AIR WAR COLLEGE

AIR UNIVERSITY

# COUNTER ELECTRICAL GENERATION AND DISTRIBUTION: AN ASSESSMENT FOR GLOBAL STRIKE IN 2035

by

Ansel L. Hills, Captain, USN

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 February 2012

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| | | |
|---|---|---|
| 1. REPORT DATE<br>**15 FEB 2012** | 2. REPORT TYPE | 3. DATES COVERED<br>**00-00-2012 to 00-00-2012** |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>**Counter Electrical Generation And Distribution: An Assessment For Global Strike In 2035** | 5a. CONTRACT NUMBER<br>5b. GRANT NUMBER<br>5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER<br>5e. TASK NUMBER<br>5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**Air War College,Air University,Maxwell AFB,AL,36112** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S)<br>11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
**The Chief of Staff of the Air Force charged the 2012 Air War College Blue Horizon Program to explore the impacts of technological advances on the Air Force?s ability to conduct Global Strike in 2035. Given this topic, this paper delves into whether the Air Force should pursue weapons that would allow the President of the United States to rapidly disrupt electrical generation and distribution (EG&D) systems for the purpose of achieving strategic ends. The scope of the paper encompasses current electrical system technology through technological advances projected through 2035. Using this projection and historical experience from strikes conducted on EG&D systems in major conflicts, the paper concludes that due to advances in energy ubiquity, transparency of information and consequences of volumetric counter electrical system attack that the strategic utility of this kind of attack is greatly diminished in 2035.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | **Same as Report (SAR)** | **36** | |

**Standard Form 298 (Rev. 8-98)**
Prescribed by ANSI Std Z39-18

## DISCLAIMER

# Biography

Captain Ansel LeRoy Hills is a U.S. Navy Information Dominance Corps Information Professional assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from the University of Missouri at Columbia Missouri in 1989 with a Bachelor of Science degree in Mechanical Engineering. He earned his Surface Warfare Officer designation in 1991 and his Information Dominance Corps warfare designation in 2010. He has served aboard various USN aircraft carriers, destroyers, cruisers and flag staffs as a Surface Warfare Officer and at the Navy's central three-star, flag-level network command and control center as an Information Professional.

# Abstract

The Chief of Staff of the Air Force charged the 2012 Air War College Blue Horizon Program to explore the impacts of technological advances on the Air Force's ability to conduct Global Strike in 2035. Given this topic, this paper delves into whether the Air Force should pursue weapons that would allow the President of the United States to rapidly disrupt electrical generation and distribution (EG&D) systems for the purpose of achieving strategic ends. The scope of the paper encompasses current electrical system technology through technological advances projected through 2035. Using this projection and historical experience from strikes conducted on EG&D systems in major conflicts, the paper concludes that due to advances in energy ubiquity, transparency of information and consequences of volumetric counter electrical system attack that the strategic utility of this kind of attack is greatly diminished in 2035.

## Introduction

Expansion of technology from the industrial revolution supporting the information age, best described by Moore's Law, is advancing at exponential rates[1]. This explosion of capability has resulted in an ever-increasing requirement for electrical power around the world. The Department of Energy (DOE) 2011 International Energy Outlook projects that world net electricity generation will "increase by 84 percent … from 19.1 trillion kilowatt hours in 2008 to 25.5 trillion kilowatt hours in 2020 and 35.2 trillion kilowatt hours in 2035."[2] This increase is nonlinear on a global scale with emerging nations experiencing more growth than today's more industrialized countries. For example, India and China's electrical demand is expected to grow at rates of 4.0 percent through 2035, while the rest of the developing world expects to see growth rates of 3.3 percent—substantially higher than the 1.2 percent predicted for today's industrialized countries.[3] With electricity becoming an ever more critical element of industry for commerce, infrastructure, manufacturing and information systems, it is prudent to assess whether disrupting electrical power generation and distribution (EG&D) is an increasingly viable coercive target set for US Global Strike assets in 2035.[i]

To achieve this end, this paper begins by reviewing counter-electrical system operations across previous major conflicts to understand the historical objectives and outcomes of this targeting strategy. Next, it examines the technology future of EG&D systems and the implications of these changes to the infrastructures on three major subcategories of targets, 1) developed nations, 2) developing nations and 3) groups and individuals. The inferences garnered from these three target sets in the future construct are then assayed versus the ability to conduct strike operations via volumetric, physical non-kinetic, electronic non-kinetic (Cyber) and

[i] For purposes of this study, Global Strike is a set of capabilities allowing the President of the United States (POTUS) to respond or pre-empt an act of war; to quickly strike any target, anywhere, in any environment, on demand in order to achieve strategic objectives (deter, force rapid conflict termination and maintain crisis stability)

alternative methodologies. Then, given the fluid nature of predicting the future, a series of signposts are offered to mark major milestones that are harbingers of the new age of EG&D systems. Finally, it concludes by providing a net assessment of the utility of EG&D strike in war fighting given risks and benefits of this type of targeting strategy and their associated effects to determine viability for the attack methodology in future conflicts.

The paper finds that historical attacks on EG&D systems in order to leverage the populace against their governments and/or cause disruption of military capabilities have been generally ineffective. Looking ahead, it finds that although dependence on electrical power will increase dramatically, the application of EG&D technologies will likely result in massive diversity and fractioning of today's electrical grids. This may make targeting these systems more difficult than it is today and drive weaponeering from precision strike to volumetric type weaponry. Volumetric weapons carry the baggage of increased collateral damage and borderline Weapon of Mass Destruction/Weapon of Mass Disruption (WMD) (see Definition Appendix) effects and must be used carefully by the striking force. Having said this, terrorist agents, or states with little or nothing to lose will leverage disruption of EG&D systems in heavily industrialized and communications centric nations for immediate and long lasting gains. Understanding these conclusions begins with understanding the history of attacking EG&D systems in war.

## Historical Analysis

The strategic efficacy of historic EG&D targeting by the US is mixed. To understand why, an analysis begins with a review and assessment of attacks on EG&D systems across five conflicts that have occurred since 1941: World War II (Germany and Japan), Korea, Vietnam, Desert Storm (Iraq) and Allied Force (Kosovo).

Going into World War II air strategists were initially attracted to the EG&D target set, and it ranked high in priority in Air War Plan Division Plan 1 (AWPD 1) and its successor AWPD 42.[4] Pessimistic combat assessments of this targeting strategy versus the German EG&D target set diminished this attraction, however. The lack of weapons precision made EG&D more difficult to target than other more lucrative target sets. The Committee of Operations Analysts came to view Germany's power grid as widespread, diverse and not likely to achieve impact on leadership and military capabilities, although this view changed in hindsight after the war. The United States Strategic Bombing Survey review of EG&D systems in Germany post war found "Had electric generating plants and substations been made primary targets as soon as they could have been brought within range of Allied attacks, the evidence indicates that their destruction would have had serious effects on Germany's war production." [5] Nevertheless, the pessimistic prevailing wisdom on the EG&D target set carried forward into the attack planning against Japan. The following assessment of the efficacy of attacking Japan's electrical target set made by General Arnold's operations analysts typified this line of thinking:

> "The subcommittee's pessimism about the effectiveness of bombing electrical power resulted from the dispersion of the power plants, which lowered the vulnerability of the system and the delay in effecting the military capability of Japan. Based on this report, and perhaps the COA's [course of action's] ambivalence toward electric power based on their German targeting experience, they concluded that, while the electrical power system was vulnerable, it would not be a profitable target overall."[6]

As with targeting in Germany, post war studies suggested this pessimism might have been misplaced. One study noted, "We justified the destruction of 66 largest cities in Japan on the ground that they contained thousands of small shops that could not be isolated and destroyed. Yet every tool in every shop was completely dependent on public electric power."[7]

Despite optimistic, "what could have been" assessments coming out of World War II, the Korean experience highlighted the difficulty of translating EG&D targeting into meaningful military effect. The efforts were poor due to substitution effects and workarounds by the North Koreans. As one author put it, "the North Koreans worked around the power interruptions by staggering shifts at workplaces to take advantage of the power available and buying small generators for mines and manufacturing plants." Moreover, because the North Koreans obtained most of their material from outside the country, primarily Russia and China, the elimination of electricity did little to affect military operations by hampering war production.[8]

The effects generated by attacking EG&D systems in the Vietnam War were similar to those in North Korea: targeting did not translate into effect, particularly in a non-industrialized country. The government allocated limited post-attack power to essential users: important industrial installations, foreign embassies, and selected government buildings in Hanoi.[9] The official USAF bombing survey from Linebacker II highlights the difficulty of totally interrupting all electrical power noting "an air campaign against the electrical power system of a country should not have as an objective the total cutoff of power. All critical elements of military and government agencies have alternate means of generating electric power."[10]

By 1991, the United States had substantially improved its ability to analyze and target EG&D systems. Specifically, the Joint Warfighting Analysis Center (JWAC) in Dahlgren Virginia was created in response to the Iranian Hostage Crisis to meet warfighter needs.[11] Its increased analysis capability was brought to bear when assessing the targeting of Iraq's EG&D systems during the 1991 Operation Desert Storm. While these improved capabilities enabled the United States to degrade the Iraqi power grid severely, this line of operations did little to affect civilian leadership or military capabilities. Instead, it had deleterious effects on the civilian populace. Some studies estimate up to 70,000 deaths were attributable to the secondary effects (contaminated water, lack of sewer systems, hospital power outages) due to loss of power from wartime efforts.[12] This was used effectively in strategic communications by Saddam Hussein to project the cruelty of the attacks on his homeland.

Finally, the April 1999 Allied Force attacks in Serbia and Kosovo targeted EG&D systems intentionally in the hope that the destruction of infrastructure would cause the inner circle of Slobodan Milošević to force the government to sue for peace rapidly. However, it is not clear these attacks had their desired results. Promised to last 3 days, the bombing extended for 11 weeks. EG&D was only one target set of many attacked. Moreover, Milošević capitulated only after Russia withdrew its support. As in Iraq, the loss of electrical power had a major impact on civilians, and it is not clear this impact translated into coercion of the government.[13]

Given this history, the academic literature is almost uniformly negative on the efficacy of widespread strategic of attack on EG&D systems either as a method of command and control disruption or as a method of coercion. Major Thomas Griffith's 1994 critique of Operation Desert Storm's focus on EG&D targets is particularly salient, at least as far as limited wars are concerned:

> "… the indirect effects to civilians in Iraq as a result of the bombing of electric power have raised questions at home and abroad. The official response is that although the attacks were more thorough than planned, they were nonetheless necessary and the postwar suffering of the Iraqi people is the fault of Saddam Hussein. Certainly this is true from the legalistic point of view, for the defender and the attacker both bear an equal responsibility for the protection of civilians; but the practical fact is that the negative impact of these attacks on world opinion far outweighed the military benefits accrued by bombing electrical power in Iraq. The implication is clear—national electrical systems are not a viable target. If the wars of the near future will be limited wars and not total wars of attrition, then attacks on electric power should not be considered. Although national power systems are vulnerable to air attack, the military is largely insulated from a loss of power, and civilian discomfort has not been shown to influence government policy***. If the true aim of eliminating electricity is to affect other systems, such as communications or computers, then the time and effort would be better spent concentrating on the intelligence and methods for attacking these systems***

[emphasis added]. In future strategic air operations, the targeting of national power systems has little utility."[14]

Similarly, Robert Pape argues against punishment-based coercive strategies, like widespread targeting of EG&D systems, maintaining, "Punishment generates more public anger against the attacker than against the target government."[15] Like Griffith, he argues that the military effects of EG&D attacks are of marginal utility, explaining that "since nearly all military and governmental facilities have backup power generation, the loss of electric power mainly shuts down public utilities (water pumping and purification systems), residential users (food refrigeration), and general manufacturing in the economy."[16]

Although the track record of targeting EG&D systems either to degrade military capabilities or coerce government leaders appears wholly negative, it's utility as a target continues to be discussed by strategists for Global Strike. There are several reasons for this continued interest. First, strategists assume electrical power is vulnerable to attack today and will continue to be in the future. This vulnerability is made even more attractive as dependence on electricity grows for the functioning of large societies and as governments move to protect their other strategic capabilities by dispersing them, making them mobile, and in some cases, going underground into hardened deeply buried bunkers.[17] Second, from a defensive standpoint, a widespread disruption of electrical power would have a devastating impact on civilian populations who have become totally dependent on electricity for everything from food, heat, light, transportation, medical logistics, water, sewer, banking and communications as highlighted in William Forstchen's "One Second After"[18]. Accordingly, strategists must ensure that an asymmetry in dependence between two competing powers does not invite an attack. To understand whether EG&D systems may grow in importance for Global Strike in 2035, one must first understand the future direction of EG&D technologies.

## Electrical Grid, Today and Future

Advances in technology across time have slowly evolved EG&D systems with wide variances seen across the globe. The First Industrial Revolution occurred in the 18th and 19th centuries with the advent of steam and press operated literature reproduction, enabling greater literacy via the written form of communication. Followed closely by the Second Industrial Revolution shift to gasoline powered engines and greater ability to make and transmit electricity vaulted electronic communications to the forefront of society. This created the power distribution system commonly seen in developed countries around the world, seen pictorially in Figure 1.

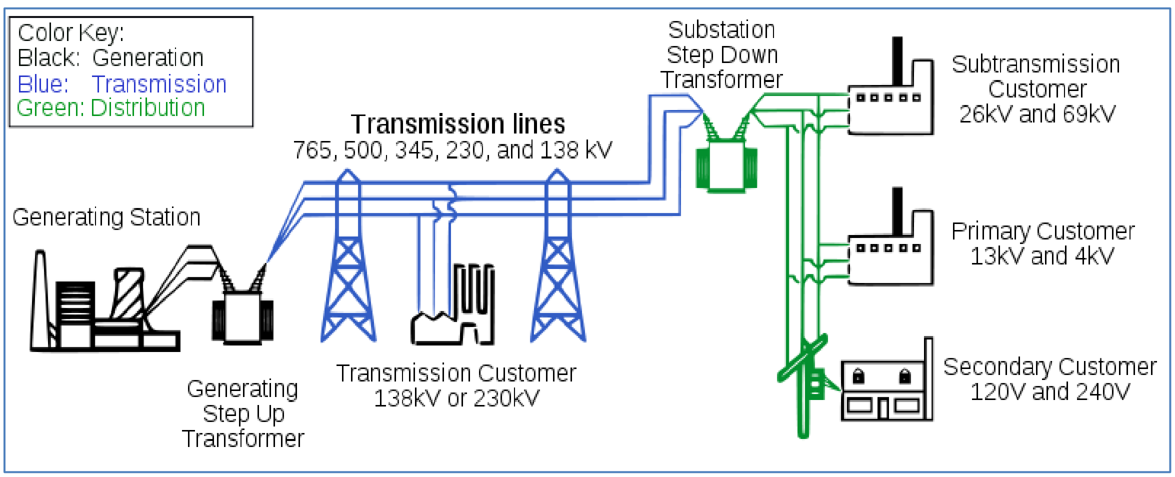


Figure 1: Modern Power Generation and Distribution System[19]

The Third Industrial Revolution (underway now) displays greater diversity of electrical power generation and storage sources, leading away from the traditional generation-distribution-user grid of the Second Industrial Revolution. Specifically, individual buildings and sites will not only generate their own electricity, but they will also store it on site and return it to the grid when needed. The Third Industrial Revolution is made up of the five following pillars as noted in the European Union (EU) Parliament Declaration on Energy and the Economy as

1) Shifting to renewable energy;

2) Transforming the building stock of every continent into micro-power plants to collect renewable energies onsite;

3) Deploying hydrogen and other storage technologies in every building and throughout the infrastructure to store intermittent energies;

4) Using Internet technology to transform the power grid of every continent into an intergrid that acts just like the Internet. When millions of buildings are generating a small amount of energy locally, onsite, they can sell surplus back to the grid and share electricity with their continental neighbors;

5) Transitioning the transport fleet to electric plug in and fuel cell vehicles that can buy and sell electricity on a smart, continental interactive power grid; and the creation of a renewable energy regime, loaded by buildings, partially stored in the form of hydrogen, distributed via smart inter grids and connected to plug in zero emission transport, opens the door to a Third Industrial Revolution."[20]

This revolution, sometimes referred to as the "Energy Internet" is represented by Figure 2.

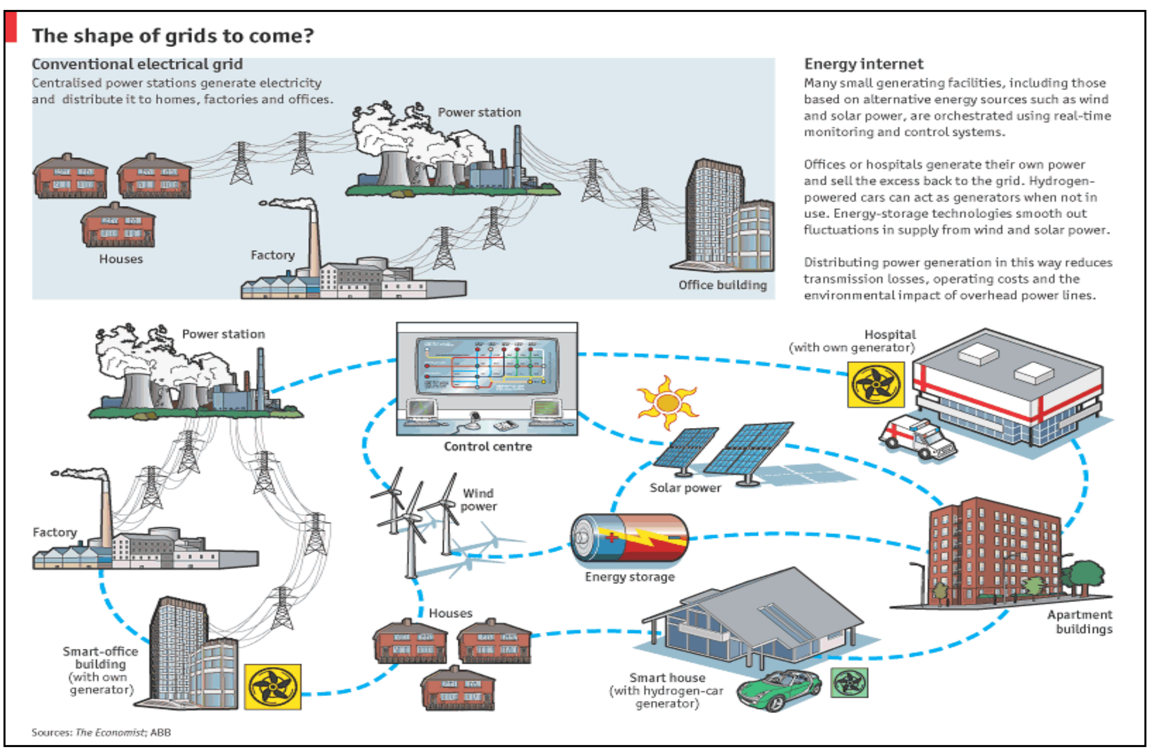


Figure 2: Electrical Grid in the Third Industrial Revolution[21]

The Third Industrial Revolution will not come cheaply as massive changes in civilian and military electrical infrastructure will be required. However, as seen in other instances, countries around the world leverage innovation and advances for their own use. The movement to the Third Industrial Revolution is not limited to the EU, and has spread around the globe to other major powers. In the United States, the Energy Information Administration pedicts “the US rate of electrical consumption is projected to rise 30% by 2035; however, growth of traditional electrical generation continues to fall due to increasing standards, improvements in efficiency and higher prices for energy to the end consumer.”[22] And “capacity additions through 2035 are projected to be in natural gas, wind and other renewables.”[23] Having briefly discussed the future of the EG&D systems, the discussion now turns toward analyzing the implications of this technological change on precision strike of EG&D systems.

## Implications of Precision Strike on EG&D Systems

Traditionally, the objective in attacking EG&D systems is to either disrupt the capacity to create new items (i.e., airplanes, tanks, trucks, ships), to deny access to information that enables command and control (C2) by leadership, to affect civilian morale or increase costs to enemy leadership.[24] Looking ahead, future strategists may also consider attacking EG&D to disrupt computer networks or computer systems in a brute-force attempt to disrupt the actions of super-empowered groups or individual actors. Given these broad objectives, changes in EG&D technologies, particularly in the area of renewable energy and power storage, will affect targeting strategies for developed nations, developing nations and groups and individuals in different ways. Unfortunately, all three cases share a common thread: the window for the strategic use of precision attack on today’s EG&D systems is closing.

**Targeting Developed Nations EG&D Systems**

Changes in future EG&D systems point to diversity of power sources and removal of dependence from Figure 1's "traditional" power plant and transmission lines electricity delivery methodology. In these sophisticated future electrical grids, the loss of a particular node will be routed around and power delivered via other means such as local storage or locally produced renewable power. This adds complexity to the Global Strike mission due to the increased amount of nodes required to be removed from a the system to achieve "lights out."

This increased sophistication increases vulnerability from other attack venues. For example, use of individual device computer controls and master computer stations provides a venue for Cyber-attacks that could affect all linked nodes in a catastrophic manner. This vulnerability already exists today as noted in Richard A. Clarke's "Cyber War" as "… another survey found at one very large electric company, 80 percent of the devices were connected to the corporate intranet, and there were, of course, connections from the intranet out to the public Internet. … thus, if you can hack into the intranet from the Internet, you can control the electrical grid"[25] Of note, this premise of this argument is aimed at large nations with budgets that can sustain the massively expensive and long term investment strategies required to achieve the Third Industrial Revolution.

**Targeting Developing Nation's EG&D Systems**

Struggling Second and Third world countries will first have to increase their civilian capacity to operate and manage technologically advanced systems before achieving Third Industrial Revolution electrical status. A good example is seen in Afghanistan today, where lack of expertise was noted by Glenn Zorpette's recent Re-Engineering Afghanistan article: "I'd asked (Mr.) Black [an Afghan Electrical Engineer] to tell me who is doing the engineering on the scores of electrical projects… 'we're doing it' he answered, and by 'we' he meant NATO… before NATO, the Russians were doing it. And as I learned later, the Americans were doing it. As near as I can tell, Ahmad is the only degreed electrical engineer in all of southern Afghanistan"[26] However, systems of relatively low technology that deliver electricity without much intervention may benefit less developed areas of the world. Shell Oil Company's assessment of developing nations in 2050 painted this scenario: "Benefits also begin to emerge from accelerated growth in distributed power generation from wind and solar energy. New wind turbines and more cost-effective solar panels are easily exported to rural areas, and in a relatively brief time, many African villages have a wind- or solar-powered energy supply for drawing water from deeper, cleaner wells — and for later development needs."[27] This infers that a point-of-use system will be developed and installed to avoid the costly massive infrastructure of a developed nation's EG&D system.

The point is that in countries where electricity is a luxury, if it is available at all, loss of the grid will have little impact on civilian, leadership or military targets. The expert user in these disadvantaged countries will leverage other modern technologies of 2035 using highly efficient alternative sources generation and storage, all without an electrical grid. This will not only provide energy independence, but also freedom of movement, and increased capability to defeat detection, complicating the Global Strike mission set.

**Targeting Groups and Individuals Via EG&D Attack**

One of the most obvious goals of an EG&D attack in 2035 might be to disrupt communications in order to deny the advantages networks provide. Applications of new EG&D and cyber-related technology suggests this may be more difficult that it seems at first glance. Research by the Pew Institute indicates that "Technology experts and stakeholders say they expect they will 'live mostly in the cloud' in 2020 and not on the desktop, working mostly through cyberspace-based applications accessed through networked devices. This will substantially advance mobile connectivity through smartphones and other internet appliances."[28] In addition, this article points out that "cloud computing will continue to expand and dominate users' information transactions because it offers many advantages, allowing users to have easy instant and individualized access to tools and information they need, wherever they are, locatable from any networked device."[29] Thus, adding the ability to access information and conduct C2 via handheld devices that are self-powered from advanced energy sources lends all three sets, nation, group and individual, immense capabilities that have nothing to do with the traditional EG&D systems. Looking from the handheld to the source of connectivity, in 2035 via the Third Industrial Revolution, all buildings and power devices will be networked lending one to postulate that the ubiquity of connectivity will also be apparent.

To summarize, developed nations will achieve a highly fractured/distributed energy "internet" capable of self-healing via nodal controls of available electricity sources. Struggling nations will bypass massive infrastructure projects due to lack of skilled engineers and install point of use systems at localities. Individuals will increase personal energy independence, and via connections to the cloud virtually around the globe, enjoy freedom of movement. All of these future developments complicate the employment of counter EG&D weapons in a Global Strike Mission.

**Post-Precision Attack of EG&D Systems**

If precision attack of EG&D systems is becoming less viable in the future, then what are the other options? There are at least three major areas that offer promise, along with a number of one-off capabilities.

**Volumetric, Electromagnetic Attack**

The first area is volumetric, electromagnetic attack that not only affects the major components of EG&D systems (transformers, storage batteries and generators), but also disrupts the hardware in devices that move, hold and control information. Two directed energy weapons of note are able to achieve this effect, one being Electromagnetic Pulse from a high altitude nuclear explosion and the other being conventionally-generated High Powered Microwaves.

Electromagnetic Pulse. While small-scale Electromagnetic Pulses can be produced using conventional means, the most impressive, wide-area capability requires a high- altitude, nuclear-driven weapon. Although high altitude detonations have little direct effect on humans, the electromagnetic pulse effects could devastate modern society with "weapons of mass destruction" quality effects. A recent House Armed Services Committee highlighted this concern: "The immediate effect of electromagnetic pulse would be the disruption of and damage to the electronic systems and electrical infrastructure. This, in turn, can seriously impact important aspects of our whole national life, including telecommunications, the financial system, government services, the means of getting food, water, medical care, trade and production, as well as electrical power itself."[30] In addition, a high altitude electromagnetic pulse burst would cause a loss of space assets as noted by the US Air Force Chief Scientist in his 2010-2030 Technology Horizons report. "Such a nuclear detonation would act to populate Earth's Van Allen radiation belts with large numbers of energetic electrons produced from beta decay of fission fragments. These high-energy electrons would remain trapped for years by Earth's magnetic field. Satellites in low earth orbit (LEO) or high earth orbit (HEO) orbits would be disabled from effects of the ionizing electrons on critical satellite parts over months or years as they pass through the resulting enhanced radiation belts." [31] The consequences of using this weapon system may have its tactical benefits for the realist view of war; however, its strategic meaning in a greater sense may very well preclude rational nations from ever using it. However, its effects must be understood and mitigation applied to our EG&D systems and information infrastructure as those less rational actors may not have the proclivity to refrain from sending one of the more powerful nations on the globe into chaos. "One second after an electromagnetic pulse attack, it will be too late to ask two simple questions; what should we have done to prevent the attack and why didn't we do it?"[32]

High Power Microwaves. High power microwave technology is nascent as of the writing of this paper. It may prove to be a viable option in 2035, however, because it does not use a nuclear weapon as its impetus. Doug Beason's 2005 "The E Bomb" predicts that in several decades (by 2035), High Powered Microwaves generators will be small and powered by megawatt-class energy sources.[33] While the provide effects similar to Electromagnetic Pulse, their range is substantially limited in comparison with their effects limited to a city block or building depending on the method of delivery.[34] High power microwaves may also offer an ability to "dial down" the electro-magnetic fields being used to fine tune the effects on the target system and reduce collateral damage. At high levels of electro-magnetic fields, permanent and catastrophic damage to circuitry, power lines and devices would be exacted. Lower levels may have the ability to "trip" power surge sensing devices off line or to alternate power sources without causing permanent damage to devices or require human touch labor to reset devices.

Even though the effects of these weapons are substantially more limited in range than Electromagnetic Pulse weapons, legal and moral concerns remain. One commentator offered this legal analysis: "Since microwave non-lethal directed energy weapons target an array of electronic systems with high powered pulses, the effects of these weapons may be difficult to predict or measure. Microwaves, especially wideband weapons, may be analogous to unguided bombs on the battlefield. To adhere to the principle of discrimination, microwave weapons must restrictively radiate and affect only particular targets. Careful consideration of military necessity must outweigh the potential for unnecessary suffering started by a microwave weapon causing an inadvertent cascade of infrastructure failures."[35] The key in the overall strategy would be to assess the effect desired, and then couple the best approach in weaponry to achieve the effect. In this way, proportionality and use of minimum force necessary to achieve the objective can be retained on the side of the aggressor as required by the Law of Armed Conflict (LOAC).

**Applied Non-Lethal Nanotechnology or Biotechnology.**

The second major area that may offer promise for Global Strike against EG&D systems is use of nanotechnologies or biotechnologies to affect the material or conductive properties of all kinds of electronic components. A review of nanotechnology and biological vectors in open literature offer several possibilities.

Nanotechnology Attack. Nanotechnology attack on electrical/electronic component base metals or substrates will yield system failure. This would require a delivery vehicle to the component (a miniaturized remotely piloted aircraft (RPA) perhaps?) then the time for the attack to have effect. With electronic components racing to the 7 nanometer gold standard for circuitry, a nano-attack at this level of computing would have immediate deleterious results to the affected system.

Biotechnology Attack. Similarly, genetically altered biological agents designed to "eat" metals or other base components of electrical/electric systems would achieve an equally catastrophic effect. Currently, biological weapons are treaty limited, but treaties are nation-state arrangements.  Given the trends in biotechnology education and technology development, the field is well postured to be dominated by group or individual actors by 2035.[36]

### Cyber Attack Against EG&D Systems

In the near term, Cyber attack offers the most promising attack vector for post-precision EG&D attack.  This is not a new topic, as found in the 2002 (!) assessment of risks associated with cyber terrorism as  "The premise of cyber terrorism is that as nations and critical infrastructure became more dependent on computer networks for their operation, new vulnerabilities are created – 'a massive electronic Achilles' heel'."[37]  Any system that can be reached via the Internet can be targeted, and effects can be made instantaneously.  On a side note, this capability may generate a new era of 'energy thieves" who re-route power across the grid to alternate storage locations and then sell it back to the highest bidder during times of excessive electrical use.

## The One Offs: Other Ways to Attack EG&D Systems

Other capabilities found during the research are highlighted to round out the quiver of arrows for the Global Strike Strategic Planner as follows:

- Use of Special Operations Forces (SOF).  SOF has the ability to apply kinetic kill or insert surreptitious controls into various components/controls of the EG&D systems.  SOF forces exist today; however, they require time to stage and infiltrate and risk loss or capture.
- Robotics use via Remotely Piloted Aircraft (RPA).  RPA technology exists today and is already weaponized for kinetic kill operations.  Future advances in miniaturization may allow clandestine insertion of RPA technology to the battlefield targeted at EG&D Systems.

- Directed lightning via ion trail to energetic clouds or conductors. This capability was tested and published in 1994.[38] It requires delivery vehicle and permissive conditions, but may yield a non-attributable attack (weather related outage).
- Space Capabilities. Space enabled technology either by directed energy weapons or kinetic kill vehicles (KKV) versus EG&D systems/components.

In respect to all of these attack avenues, one must consider the post-war effects on attacks versus EG&D systems in view of rebuilding efforts. Unfortunately, Iraq was a "you break it, you buy it" war, and as seen in the post war reconstruction of national electrical systems; it was an expensive and long labor item for the US and her allies. This belies that volumetric attacks with far reaching major damage capability will have long term detrimental effects after the conflict is well over. Second and third order effects must also be understood as in some cases EG&D systems cross country borders. Where a specific attack was aimed in a country to achieve political effects, if the outage crosses the border to neighboring nations, the strategic outcome may become tainted. Deep intelligence understanding of electrical systems engineering and inter-connectivity will be required before entering a war with a country if electrical systems are being considered as a target set.

Summing up the discussion on post precision attack on EG&D systems, volumetric weapons while massively effective, also carry strategic-level consequence management concerns. Physical non-kinetic avenues found in nanotechnology and biological vectors are budding technologies today and will require delivery vehicles to the target site to be effective. Cyber promises the greatest potential reward as the global infrastructures become more and more networked. One-off capabilities are highly specialized and require significant "last mile" pre-staging to target areas, and/or quantity to cover global environs to enable "rapidity of action" found in the Global Strike Mission. There is no one size fits all, each capability must be assessed versus the situation at hand before engaging the target.

## Signposts Marking Increased Difficulty in Targeting EG&D Systems

While many of the science realities of 2035 are still in the formative stages, one can project signposts or milestones of technological advances that provide warning of approach to the electrical power ubiquity and increased Global Strike target complexity. As described at the beginning of the paper, due to the exponential rise in technology over time, an exhaustive and comprehensive listing of signposts is not feasible. However, some of these signposts are predictable today including:

- Improved hardening of electronics. Widespread use of nanotechnology enabled Faraday cages for electrical and electronic devices (fixed or mobile) that would defeat electromagnetic pulse and High power microwave attacks. Faraday cages are enclosures that capture and drain off the electro-magnetic impulse of these weapons and succor the devices inside. Work in this area is already underway with carbon nanotube technology as of the penning of this paper.
- Realization of the Third Industrial Revolution. Media releases or intelligence gathered regarding major portions/states within a nation or group that achieve Third Industrial Revolution power independence. Detection of economic lessening of power and energy requirements from external nations while energy use increases. Civilian media releases on "energy internet" achievements for a specific region, area or nation, especially with the ability to move energy around the grid by a computer networked Energy Management System (EMS). Green energy installations, especially third world areas that provide point of use power to indigenous population.

- Individual increased use of distributed generation and storage. Widespread use of fuel cell, electrical storage and hydrogen storage capabilities to the individual building and home level at prices that allow individual home owners/business owners to invest and realize positive return on investment over the lifetime of the devices. Ability to sell back energy to the grid during peak demand hours from site located power generation (solar, wind, hydrogen, etc..) systems. Development, fielding and widespread civilian (and military) employment of cheap, reliable, non-technical point of use power devices that use fuel cell or stored energy from green resources that allow the individual to have his/her own "portable power plant".
- Advances in Computers and Dependence on Cloud Computing. Ability of individuals, militaries and nations to conduct Command and Control (C2) via applications and information stored in "cloud computing" sites, supported by energy source insensitive devices that do not fail in EG&D outages. Use of optical computing and transmission of information. While the power to these devices may yet still ride metallic conduits, the actual machines themselves use light instead of electricity and are not affected by electromagnetic pulse/high power microwave attacks.

## Conclusion

Having studied the gamut of issues related to EG&D systems and Global Strike, several themes emerge. First, the strategic effectiveness of strikes against EG&D systems has a mixed record. Whether the objective is to degrade command and control, disrupt industrial production or coerce governments to capitulate; obtaining EG&D effects required persistence and time. Even without the advanced technology of 2035, nations have proven resilient against kinetic targeting using methods such as substitution and backup power. In the future of energy ubiquity, these nations will have more options to fall back on in case of loss of traditional EG&D systems.

Short of large-scale, volumetric attacks using electromagnetic pulse or high power microwave, connectivity via alternative power sources or cloud computing will likely will be retained and strategic impact of loss of EG&D systems will be minimized. If volumetric attack options are chosen, the 2nd and 3rd order effects and consequences must also be understood due to impact critical life support and health sustainment systems from loss of electrical power at the outset, and the likely requirement for nation rebuilding in the long run.

Second, even as dependence on electricity rises, the window for effective precision strike against these systems may be closing. As countries upgrade their electrical systems, they will in general, use the best technology of the day they can afford and staff, not yester-year antiquated systems. This in itself may seem to offer less vulnerability; however, for example, the marrying of electrical support systems to the Internet for ease of monitoring and operations offers a wholly different venue of attack. Power generation and storage at the site vice delivered by a remotely located power plant is becoming the kernel of life in the Third Industrial Revolution. Those nations, groups or individuals that achieve the Third Industrial Revolution not only removes them from dependence on fossil fuels, and at a minimum, reduces the impact of loss to electricity due to single point failure of the same to near negligible proportions. Additionally, technological advances providing uninterrupted power at the hand held device coupled to the globalization of networked devices and move of information into cloud computing enables continuous C2 by any of the aforementioned groups in EG&D denied environments. Indeed, as highlighted by Thomas L. Friedman in "The World is Flat" "… everything from photography to entertainment to communication … are being digitized and therefore can be shaped, manipulated, and transmitted over computers, the Internet, satellites or fiber optic cable… it is mobile and can be done from your personal device."[39] Thus, ubiquitous power and computer connectivity virtually assures uninterrupted connectivity despite EG&D strikes regardless if the person in question is a civilian leader, military general or terrorist on short final to his final detonation site.

Third, the best results against EG&D systems in the future may be gained using volumetric or cyber weapons. Volumetric weapons bring the ability to encompass all of the fractionated and widespread power sources, electrical and electronic components in the target area. In the case of high-powered microwave technology, the ability to execute a “dial-able” effect may enable more precision/less collateral damage. However, high-powered microwave devices must be placed near their target, thus logistics and prepositioning of the asset are a concern when employing this weapon. Electromagnetic pulse technology is currently nuclear related, which carries its own set of problems in the strategic implications of use of nuclear force versus the adversary. Cyber-attack offers many positive capabilities; moving at the speed of the network, can be emplaced from afar and engagement of effects may be able to be exacted without attribution to the source. This said, however, these attacks must be supported by intelligence, surveillance and reconnaissance in cyberspace as well as the continued development and fielding of cyber weaponry and defenses.

Fourth, even so, volumetric and cyber weapons are not without their own problems. Consequences of a large-scale loss of electricity from volumetric attacks may be construed as a near weapon of mass destruction/disruption (WMD) by the engaged territory/country. Enemy states may retaliate in kind against the US, provided they possess the technological capability. The weapons capabilities seen above will not be the sole province of the US and her allies and the same catastrophic effects could be implemented on/above US soil from afar without attribution to the attacker. Moreover, many nations are aware of the devastating effects of electromagnetic pulses and are working on hardening measures and backup via cloud computing for their critical command and control (C2) systems. Unfortunately, some of these nations also have the proclivity to sell their advances on the open/black markets, thus enabling other nations, groups and individuals to enjoy the fruits of their labor. Similarly, the global cyber communities understands the burgeoning capabilities and vulnerabilities of cyber space and are developing cyber defense counter measures and firewalls to harden this domain.

In summation, attacks on EG&D systems historically have not achieved coercive effects sought by the planners of the age. Based on these findings, Global Strike on EG&D systems should be in the closing chapter of the US Air Force's library of capabilities for Global Strike by 2035. Added to the diversity of power systems, the exponential explosion of information transparency is already enabling C2 from anywhere on the globe. Next generation counter EG&D weapons, on the cusp of fielding now, will have limited effectiveness in the 2035 future of energy ubiquity and communications connectivity. Cyber capabilities exist today to attack EG&D systems, but the competition between offense and defense is moving quickly in this area. The window of opportunity to strike these systems is still open, but is closing rapidly.

## Appendix: Definitions

For the purpose of this paper, the following definitions were used and are presented to add clarity if needed by the reader.

**Dis·rupt** (dĭs-rŭpt') *tr.v.* **dis·rupt·ed**, **dis·rupt·ing**, **dis·rupts** **1.** To throw into confusion or disorder: *Protesters disrupted the candidate's speech.* **2.** To interrupt or impede the progress, movement, or procedure of: *Our efforts in the garden were disrupted by an early frost.* **3.** To break or burst; rupture. (Author's Note) This definition is offered as JP 1-02 does not have a military definition for "disrupt", a key verb affecting the weapons effects being sought by the strategic planner.

**EG&D:** Nominally details the power generation source, transmission lines, electrical stations and substations to power attachment point to end user domicile. Includes domicile alternative power generation (green energy or hydrocarbon) capabilities and major storage devices. Does not include internal to domicile individual component electrical generation (device specific fuel or solar cells) or storage (batteries, uninterruptable power supply (UPS)).

**Weapons of Mass Destruction (US military definition) —** Chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties and exclude the means of transporting or propelling the weapon where such means is a separable and divisible part from the weapon. Also called **WMD**.[40]

**Weapons of Mass Disruption (WMD) —** weapons of information warfare characterized as weapons of mass disruption, which may include various forms of malicious code, perception management activities, and flexible deterrent options. Malicious code is broken into four categories: viruses, worms, Trojan horses and logic bombs. These weapons offer remarkable attack potential at a low cost and low risk. Targets may include hardware, software, firmware, wetware, information, or any combination. Other high technology disruptive weaponry, such as mass spectrum directed energy weapons and surgically precise low power particle beam weapons that cause disruption through destruction of key components in an adversary's information systems.[41]

## ENDNOTES


1. Shaller, Bob. *The Origin, Nature and Implications of Moore's Law.* Report to fulfill Graduate Course Requirements, N/A: Bob Shaller, 1996. Pages 7-8. http://research.microsoft.com/en-us/um/people/gray/Moore_Law.html (Accessed 01 Oct, 2011)

2. Department of Energy, Energy Information Administration *International Energy Outlook 2011*, Report, Washington DC, DOE EIA September 2011. Page 4. http://www.eia.gov/forecasts/ieo/pdf/0484(2011).pdf (Accessed 13 Jan, 2012)

3. Department of Energy, Energy Information Administration *International Energy Outlook 2011*, Report, Washington DC, DOE EIA September 2011. Page 4. http://www.eia.gov/forecasts/ieo/pdf/0484(2011).pdf (Accessed 13 Jan, 2012)

4. Major General Haywood S. Hansell, Jr. *The Air Plan that Defeated Hitler,* Atlanta Georgia, 1972, Page 163.

5. Secretary of War, *The United States Strategic Bombing Survey*, United States Government Printing Office, Washington DC, 03 Nov, 1944. Page 14

6. Memorandum, Committee of Operations Analysts, to General Arnold, chief Army Air Forces, subject: Report of Committee of Operations Analysts on Economic Objectives in the Far East, 11 November 1943, Pages 4 and 53

7. Major General Haywood S. Hansell, Jr. *Strategic Air War Against Japan*, Air Power Research, Maxwell Air Force Base, Montgomery AL: Air University Press, 1980. Page 78

8. Thomas E. Griffith, Jr. *Strategic Attack of National Electrical Systems.* Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 1994. Page 36. www.comw.org/pda/fulltext/griffith.pdf (Accessed 08 Dec, 2011)

9. Herman L. Gilster and Robert E. M. Frady, *Linebacker II USAF Bombing Survey* (Headquarters Pacific Air Forces, April 1973). Pages 13-14

10. Thomas E. Griffith, Jr., *Strategic Attack of National Electrical Systems.* Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 1994. Page 52. www.comw.org/pda/fulltext/griffith.pdf (Accessed 08 Dec, 2011)

11. Transforming from its inception into a 500+ person joint command, in July 2011, JWAC was realigned as a subordinate to Strategic Command as part of the 2010 Department of Defense efficiency initiative. Today, JWAC coordinates directly with the staffs of all Unified Commands, Department of Defense elements, Combatant Commands, military services, and other government departments and agencies to respond to crises. Joint Warfare Analysis Center Homepage. JWAC Mission and Vision Page, http://www.jwac.mil/ (Accessed 08 Feb, 2012)

12. Thomas E. Griffith, Jr. *Strategic Attack of National Electrical Systems.* Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 1994. Page 42. www.comw.org/pda/fulltext/griffith.pdf (Accessed 08 Dec, 2011)

13. Earl H. Tilford, Jr. Operation Allied Force and the Role of Air Power, Article from Parameters, Winter 1999-2000, pp 24-38 http://www.carlisle.army.mil/USAWC/parameters/Articles/99winter/tilford.htm (Accessed 30 Jan, 2012)

14. Thomas E. Griffith, Jr. *Strategic Attack of National Electrical Systems.* Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 1994. Page 58. www.comw.org/pda/fulltext/griffith.pdf (Accessed 08 Dec, 2011)

15. Pape, Robert A. *Bombing to Win: Air Power and Coercion in War.* Cornell: Cornell University Press, 1996. Page 25.

16. Pape, Robert A. *Bombing to Win: Air Power and Coercion in War.* Cornell: Cornell University Press, 1996. Page 68

17. Russel J. Hart, COL, USAF, *Defeating Hard and Deeply Buried Targets in 2035*, Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 15 February 2012. Pages 1 and 11

18. Forstchen, William R. One Second After. New York, NY: "A Forge Book" Tom Doherty Associates, LLC, 2009. Pages 348-350

19. U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004, Page 5. http://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf (accessed 29 Jan, 2012)

20. Authors, Various. "EU Parliament Declaration on Energy and the Economy." *EU Parliament Declaration.* European Commission, 2007. Page 2. http://www.ueapme.com/IMG/pdf/EU_PARLIAMENT_DECLARATION_ON_ENERGY_AND_THE_ECONOMY_final.pdf (Accessed 12 Oct, 2011)

21. The Economist, "Building the Energy Internet" May 11, 2004. Electronic Edition. http://www.economist.com/node/2476988 (Accessed 12 Dec, 2011)

22. Authors, Multiple. *Annual Energy Outlook 2011 with Projections to 2035.* Annual Report,Washington DC: U.S. Energy Information Administration, Office of Integrated and International Energy Analysis, 2011. Page 15 http://www.eia.gov/neic/speeches/newell_12162010.pdf (Accessed 11 Nov, 2011)

23. Authors, Multiple. *Annual Energy Outlook 2011 with Projections to 2035.* Annual Report, Washington DC: U.S. Energy Information Administration, Office of Integrated and International Energy Analysis, 2011. Page 19 http://www.eia.gov/neic/speeches/newell_12162010.pdf (Accessed 11 Nov, 2011)

24. Thomas E. Griffith, Jr. *Strategic Attack of National Electrical Systems.* Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 1994. Page 58. www.comw.org/pda/fulltext/griffith.pdf (Accessed 08 Dec, 2011)

25. Clark, Richard A. *Cyber War - The next threat to national security and what to do about it.* New York: HarperCollins Publishers, 2010. Page 99

26. Zorpette, Glenn. "Re-Engineering Afghanistan." *EEE Spectrum*, 2011. Journal Page 36. http://spectrum.ieee.org/energy/the-smarter-grid/reengineering-afghanistan (Accessed 12 Dec, 2011)

27. Shell Oil Company. *Shell energy scenarios to 2050.* Report, (Fill in): Shell International BV, 2008. Page 30. http://www-static.shell.com/static/public/downloads/brochures/corporate_pkg/scenarios/shell_energy_scenarios_2050.pdf (Accessed 10 Oct, 2011)

28. Janna Quitney Anderson, Elon University, Lee Rainie, Pew Research Center's Internet & American Life Project. *The Future of Cloud Computing.* Report, Washington, D.C. 20036: Pew Research Center's Internet & American Life Project, 2010. Page 1. http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx (Accessed 11 Nov, 2011)

29. Janna Quitney Anderson, Elon University, Lee Rainie, Pew Research Center's Internet & American Life Project. *The Future of Cloud Computing.* Report, Washington, D.C. 20036: Pew Research Center's Internet & American Life Project, 2010. Page 9. http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx (Accessed 11 Nov, 2011)

30. Committee on Armed Services House of Representatives One Hundred Tenth Congress Second Session. *Threat Posed by Electromagnetic Pulse (EMP) Attack.* HASC Report, Washington DC: U.S. Government Printing Office, 2008. Page 8. http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg45133/pdf/CHRG-110hhrg45133.pdf (Accessed 11 Nov, 2011)

31. Chief Scientist of the Air Force. *Report on Technology Horizons: A Vision for Air Force Science & Technology for 2010-2030.* Predictive Futures Report, Washington DC: United States Air Force, 2010. Page 28.

http://www.aviationweek.com/media/pdf/Check6/USAF_Technology_Horizons_report.pdf
(Accessed 10 Oct, 2011)

32. Forstchen, William R. *One Second After.* New York, NY: "A Forge Book" Tom Doherty Associates, LLC, 2009. Afterword page 4, quote from Captain Bill Sanders, US Navy

33. Beason, Doug. *The E-Bomb - How America's new directed energy weapons will change the way future wars will be fought.* Cambridge Center, Cambridge: Da Capo Press, 2005. Pages 183-184

34. Defense Science Board. *Time Critical Conventional Strike from Strategic Standoff.* Assessment and Recommendation, Washington,DC: Office of the Under Secretary of Defense,For Acquisition, Technology, and Logistics, 2009. Page 43. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA498403
(Accessed 15 Oct, 2011)

35. Ciero, Mark K. *No Sticks, Stones or Broken Bones: Nonlethal Directed Energy Weapons for Air Power.* Thesis, Maxwell Air Force Base, Alabama, USA: School for Advanced Air and Space Studies, Air University, 2006. Page 60.

36. Interview with Research Laboratory Scientist, Sandia National Laboratories, 17 September, 2011. All interviews were conducted under non-attribution to the specific person.

37. Lewis, James A. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Analysis, Washington DC: Center for Strategic and International Studies, 2002. Page 1 http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (Accessed 11 Dec, 2011)

38. Kozma, Matthew A. *A Brief History of Laser Guided Lightning Discharge Models and Experiments.* Scientific Paper, Air Force Materiel Command, Hanscom Air Force Base, MA: Phillips Laboratory, Directorate of Geophysics, 1994. Page 7 http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA289448&Location=U2&doc=GetTRDoc.pdf
(Accessed 22 Oct, 2011)

39. Friedman, Thomas L. The World is Flat - A brief history of the Twenty-First Century. UnionSquare West, New York: Farrar, Straus and Giroux, 2005. Pages 161-162

40. Joint Chiefs of Staff. *Joint Publication 1-02: Dictionary of Military and Associated Terms.* Washington DC: US Government Printing Office, 2011. Page 365 www.dtic.mil/doctrine/new_pubs/jp1_02.pdfSimilarf (Accessed 10 Dec, 2011)

41. Michael W. Lamb, Sr., *Bytes: Weapons of Mass Disruption,* Maxwell AFB, Montgomery AL. Air War College, 2002. Page 128. http://www.au.af.mil/au/awc/awcgate/awc/lamb.pdf
(Accessed 07 Feb, 2012)

# BIBLIOGRAPHY


Annual Energy Outlook 2011 with Projections to 2035. Annual Report, Washington DC: U.S. Energy Information Administration, Office of Integrated and International Energy Analysis, 2011. http://www.eia.gov/neic/speeches/newell_12162010.pdf

Beason, Doug. The E-Bomb - How America's new directed energy weapons will change the way future wars will be fought. Cambridge Center, Cambridge MA. Da Capo Press, 2005.

Chief Scientist of the Air Force. Report on Technology Horizons: A Vision for Air Force Science & Technology for 2010-2030. Predictive Futures Report, Washington DC: United States Air Force, 2010.
http://www.aviationweek.com/media/pdf/Check6/USAF_Technology_Horizons_report.pdf

Ciero, Mark K. No Sticks, Stones or Broken Bones: Nonlethal Directed Energy Weapons for Air Power. Thesis, Maxwell Air Force Base, Alabama, USA: School for Advanced Air and Space Studies, Air University, 2006.

Clark, Richard A. Cyber War - The next threat to national security and what to do about it. New York: HarperCollins Publishers, 2010.

Committee on Armed Services House of Representatives One Hundred Tenth Congress Second Session. Threat Posed by Electromagnetic Pulse (EMP) Attack. HASC Report, Washington DC: U.S. Government Printing Office, 2008. http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg45133/pdf/CHRG-110hhrg45133.pdf

Defense Science Board. Time Critical Conventional Strike from Strategic Standoff. Assessment and Recommendation, Washington, DC: Office of the Under Secretary of Defense,For Acquisition, Technology, and Logistics, 2009. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA498403

Department of Energy, Energy Information Administration International Energy Outlook 2011, Report, Washington DC, DOE EIA September 2011.
http://www.eia.gov/forecasts/ieo/pdf/0484(2011).pdf

Earl H. Tilford, Jr. Operation Allied Force and the Role of Air Power, Article from Parameters, Winter 1999-2000,
http://www.carlisle.army.mil/USAWC/parameters/Articles/99winter/tilford.htm

"EU Parliament Declaration on Energy and the Economy." EU Parliament Declaration. European Commission, 2007.
http://www.ueapme.com/IMG/pdf/EU_PARLIAMENT_DECLARATION_ON_ENERGY_AND_THE_ECONOMY_final.pdf

Forstchen, William R. One Second After. New York, NY: "A Forge Book" Tom Doherty Associates, LLC, 2009.

Friedman, Thomas L. The World is Flat - A brief history of the Twenty-First Century. Union Square West, New York: Farrar, Straus and Giroux, 2005.

Herman L. Gilster and Robert E. M. Frady, Linebacker II USAF Bombing Survey (Headquarters Pacific Air Forces, April 1973).

Interview with Research Laboratory Scientist, Sandia National Laboratories, 17 September, 2011. All interviews were conducted under non-attribution to the specific person.

Janna Quitney Anderson, Elon University, Lee Rainie, Pew Research Center's Internet & American Life Project. The Future of Cloud Computing. Report, Washington, D.C. 20036: Pew Research Center's Internet & American Life Project, 2010. http://pewinternet.org/Reports/2010/The-future-of-cloud-computing.aspx

Joint Chiefs of Staff. Joint Publication 1-02: Dictionary of Military and Associated Terms. Washington DC: US Government Printing Office, 2011. www.dtic.mil/doctrine/new_pubs/jp1_02.pdfSimilarf

Joint Warfare Analysis Center Homepage. JWAC Mission and Vision Page, http://www.jwac.mil/

Kozma, Matthew A. A Brief History of Laser Guided Lightning Discharge Models and Experiments. Scientific Paper, Air Force Materiel Command, Hanscom Air Force Base, MA: Phillips Laboratory, Directorate of Geophysics, 1994. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA289448&Location=U2&doc=GetTRDoc.pdf

Lewis, James A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Analysis, Washington DC: Center for Strategic and International Studies, 2002. http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Major General Haywood S. Hansell, Jr. The Air Plan that Defeated Hitler, Atlanta Georgia, 1972.

Major General Haywood S. Hansell, Jr. Strategic Air War Against Japan, Air Power Research, Maxwell Air Force Base, Montgomery AL: Air University Press, 1980.

Memorandum, Committee of Operations Analysts, to General Arnold, chief Army Air Forces, subject: Report of Committee of Operations Analysts on Economic Objectives in the Far East, 11 November 1943.

Michael W. Lamb, Sr., Bytes: Weapons of Mass Disruption, Maxwell AFB, Montgomery AL. Air War College, 2002. http://www.au.af.mil/au/awc/awcgate/awc/lamb.pdf

Pape, Robert A. Bombing to Win: Air Power and Coercion in War. Cornell: Cornell University Press, 1996.

Russel J. Hart, COL, USAF, Defeating Hard and Deeply Buried Targets in 2035, Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 15 February 2012.

Secretary of War, The United States Strategic Bombing Survey, United States Government Printing Office, Washington DC, 03 Nov, 1944.

Shaller, Bob. The Origin, Nature and Implications of Moore's Law. Report to fulfill Graduate Course Requirements, N/A: Bob Shaller, 1996. http://research.microsoft.com/en-us/um/people/gray/Moore_Law.html

Shell Oil Company. Shell energy scenarios to 2050. Report, (Fill in): Shell International BV, 2008. http://www-static.shell.com/static/public/downloads/brochures/corporate_pkg/scenarios/shell_energy_scenarios_2050.pdf

The Economist, "Building the Energy Internet" May 11, 2004. Electronic Edition. http://www.economist.com/node/2476988

Thomas E. Griffith, Jr., Strategic Attack of National Electrical Systems. Thesis Paper, Maxwell Air Force Base, Montgomery AL: Air University Press, 1994. www.comw.org/pda/fulltext/griffith.pdf

U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004. http://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf

Zorpette, Glenn. "Re-Engineering Afghanistan." EEE Spectrum, 2011. http://spectrum.ieee.org/energy/the-smarter-grid/reengineering-afghanistan