# 1AC

## Advantage 1- Islanding

#### Small nuclear reactors key to prevent bases from being vulnerable to inevitable grid outages.

Andres and Breetz 11

(Richard B. Andres is Professor of ¶ national Security Strategy at the ¶ national War College and a Senior fellow and energy and environmental ¶ Security and Policy Chair in the Center ¶ for Strategic research, institute for national Strategic Studies, at the national Defense University. Hanna L. Breetz is a doctoral candidate in the Department of Political Science at the Massachusetts institute of technology, “Small Nuclear Reactors ¶ for Military Installations:¶ Capabilities, Costs, and ¶ Technological Implications” Institute for National Strategic Studies, <http://www.ndu.edu/press/lib/pdf/strforum/sf-262.pdf>, SEH)

Grid Vulnerability. DOD is unable to provide its ¶ bases with electricity when the civilian electrical grid is ¶ offline for an extended period of time. Currently, domestic military installations receive 99 percent of their ¶ electricity from the civilian power grid. As explained in a ¶ recent study from the Defense Science Board:¶ DOD’s key problem with electricity is that critical ¶ missions, such as national strategic awareness and ¶ national command authorities, are almost entirely ¶ dependent on the national transmission grid . . . ¶ [which] is fragile, vulnerable, near its capacity ¶ limit, and outside of DOD control. In most cases, ¶ neither the grid nor on-base backup power provides¶ sufficient reliability to ensure continuity of critical ¶ national priority functions and oversight of ¶ strategic missions in the face of a long term (several ¶ months) outage.¶ 7¶ The grid’s fragility was demonstrated during the 2003 ¶ Northeast blackout in which 50 million people in the ¶ United States and Canada lost power, some for up to a ¶ week, when one Ohio utility failed to properly trim trees. ¶ The blackout created cascading disruptions in sewage ¶ systems, gas station pumping, cellular communications, ¶ border check systems, and so forth, and demonstrated the ¶ interdependence of modern infrastructural systems.¶ 8¶ More recently, awareness has been growing that ¶ the grid is also vulnerable to purposive attacks. A report sponsored by the Department of Homeland Security suggests that a coordinated cyberattack on the grid ¶ could result in a third of the country losing power for ¶ a period of weeks or months.¶ 9¶ Cyberattacks on critical ¶ infrastructure are not well understood. It is not clear, for ¶ instance, whether existing terrorist groups might be able ¶ to develop the capability to conduct this type of attack. It ¶ is likely, however, that some nation-states either have or ¶ are working on developing the ability to take down the ¶ U.S. grid. In the event of a war with one of these states, ¶ it is possible, if not likely, that parts of the civilian grid ¶ would cease to function, taking with them military bases ¶ located in affected regions.¶ Government and private organizations are currently ¶ working to secure the grid against attacks; however, it is ¶ not clear that they will be successful. Most military bases ¶ currently have backup power that allows them to function for a period of hours or, at most, a few days on their ¶ own. If power were not restored after this amount of time, ¶ the results could be disastrous. First, military assets taken ¶ offline by the crisis would not be available to help with disaster relief. Second, during an extended blackout, global ¶ military operations could be seriously compromised; this ¶ disruption would be particularly serious if the blackout ¶ was induced during major combat operations. During the ¶ Cold War, this type of event was far less likely because the United States and Soviet Union shared the common understanding that blinding an opponent with a grid blackout could escalate to nuclear war. America’s current opponents, however, may not share this fear or be deterred ¶ by this possibility.¶ In 2008, the Defense Science Board stressed that ¶ DOD should mitigate the electrical grid’s vulnerabilities by turning military installations into “islands” of ¶ energy self-sufficiency.¶ 10¶ The department has made efforts to do so by promoting efficiency programs that ¶ lower power consumption on bases and by constructing ¶ renewable power generation facilities on selected bases. ¶ Unfortunately, these programs will not come close to ¶ reaching the goal of islanding the vast majority of bases. ¶ Even with massive investment in efficiency and renewables, most bases would not be able to function for more ¶ than a few days after the civilian grid went offline. Unlike other alternative sources of energy, small reactors have the potential to solve DOD’s vulnerability to ¶ grid outages. Most bases have relatively light power demands when compared to civilian towns or cities. Small ¶ reactors could easily support bases’ power demands separate from the civilian grid during crises. In some cases, ¶ the reactors could be designed to produce enough power ¶ not only to supply the base, but also to provide critical ¶ services in surrounding towns during long-term outages.¶ Strategically, islanding bases with small reactors ¶ has another benefit. One of the main reasons an enemy ¶ might be willing to risk reprisals by taking down the ¶ U.S. grid during a period of military hostilities would ¶ be to affect ongoing military operations. Without the ¶ lifeline of intelligence, communication, and logistics ¶ provided by U.S. domestic bases, American military operations would be compromised in almost any conceivable contingency. Making bases more resilient to ¶ civilian power outages would reduce the incentive for ¶ an opponent to attack the grid. An opponent might ¶ still attempt to take down the grid for the sake of disrupting civilian systems, but the powerful incentive to ¶ do so in order to win an ongoing battle or war would ¶ be greatly reduced.

#### Grid failure in the next 3 years

Huff 12

(Ethan A, staff writer at natural news “Hacking expert says catastrophic failure of smart energy grid within 3 year” <http://usahitman.com/hcfseg/>, SEH)

For at least the past five years, the federal government has been pushing utility companies across America to “upgrade” their infrastructures to support “smart grid” technology that allows two-way communication with, and centralized control of, the energy grid through an internet-based network. But cyber expert David Chalk says that a complete and catastrophic failure of the entire smart energy grid is definitely going to occur within the next three years, and that few are aware of this.¶ Traditionally, the electric meters attached to structures, the wired and underground poles that deliver electricity to them, and the plants where electricity are generated have all been operated and maintained independently by field workers who gather data in a one-way system of communication. In other words, when a problem occurs with an electric meter or a pole in the traditional system, an expert has to go out and assess the problem, as there is no automated way for the system itself to send feedback.¶ For this reason and others, many have hailed smart grid technology as the solution, and as the way to bring the electric grid into the 21st century. But according to Chalk and many other experts in the field, smart grid technology is highly vulnerable to cyber attacks, and the technology is so digitally centralized that hackers are sure to “crack the code,” so to speak, and eventually bring down the system.¶ “We’re in a state of crisis,” says Chalk. “The front door is open and there is no lock to be had. There is not a power meter or device on the grid that is protected from hacking — if not already infected — with some sort of trojan horse that can cause the grid to be shut down or completely annihilated.”¶ Solar storms, digital warfare threaten to bring down the smart grid¶ Smart grid technology is also vulnerable to failure from solar storms and digital warfare, both of which could quickly take down the entire system in an instant, leaving millions, and potentially billions, of people in the dark without power. Smart grid technology also comes with its own unique health and privacy risks that are being ignored by its proponents as well.¶ “Unless we wake up and realize what we’re doing, there is 100 percent certainty of total catastrophic failure of the entire power infrastructure within three years,” adds Chalk. “This could actually be worse than a nuclear war, because it would happen everywhere. How governments and utilities are blindly merging the power grid with the Internet, and effectively without any protection, is insanity at its finest.”

#### Grid will go down- four reasons

Defense Science Board 8

(The DSB is a Federal ¶ Advisory Committee established to provide independent advice to the Secretary of ¶ Defense, “More Fight – Less Fuel” <http://www.acq.osd.mil/dsb/reports/ADA477619.pdf>, SEH)

5.3 Four Sources of Risk for Grid Outages ¶ The first risk is from overload. As wires become overloaded, they heat up and sag, ¶ making them vulnerable to entanglement with trees and other objects. This happened ¶ near Cleveland, Ohio on August 14, 2003. According to the U.S.-Canada Power ¶ System Outage Task Force, high demand caused a high-voltage line to come in contact ¶ with overgrown trees. The resulting cascade of failures plunged many of the 50 million ¶ people in the Northeast U.S. and Canada living in an area covering 9,300 square miles ¶ into darkness. It shut down more than 500 generating units at 265 power plants, ¶ including 22 nuclear plants.¶ 29¶ ¶ A second risk comes from natural disasters, such as hurricanes, tornadoes, electrical ¶ storms or other extreme weather events. The consequences could be very much as ¶ described above, but with the added risk of physical damage to the infrastructure. ¶ Favorable commentary about the performance of the grid following the August 2003 ¶ outage focused on the fact that restoration occurred fairly quickly. Within a few days ¶ power was restored virtually everywhere, with much of the area back up within a few ¶ hours. This was largely because safety features built into the grid successfully ¶ prevented damage to critical equipment such as generators, breakers and ¶ transformers.¶ 30¶ However, the Task Force is concerned that such an extensive outage could be caused by such a commonplace event – a single line contacting a tree. This ¶ inevitably raises the next issue below: what the result might have been had there been ¶ physical damage to infrastructure, such as from a deliberate attack by knowledgeable ¶ adversaries? ¶ A third risk comes from sabotage or terrorist activity, whether local, trans-national, or ¶ state-sponsored, and including both conventional and nuclear attack. Nuclear attack ¶ could take place either directly or through the generation of a high altitude ¶ electromagnetic pulse (EMP). The grid is a relatively easy target for a terrorist. It is ¶ brittle, increasingly centralized, capacity-strained, and largely unprotected from physical ¶ attack, with little stockpiling of critical hardware. Although the system is designed to ¶ survive single points of failure, increasing demand on the system and increasing ¶ network constraints make multiple points of failure more likely. These are difficult to ¶ anticipate and more likely to result in cascading outages and catastrophic outages that ¶ cover large areas for long periods of time. Network Single Points of Failure (NSPF) are ¶ abundant. High voltage transformers, breakers, and other long-lead time items are ¶ particularly critical system elements.¶ 31¶ They can be easily targeted and destroyed. Grid ¶ sections could be taken down for months even if replacement transformers and ¶ breakers could be found; or for years if certain components need to be newly ¶ manufactured and transported. There are only limited backups located around the ¶ country—generally co-located with operating equipment. For some of the largest ¶ equipment, there is no domestic supply and only limited overseas production capacity ¶ which is fully booked years ahead.¶ 32¶ For example, 765 kV transformers are ¶ manufactured only by one company in Canada. Armed with the right knowledge, a ¶ small number of people could shut down electricity over significant areas for an ¶ extended period of time, including power to critical DoD missions. The grid is not ¶ designed to withstand a coordinated multi-pronged or wide-area attack.¶ 33¶ The Task ¶ Force noted that attacks on the grid are one of the most common and effective tactics of ¶ insurgents in Iraq, and are increasingly seen in Afghanistan.¶ 34¶ In addition to physical attacks on the grid, there is the potential for cyber attacks. U.S. ¶ grid control systems are continuously probed electronically, and there have been ¶ numerous attempted attacks on the Supervisory Control and Data Acquisition (SCADA) ¶ systems that operate the grid. None have yet resulted in major problems in the U.S., ¶ but the potential exists for major outages in the same way successful hackers can ¶ disrupt computer networks.¶ 35¶ Further details regarding the potential for deliberate attacks to the grid and their potential consequences are contained in a classified annex ¶ to this report. ¶ A fourth risk comes from interruptions in supplies to generating plants, which can be ¶ caused by natural events, infrastructure failures, attack or even market forces. This ¶ occurred in California during 2000 and 2001 when supplies of natural gas were ¶ interrupted and forced a reduction in electricity generation.¶ 36¶ Approximately 20% of ¶ U.S. electricity is generated by natural gas and market prices have swung wildly over ¶ the past several years.¶ 37¶ Approximately 52% of U.S. electricity is generated by coal and ¶ transportation routes that move coal from mines to generating plants are sometimes ¶ remote and lacking in alternatives. Critical rail lines or bridges could be taken out by ¶ determined saboteurs. For example, in May 2005, 43 rail cars came off the tracks. The ¶ disruption to coal deliveries caused prices to spike, and raised electricity prices by 6% ¶ nationally, according to the Bureau of Labor Statistics. The 100 mile length of rail line ¶ through Wyoming that carries the output of the Western coal belt to power plants is the ¶ most heavily traveled in the nation.¶ 38¶ So in addition to risks from grid outage, there are ¶ risks to the supply chain that enables the grid to work—not least from electricity supply ¶ failures themselves, which could disable the pipelines and controls used by other forms ¶ of energy, notably oil and gas.

#### That undermines the military and risks nuclear war

The Examiner 7/27

(Robert Tilford, Graduate US Army Airborne School, Ft. Benning, Georgia, “Cyber attackers could shut down the electric grid for the entire east coast” <http://www.examiner.com/article/cyber-attackers-could-easily-shut-down-the-electric-grid-for-the-entire-east-coa>, SEH)

To make matters worse a cyber attack that can take out a civilian power grid, for example could also cripple the U.S. military.¶ The senator notes that is that the same power grids that supply cities and towns, stores and gas stations, cell towers and heart monitors also power “every military base in our country.”¶ “Although bases would be prepared to weather a short power outage with backup diesel generators, within hours, not days, fuel supplies would run out”, he said.¶ Which means military command and control centers could go dark.¶ Radar systems that detect air threats to our country would shut¶ Down completely.¶ “Communication between commanders and their troops would also go silent. And many weapons systems would be left without either fuel or electric power”, said Senator Grassley.¶ “So in a few short hours or days, the mightiest military in the world would be left scrambling to maintain base functions”, he said.¶ We contacted the Pentagon and officials confirmed the threat of a cyber attack is something very real.¶ Top national security officials—including the Chairman of the Joint Chiefs, the Director of the National Security Agency, the Secretary of Defense, and the CIA Director— have said, “preventing a cyber attack and improving the nation’s electric grids is among the most urgent priorities of our country” (source: Congressional Record).¶ So how serious is the Pentagon taking all this?¶ Enough to start, or end a war over it, for sure (see video: Pentagon declares war on cyber attacks http://www.youtube.com/watch?v=\_kVQrp\_D0kY&feature=relmfu ).¶ A cyber attack today against the US could very well be seen as an “Act of War” and could be met with a “full scale” US military response.¶ That could include the use of “nuclear weapons”, if authorized by the President.

#### Al Qaeda can and will pull off a cyber-attack – Al Qaeda video proves

Cloherty ‘12

(Jack Cloherty is the lead producer for the Justice Department/Homeland Security beat at World News. “Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad'” May 22, 2012 accessed online September 15, 2012 at http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UFS0p42PVe-, TSW)

Al Qaeda may be turning its destructive attention to cyber-warfare against the United States. In a chilling video, an al Qaeda operative calls for "electronic jihad" against the United States, and compares vulnerabilities in vital American computer networks to the flaws in aviation security before the 9/11 attack.¶ The al Qaeda video calls upon the "covert mujahidin" to launch cyber attacks against the U.S. networks of both government and critical infrastructure, including the electric grid. The video was obtained by the FBI last year, and released today by the Senate Committee on Homeland Security and Governmental Affairs.¶ "This is the clearest evidence we've seen that al Qaeda and other terrorist groups want to attack the cyber systems of our critical infrastructure," Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman, I-Conn., said in a statement.¶ "This video is troubling as it urges al Qaeda adherents to launch a cyber attack on America," said Sen. Susan Collins, R-Maine, the ranking member on the committee. "It's clear that al Qaeda is exploring all means to do us harm and this is evidence that our critical infrastructure is a target."¶ ¶ Dept. of Homeland Security¶ In this screenshot obtained by the FBI, an Al... View Full Size¶ ¶ If Israel Attacks Iran Watch Video¶ The national security community says the threat of cyber attack is real, and the gap between terrorist aspirations and capability is closing. The senior intelligence official at Cyber Command, Rear Adm. Samuel Cox, has said al Qaeda operatives are seeking the capability to stage cyber attacks against U.S. networks and terrorists could purchase the capabilities to do so from expert criminal hackers.¶ Increasing evidence also suggests that Iran is looking to commit cyber attacks against the United States, according to testimony last month before the House Committee on Homeland Security. Iran's sponsorship of terrorist groups takes on a new dimension in cyberspace, where it could develop a powerful cyber weapon and pass it on to a terrorist group..¶ Lieberman is using the al Qaeda video to underline what he says is the need for new legislation..¶ "Congress needs to act now to protect the American public from a possible devastating attack on our electric grid, water delivery systems, or financial networks," he said. "As numerous, bipartisan national security experts have said, minimum cyber security standards for those networks are necessary to protect our national and economic security. That is why the Senate needs to act on our bipartisan Cyber Security Act that requires minimum security performance requirements for key critical infrastructure cyber networks."¶ The Homeland Security Committee says the Department of Homeland Security received more than 50,000 reports of cyber intrusions or attempted intrusions since October, an increase of 10,000 reports over the same period the previous year.

#### Current policy of cyber deterrence risks spoofing- leads to nuclear war.

Gelinas 10

(Ryan Richard, thesis for Master of Arts¶ in Security Studies from Georgetown, “CYBERDETERRENCE AND THE PROBLEM OF ATTRIBUTION” <https://repository.library.georgetown.edu/bitstream/handle/10822/553494/gelinasRyan.pdf?sequence=1>, SEH)

The set of cases analyzed here demonstrate decisively that attribution of cyber attacks is ¶ technically difficult and often politically unpalatable. Established networking protocols allow ¶ easy spoofing and obfuscation of source, destination, and intent of packets as they stream around ¶ the world. Attribution, as demonstrated in these cases, is often circumstantial at best. While ¶ victims often have strong suspicions of attackers‘ identities built from pieces of intelligence, the ¶ decisions of war and peace involved in a deterrence policy require a higher level of confidence ¶ than a measured hunch. To reach even elementary levels of attribution significant resources, ¶ expertise, and time are required.¶ The chilling suspicion of the unknown unknowns, the realization that undetected attacks ¶ may be underway at any moment, is potentially paralyzing to any deterrence policy. A ¶ deterrence policy of ―I will attack you back if you attack me, but only if I find out that you did it‖ ¶ is not an appropriate cornerstone of a computer network defense strategy. Without a response, ¶ an attacker can assume that the victim is either unable to detect the attack or, even more ¶ emboldening, the victim is unable or unwilling to make good on its threat. Cyber attacks can be ¶ a powerful part of salami tactics on the part of the attacker. If attacks are unable to generate a ¶ deterrent response in the cyber realm, what other lines can the attacker cross?¶ Addressing cases where the victim state realizes that it is being attacked, Lt. Gen. Keith ¶ Alexander, director of the National Security Agency, recently proposed that his future U.S. ¶ CYBERCOMMAND would support a deterrence doctrine by attacking back in a proportional and discriminating way against the sources of any cyber attack against the United States.¶ 69¶ He ¶ extended this case specifically to those where the identities of the attackers are unknown. ¶ According to Gen. Alexander, the U.S. will attack back in accordance with the rules of ¶ engagement and in accordance with the principles of proportionality and discrimination, with the ¶ caveat that ―neither proportionality nor discrimination requires that we know who is responsible ¶ before we take defensive action.‖¶ 70¶ With statements like this, Gen. Alexander and others are ¶ providing a strong incentive for enemies of the U.S. to launch cyber attacks on the United States ¶ from third-party territory, hoping to lure the U.S. into conflict with a nation that had no role in or ¶ idea of the attack.¶ What the cases analyzed in this paper illustrate is that deterrence is a phenomenally poor ¶ choice as a core component in a computer network defense strategy. Bloviation and bluster, ¶ vowing deterrent responses to attacks, make for good sound bites and allow for easy porting of¶ deep deterrence scholarship to the cyber realm. But less flashy policies and measures are more ¶ effective. Defense in depth, better security standards for software and hardware, robust ¶ computer network intelligence systems, and information sharing between and among industry ¶ and government are all good and necessary elements of a more successful computer network ¶ defense strategy. Combined with aggressive hack-back defensive measures that work to disrupt ¶ or exploit attacker infrastructure, vital networks will be better defended and deterrence as a ¶ general national policy tool will be better preserved for realms where it is more applicable.

#### That risks terrorism

Defense Science Board 8

(The DSB is a Federal ¶ Advisory Committee established to provide independent advice to the Secretary of ¶ Defense, “More Fight – Less Fuel” <http://www.acq.osd.mil/dsb/reports/ADA477619.pdf>, SEH)

DoD’s key problem with electricity is that critical missions, such as national strategic ¶ awareness and national command authorities, are almost entirely dependent on the ¶ national transmission grid. About 85% of the energy infrastructure upon which DoD ¶ depends is commercially owned, and 99% of the electrical energy DoD installations ¶ consume originates outside the fence.¶ 3¶ As noted below, however, the grid is fragile, ¶ vulnerable, near its capacity limit, and outside of DoD control. In most cases, neither ¶ the grid nor on-base backup power provides sufficient reliability to ensure continuity of ¶ critical national priority functions and oversight of strategic missions in the face of a long ¶ term (several months) outage. ¶ 2.3.1 State of the Grid ¶ The U.S.-Canadian electric grid is very efficient and cost effective but its design metric ¶ is efficiency more than resiliency. As a consequence, it is vulnerable to natural disaster or deliberate attack. The Task Force received several briefings from the Mission ¶ Assurance Division at Dahlgren (MAD), the Department of Energy and the utility ¶ industry. Based on these briefings, the Task Force is concerned about the condition of ¶ the grid and the ability to effect timely repairs. ¶ This concern extends not only to the complete dependency of critical national security ¶ missions on the grid, but also to its centrality to all facets of the nation’s economic life. ¶ To appreciate the seriousness of the impacts of an extended disruption, consider the ¶ 2003 Northeast blackout. At around 4:15pm EST on August 14, 2003 about 50 million ¶ people living in a 9,300 square mile area in the U.S. and Canada lost electrical power. ¶ More than 500 generating units at 265 power plants shut down during the outage, 22 of ¶ which were nuclear. Those plants took about two weeks to regain full capacity, and lost ¶ an average of more than half their capacity for 12 days. The shutdown was in part ¶ precautionary in nature. If an imbalance between load and supply occurs, power lines ¶ grow longer and sag from overheating and other hardware can fail. These imbalances ¶ can damage equipment that is hard-to-repair, requires long lead time to produce and is ¶ expensive. So, the grid quickly disconnects itself when a threatening imbalance is ¶ detected. Nuclear plants are required for safety reasons to shut down when the grid ¶ they’re connected to is de-energized.¶ 4¶ A U.S.-Canada Task Force found the main cause of the blackout to be the failure of a ¶ utility in Ohio to properly trim trees near a power line, causing the first in what became a ¶ set of cascading failures.¶ 5¶ Secretary of Energy Spencer Abraham said there would be ¶ no punishment for the utility because current U.S. law does not require electric reliability ¶ standards. However, the Energy Policy Act of 2005 (EPAct 2005) gave the Federal ¶ Energy Regulatory Commission (FERC) new authority to direct the industry to develop ¶ reliability standards. It directs FERC to designate an Electric Reliability Organization ¶ (ERO) to develop and propose reliability standards, which only after agreement by the ¶ industry become mandatory. The ERO chosen by the FERC is a volunteer, industry run ¶ organization. While FERC oversight of industry developed standards is an ¶ improvement over the previous situation, the Task Force remains concerned that FERC ¶ may be unable to reduce the risk to critical DoD missions to acceptable levels in a ¶ reasonable timeframe. ¶ Some have argued that the August 2003 incident shows that the protections built into ¶ the grid worked. Within several hours electricity was restored to many areas, though a ¶ few areas waited nearly a week. However, the incident highlights how easily the power ¶ grid could be taken down. Also, quick restoration was possible because no significant ¶ equipment was damaged, something that might not occur in future incidents. Further, ¶ during the blackout most systems failed that would detect unauthorized border ¶ crossings, port landings, or unauthorized access to vulnerable sites. Future such blackouts could be exploited for terrorist activity, with potentially far more catastrophic ¶ results. ¶ These risks exist elsewhere than in the U.S. For example, on September 28, 2003 Italy ¶ experienced the largest of a series of blackouts suffered through that year, affecting a ¶ total of 56 million people, and spilling into Switzerland.¶ 6¶ It was also the most serious ¶ blackout in Italy in 20 years. DoD installations located outside the continental United ¶ States (OCONUS) are dependent on the commercial grids serving their locations. ¶ Security of their power supplies and continuation of their missions is as important as ¶ within the U.S.

#### Numerous attempts prove our impact

Wagner 9/11

(Dr. Abraham R. Wagner is a Professor of International and Public Affairs at the ¶ Arnold A. Saltzman Institute of War & Peace Studies at Columbia University. “Counter-Terrorism Technologies -- Taking Stock on 9/11” 09/11/2012 2:13 pm accessed online September 11, 2012 at <http://www.huffingtonpost.com/abraham-r-wagner/counterterrorism-technolo_b_1874521.html>, TSW)

On this 11th anniversary of the 9/11 attacks, it makes sense to take stock of where the nation has progressed in its effort to deter and combat future terrorist attacks, both at home and abroad. The 9/11 attacks came as a shock, and have rightfully come to be regarded as a major U.S. intelligence failure. In the aftermath, the nation undertook significant organizational reforms designed to enable more effective intelligence and law enforcement operations against evolving terrorist threats. The country also looked to see what science, engineering and technology could do to help addresses these threats.¶ Technology has long been the nation's strong suit. Americans tend to believe that where there is a problem, there must certainly be a solution and it most likely involves technology and money. During the decade that followed 9/11, billions of dollars were spent on a vast range of programs and technologies in the name of counter-terrorism. For the first two years after 9/11, I joined with other scientists and engineers at the Department of Defense and the Intelligence Community in efforts to identify the most promising approaches to the problem. Ultimately we found that there was no magic bullet or perfect solution to this thorny problem, but were able to suggest a range of investments that could be made to address the evolving terrorist threat.¶ An honest assessment of these investments in counter-terrorism technologies reveals that the results have been mixed -- as one might well expect. A combination of greatly improved intelligence and law enforcement personnel have employed some of the better technologies with considerable success. Indeed, some 45 terrorist plots have been stopped and others deterred. How much of this has been simply luck and how much can be traced to any new technology program is a matter of debate, and there are clearly examples of both that can be found.¶ One area where technology has made a significant contribution has been in new systems to aid in intelligence and surveillance against terrorist operations. While terrorists may hold to an eighth century ideology, they have not been reluctant to employ 21st century communications and information technologies. They have utilized the Internet and cell phones for a number of purposes, and at the time of 9/11 the nation was in need of systems to intercept and sort out terrorist communications. While highly sensitive, public disclosures about several key programs show that considerable progress has been made in this critical area, giving the intelligence agencies some key tools in locating terrorists and stopping their plots. Aside from communications intercept, a new area of "data mining" has also shown considerable promise in locating terrorists and their plots.¶ At the same time, several of key surveillance programs used for counter-terrorism have come under fire from civil liberties groups as being unconstitutional violations of the Fourth Amendment privacy protections, and others. Critics of the Bush Administration saw this as "running roughshod over the Constitution." Even now there are still federal court challenges to laws such as the 2008 FISA Amendments Act and others that have enabled counter-terrorist efforts since 9/11. Ultimately a balance needs to be struck between the essential needs for intelligence to thwart future attacks and protected privacy rights, but as yet it remains an unsettled area where the Supreme Court will need to rule at some future point in time.¶ Less controversial have been efforts over the past decade to employ new information technologies to what has been termed the Information Sharing Environment -- collaborative efforts to best utilize available intelligence and other data among the various federal, state and local agencies with counter-terrorism responsibilities. While certainly some progress has been made over the past 11 years, the net result is largely a national embarrassment, and clearly a triumph of politics over physics. The information and communications technologies are all well-developed, but multiple bureaucracies have generated a set of plans and an even larger set of excuses as to why the fundamental problems in this area remain to be solved.

#### Leads to a bioattack.

De Rugy and Pena 2

, \*policy analyst, \*senior defense policy analyst at the Cato Institute, (Veronique and Charles, “ Responding to the Threat of Smallpox Bioterrorism An Ounce of Prevention Is Best Approach” April 18, Policy Analysis No. 432 <http://www.cato.org/pubs/pas/pa434.pdf>)

There is evidence that al-Qaeda members have been trying to acquire nuclear materials since at least 1994 and have experimented with using chemical weapons (cyanide).4 Intelligence sources have pointed to an alQaeda training camp (called abu-Khabab after the Egyptian chemical-biological weapons expert who directed it) outside Jalalabad, Afghanistan, as a chemical and biological weapons training facility.5 And a manual (“Encyclopedia of Afghan Resistance”) distributed on CD-ROM includes a section on how to make chemical and biological weapons.6 Finally, there is evidence that the September 11 terrorists were interested in crop-dusters, which could be used to distribute a chemical or biological agent.7 Terrorism and WMD Although the use of any WMD by a terrorist group would be an event of devastating proportions, there are differences worth noting and understanding between potential nuclear, chemical, and biological terrorist attacks. A low-yield nuclear weapon would cause immediate damage to a circumscribed area by explosive blast, overpressure, extreme heat, and radiation. If such a weapon were detonated in a major metropolitan area, the casualties would likely be in excess of 100,000 dead, injured, and subjected to lethal doses of radiation.8 The Aum Shinrikyo cult used a chemical weapon, Sarin (a nerve agent so deadly that a single drop on the skin can be fatal) in the 1995 Tokyo subway attack. The attack was not a complete success because of ineffective dissemination, but 12 people died and nearly 3,800 were injured.9 Aum Shinrikyo also used VX (10 to 1,000 times stronger than Sarin) in four other attacks. Those attacks were targeted against specific individuals or groups of people rather than aimed at inflicting massive casualties. In one instance, there was 1 fatality and in another 20 deaths, but the other attacks failed because of ineffective release of the VX agent.10 It is estimated that, under ideal conditions, a quart of VX properly distributed in a major metropolitan area could kill about 12 million people in 60 minutes.11 As catastrophic as either a nuclear or a chemical terrorist attack would be, the effects of the attack would be immediate and limited to people in the vicinity of the attack. Although the damage and casualties would likely be an order of magnitude or more greater than those of the World Trade Center attacks, it would be possible to know that an attack had taken place and respond accordingly. According to D. A. Henderson at Johns Hopkins University, “After an explosion or a chemical attack, the worst effects are quickly over, the dimensions of the catastrophe can be defined, the toll of injuries and deaths can be ascertained, and efforts can be directed to stabilization and recovery.”12 Bioterrorism Is Different from Nuclear or Chemical Attacks The nature of bioterrorism, however, is very different from that of nuclear or chemical attacks. Biological agents are diseasecausing organisms. If the organisms used are contagious pathogens, their effects can be passed on unknowingly, thereby spreading the damage well beyond the people who are initially infected. If successful, a smallpox attack could be more devastating than even a nuclear weapon. Unlike a nuclear or chemical attack, a biological attack would not be detected immediately; there is usually an incubation period of several days to a few weeks before the first symptoms appear in infected persons. Furthermore, it would be difficult to know immediately whether infection was the result of a natural outbreak of a disease or of a premeditated release of the pathogen. And even if there is an antidote for the disease, detection of the attack may occur too late for the antidote to be effective. The devastation that could be caused by a biological attack can be demonstrated by the natural outbreak of influenza in the United States during the winter of 1918–19. The first signs of the influenza virus (the symptoms being no different than those of a common cold, which further highlights the difficulties associated with detecting and diagnosing biological infection) occurred in the spring of 1918 in military camps throughout the United States. American soldiers carried the flu to Europe where it mutated into a killer virus. Returning troops brought the disease back to the United States where it spread to the civilian population. By the fall of 1918 the United States was in the grips of an influenza epidemic that killed an estimated 675,000 Americans.13 But, unlike a natural outbreak of a disease such as influenza, a bioterrorist attack would be an intentional release of a deadly disease by a thinking enemy intent on inflicting mass casualties. In all likelihood, an effective bioterrorist attack would ultimately exact a similar or greater toll. The threat of bioterrorism is especially worrisome because of the vulnerability of the U.S. population to such an attack. Indeed, according to the Chemical and Biological Arms Control Institute, “The vulnerabilities of the United States to bioterrorism attack are virtually infinite.”14 As a result, the problem of bioterrorism can paralyze policymakers and response planners. Frequently, such a large threat is downplayed, dismissed, or ignored. For example, Milton Leitenberg at the Center for International and Security Studies at the University of Maryland wrote (before September 11), “As regards bioterrorism, the current national discussion is characterized by gross exaggeration, hype, and abstract vulnerability assessments.”15 Leitenberg further asserted, “The greatest problem that the United States—and the world—face regarding biological weapons is their proliferation among nation states, and not the potential of their use by non-state, or ‘terrorist’ actors.”16 In other words—at least before September 11—Leitenberg thought not only that the threat of bioterrorism was exaggerated but also that terrorists were not the problem the United States should focus on. September 11 demonstrated that the United States can ill afford such an attitude. No one can predict a bioterrorist attack with high certainty and confidence. But a simple “back of the envelope” threat assessment using a model used by Col. Lani Kass (USAF, Ret.) at the National War College,17 Vulnerability x Intentions x Capabilities = Threat provides insight about and understanding of the potential of a future bioterrorist attack. The vulnerability of the United States to such an attack is quite high. The attacks on the World Trade Center and the Pentagon demonstrate the seriousness of al-Qaeda’s intentions. The big unknown is whether alQaeda possesses the capabilities to carry out an attack with biological weapons. But, as demonstrated by September 11, the United States can ill afford to ignore the possibility. The Smallpox Threat A bioterrorist attack could come in one (or more) of many forms (plague, smallpox, or anthrax, for example). Of those, smallpox is the threat most often discussed. Concerns about smallpox as a potential bioweapon were heightened when Ken Alibek, a former deputy director of the Soviet Union’s civilian bioweapons program, alleged that the Soviet government produced the smallpox virus in large quantities and weaponized it. Alibek also contended that Russia continued the program after the disintegration of the USSR.18 Given the deterioration of the Russian military and the supporting industrial complex, there are legitimate concerns that equipment, expertise, and possibly even the virus or weaponized smallpox19 could have fallen into non-Russian hands.20 Smallpox is an especially serious threat because of its high case-fatality rate (30 percent or more of unvaccinated persons)21 and transmissibility (it spreads easily via inhalation of droplets or direct contact with contaminated objects such as clothing or bed linens).22 There is also no known effective treatment for smallpox.23 Smallpox has long been feared as the most devastating of all infectious diseases (before its supposed eradication from the world in 1978, smallpox had killed more people than any other infectious disease in human history),24 and its potential for devastation is far greater today since there has been no routine vaccination in the United States for more than 25 years. 25 Therefore, in a highly susceptible and mobile population, smallpox would be able to spread widely and rapidly. The smallpox virus is also easy to disperse. It is one of the smallest living organisms and can be easily prepared as an aerosol and released into the air in a crowded place such as a shopping mall or a sports stadium. Or a suicide terrorist with the virus could infect passersby simply by coughing and sneezing, which can release millions of virus particles into the air.26 One example of the magnitude of the consequences of a potential bioterrorist attack with smallpox is the Dark Winter exercise conducted in June 2001.27 Dark Winter was a fictional scenario depicting a terrorist attack using smallpox released via aerosol at three shopping malls in Oklahoma, Georgia, and Pennsylvania. On day 1 of the crisis (nine days after initial exposure), all that was known was that some two dozen people reported to hospitals in Oklahoma City (there were no similar signs of potential outbreak in Georgia and Pennsylvania where the dispersion was not as effective but nonetheless resulted in infected people) with flulike symptoms of a strange illness, which was later confirmed by the Centers for Disease Control as smallpox. Assuming that each case was expected to infect at least 10 other people,28 on day 6 of the crisis there were 2,000 known cases of smallpox and 300 deaths. Due to limited amounts (12 million doses) on hand, the reserve of smallpox vaccine was effectively used up on day 6. By day 12 of the crisis, there were 3,000 cases and 1,000 dead in 25 states. With no vaccine, the smallpox virus was projected to explode as follows: • After 3 weeks: 30,000 cases and 10,000 dead • After 5 weeks: 300,000 cases and 100,000 dead • After 7 weeks: 3 million cases and 1 million dead It is important to emphasize that the purpose of the Dark Winter exercise was not to make the case that smallpox is the weapon most likely to be used in a bioterrorist attack (it is impossible to make such predictions). However, the Dark Winter exercise did demonstrate that the use of a contagious pathogen as a weapon of bioterrorism can have devastating and far-reaching effects. The consequences of an attack with smallpox are potentially catastrophic, and such an attack is the only external threat to the continued existence of the United States other than a massive nuclear attack from Russia. Therefore, even if likelihood cannot be established, the effects of smallpox as a weapon of bioterrorism warrant taking the threat seriously in order to understand the efficacy of potential response options. Also, preventive measures, which might act as a potential deterrent, reduce the risk, and mitigate the consequences of an attack, need to be examined and evaluated.

#### Terrorists can obtain Bio-weapons and will use them – Syria Demise

Blair ‘12

(Charles P. Blair joined FAS in June 2010. He is the Senior Fellow on State and Non-State Threats. Born and raised in Los Alamos, New Mexico, Mr. Blair was an exchange student in Moscow in the mid-1980s, witnessing firsthand the closing salvos of the Cold War. Since the end of that era, Mr. Blair has worked on issues relating to the diffusion and diversification of weapons of mass destruction (WMD) in the context of proliferation amid the rise of mass casualty terrorism incidents and the centripetal and centrifugal elements of globalization. Mr. Blair’s work focuses on state and violent non-state actors (VNSA) – amid a dystopic and increasingly tribal world. “Fearful of a nuclear Iran? The real WMD nightmare is Syria” 1 MARCH 2012 accessed online August 22, 2012 at http://www.thebulletin.org/web-edition/op-eds/fearful-of-nuclear-iran-the-real-wmd-nightmare-syria)

As possible military action against Iran's suspected nuclear weapons program looms large in the public arena, far more international concern should be directed toward Syria and its weapons of mass destruction. When the Syrian uprising began more than a year ago, few predicted the regime of President Bashar al-Assad would ever teeter toward collapse. Now, though, the demise of Damascus's current leadership appears inevitable, and Syria's revolution will likely be an unpredictable, protracted, and grim affair. Some see similarities with Libya's civil war, during which persistent fears revolved around terrorist seizure of Libyan chemical weapons, or the Qaddafi regime's use of them against insurgents. Those fears turned out to be unfounded.¶ But the Libyan chemical stockpile consisted of several tons of aging mustard gas leaking from a half-dozen canisters that would have been impossible to utilize as weapons. Syria likely has one of the largest and most sophisticated chemical weapon programs in the world. Moreover, Syria may also possess an offensive biological weapons capability that Libya did not.¶ While it is uncertain whether the Syrian regime would consider using WMD against its domestic opponents, Syrian insurgents, unlike many of their Libyan counterparts, are increasingly sectarian and radicalized; indeed, many observers fear the uprising is being "hijacked" by jihadists. Terrorist groups active in the Syrian uprising have already demonstrated little compunction about the acquisition and use of WMD. In short, should Syria devolve into full-blown civil-war, the security of its WMD should be of profound concern, as sectarian insurgents and Islamist terrorist groups may stand poised to seize chemical and perhaps even biological weapons.¶ An enormous unconventional arsenal. Syria's chemical weapons stockpile is thought to be massive. One of only eight nations that is not a member of the Chemical Weapons Convention -- an arms control agreement that outlaws the production, possession, and use of chemical weapons -- Syria has a chemical arsenal that includes several hundred tons of blistering agents along with likely large stockpiles of deadly nerve agents, including VX, the most toxic of all chemical weapons. At least four large chemical weapon production facilities exist. Additionally, Syria likely stores its deadly chemical weapons at dozens of facilities throughout the fractious country. In contrast to Libya's unusable chemical stockpile, analysts emphasize that Syrian chemical agents are weaponized and deliverable. Insurgents and terrorists with past or present connections to the military might feasibly be able to effectively disseminate chemical agents over large populations. (The Global Security Newswire recently asserted that "[t]he Assad regime is thought to possess between 100 and 200 Scud missiles carrying warheads loaded with sarin nerve agent. The government is also believed to have several hundred tons of sarin agent and mustard gas stockpiled that could be used in air-dropped bombs and artillery shells, according to information compiled by the James Martin Center.")¶ Given its robust chemical weapons arsenal and its perceived need to deter Israel, Syria has long been suspected of having an active biological weapons program. Despite signing the Biological Weapons and Toxins Convention in 1972 (the treaty prohibits the development, production, and stockpiling of biological and toxin weapons), Syria never ratified the treaty. Some experts contend that any Syrian biological weapons program has not moved beyond the research and development phase. Still, Syria's biotechnical infrastructure undoubtedly has the capability to develop numerous biological weapon agents. After Israel destroyed a clandestine Syrian nuclear reactor in September 2007, Damascus may have accelerated its chemical and biological weapons programs.¶ It's hard to guard WMD when a government collapses. Although the United States and its allies are reportedly monitoring Syria's chemical weapons, recent history warns that securing them from theft or transfer is an extraordinary challenge. For example, during Operation Iraqi Freedom, more than 330 metric tons of military-grade high explosives vanished from Iraq's Al-Qaqaa military installation. Almost 200 tons of the most powerful of Iraq's high-explosives, HMX -- used by some states to detonate nuclear weapons -- was under International Atomic Energy Agency seal. Many tons of Al-Qaqaa's sealed HMX reportedly went missing in the early days of the war in Iraq. Forensic tests later revealed that some of these military-grade explosives were subsequently employed against US and coalition forces.¶ Even with a nationwide presence of 200,000 coalition troops, several other sensitive military sites were also looted, including Iraq's main nuclear complex, Tuwaitha. Should centralized authority crumble in Syria, it seems highly unlikely that the country's 50 chemical storage and manufacturing facilities -- and, possibly, biological weapon repositories -- can be secured. The US Defense Department recently estimated that it would take more than 75,000 US military personnel to guard Syria's chemical weapons. This is, of course, if they could arrive before any WMD were transferred or looted -- a highly unlikely prospect.¶ Complicating any efforts to secure Syria's WMD, post-Assad, are its porous borders. With Syria's government distracted by internal revolt and US forces now fully out of Iraq, it is plausible that stolen chemical or biological weapons could find their way across the Syrian border into Iraq. Similarly, Syrian WMD could be smuggled into southern Turkey, Jordan, Lebanon, the West Bank, Israel, and, potentially, the United States and Europe.¶ At least six formal terrorist organizations have long maintained personnel within Syria. Three of these groups -- Hamas, Hizbollah, and Palestinian Islamic Jihad -- have already attempted to acquire or use chemical or biological agents, or both. Perhaps more troubling, Al Qaeda-affiliated fighters from Iraq have streamed into Syria, acting, in part, on orders from Al Qaeda leader Ayman al-Zawahiri. In the past, Al Qaeda-in-Iraq fighters attempted to use chemical weapons, most notably attacks that sought to release large clouds of chlorine gas. The entry of Al Qaeda and other jihadist groups into the Syrian crisis underscores its increasingly sectarian manifestation. Nearly 40 percent of Syria's population consists of members of minority communities. Syria's ruling Alawite regime, a branch of Shia Islam, is considered heretical by many of Syria's majority Sunni Muslims -- even those who are not jihadists. Alawites, Druze, Kurds, and Christians could all become targets for WMD-armed Sunni jihadists. Similarly, Shiite radicals could conceivably employ WMD agents against Syria's Sunnis.¶ Religious fanaticism and WMD. Evidence of growing religious fanaticism is also reflected in recent Syrian suicide attacks. Since last December, at least five suicide attacks occurred in Syria. In the 40 years preceding, only two suicide attacks were recorded. Al Qaeda-linked mujahidin are believed to be responsible for all of these recent attacks. Civil wars are often the most violent and unpredictable manifestations of war. With expanding sectarian divisions, the use of seized WMD in Syria's uprising is plausible. To the extent that religious extremists believe that they are doing God's bidding, fundamentally any action they undertake is justified, no matter how abhorrent, since the "divine" ends are believed to legitimize PDF the means.¶ The situation in Syria is unprecedented. Never before has a WMD-armed country fallen into civil war. All states in the region stand poised to lose if these weapons find their way outside of Syria. The best possible outcome, in terms of controlling Syria's enormous WMD arsenal, would be for Assad to maintain power, but such an outcome seems increasingly implausible. And there is painfully little evidence that democratic forces are likely to take over in Syria. Even if they do eventually triumph, it will take months or years to consolidate control over the entire country.¶ If chaos ensues in Syria, the United States cannot go it alone in securing hundreds of tons of Syrian WMD. Regional leaders -- including some, such as Sunni Saudi Arabia and Shiite Iran, that are now backing the insurgency and the regime, respectively -- must come together and begin planning to avert a dispersion of Syrian chemical or biological weapons that would threaten everyone, of any political or religious persuasion, in the Middle East and around the world.

#### Extinction

Ochs 2

**(**Richard, Naturalist – Grand Teton National park with Masters in Natural Resource Management – Rutgers, “Biological Weapons must be abolished immediately” 6-9, http://www.freefromterror.net/other\_articles/abolish.html)

Of all the weapons of mass destruction, the genetically engineered biological weapons, many without a known cure or vaccine, are an extreme danger to the continued survival of life on earth. Any perceived military value or deterrence pales in comparison to the great risk these weapons pose just sitting in vials in laboratories. While a "nuclear winter," resulting from a massive exchange of nuclear weapons, could also kill off most of life on earth and severely compromise the health of future generations, they are easier to control. Biological weapons, on the other hand, can get out of control very easily, as the recent anthrax attacks has demonstrated. There is no way to guarantee the security of these doomsday weapons because very tiny amounts can be stolen or accidentally released and then grow or be grown to horrendous proportions. The Black Death of the Middle Ages would be small in comparison to the potential damage bioweapons could cause. Abolition of chemical weapons is less of a priority because, while they can also kill millions of people outright, their persistence in the environment would be less than nuclear or biological agents or more localized. Hence, chemical weapons would have a lesser effect on future generations of innocent people and the natural environment. Like the Holocaust, once a localized chemical extermination is over, it is over. With nuclear and biological weapons, the killing will probably never end. Radioactive elements last tens of thousands of years and will keep causing cancers virtually forever. Potentially worse than that, bio-engineered agents by the hundreds with no known cure could wreck even greater calamity on the human race than could persistent radiation. AIDS and ebola viruses are just a small example of recently emerging plagues with no known cure or vaccine. Can we imagine hundreds of such plagues? HUMAN EXTINCTION IS NOW POSSIBLE.

#### Even if it doesn’t kill everyone retaliation would

Conley 03

(Harry W., chief of the systems analysis Branch, Directorate of Requirements, Air and Space Power Journal- Spring 2003- http://www.airpower.maxwell.af.mil/airchronicles/apj/apj03/spr03/conley.html

The number of American casualties suffered due to a WMD attack may well be the most important variable in determining the nature of the US reprisal. A key question here is how many Americans would have to be killed to prompt a massive response by the United States. The bombing of marines in Lebanon, the Oklahoma City bombing, and the downing of Pan Am Flight 103 each resulted in a casualty count of roughly the same magnitude (150–300 deaths). Although these events caused anger and a desire for retaliation among the American public, they prompted no serious call for massive or nuclear retaliation. The body count from a single biological attack could easily be one or two orders of magnitude higher than the casualties caused by these events. Using the rule of proportionality as a guide, one could justifiably debate whether the United States should use massive force in responding to an event that resulted in only a few thousand deaths. However, what if the casualty count was around 300,000? Such an unthinkable result from a single CBW incident is not beyond the realm of possibility: “According to the U.S. Congress Office of Technology Assessment, 100 kg of anthrax spores delivered by an efficient aerosol generator on a large urban target would be between two and six times as lethal as a one megaton thermo-nuclear bomb.”46 Would the deaths of 300,000 Americans be enough to trigger a nuclear response? In this case, proportionality does not rule out the use of nuclear weapons. Besides simply the total number of casualties, the types of casualties- predominantly military versus civilian- will also affect the nature and scope of the US reprisal action. Military combat entails known risks, and the emotions resulting from a significant number of military casualties are not likely to be as forceful as they would be if the attack were against civilians. World War II provides perhaps the best examples for the kind of event or circumstance that would have to take place to trigger a nuclear response. A CBW event that produced a shock and death toll roughly equivalent to those arising from the attack on Pearl Harbor might be sufficient to prompt a nuclear retaliation. President Harry Truman’s decision to drop atomic bombs on Hiroshima and Nagasaki- based upon a calculation that up to one million casualties might be incurred in an invasion of the Japanese homeland 47- is an example of the kind of thought process that would have to occur prior to a nuclear response to a CBW event. Victor Utgoff suggests that “if nuclear retaliation is seen at the time to offer the best prospects for suppressing further CB attacks and speeding the defeat of the aggressor, and if the original attacks had caused severe damage that had outraged American or allied publics, nuclear retaliation would be more than just a possibility, whatever promises had been made.”48

## Advantage 2 Leadership

#### SMR key to nuclear leadership

Rosner and Goldberg 11

(Robert Rosner, astrophysicist and founding director of the Energy Policy Institute at Chicago. He was the director of Argonne National Laboratory from 2005 to 2009, Stephen Goldberg, Special Assistant to the Director, Argonne National Laboratory ¶ Senior Fellow, Energy Policy Institute at Chicago¶ Research Coordinator, Global Nuclear Future Initiative ¶ American Academy of Arts and Sciences, “Small Modular Reactors – Key to Future Nuclear Power ¶ Generation in the U.S.” Energy Policy Institute at Chicago, <http://csis.org/files/attachments/111129_SMR_White_Paper.pdf>, SEH)

As stated earlier, SMRs have the potential to achieve significant greenhouse gas emission ¶ reductions. They could provide alternative baseload power generation to facilitate the retirement ¶ of older, smaller, and less efficient coal generation plants that would, otherwise, not be good ¶ candidates for retrofitting carbon capture and storage technology. They could be deployed in ¶ regions of the U.S. and the world that have less potential for other forms of carbon-free ¶ electricity, such as solar or wind energy. There may be technical or market constraints, such as ¶ projected electricity demand growth and transmission capacity, which would support SMR ¶ deployment but not GW-scale LWRs. From the on-shore manufacturing perspective, a key point ¶ is that the manufacturing base needed for SMRs can be developed domestically. Thus, while the ¶ large commercial LWR industry is seeking to transplant portions of its supply chain from current ¶ foreign sources to the U.S., the SMR industry offers the potential to establish a large domestic ¶ manufacturing base building upon already existing U.S. manufacturing infrastructure and ¶ capability, including the Naval shipbuilding and underutilized domestic nuclear component and ¶ equipment plants. The study team learned that a number of sustainable domestic jobs could be ¶ created – that is, the full panoply of design, manufacturing, supplier, and construction activities – ¶ if the U.S. can establish itself as a credible and substantial designer and manufacturer of SMRs. ¶ While many SMR technologies are being studied around the world, a strong U.S. ¶ commercialization program can enable U.S. industry to be first to market SMRs, thereby serving ¶ as a fulcrum for export growth as well as a lever in influencing international decisions on ¶ deploying both nuclear reactor and nuclear fuel cycle technology. A viable U.S.-centric SMR ¶ industry would enable the U.S. to recapture technological leadership in commercial nuclear ¶ technology, which has been lost to suppliers in France, Japan, Korea, Russia, and, now rapidly ¶ emerging, China.

#### US dominance in SMR’s key to nuclear leadership which prevents proliferation

Loudermilk 11

(Micah J. Loudermilk is a Research Associate for the Energy & Environmental Security Policy program with the Institute for National Strategic Studies at National Defense University, “Small Nuclear Reactors and US Energy Security: Concepts, Capabilities, and Costs” Journal of Energy Security, May 2011, <http://www.ensec.org/index.php?option=com_content&view=article&id=314:small-nuclear-reactors-and-us-energy-security-concepts-capabilities-and-costs&catid=116:content0411&Itemid=375>, SEH)

Combating proliferation with US leadership¶ Reactor safety itself notwithstanding, many argue that the scattering of small reactors around the world would invariably lead to increased proliferation problems as nuclear technology and know-how disseminates around the world. Lost in the argument is the fact that this stance assumes that US decisions on advancing nuclear technology color the world as a whole. In reality, regardless of the US commitment to or abandonment of nuclear energy technology, many countries (notably China) are blazing ahead with research and construction, with 55 plants currently under construction around the world—though Fukushima may cause a temporary lull.¶ Since Three Mile Island, the US share of the global nuclear energy trade has declined precipitously as talent and technology begin to concentrate in countries more committed to nuclear power. On the small reactor front, more than 20 countries are examining the technology and the IAEA estimates that 40-100 small reactors will be in operation by 2030. Without US leadership, new nations seek to acquire nuclear technology turn to countries other than the US who may not share a deep commitment to reactor safety and nonproliferation objectives. Strong US leadership globally on nonproliferation requires a vibrant American nuclear industry. This will enable the US to set and enforce standards on nuclear agreements, spent fuel reprocessing, and developing reactor technologies.¶ As to the small reactors themselves, the designs achieve a degree of proliferation-resistance unmatched by large reactors. Small enough to be fully buried underground in independent silos, the concrete surrounding the reactor vessels can be layered much thicker than the traditional domes that protect conventional reactors without collapsing. Coupled with these two levels of superior physical protection is the traditional security associated with reactors today. Most small reactors also are factory-sealed with a supply of fuel inside. Instead of refueling reactors onsite, SMRs are returned to the factory, intact, for removal of spent fuel and refueling. By closing off the fuel cycle, proliferation risks associated with the nuclear fuel running the reactors are mitigated and concerns over the widespread distribution of nuclear fuel allayed.

#### Proliferation risks nuclear war due to brinkmanship games- questions of deterrence miss the point.

Kroenig 12

(Matthew, assistant professor of Government at Georgetown University and a Stanton Nuclear Security Fellow at the Council on Foreign Relations, “The History of Proliferation Optimism: Does It Have A Future?” Non Proliferation Policy Center, <http://npolicy.org/article.php?aid=1182&tid=30#_ftn11>, SEH)

First and foremost, proliferation optimists do not appear to understand contemporary deterrence theory. I do not say this lightly in an effort to marginalize or discredit my intellectual opponents. Rather, I make this claim with all due caution and with complete sincerity. A careful review of the contemporary proliferation optimism literature does not reflect an understanding of, or engagement with, the developments in academic deterrence theory in top scholarly journals such as the American Political Science Review and International Organization over the past few decades.[35] While early optimists like Viner and Brodie can be excused for not knowing better, the writings of contemporary proliferation optimists ignore the past fifty years of academic research on nuclear deterrence theory. ¶ In the 1940s, Viner, Brodie, and others argued that the advent of Mutually Assured Destruction (MAD) rendered war among major powers obsolete, but nuclear deterrence theory soon advanced beyond that simple understanding.[36] After all, great power political competition does not end with nuclear weapons. And nuclear-armed states still seek to threaten nuclear-armed adversaries. States cannot credibly threaten to launch a suicidal nuclear war, but they still want to coerce their adversaries. This leads to a credibility problem: how can states credibly threaten a nuclear-armed opponent? Since the 1960s academic nuclear deterrence theory has been devoted almost exclusively to answering this question.[37] And, unfortunately for proliferation optimists, the answers do not give us reasons to be optimistic.¶ Thomas Schelling was the first to devise a rational means by which states can threaten nuclear-armed opponents.[38] He argued that leaders cannot credibly threaten to intentionally launch a suicidal nuclear war, but they can make a “threat that leaves something to chance.”[39] They can engage in a process, the nuclear crisis, which increases the risk of nuclear war in an attempt to force a less resolved adversary to back down. As states escalate a nuclear crisis there is an increasing probability that the conflict will spiral out of control and result in an inadvertent or accidental nuclear exchange. As long as the benefit of winning the crisis is greater than the incremental increase in the risk of nuclear war, threats to escalate nuclear crises are inherently credible. In these games of nuclear brinkmanship, the state that is willing to run the greatest risk of nuclear war before back down will win the crisis as long as it does not end in catastrophe. It is for this reason that Thomas Schelling called great power politics in the nuclear era a “competition in risk taking.”[40] This does not mean that states eagerly bid up the risk of nuclear war. Rather, they face gut-wrenching decisions at each stage of the crisis. They can quit the crisis to avoid nuclear war, but only by ceding an important geopolitical issue to an opponent. Or they can the escalate the crisis in an attempt to prevail, but only at the risk of suffering a possible nuclear exchange.¶ Since 1945 there were have been many high stakes nuclear crises (by my count, there have been twenty) in which “rational” states like the United States run a risk of nuclear war and inch very close to the brink of nuclear war.[41] By asking whether states can be deterred or not, therefore, proliferation optimists are asking the wrong question. The right question to ask is: what risk of nuclear war is a specific state willing to run against a particular opponent in a given crisis? Optimists are likely correct when they assert that Iran will not intentionally commit national suicide by launching a bolt-from-the-blue nuclear attack on the United States or Israel. This does not mean that Iran will never use nuclear weapons, however. Indeed, it is almost inconceivable to think that a nuclear-armed Iran would not, at some point, find itself in a crisis with another nuclear-armed power and that it would not be willing to run any risk of nuclear war in order to achieve its objectives. If a nuclear-armed Iran and the United States or Israel have a geopolitical conflict in the future, over say the internal politics of Syria, an Israeli conflict with Iran’s client Hezbollah, the U.S. presence in the Persian Gulf, passage through the Strait of Hormuz, or some other issue, do we believe that Iran would immediately capitulate? Or is it possible that Iran would push back, possibly even brandishing nuclear weapons in an attempt to deter its adversaries? If the latter, there is a real risk that proliferation to Iran could result in nuclear war.¶ An optimist might counter that nuclear weapons will never be used, even in a crisis situation, because states have such a strong incentive, namely national survival, to ensure that nuclear weapons are not used. But, this objection ignores the fact that leaders operate under competing pressures. Leaders in nuclear-armed states also have very strong incentives to convince their adversaries that nuclear weapons could very well be used. Historically we have seen that in crises, leaders purposely do things like put nuclear weapons on high alert and delegate nuclear launch authority to low level commanders, purposely increasing the risk of accidental nuclear war in an attempt to force less-resolved opponents to back down.¶ Moreover, not even the optimists’ first principles about the irrelevance of nuclear posture stand up to scrutiny. Not all nuclear wars would be equally devastating.[42] Any nuclear exchange would have devastating consequences no doubt, but, if a crisis were to spiral out of control and result in nuclear war, any sane leader would rather be facing a country with five nuclear weapons than one with thirty-five thousand. Similarly, any sane leader would be willing to run a greater risk of nuclear war against the former state than against the latter. Indeed, systematic research has demonstrated that states are willing to run greater risks and, therefore, more likely to win nuclear crises when they enjoy nuclear superiority over their opponent.[43] Proliferation optimists miss this point, however, because they are still mired in 1940s deterrence theory. It is true that no rational leader would choose to launch a nuclear war, but, depending on the context, she would almost certainly be willing to risk one. Nuclear deterrence theorists have proposed a second scenario under which rational leaders could instigate a nuclear exchange: a limited nuclear war.[44] By launching a single nuclear weapon against a small city, for example, it was thought that a nuclear-armed state could signal its willingness to escalate the crisis, while leaving its adversary with enough left to lose to deter the adversary from launching a full-scale nuclear response. In a future crisis between a nuclear-armed China and the United States over Taiwan, for example, China could choose to launch a nuclear attack on Honolulu to demonstrate its seriousness. In that situation, with the continental United States intact, would Washington choose to launch a full-scale nuclear war on China that could result in the destruction of many more American cities? Or would it back down? China might decide to strike hoping that Washington will choose a humiliating retreat over a full-scale nuclear war. If launching a limited nuclear war could be rational, it follows that the spread of nuclear weapons increases the risk of nuclear use. Again, by ignoring contemporary developments in scholarly discourse and relying exclusively on understandings of nuclear deterrence theory that became obsolete decades ago, optimists reveal the shortcomings of their analysis and fail to make a compelling case.

#### Proliferation draws major powers in to regional disputes

Kroenig 9

(Matthew, assistant professor of Government at Georgetown University and a Stanton Nuclear Security Fellow at the Council on Foreign Relations, “Beyond Optimism and Pessimism: ¶ The Differential Effects of Nuclear Proliferation” Harvard Kennedy School of Government, <http://belfercenter.ksg.harvard.edu/files/Beyond-Optimism-and-Pessimism.pdf>, SEH)

There is direct evidence that regional conflicts involving nuclear powers can ¶ encourage power-projecting states to become involved in nuclear disputes. Secretary of ¶ State Henry Kissinger was reluctant to aid Israel in the 1973 Yom Kippur War until Israeli ¶ Prime Minister Golda Meir threatened that, without U.S. assistance, she might be forced to ¶ use nuclear weapons against the Arab armies.¶ 52¶ In response, Kissinger reversed his decision ¶ and provided emergency aid to the Israeli Defense Forces.¶ 53¶ The Soviet Union also ¶ considered a military intervention to help its Arab proxies in the Yom Kippur War, causing ¶ the United States to go on nuclear alert, and leading leaders in both Moscow and ¶ Washington to consider the very real possibility that a conflict involving a regional nuclear ¶ power could spiral into a superpower war.¶ 54¶ Similarly, in 1999 and 2002, the United States became caught in diplomatic initiatives to prevent nuclear war in crises between the nuclear armed countries of India and Pakistan.¶ 55¶ ¶ Indeed, the expectation that powerful states will intervene in conflicts involving a ¶ nuclear-armed state is so firmly ingrained in the strategic thinking of national leaders that ¶ small nuclear powers actually incorporate it into their strategic doctrines. South Africa’s ¶ nuclear doctrine envisioned, in the event of an imminent security threat, the detonation of a ¶ nuclear weapon, not against the threatening party, but over the Atlantic Ocean in an attempt ¶ to jolt the United States into intervening on South Africa’s behalf.¶ 56¶ Israel’s nuclear ¶ doctrine was also constructed along similar lines. While the Israelis are notoriously silent ¶ about the existence and purpose of their nuclear arsenal, Francis Perrin, a French official ¶ who assisted in the development of Israel’s nuclear program in the 1950s and 1960s, ¶ explained that Israel’s arsenal was originally aimed “against the Americans, not to launch ¶ against America, but to say ‘If you don’t want to help us in a critical situation, we will require you to help us. Otherwise, we will use our nuclear bombs. Similarly, Pakistan’s surprise raid on Indian-controlled Kargil in 1999 was motivated partly by the expectation that Pakistan would be able to retain any territory it was able to seize quickly, because Pakistani officials calculated that the United States would never allow an extended conflict in nuclear South Asia.

#### That leads to great power war

Kroenig 9

(Matthew, assistant professor of Government at Georgetown University and a Stanton Nuclear Security Fellow at the Council on Foreign Relations, “Beyond Optimism and Pessimism: ¶ The Differential Effects of Nuclear Proliferation” Harvard Kennedy School of Government, <http://belfercenter.ksg.harvard.edu/files/Beyond-Optimism-and-Pessimism.pdf>, SEH)

Leaders in power-projecting states also fear that regional instability set off by nuclear¶ proliferation could entrap power-projecting states in a great power war. Other power projecting states, facing a mirror-image situation, may feel compelled to intervene in a crisis ¶ to secure their own interests, entangling multiple great powers in a regional conflict. In a¶ 1963 NIE, U.S. intelligence analysts assessed that “the impact of (nuclear proliferation in the¶ Middle East) will be the possibility that hostilities arising out of existing or future ¶ controversies could escalate into a confrontation involving the major powers.”¶ 67¶ President ¶ Johnson believed that a nuclear Israel meant increased Soviet involvement in the Middle¶ East and perhaps superpower war.¶ 68¶ If historical experience provides a guide, U.S. ¶ strategists at the time of writing are undoubtedly concerned by the possibility that China m¶ feel compelled to intervene in any conflict involving a nuclear-armed North Korea, making the Korean Peninsula another dangerous flash-point in the uncertain Sino-American strategic relationship.

#### US investment in SMRs key to beat china

Chu ‘10

(Mr. Chu is the U.S. Secretary of Energy. “America's New Nuclear Option” March 23, 2010 <http://online.wsj.com/article/SB10001424052748704231304575092130239999278.html>)

Perhaps most importantly, investing in nuclear energy will position America to lead in a growing industry. World-wide electricity generation is projected to rise 77% by 2030. If we are serious about cutting carbon pollution then nuclear power must be part of the solution. Countries such as China, South Korea and India have recognized this and are making investments in nuclear power that are driving demand for nuclear technologies. Our choice is clear: Develop these technologies today or import them tomorrow.¶ That is why—even as we build a new generation of clean and safe nuclear plants—we are constantly looking ahead to the future of nuclear power. As this paper recently reported, one of the most promising areas is small modular reactors (SMRs). If we can develop this technology in the U.S. and build these reactors with American workers, we will have a key competitive edge.¶ Small modular reactors would be less than one-third the size of current plants. They have compact designs and could be made in factories and transported to sites by truck or rail. SMRs would be ready to "plug and play" upon arrival.¶ If commercially successful, SMRs would significantly expand the options for nuclear power and its applications. Their small size makes them suitable to small electric grids so they are a good option for locations that cannot accommodate large-scale plants. The modular construction process would make them more affordable by reducing capital costs and construction times.¶ Their size would also increase flexibility for utilities since they could add units as demand changes, or use them for on-site replacement of aging fossil fuel plants. Some of the designs for SMRs use little or no water for cooling, which would reduce their environmental impact. Finally, some advanced concepts could potentially burn used fuel or nuclear waste, eliminating the plutonium that critics say could be used for nuclear weapons.

#### Without increasing nuclear technology, we lose out to China in nuclear leadership. The impact is Asian influence and proliferation.

Cullinane ‘11

[Scott Cullinane is a graduate student at the Institute of World Politics in Washington, D.C <http://www.ensec.org/index.php?option=com_content&view=article&id=319:america-falling-behind-the-strategic-dimensions-of-chinese-commercial-nuclear-energy&catid=118:content&Itemid=376> ETB]

Due to a confluence of events the United States has recently focused more attention on nuclear weapons policy than it has in previous years; however, the proliferation of commercial nuclear technology and its implications for America’s strategic position have been largely ignored. While the Unites States is currently a participant in the international commercial nuclear energy trade, America’s own domestic construction of nuclear power plants has atrophied severely and the US risks losing its competitive edge in the nuclear energy arena.¶ Simultaneously, the People’s Republic of China (PRC) has made great strides in closing the nuclear energy development gap with America. Through a combination of importing technology, research from within China itself, and a disciplined policy approach the PRC is increasingly able to leverage the export of commercial nuclear power as part of its national strategy. Disturbingly, China does not share America’s commitment to stability, transparency, and responsibility when exporting nuclear technology. This is a growing strategic weakness and risk for the United States. To remain competitive and to be in a position to offset the PRC when required the American government should encourage the domestic use of nuclear power and spur the forces of technological innovation.¶ History has recorded well American wartime nuclear developments which culminated in the July 1945 Trinity Test, but what happened near Arco, Idaho six years later has been overlooked. In 1951, scientists for the first time produced usable electricity from an experimental nuclear reactor. Once this barrier was conquered the atom was harnessed to generate electricity and permitted America to move into the field of commercial nuclear power. In the next five years alone the United States signed over 20 nuclear cooperation agreements with various countries. Not only did the US build dozens of power plants domestically during the 1960s and 1970s, the US Export-Import Bank also distributed $7.1 billion dollars in loans and guarantees for the international sale of 49 reactors. American built and designed reactors were exported around the world during those years. Even today, more than 60% of the world’s 440 operating reactors are based on technology developed in the United States. The growth of the US civilian nuclear power sector stagnated after the Three Mile Island incident in 1979 – the most serious accident in American civilian nuclear power history. Three Mile Island shook America’s confidence in nuclear power and provided the anti-nuclear lobby ample fuel to oppose the further construction of any nuclear power plants. In the following decade, 42 planned domestic nuclear power plants were cancelled, and in the 30 years since the Three Mile Island incident the American nuclear power industry has survived only through foreign sales and merging operations with companies in Asia and Europe. Westinghouse sold its nuclear division to Toshiba and General Electric joined with Hitachi. Even the highest levels of the American government came to cast nuclear power aside. President Bill Clinton bragged in his 1993 State of the Union Address that “we are eliminating programs that are no longer needed, such as nuclear power research and development.” ¶ America’s slow pace of reactor construction over the past three decades has stymied innovation and caused the nuclear sector and its industrial base to shrivel. While some aspects of America’s nuclear infrastructure still operate effectively, many critical areas have atrophied. For example, one capability that America has entirely lost is the means to cast ultra heavy forgings in the range of 350,000 – 600,000 pounds, which impacts the construction of containment vessels, turbine rotors, and steam generators. In contrast, Japan, China, and Russia all possess an ultra heavy forging capacity and South Korea and India plan to build forges in this range. Likewise, the dominance America enjoyed in uranium enrichment until the 1970s is gone. The current standard centrifuge method for uranium enrichment was not invented in America and today 40% of the enriched uranium US power plants use is processed overseas and imported. Another measure of how much the US nuclear industry has shrunk is evident in the number of companies certified to handle nuclear material. In the 1980s the United States had 400 nuclear suppliers and 900 holders of N-stamp certificates (N-stamps are the international nuclear rating certificates issued by the American Society of Mechanical Engineers). By 2008 that number had reduced itself to 80 suppliers and 200 N-stamp holders. A recent Government Accountability Office report, which examined data from between 1994 and 2009, found the US to have a declining share of the global commercial nuclear trade. However, during that same period over 60 reactors were built worldwide. Nuclear power plants are being built in the world increasingly by non-American companies.¶ The American nuclear industry entered the 1960s in a strong position, yet over the past 30 years other countries have closed the development gap with America. The implications of this change go beyond economics or prestige to include national security. These changes would be less threatening if friendly allies were the ones moving forward with developing a nuclear export industry;however, the quick advancement of the PRC in nuclear energy changes the strategic calculus for America.¶ The shifting strategic landscape¶ While America’s nuclear industry has languished, current changes in the world’s strategic layout no longer allow America the option of maintaining the status quo without being surpassed. The drive for research, development, and scientific progress that grew out of the Cold War propelled America forward, but those priorities have long since been downgraded by the US government. The economic development of formerly impoverished countries means that the US cannot assume continued dominance by default. The rapidly industrializing PRC is seeking its own place among the major powers of the world and is vying for hegemony in Asia; nuclear power is an example of their larger efforts to marshal their scientific and economic forces as instruments of national power.¶ The rise of China is a phrase that connotes images of a backwards country getting rich off of exporting cheap goods at great social and environmental costs. Yet, this understanding of the PRC has lead many in the United States to underestimate China’s capabilities. The Communist Party of China (CPC) has undertaken a comprehensive long-term strategy to transition from a weak state that lags behind the West to a country that is a peer-competitor to the United States. Nuclear technology provides a clear example of this. ¶ In 1978, General Secretary Deng Xiaoping began to move China out of the destructive Mao era with his policies of 'reform and opening.' As part of these changes during the 1980s, the CPC began a concerted and ongoing effort to modernize the PRC and acquire advanced technology including nuclear technology from abroad. This effort was named Program 863 and included both legal methods and espionage. By doing this, the PRC has managed to rapidly catch up to the West on some fronts. In order to eventually surpass the West in scientific development the PRC launched the follow-on Program 973 to build the foundations of basic scientific research within China to meet the nation’s major strategic needs. These steps have brought China to the cusp of the next stage of technological development, a stage known as “indigenous innovation.”¶ ¶ In 2006 the PRC published their science and technology plan out to 2020 and defined indigenous innovation as enhancing original innovation, integrated innovation, and re-innovation based on assimilation and absorption of imported technology in order improve national innovation capability. The Chinese seek to internalize and understand technological developments from around the world so that they can copy the equipment and use it as a point to build off in their own research. This is a step beyond merely copying and reverse engineering a piece of technology. The PRC sees this process of absorbing foreign technology coupled with indigenous innovation as a way of leapfrogging forward in development to gain the upper hand over the West. The PRC’s official statement on energy policy lists nuclear power as one of their target fields. When viewed within this context, the full range of implications from China’s development of nuclear technology becomes evident. The PRC is now competing with the United States in the areas of innovation and high-technology, two fields that have driven American power since World War Two. China’s economic appeal is no longer merely the fact that it has cheap labor, but is expanding its economic power in a purposeful way that directly challenges America’s position in the world.¶ ¶ The CPC uses the market to their advantage to attract nuclear technology and intellectual capital to China. The PRC has incentivized the process and encouraged new domestic nuclear power plant construction with the goal of having 20 nuclear power plants operational by 2020. The Chinese Ministry of Electrical Power has described PRC policy to reach this goal as encouraging joint investment between State Owned Corporations and foreign companies. 13 reactors are already operating in China, 25 more are under construction and even more reactors are in the planning stages. ¶ In line with this economic policy, China has bought nuclear reactors from Westinghouse and Areva and is cooperating with a Russian company to build nuclear power plants in Taiwan. By stipulating that Chinese companies and personnel be involved in the construction process, China is building up its own domestic capabilities and expects to become self-sufficient. China’s State Nuclear Power Technology Corporation has partnered with Westinghouse to build a new and larger reactor based on the existing Westinghouse AP 1000 reactor. This will give the PRC a reactor design of its own to then export. If the CPC is able to combine their control over raw materials, growing technical know-how, and manufacturing base, China will not only be a powerful economy, but be able to leverage this power to service its foreign policy goals as well.¶ Even though the PRC is still working to master third generation technology, their scientists are already working on what they think will be the nuclear reactor of the future. China is developing Fourth Generation Fast Neutron Reactors and wants to have one operational by 2030. Additionally, a Chinese nuclear development company has announced its intentions to build the “world’s first high-temperature, gas-cooled reactor” in Shandong province which offers to possibility of a reactor that is nearly meltdown proof. A design, which if proved successful, could potentially redefine the commercial nuclear energy trade.¶ The risk to America¶ The international trade of nuclear material is hazardous in that every sale and transfer increases the chances for an accident or for willful misuse of the material. Nuclear commerce must be kept safe in order for the benefits of nuclear power generation to be realized. Yet, China has a record of sharing dangerous weapons and nuclear material with unfit countries. It is a risk for America to allow China to become a nuclear exporting country with a competitive technical and scientific edge. In order to limit Chinese influence and the relative attractiveness of what they can offer, America must ensure its continuing and substantive lead in reactor technology.¶ ¶ The PRC’s record of exporting risky items is well documented. It is known that during the 1980s the Chinese shared nuclear weapon designs with Pakistan and continues to proliferate WMD-related material. According to the Office of the Director of National Intelligence to Congress, China sells technologies and components in the Middle East and South Asia that are dual use and could support WMD and missile programs. Jane’s Intelligence Review reported in 2006 that China,¶ Despite a 1997 promise to Washington to halt its nuclear technology sales to Iran, such assistance is likely to continue. In 2005, Iranian resistance groups accused China of selling Iran beryllium, which is useful for making nuclear triggers and maraging steel (twice as hard as stainless steel), which is critical for fabricating centrifuges needed to reprocess uranium into bomb-grade material. ¶ China sells dangerous materials in order to secure its geopolitical objectives, regardless if those actions harm world stability. There is little reason to believe China will treat the sale of nuclear reactors any differently. Even if the PRC provides public assurances that it will behave differently in the future, the CPC has not been truthful for decades about its nuclear material and weapons sales and hence lacks credibility. For example, in 1983 Chinese Vice Premier Li Peng said that China does not encourage or support nuclear proliferation. In fact, it was that same year that China contracted with Algeria, then a non-NPT [Non-Proliferation Treaty] state, to construct a large, unsafeguarded plutonium production reactor. In 1991 a Chinese Embassy official wrote in a letter to the The Washington Post that 'China has struck no nuclear deal with Iran.' In reality, China had provided Iran with a research reactor capable of producing plutonium and a calutron, a technology that can be used to enrich uranium to weapons-grade. It has been reported that even after United Nation sanctions were put on Iran, Chinese companies were discovered selling “high-quality carbon fiber” and “pressure gauges” to Iran for use in improving their centrifuges.¶ In 2004 the PRC joined the Nuclear Suppliers Groups (NSG), gaining international recognition of their growing power in the nuclear field. In spite of this opportunity for China to demonstrate its responsibility with nuclear energy, it has not fulfilled it NSG obligations. The PRC has kept the terms of its nuclear reactor sale to Pakistan secret and used a questionable legal technicality to justify forgoing obtaining a NSG waiver for the deal. Additionally, China chose to forgo incorporating new safety measures into the reactors in order to avoid possible complications.¶ A further consequence of China exporting reactors is that these countries may wish to control the fuel cycle which provides the uranium to power their new reactors. The spread of fuel cycle technology comes with two risks: enrichment and reprocessing. Uranium can be enriched to between 3% and 5% for reactor use, but the process can be modified to produce 90% enriched uranium which is weapons-grade. Even if a country only produces low enriched uranium they could easily begin enriching at a higher level if they so choose. Every new country that nuclear technology or information is spread to exponentially increases the risk of material being stolen, given to a third party or being used as the launching point for a weapons program. China’s history of proliferation and willingness to engage economically with very unsavory governments seems likely to increase the risks involving nuclear material.

#### U.S. leadership in Asia solves multiple scenarios for war

Goh 8

(Evelyn, Lecturer in International Relations in the Department of Politics and International Relations at the Univ of Oxford, International Relations of the Asia-Pacific, “Hierarchy and the role of the United States in the East Asian security order,” 2008 8(3):353-377, Oxford Journals Database)

This is the main structural dilemma: as long as the United States does not give up its primary position in the Asian regional hierarchy, China is very unlikely to act in a way that will provide comforting answers to the two questions. Yet, the East Asian regional order has been and still is constituted by US hegemony, and to change that could be extremely disruptive and may lead to regional actors acting in highly destabilizing ways. Rapid Japanese remilitarization, armed conflict across the Taiwan Straits, Indian nuclear brinksmanship directed toward Pakistan, or a highly destabilized Korean peninsula are all illustrative of potential regional disruptions. 5 Conclusion To construct a coherent account of East Asia’s evolving security order, I have suggested that the United States is the central force in constituting regional stability and order. The major patterns of equilibrium and turbulence in the region since 1945 can be explained by the relative stability of the US position at the top of the regional hierarchy, with periods of greatest insecurity being correlated with greatest uncertainty over the American commitment to managing regional order. Furthermore, relationships of hierarchical assurance and hierarchical deference explain the unusual character of regional order in the post-Cold War era. However, the greatest contemporary challenge to East Asian order is the potential conflict between China and the United States over rank ordering in the regional hierarchy, a contest made more potent because of the intertwining of regional and global security concerns. Ultimately, though, investigating such questions of positionality requires conceptual lenses that go beyond basic material factors because it entails social and normative questions. How can China be brought more into a leadership position, while being persuaded to buy into shared strategic interests and constrain its own in ways that its vision of regional and global security may eventually be reconciled with that of the United States and other regional players? How can Washington be persuaded that its central position in the hierarchy must be ultimately shared in ways yet to be determined? The future of the East Asian security order is tightly bound up with the durability of the United States’ global leadership and regional domination. At the regional level, the main scenarios of disruption are an outright Chinese challenge to US leadership, or the defection of key US allies, particularly Japan. Recent history suggests, and the preceding analysis has shown, that challenges to or defections from US leadership will come at junctures where it appears that the US commitment to the region is in doubt, which in turn destabilizes the hierarchical order. At the global level, American geopolitical over-extension will be the key cause of change. This is the one factor that Hierarchy and the role of the United States in the East Asian security order 373lead to both greater regional and global turbulence, if only by the attendant strategic uncertainly triggering off regional challenges or defections. However, it is notoriously difficult to gauge thresholds of over-extension. More positively, East Asia is a region that has adjusted to previous periods of uncertainty about US primacy. Arguably, the regional consensus over the United States as primary state in a system of benign hierarchy could accommodate a shifting of the strategic burden to US allies like Japan and Australia as a means of systemic preservation. The alternatives that could surface as a result of not doing so would appear to be much worse.

#### Asian wars go nuclear

Landy 2k

 National Security Expert @ Knight Ridder, 3/10

(Jonathan, Knight Ridder, lexis)

Few if any experts think China and Taiwan, North Korea and South Korea, or India and Pakistan are spoiling to fight. But even a minor miscalculation by any of them could destabilize Asia, jolt the global economy and even start a nuclear war. India, Pakistan and China all have nuclear weapons, and North Korea may have a few, too. Asia lacks the kinds of organizations, negotiations and diplomatic relationships that helped keep an uneasy peace for five decades in Cold War Europe. “Nowhere else on Earth are the stakes as high and relationships so fragile,” said Bates Gill, director of northeast Asian policy studies at the Brookings Institution, a Washington think tank. “We see the convergence of great power interest overlaid with lingering confrontations with no institutionalized security mechanism in place. There are elements for potential disaster.” In an effort to cool the region’s tempers, President Clinton, Defense Secretary William S. Cohen and National Security Adviser Samuel R. Berger all will hopscotch Asia’s capitals this month. For America, the stakes could hardly be higher. There are 100,000 U.S. troops in Asia committed to defending Taiwan, Japan and South Korea, and the United States would instantly become embroiled if Beijing moved against Taiwan or North Korea attacked South Korea. While Washington has no defense commitments to either India or Pakistan, a conflict between the two could end the global taboo against using nuclear weapons and demolish the already shaky international nonproliferation regime. In addition, globalization has made a stable Asia \_ with its massive markets, cheap labor, exports and resources \_ indispensable to the U.S. economy. Numerous U.S. firms and millions of American jobs depend on trade with Asia that totaled $600 billion last year, according to the Commerce Department.

## Solvency

#### SMRs deployable soon

U.S. Department of Commerce International Trade Administration 11

(“The Commercial Outlook for¶ U.S. Small Modular Nuclear¶ Reactors” <http://www.trade.gov/publications/pdfs/the-commercial-outlook-for-us-small-modular-nuclear-reactors.pdf>, SEH)

Although SMRs have significant potential and ¶ the market for their deployment is growing, their ¶ designs must still go through the technical and ¶ regulatory processes necessary to ensure that ¶ they can be safely and securely deployed. Lightwater technology–based SMRs may not be ready ¶ for deployment in the United States for at least ¶ a decade, and advanced designs might be even ¶ further off. Light-water SMRs and SMRs that have ¶ undergone significant testing are the most likely ¶ candidates for near-term deployment, because ¶ they are most similar to existing reactors that ¶ have certified designs and significant operating ¶ histories. NuScale is on track to submit its reactor ¶ design to the NRC by 2012, as is Babcock & Wilcox ¶ for its mPower design. In addition, GE-Hitachi, ¶ which already completed an NRC preapplication ¶ review for its PRISM reactor in 1994, plans to submit its PRISM design for certification in 2012. ¶ With fierce competition for commercial deployment of U.S. SMRs anticipated, the U.S. government is accelerating its efforts to support the ¶ licensing of new reactor designs. The fiscal year ¶ 2011 budget request for the Department of Energy ¶ includes $39 million for a program to support ¶ design certification of SMRs for commercial deployment, as well as a research and development ¶ portfolio that will address the technology development needs of both near- and longer-term SMRs. ¶ The Department of Energy is also in discussions ¶ with several U.S. companies to facilitate the lightwater SMR design certification by the NRC within ¶ a reasonable timeframe. The department also ¶ continues to support research and development ¶ efforts toward advanced reactor designs through ¶ the Advanced Reactor Concepts program, which ¶ focuses on metal-cooled reactor technologies.

#### Military procurement- solves commercial use proliferation and islanding- avoid regulation

Andres and Loudermilk 10

(Richard B. Andres, Professor of ¶ national Security Strategy at the ¶ national War College and a Senior fellow and energy and environmental ¶ Security and Policy Chair in the Center ¶ for Strategic research, institute for national Strategic Studies, at the national Defense University, Micah J, Research Associate for the Energy & Environmental Security Policy program with the Institute for National Strategic Studies at National Defense University, “Small Reactors and the Military’s Role in Securing America’s Nuclear IndustryPosted” <http://robertmayer.wordpress.com/2010/08/28/small-reactors-and-the-militarys-role-in-securing-americas-nuclear-industryposted/>, SEH)

Unlike private industry, the military does not face the same regulatory and congressional hurdles to constructing reactors and would have an easier time in adopting them for use. By integrating small nuclear reactors as power sources for domestic U.S. military bases, three potential energy dilemmas are solved at the same time. First, by incorporating small reactors at its bases, the military addresses its own energy security quandary. The military has recently sought to “island” its bases in the U.S. -protecting them from grid outages, be they accidental or intentional. The Department of Defense has promoted this endeavor through lowering energy consumption on bases and searching for renewable power alternatives, but these measures alone will prove insufficient. Small reactors provide sufficient energy output to power military installations and in some cases surrounding civilian population centers.¶ Secondly, as the reactors become integrated on military facilities, the stigma on the nuclear power industry will ease and inroads will be created for the adoption of small-scale reactors as a viable source of energy. Private industry and the public will see that nuclear reactors can indeed be utilized safely and effectively, resulting in a renewed push toward the expansion of nuclear power. Although many of the same hurdles will still be in place, a shift in public opinion and a stronger effort by utilities, coupled with the demonstrated success of small reactors on military bases, could prove the catalysts necessary for the federal government and the NRC to take more aggressive action.¶ Finally, while new reactors are not likely in the near future, the military’s actions will preserve, for a while longer, the badly ailing domestic nuclear energy industry. Nuclear power is here to stay around the globe, and the United States has an opportunity to take a leading role in supplying the world’s nuclear energy and reactor technology. With the U.S. nuclear industry dormant for three decades, much of the attention, technology, and talent have concentrated overseas in countries with a strong interest in nuclear technology. Without the United States as a player in the nuclear energy market, it has little say over safety regulations of reactors or the potential risks of proliferation from the expansion of nuclear energy. If the current trend continues, the U.S. will reach a point where it is forced to import nuclear technology and reactors from other countries. Action by the military to install reactors on domestic bases will both guarantee the survival of the American nuclear industry in the short term, and work to solidify support for it in the long run.¶ Ultimately, between small-scale nuclear reactors and the U.S. military, the capability exists to revitalize America’s sleeping nuclear industry and promoting energy security and clean energy production. The reactors offer the ability to power domestic military bases, small towns, and other remote locations detached from the energy grid. Furthermore, reactor sites can house multiple units, allowing for greater energy production – rivaling even large reactors. Small reactors offer numerous benefits to the United States and a path initiated by the military presents a realistic route by which their adoption can be achieved.

#### DOD key- prevents unfavorable lock-in

Andres and Breetz 11

(Richard B. Andres is Professor of ¶ national Security Strategy at the ¶ national War College and a Senior fellow and energy and environmental ¶ Security and Policy Chair in the Center ¶ for Strategic research, institute for national Strategic Studies, at the national Defense University. Hanna L. Breetz is a doctoral candidate in the Department of Political Science at the Massachusetts institute of technology, “Small Nuclear Reactors ¶ for Military Installations:¶ Capabilities, Costs, and ¶ Technological Implications” Institute for National Strategic Studies, <http://www.ndu.edu/press/lib/pdf/strforum/sf-262.pdf>, SEH)

Technological Lock-in. A second risk is that if ¶ small reactors do reach the market without DOD assistance, the designs that succeed may not be optimal for ¶ DOD’s applications. Due to a variety of positive feedback and increasing returns to adoption (including demonstration effects, technological interdependence, network and learning effects, and economies of scale), the ¶ designs that are initially developed can become “locked ¶ in.”¶ 34¶ Competing designs—even if they are superior in ¶ some respects or better for certain market segments—¶ can face barriers to entry that lock them out of the market. If DOD wants to ensure that its preferred designs ¶ are not locked out, then it should take a first mover role ¶ on small reactors. ¶ It is far too early to gauge whether the private ¶ market and DOD have aligned interests in reactor designs. On one hand, Matthew Bunn and Martin Malin argue that what the world needs is cheaper, safer, ¶ more secure, and more proliferation-resistant nuclear ¶ reactors; presumably, many of the same broad qualities would be favored by DOD.¶ 35¶ There are many varied ¶ market niches that could be filled by small reactors, ¶ because there are many different applications and settings in which they can be used, and it is quite possible that some of those niches will be compatible with ¶ DOD’s interests.¶ 36¶ On the other hand, DOD may have specific needs ¶ (transportability, for instance) that would not be a high ¶ priority for any other market segment. Moreover, while ¶ DOD has unique technical and organizational capabilities that could enable it to pursue more radically innovative reactor lines, DOE has indicated that it will ¶ focus its initial small reactor deployment efforts on ¶ LWR designs.¶ 37¶ If DOD wants to ensure that its preferred reactors ¶ are developed and available in the future, it should take ¶ a leadership role now. Taking a first mover role does not ¶ necessarily mean that DOD would be “picking a winner” ¶ among small reactors, as the market will probably pursue multiple types of small reactors. Nevertheless, DOD ¶ leadership would likely have a profound effect on the industry’s timeline and trajectory.

## Slayers

#### Obama supports nuclear power plants – first one built under his administration in 30 years

Politifact 3/2

(Politifact quoting President Obama’s 2/23/12 speech. “Obama says he supported the first new nuclear power plant in three decades” Friday, March 2nd, 2012 at 10:25 a.m. <http://www.politifact.com/florida/statements/2012/mar/02/barack-obama/obama-says-he-supported-first-nuclear-power-plant-/>, TSW)

One of his speech’s shortest lines caught our attention: "We supported the first new nuclear power plant in three decades."¶ Thirty years -- really? And why has it been so long? To satisfy our curiosity, we decided to check it out. (We fact-checked Obama’s claims about drilling in a separate report.)¶ If you haven’t been keeping tabs on the nuclear energy industry, it has indeed been awhile since a new reactor was built. But Obama’s 30-year claim hinges on licensing.¶ On Feb. 9, 2012, the U.S. Nuclear Regulatory Commission approved a license for two new nuclear reactors in Georgia. The electricity giant Southern Co. intends to build them at its Vogtle site south of Augusta. (The White House pointed us to news coverage of the approval when we asked for evidence of Obama’s statement.)¶ Prior to this year, the last time the commission granted a license to build a new reactor was in 1978, which was 34 years ago, according to a commission spokesperson. The permit was for the Shearon Harris plant operated by Carolina Power & Light near Raleigh, N.C. But it takes a long time to build nuclear reactors, so the plant didn’t get operational approval until 1986.¶ And the North Carolina plant isn’t the most recent to go operational. That distinction goes to the Tennessee Valley Authority’s Watts Bar site in Tennessee. It received a construction license in 1973 and an operating license in 1996, or 16 years ago.¶ Still, as we ran this claim by people who watch the nuclear industry closely -- both those opposed to nuclear energy and those in favor of it –

MARK

- they agreed Obama’s claim to have "supported the first new nuclear power plant in three decades" was largely accurate.¶ A technical note: The Georgia project adds two reactors to an existing electricity generation site with two existing reactors. We wondered if that diminished the accuracy of Obama’s statement, but the experts said it’s fair to call each reactor its own "power plant."