency operations in Iraq and Afghanistan, for example, to identify insurgents responsible for implanting improvised explosive devices.[21] Unfortunately, the lack of ubiquitous video makes this a more difficult problem for today's analysts.

Ironically, the sheer volume of video data generated by the various sources listed above also creates a challenge in finding tomorrow's VNSAs. Although this data clearly benefits the government once a member of the VNSA has been flagged, it benefits the VNSA prior to the flagging. Like the volumes of computer data described above, the mounds of video become the background noise in which the VNSA can hide. As long as the VNSA keeps the signature of his nefarious activities below the noise floor, he will be out-prioritized by other, less-circumspect criminals.

As noted earlier, the size of a VNSA can vary from very large groups to very small ones. For the purposes of evasion, smaller groups will generally have an advantage over larger ones since smaller groups will tend to have smaller emissions that can be flagged by the government. The ideal extreme would be the "evil genius" or a lone assassin, whose signature would likely be kept to an absolute minimum through polished tradecraft.

Admittedly, a major difficult for the VNSA in this environment becomes doing anything productive (e.g., raising funds for an operation, recruiting new followers, or actually conducting

[21] Anderson, *AFDD 3-60*, 52.

an attack) without first being flagged as a person of interest. Relocating to isolated mountains or dense jungles may help prevent detection, but doing so would likely hinder the group's ability to harm the U.S. and its allies. Keeping a group small could likewise help avoid detection, whereas a large hierarchical group increases the probability that some member of the group will be flagged, enabling the eventual identification of the other group members. Thus, the "evil genius" – who can plan and execute his attack with minimal assistance from others, and who understands the detection measures and how to circumvent them – perhaps poses the most lethal non-state threat since he is most likely to stay below the detection noise floor while planning his attack.

Obviously, a VNSA's best defense from global strike is to simply avoid detection, thereby breaking the first link in the F2T2EA kill chain. However, the projected advancements in computational and surveillance capabilities make it unlikely that a future VNSA in an urban area can remain invisible indefinitely, unless he forswears illicit behavior – in which case, the U.S. has effectively won by deterring aggression. In the more likely scenario where the VNSA remains committed to his cause, his probability for success is directly dependent on speed. For the evil genius, this means developing his weapon – whether it consists of a cyber-attack against America's banking system or an unmanned aircraft to deploy an aerosolized bio-agent over the superdome – in a disconnected, isolated environment, and not going online until the last possible moment.

What happens after detection? Per AFDD 3-60, the potential target is placed into one of the following four categories once the noise floor has been penetrated: 1) probable time-sensitive target, 2) probable non-time-sensitive target, 3) not a target, or 4) unknown; the lower the number, the higher the target priority and the higher the amount of resources dedicated to

neutralizing it.[22] Having failed to remain undetected, the VNSA's next opportunity to evade attack is by being classified as a non-target or an unknown. This can perhaps be accomplished by camouflaging one's activities to look non-threatening. For instance, the VNSA that disguises its activities as farming is less likely to be questioned about buying large quantities of diesel fuel and fertilizer.

So You Found Me … But Can You Fix Me?

Now consider the actions a VNSA might employ to break the next link in the F2T2EA kill chain once he has penetrated the noise floor and been identified as a probable target. According to *AFDD 3-60*, the second step in the kill chain is the Fix phase, where the targeting cell "positively identifies an emerging target as worthy of engagement and determines its position and other data with sufficient fidelity to permit engagement."[23] During this phase, decisions must be made about the prioritization of assets, i.e., does the new person of interest appear to merit the reprioritization of limited resources, or should those resources remain focused on previously-tagged targets? Advancements in sensor technology and data links have already enabled the integration of data from various non-traditional platforms (e.g., targeting pods on fighter aircraft or seeker video from the weapon itself), yielding a "common operating picture that commanders can use to shorten the F2T2EA cycle."[24] Today, this trend is also helping to alleviate resource bottlenecks. By 2035, most – if not all – aircraft and weapons will likely contain similar sensors. This capability, combined with the ubiquitous video environment described above, will make it difficult for the "evil genius" to break this link in the kill chain once he has been flagged as a potential target.

[22] Anderson, *AFDD 3-60*, 50.
[23] Ibid, 51.
[24] Ibid.

One potential wildcard in this cat-and-mouse game is the result of directed energy research efforts currently underway at various laboratories around the globe. If high-powered microwave or electromagnetic pulse weapons become viable by 2035, VNSAs could employ such devices to damage the electronics in the tracking sensors. The U.S. Navy is already employing early prototypes of this technology to fry the electronics in improvised explosive devices.[25] However, Doug Beason, a noted physicist at Los Alamos National Laboratory, predicts these systems are still "decades away" from becoming fully operational: current versions are too bulky, require "a cadre of researchers" to operate, and possess very limited range.[26] Another option from the directed energy family would be to utilize lasers to dazzle, or perhaps destroy, the sensor. According to defense journalist Vago Muridian, China demonstrated a prototype of this capability as early as September 2006 when it "fired high-power lasers at U.S. spy satellites flying over its territory in what experts see as a test of China's ability to blind the spacecraft."[27]

An evader might also leverage cyber tools to break the "Fix" link in 2035. Although attacks against the data fusion center would likely encounter strong firewalls, sensors and related components would likely be more vulnerable. Cyber tools could remotely override the camera controls, enabling the evader to change the units viewing angle, field of view, or focal length, or simply power off the unit. Depending on how the cameras are networked, malicious code, denial of service attacks, or even radio-frequency jamming could be employed to disrupt the link between the cameras and the router, or the link between the router and the data fusion center.

---

[25] Doug Beason, *The E-Bomb: How America's New Directed Energy Weapons Will Change the Way Future Wars Will be Fought* (Cambridge, MA: Da Capo), 2005, 184.
[26] Ibid.
[27] Vago Muradian, "China Attempted to Blind U.S. Satellites with Laser," *Defense News*, 28 September 2006. http://www.infowars.com/articles/science/china_attempt_blind_us_satellites_with_lasers.htm.

Track Me If You Can

According to *AFDD 3-60*, the third step in the kill chain is the Track phase, where the targeting cell maintains track on the confirmed target, while weaponeers determine the desired effect against it.[28] Much like the Fix phase, this is a sensor-intensive process, and assets may need to be reprioritized to maintain track on the target. If track continuity is broken, the Fix phase – and possibly the Find phase – must be reaccomplished. In today's battlefield, where video coverage is spotty, an insurgent might plan his activities to exploit blind spots in terrestrial camera coverage or trees and buildings that obscure Predator video imagery. However, in the ubiquitous video environment of 2035, evasion would be far less simplistic. The evader could again employ the advanced technologies described above for breaking the "fix" link at this point.

However, the fact that the U.S. has already completed the Fix phase implies something more creative is required. One potential option here is the employment of denial and deception techniques using body doubles, as reportedly employed by Saddam Hussein[29] and his eldest son Uday,[30] among others. Even such western leaders as George Washington, Franklin Roosevelt, and Winston Churchill are believed to have used doubles, albeit for convenience more than security.[31] Admittedly, this has become much more difficult to do over the last few decades as images and sound clips of world leaders have become more prevalent and tools for comparing these multimedia products more sophisticated.[32] Since this trend will almost certainly continue over the next 25 years, viable body doubles will likely require surgical alteration to evade even

---

[28] Anderson, *AFDD 3-60*, 51-52.
[29] Hussein was considered a "master of deception," with "as many as 16 doubles" by one estimate. Liz Doup & Kathleen Kernicky, "Who's That Hussein, And Other Decoy Games," *South Florida Sun-Sentinel* (Fort Lauderdale, FL: Tribune Newspapers), 22 March 2003. http://articles.sun-sentinel.com/2003-03-22/lifestyle/0303210416_1_human-decoys-high-powered-media-technology-body-doubles.
[30] Carla Buzasi, ed., "Latif Yahia, Uday Hussein's Body Double, Asks Western Governments To Stop Supporting Dictatorships," *Huffington Post*, 10 August 2011. http://www.huffingtonpost.com/2011/08/10/latif-yahia-uday-hussein-body-double_n_923866.html.
[31] Doup & Kernicky, "Who's That Hussein, And Other Decoy Games."
[32] Ibid.

real-time comparative algorithms. The ultimate body double of the future would be a genetic clone, capable of passing not only voice and video comparisons, but also DNA and fingerprint; however, the challenge with this approach would be accelerating clone aging to match the original's appearance.

Other forms of denial and deception could be orchestrated through the cyber world. Rather than creating genetic clones, a less radical approach to defeating DNA and fingerprint analyses would be to track down all digital copies of this information, hack into the appropriate servers, and replace the files with those of the body double. Alternatively, one could create hundreds of similar digital personas that amalgamate the biometric data from dozens of people so that, for instance, a fingerprint sample is tied to not one but perhaps 50 different people scattered around the globe. Conflating the data in this manner would, in effect, create even more hay in which to hide the needle. A third approach would be to employ a "botnet," consisting of hundreds of computers that have been silently coopted using malicious code, to fabricate the digital footprints of other, higher-priority persons or events, thereby forcing the reprioritization of tracking resources. Rather than adding more hay to the pile, this approach adds more needles. The challenge to any of these cyber approaches would be avoiding detection and eliminating any digital footprints that might otherwise result in the restoration of the data using an earlier archived copy.

Target Me If You Dare

According to *AFDD 3-60*, the Target phase begins once the target has been "identified, classified, located, and prioritized"; the objective of this phase is to finalize the desired effect and targeting solution against it; and to obtain approval to strike.[33] During this process, the target

[33] Anderson, *AFDD 3-60*, 52.

must be assessed for collateral damage potential, in addition to compliance with the combatant commander's rules of engagement and the laws of armed conflict. In a complex targeting scenario, this phase is often the lengthiest "due to the large number of requirements that must be satisfied."[34]

A clever VNSA will choose a base of operations that complicates and delays the target approval process. Basing operations in a sovereign country, preferably one that dislikes the U.S., is one way to delay the approval process. Al Qaeda successfully demonstrated this tactic, first in Afghanistan, where the organization was able to operate with near-impunity until the 9/11 attacks, and later in Pakistan, where tenuous relations between Washington and Islamabad, combined with Pakistan's nuclear arsenal, tempered U.S. zeal for attacking terrorist training sites. A host country with a strong military would also help to delay the target approval process, since the host might take exception to a U.S. violation of its territorial sovereignty.

Savvy VNSAs might also base their operations in a location that increases the probability of collateral damage. Such damage often engenders anti-U.S. sentiment among the local populace while creating tension between heads of state, as recent events in Pakistan depict. According to *The Economist*, relations between Washington and Islamabad have become "deeply troubled by the issue of drones," with General Ashfaq Kayani, Pakistan's Chief of Army Staff , calling the strike a "complete violation of human rights."[35]

Another option available to the VNSA in a last-ditch effort to avoid attack is deterrence. One might threaten to employ nuclear, biological, chemical or other doomsday weapons against the local populace in order to deter a U.S. attack. Alternatively, he might threaten a cyber-attack against U.S. power grids, the banking system, or other pillars of American economic strength.

---

[34] Ibid.

[35] Daniel Franklin, ed., "Out of the Blue: A Growing Controversy Over the Use of Unmanned Aerial Strikes," *The Economist*, 30 July 2011. Available at: http://www.economist.com/node/21524916.

Richard A. Clarke, counterterrorism advisor to three previous presidents, claims that logic bombs – malicious code capable of frying the circuits inside power transformers – have been found "all over our electric grid."[36] Clarke also described the financial sector as "particularly vulnerable," and ill-prepared to cope with attacks that might shred financial data, causing "unimaginable damage to the economy."[37] Even the 2010 *National Security Strategy* acknowledges that such threats are among "the most serious national security, public safety, and economic challenges we face as a nation."[38] Clearly, the U.S. would think twice before striking an enemy capable of executing such attacks.

Finally, any delay in the target approval process gives the VNSA an opportunity to initiate an information campaign. Such campaigns could be tailored to tilt local, regional, or international opinion away from the U.S. They might also be used to create a strategic distraction and domestic political backlash against U.S. leaders. Al Qaeda has already demonstrated that a VNSA can beat us at our own game in this arena. Their sophisticated production companies have produced "high-quality videos…rigorously evaluated for quality control," employing "cutting-edge techniques" that reveal "political savvy and an ability to capitalize on rapidly changing circumstances." [39] Portraying themes of "injustice, suffering, humiliation and the presence of foreigners in Muslim lands," al Qaeda has proven masterful in crafting messages that resonate with its audience.[40]

---

[36] Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security* (New York: Harper Collins), 2010, 92.
[37] Ibid, 114.
[38] Barack H. Obama, *National Security Strategy* (Washington, D.C.: The White House), 2010, 27. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.
[39] James P. Farwell, "Jihadi Video in the 'War of Ideas,'" *Survival*, vol. 52 no. 6, December 2010–January 2011, 132. http://dx.doi.org/10.1080/00396338.2010.540787.
[40] Ibid, 143.

Shoot Me If You Must

During step five of the F2T2EA process (i.e., Engage), the target is confirmed as a "hostile" and the operator is authorized to engage, ideally resulting in "successful action against the target."[41] At this point the U.S. will have completed its cost-benefit analysis and determined that the target is simply too valuable not to strike, despite violations of sovereignty, risk to collateral damage, and threats of counterattacks.

At this point, the non-state actor's options are few, particularly if the weapon of choice is a circa-2035 hypersonic missile. Such weapons, which are now entering early conceptual testing, offer the ability to strike any location on the globe in about an hour. Because of their speed, these weapons would be difficult to defeat with traditional anti-aircraft countermeasures.

One potential option that may be available to non-states in 2035 is deeply buried facilities. Hezbollah has already proved that this is a viable option for VNSAs – at lease for a larger one: in preparation for its 2006 conflict with Israel, the group constructed nearly 600 underground bunkers, some as deep as 130 feet below ground.[42] Advances in concrete formulations and excavation equipment should make hardened, deeply buried bunkers a viable option for smaller VNSAs by 2035.

Okay, You Got Me…Or Maybe Not

In the final step of the F2T2EA process (i.e., Assess), ISR assets are employed to "collect information about the engagement…to determine whether desired effects and objectives were achieved" and to determine whether additional strikes are needed to achieve the desired effect on

[41] Anderson, *AFDD 3-60*, 52.
[42] Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: Combat Studies Institute), 2008, 19.

the target.[43] Even at this point in the process, the savvy VNSA may still have a few cards to play. In the "evil genius" scenario, if the genius survived, he may want to fabricate physical and/or digital evidence indicating otherwise. Alternatively, once safely out of danger, he may want to provide proof of survival as part on an information operation depicting the impotence of America. In the case where the strike terminated the genius, others may want to destroy or discredit evidence of the kill so that they can coopt the genius' persona. Such actions would make confirmation difficult, and perhaps impossible.

Larger non-state groups would also need to assess the impact of the strike, and respond accordingly. This would include reviewing the impact of personnel losses on their organization. Were the victims the leaders of the movement, or merely the drones? Was anyone captured alive who may be able to compromise other personnel or future operations? Herein lies the advantage of a cellular organization, in which each member can only identify a handful of other members and is only familiar with a few upcoming missions.

They may also conduct an information campaign to further their cause. This could include exploiting any collateral damage to shift worldwide opinion in their favor. As in the case of the evil genius described above, they may want to provide "proof of life," showing the attack did not kill the group's leaders. If the attack was successful, they may want to fabricate this proof. As web searches on such topics as "Osama lives," "9/11 conspiracy," or "alien abductions" prove, a certain segment of the population readily accepts nearly any fringe conspiracy based on the flimsiest of data; VNSAs can leverage this acceptance to keep their cause alive following the loss of a key leader.

Finally, these groups might adapt to better thwart future attacks. This might include going underground – literally and figuratively – until U.S. priorities shift to other targets.

[43] Anderson, *AFDD 3-60*, 52.

Alternatively, they might shift to a more cellular vice hierarchical structure to reduce the likelihood of compromising the identities or locations of large portions of the group. A third possibility would be to strengthen the group by forming alliances with other groups. Anecdotal evidence includes examples of alliances between enemies and competitors, as well as alliances between different types of groups, such as between criminal gangs and terrorist groups. [44] In extreme situations, the group may even change its primary focus to remain viable. The *Fuerzas Armadas Revolucionarias de Colombia* (FARC), for instance, entered the cocaine business to fund its leftwing insurgency operations; today, the FARC is a major drug-trafficker that "in some regions, [now] cooperates with former rightwing paramilitary organizations turned drug traffickers."[45]

Conclusions & Implications

The above analysis revealed no guaranteed formula enabling the VNSA to permanently *defeat* the F2T2EA kill chain in 2035, aside from foreswearing violence altogether. However, *delaying* the process does appear to be a viable strategy, despite the ubiquity of interconnected computers and sensors in 2035. The most effective strategy is to avoid the initial detection altogether. Because the amount of available information is growing at a faster rate than the computing capacity to process this information, resources dedicated to culling that information will necessarily be focused on people who have already been flagged as a potential threat, as well as certain actions deemed to be potentially threatening, e.g., purchasing large quantities of fuel and fertilizer – common ingredients in homemade bombs, including the one used in the 1995

[44] Douglas Farah, "Terrorist-Criminal Pipelines and Criminalized States," *Prism 2 # 3* (National Defense University Press), June 2011p. 17.
[45] Phil Williams, "Violent Non-State Actors and National and International Security," 4.

Oklahoma City bombing.[46] In our day, Osama bin Laden proved that the world's most hunted man could evade detection by the intelligence community for over 10 years. Imagine how much easier evasion might be for someone not already on the Federal Bureau of Investigation's list of "Ten Most Wanted Fugitives."[47]

The savvy VNSA will devise clever methods to sanitize his base of operation from the global web of cameras and computers in 2035, creating an environment where he is safe to plan, prepare for, and perhaps even initiate his illicit activities, while blending into the background noise created the digital personas of billions of interconnected individuals. However, once his signature penetrates this noise floor – either through some action or association with another suspected criminal – evasion becomes a greater challenge. Yes, the VNSA can select a base of operations that slows down the attack approval process due to concerns about sovereignty or collateral damage, and he can employ threats and attacks to temporarily evade the all-seeing eye. However, once found, odds of thwarting U.S. attack indefinitely appear low, especially if the 2035 suspect has been elevated to the "most wanted" level.

The implication of this study is clear: the key to a successful global strike against a VNSA in 2035 is the intelligence that enables the strike, and not the strike weapon itself. Yes, hypersonic cruise missiles, orbital lasers, intercontinental ballistic missiles with conventional warheads, and "rods from God" could all be effectively employed to take out the non-state. The operator will never get to the "Engage" step without ISR; however, with adequate ISR, many of our current weapons would suffice for striking the VNSA. Consider how the U.S. killed Osama bin Laden: not with an armed Predator, not even with a MK-82 "dumb" bomb, but rather with a

[46] Associated Press, "Fertilizer Bomb A Popular Terrorist Weapon," *USA Today*, 14 April 2004. http://www.usatoday.com/news/world/2004-04-14-fertilier-bombs_x.htm.
[47] Federal Bureau of Investigation, *FBI Ten Most Wanted Fugitives List: Usama Bin Laden* (New York), June 1999. http://www.fbi.gov/wanted/topten/usama-bin-laden.

pair of 5.56 mm bullets fired from an assault rifle.[48] Even this mission could not have been accomplished without an intelligence source to align the SEAL team shooter's crosshairs with Osama's cranium.

To enable similar missions in the future, the Air Force must continue to invest in a full spectrum of ISR technologies. In terms of sensors, this means that large constellations of small, inexpensive sensors are preferred over fewer, more-expensive systems since the former offers better redundancy. Multi-spectral and wideband capabilities will decrease sensor susceptibility to single-frequency jamming, e.g., laser dazzling. Terrestrial, airborne, and satellite sensors are all needed to build a robust common operating picture.

In terms of ISR processing, a number of key capabilities merit additional research and development funding. Foremost among these is automated pattern recognition logic. This capability will be vital to shifting a greater percentage of the imagery review from man to machine, since the volume of data available to analysts in 2035 is projected to be nearly 8.4 million times than that of today,[49] while growth in the number of human analysts available to review this data is likely to be comparatively negligible.[50] Data fusion, the ability to integrate

---

[48] Paul Bedard, Paul, "The Gun That Killed Osama bin Laden Revealed," *USA Today* (Online Edition), 11 May 2011. http://www.usnews.com/news/washington-whispers/articles/2011/05/11/the-gun-that-killed-osama-bin-laden-revealed.

[49] Kurzweil, *The Singularity is Near*, 80-81. According to Kurzweil, the amount of data traffic on the Internet has "doubled every year" since 1990. Assuming that the growth rate of Internet data traffic approximates the growth rate of intelligence data, and assuming this growth rate continues through 2035, the amount of intelligence available in 2035 will be 8,388,608 times that of today.

[50] Although "comparatively negligible" is the author's personal opinion, this opinion is based upon concerns such as those voiced by the Washington Post following a two-year investigation into the growth of the intelligence community, which concluded that "[a]fter nine years of unprecedented spending and growth, the result is that the system put in place to keep the United States safe is so massive that its effectiveness is impossible to determine" and that the system "has become so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it or exactly how many agencies do the same work." In the same article, Leon Ponetta, then Director of the Central Intelligence Agency, noted that "the levels of spending since 9/11 are not sustainable," implying that budget *cuts* are more probable scenario, given the $15 trillion national debt. Dana Priest & William M. Arkin, "Top Secret America: A Hidden World, Growing Beyond Control," *The Washington Post* (Washington, DC), 19 July 2010. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control.

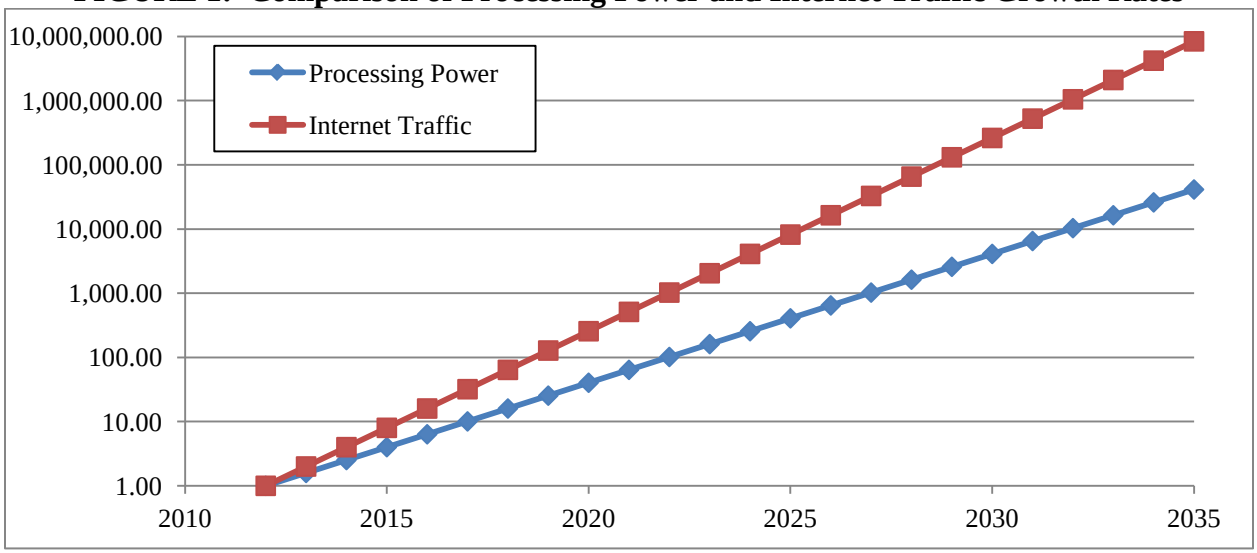
data from a wide variety of sources and spectra into a single common operating picture, also merits continued investment. Finally, data integrity assurance must also be advanced. No matter how much advancement we make in the pattern recognition and data fusion fields, the results generated by the computers of 2035 will only be as good as the source data used to generate those results.

Ultimately the lethality of America's future global strike capability will only be as good as the intelligence sources that provide the target cueing to the strike weapon. Investment in pattern recognition, data fusion, data integrity, and myriad sensor technologies is vital to ensuring the U.S. can find and kill the bin Ladens of 2035. Should our capabilities in these areas stagnate, tomorrow's adversaries will likely develop clever methods to circumvent them.

Appendix A: The Shrinking Haystack Scenario

A key premise in the analysis presented above is that the growth of data will outpace the growth of processing capability. This premise is based upon studies that have shown processor power is doubling every 18 months, whereas the amount of Internet traffic is doubling every 12 months. Although the difference in these rates may seem relatively small, the net effect is that Internet traffic will double 23 times between 2012 and 2035, making it 2^{23} or 8,388,608 times larger than it is today. Although computational power will also grow, it will only double 15.333 times, making it only $2^{15.333}$ or 41,285 times larger than today. Assuming these trends continue through 2035, this means the ratio of increased Internet traffic to increased processor power will 8,388,608/41,285 or 203.2 times greater than today. This concept is presented graphically in Figure 1 below. (Note the vertical axis is a logarithmic scale, where each horizontal line represents an order of magnitude increase in size.)

FIGURE 1: Comparison of Processing Power and Internet Traffic Growth Rates



If this proves to be the case, intelligence analysts may well have a tougher challenge finding savvy VNSAs in 2035 than they do today. If finding the bin Ladens of today is the proverbial equivalent of finding a needle in a large haystack, the challenge of 2035 will be to

find that same needle in a field containing 203 such haystacks. The amount of hay to sort through will have grown so much that the net effect would be a *decreased* capability to find the needle despite having far more computational horsepower to execute the search.

Could this premise prove incorrect? Absolutely! Perhaps a quantum leap in computer processing power, pattern recognition, or artificial intelligence occurs, shrinking the growth rate of the haystacks. Such developments might even shrink today's single haystack. However, as long as any hay remains, the VNSA still has a potential of escape. Only when all the straw is gone does Osama's protégé cease to have a prayer of evading America's global strike capability.

Ultimately, the actual value of ratio – whether it be 200:1, 1:1, or 1:200 – is somewhat academic with regard to the conclusion of this paper. Osama's 10-year evasion proves today's ISR capabilities have gaps. Whether those gaps grow or shrink and the rate with which they change will be a function of the actions taken between now and 2035. Thus, the Air Force should still continue to invest in the ISR capabilities recommended above as these investments are crucial to inching us closer to the quixotic scenario where the fog of war is lifted and our intelligence is all-knowing.

References

Anderson, Thomas K., et al., *Air Force Doctrine Document (AFDD) 3-60: Targeting* (Montgomery, AL: Lemay Center), 28 Jul 2001. http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-60.pdf. (Accessed 21 January 2012).

Associated Press, "Fertilizer Bomb A Popular Terrorist Weapon," *USA Today*, 14 April 2004. http://www.usatoday.com/news/world/2004-04-14-fertilier-bombs_x.htm. (Accessed 21 January 2012).

Beason, Doug, *The E-Bomb: How America's New Directed Energy Weapons Will Change the Way Future Wars Will be Fought* (Cambridge, MA: Da Capo), 2005.

Bedard, Paul, "The Gun That Killed Osama bin Laden Revealed," *USA Today* (Online Edition), 11 May 2011. http://www.usnews.com/news/washington-whispers/articles/2011/05/11/the-gun-that-killed-osama-bin-laden-revealed. (Accessed 21 January 2012).

Belasco, *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11*, (Washington, DC: Congressional Research Service), 29 March 2011. http://assets.opencrs.com/rpts/RL33110_20110329.pdf. (Accessed 21 January 2012).

Bush, George W., *United States National Security Strategy* (Washington, D.C.: The White House), 2002. http://merln.ndu.edu/whitepapers/USnss2002.pdf. (Accessed 21 January 2012).

Buzasi, Carla, ed., "Latif Yahia, Uday Hussein's Body Double, Asks Western Governments To Stop Supporting Dictatorships," *Huffington Post*, 10 August 2011. http://www.huffingtonpost.com/2011/08/10/latif-yahia-uday-hussein-body-double_n_923866.html. (Accessed 21 January 2012).

Carafono, James J. and Zuckerman, Jessica, *40 Terror Plots Foiled Since 9/11: Combating Complacency in the Long War on Terror* (Washington, D.C.: The Heritage Foundation), 2011. http://www.heritage.org/research/reports/2011/09/40-terror-plots-foiled-since-9-11-combating-complacency-in-the-long-war-on-terror. (Accessed 21 January 2012).

Clark, Richard A. and Robert K. Knake, *Cyberwar: The Next Threat to National Security* (New York: Harper Collins), 2010.

Doup, Liz & Kernicky, Kathleen, "Who's That Hussein, And Other Decoy Games," *South Florida Sun-Sentinel* (Fort Lauderdale, FL: Tribune Newspapers), 22 March 2003. http://articles.sun-sentinel.com/2003-03-22/lifestyle/0303210416_1_human-decoys-high-powered-media-technology-body-doubles. (Accessed 21 January 2012).

Farah, Douglas, "Terrorist-Criminal Pipelines and Criminalized States," *Prism* 2 # 3 (National Defense University Press), June 2011.

Farwell, James P., "Jihadi Video in the 'War of Ideas,'" *Survival*, vol. 52 no. 6, December 2010–January 2011. http://dx.doi.org/10.1080/00396338.2010.540787. (Accessed 21 January 2012).

Federal Bureau of Investigation, *FBI Ten Most Wanted Fugitives List: Usama Bin Laden*, (New York), June 1999. http://www.fbi.gov/wanted/topten/usama-bin-laden. (Accessed 21 January 2012).

Franklin, Daniel, ed., "Out of the Blue: A Growing Controversy Over the Use of Unmanned Aerial Strikes," *The Economist*, 30 July 2011. http://www.economist.com/node/21524916. (Accessed 21 January 2012).

Kaku, Michio, *Physics of the Future: How Science Will Shape Human Destiny and Our Daily Lives by the Year 2100* (New York: Doubleday), 2011.
Kurzweil, Ray, *The Singularity Is Near: When Humans Transcend Biology* (New York, NY: Penguin), 2005.
Lochard, Itamara, *About Us – Research*, (Medford, MA: Tufts University's Fletcher School of Law and Diplomacy), 2011. http://fletcher.tufts.edu/ISSP/About_Us/Lochard. (Accessed 21 January 2012).
Looney, Robert, *Strategic Insight: Economic Costs to the United States Stemming From the 9/11 Attacks* (Monterey, CA: Naval Postgraduate School), 5 Aug 2002. http://www.hsdl.org/?view&did=1459. (Accessed 21 January 2012).
Matthews, Matt M., *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: Combat Studies Institute), 2008.
Mixon, Robert W., et al., *Multi-Service Tactics, Techniques, and Procedures for Targeting Time-Sensitive Targets* (Ft Monroe, VA: U.S. Army Training and Doctrine Command), April 2004). http://www.alsa.mil/library/mttps/tst.html. (Accessed 21 January 2012).
Muradian, Vago, "China Attempted to Blind U.S. Satellites with Laser," *DefenseNews*, 28 September 2006. http://www.infowars.com/articles/science/china_attempt_blind_us_satellites_with_lasers.htm. (Accessed 21 January 2012).
Obama, Barack H., *National Security Strategy* (Washington, D.C.: The White House), 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf. (Accessed 21 January 2012).
Priest, Dana & Arkin, William M., "Top Secret America: A Hidden World, Growing Beyond Control," *The Washington Post*, (Washington, DC) 19 July 2010. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control. (Accessed 21 January 2012).
Schwartz, Norman A., *Invitation to Participate in the Blue Horizons Program for Academic Year 2012*, 19 May 2011.
Williams, Phil, "Violent Non-State Actors and National and International Security," *International Relations and Security Network* (Zurich, Switzerland: Swiss Federal Institute of Technology), 2008. http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=93880&lng=en. (Accessed 21 January 2012).