**Plano West negates Resolved: The United States should increase its use of nuclear energy for commercial energy production**

## Contention 1 is Cutting Emissions

The US is rapidly shifting to renewable energy sources right now

[EIA 2019](https://www.eia.gov/todayinenergy/detail.php?id=38752)

**Renewable generation provided a new record of 742 million megawatthours (MWh) of electricity in 2018,**nearly double the 382 million MWh produced in 2008. Renewables provided 17.6% of electricity generation in the United States in 2018. **Nearly 90% of the increase in U.S. renewable electricity between 2008 and 2018 came from wind and solar generation.**

Expanding nuclear energy will hurt the renewable sector for two reasons

The first is an investment tradeoff

[Karpov](https://thebulletin.org/2019/06/why-nuclear-power-plants-cost-so-much-and-what-can-be-done-about-it/) in 2019 explains that

 The cost of nuclear power is often broken down into capital costs and operating costs. Capital costs include site preparation, engineering, manufacturing, construction, commissioning, and financing. Operating costs include fuel costs (from uranium mining to fuel fabrication), maintenance, decommissioning, and waste disposal. **The capital costs of a nuclear power plant are much higher than** for **[other] energy sources** such as coal and natural gas—and the annual cost of repaying the initial investment is substantially higher than the annual operating costs. This is because nuclear power plants are technically complex and must satisfy strict licensing and design requirements. The design and construction of a new nuclear power plant requires many highly qualified specialists and often takes many years, compounding financing costs, which can become significant. Design changes or lawsuits can cause delays that further increase the financing charges, which in some cases exceed the actual construction costs.

Due to the market’s limited supply of investment capital, [Kanellos](https://www.greentechmedia.com/articles/read/time-to-end-nuclear-socialism-says-new-study) corroborates in 2010 that

Unlike computers, solar panels,[and] wind turbines and most other high tech projects, **nuclear power plants** and projects **don't go down in price over time.** Instead, the costs escalate, and that's a recipe for a disaster, according to a report released today by Mark Cooper, senior fellow for economic analysis at the Institute for Energy and the Environment at Vermont Law School. (Here is a link to the full report.) **Rising costs** means more expensive energy, he said. It also undermines the purpose of subsidies like government-backed loan guarantees, because the subsidies can't be phased out due to the continuing price increases. Worse, the vast scope of nuclear projects [which] invariably absorbs the mental energy of utilities and **crowd outs investment in other renewables** and energy efficiency.

The second is lobbying

[Cooper](https://www.power-eng.com/wp-content/uploads/content/dam/pe/online-articles/documents/2014/May/Cooper%20SMRs%20are%20Part%20of%20the%20Problem%2C%20Not%20the%20Solution%20FINAL2.pdf) finds in 2014 that

The ongoing collapse of nuclear power in the U.S. is readily apparent in the failure to launch 90 percent of “nuclear renaissance” reactors, delays and cost overruns for those that got started, the cancellation of projects **to increase** the capacity ofexisting **reactors**, and the early retirement of aging reactors. To reverse its fate, **the U.S. nuclear industry has** • gone in search of a new technology to champion (small modular reactor [SMR]), • **launched an aggressive campaign to sell nuclear power as the primary solution to climate change**, and • sought to slow the growth of alternatives with vigorous attacks on the policies that have enabled renewable resources to grow at record levels. Thus the collapse has lent greater intensity and significance to the 50-year debate over the economic viability and safety of commercial nuclear power: • It is not only the fate of nuclear power at stake, but also the fundamental direction of the policy response to climate change. This paper examines the fundamental choice policymakers are being asked to make. It reviews the prospects for nuclear technology in light of the past and present performance of nuclear power (Section I), assesses the economic and safety challenges that SMR technology faces (Section II) when confronting the alternatives that are ava

As a result, [Lyderson 15](https://energynews.us/2015/02/06/midwest/why-the-nuclear-industry-targets-renewables-instead-of-gas/) finds that

**Nuclear generators have successfully** fought against renewable and energy efficiency standards on the state level, and **lobbied against tax incentives for wind and solar on the federal level**. They’re in the process of securing changes in regional capacity markets that would benefit nuclear and harm solar and wind. And **as states** develop their Clean Power Plans to **fulfill the federal mandate to reduce carbon emissions, nuclear is often pitted against renewables.** In deregulated states like Illinois, Ohio, Michigan and Pennsylvania, nuclear generators have found it increasingly difficult to sell their power at a profit on open markets, **because of competition** primarily from gas but also **from wind**. Meanwhile, energy efficiency **and** distributed **solar** generation have reduced demand for electricity and are [being a] part of a fundamental shift which could significantly shrink the role of[from] large, centralized power plants.

Because of these two reasons, [Dvork](https://www.windpowerengineering.com/french-%E2%80%9Cnuclear-miracle%E2%80%9D-plagued-by-fast-rising-costs-crowds-out-renewables/) concludes in 2010 that

With respect to efficiency and renewable energy the “no nuclear plans” **U.S. states [with no nuclear plans] have** (in comparison to U.S. “nuclear states”): had three times as much renewable energy and **ten times as much** non-hydro **renewable energy** in their 1990 generation mix, set Renewable Portfolio Standards (RPS) goals for the next decade that are 50% higher; spent three times as much on efficiency in 2006. Furthermore, nonnuclear U.S. states saved over three times as much energy in 1992 to 2006 and have much stronger utility efficiency programs in place.

### Impact is climate change

[Chestney 13 Reuters](https://in.reuters.com/article/emissions-climate/emissions-limits-could-cut-climate-damage-by-two-thirds-study-idINDEE90C08A20130113)

Global average sea level rise could be reduced to 30cm (12 inches) by 2100, compared to 47-55cm (18-22 inches) if no action to cut emissions is taken, it said. Some **adverse climate impacts could** also **be delayed by many decades.** The global productivity of spring wheat could drop by 20 percent by the 2050s, but the fall in yield could be delayed until 2100 if strict emissions curbs were enforced. **"Reducing greenhouse gas emissions** won't avoid the impacts of climate change altogether of course, but our research shows it **will buy time to make things like buildings, transport systems and agriculture more resilient to climate change,**"

Nuclear energy will not be fast enough because [Jacobson](https://www.leonardodicaprio.org/the-7-reasons-why-nuclear-energy-is-not-the-answer-to-solve-climate-change/) 19 from Stanford writes that

There is a small group of scientists that have proposed replacing 100% of the world’s fossil fuel power plants with nuclear reactors as a way to solve climate change. Many others propose nuclear grow to satisfy up to 20 percent of all our energy (not just electricity) needs. They advocate that nuclear is a “clean” carbon-free source of power, but they don’t look at the human impacts of these scenarios. Let’s do the math..**One nuclear power plant takes** on average about **14**-1/2 **years to build**, from the planning phase all the way to operation*.*According to the World Health Organization, about 7.1 million people die from air pollution each year, with more than 90% of these deaths from energy-related combustion.

Meanwhile,

In addition, 10 of the reactors were completed between 1991-2000. As such, the whole planning-to-operation time for these reactors was at least 32 years, not 15. That of any individual reactor was 10 to 19 years. Utility-scale **wind and solar farms,** on the other hand, **take** on average **only 2 to 5 years**, from the planning phase to operation. Rooftop solar PV projects are down to only a 6-month timeline. So transitioning to 100% renewables as soon as possible would result in tens of millions fewer deaths.

Jacobson concludes that

According to the World Health Organization, about 7.1 million people die from air pollution each year, with more than 90% of these deaths from energy-related combustion*.*So **switching our energy system to nuclear would result in** about **93 million people dying , as we wait for** all **the new nuclear plants to be built** in the all-nuclear scenario. Utility-scale wind and solar farms, on the other hand, take on average only 2 to 5 years, from the planning phase to operation. Rooftop solar PV projects are down to only a 6-month timeline. **So transitioning to** 100% **renewables as soon as possible would result in tens of millions fewer deaths.**

# Our second contention is a nuclear catastrophe

#### There are multiple reasons why increasing nuclear energy would lead to disastrous failures

### First is coverups

####  The nuclear industry pays off officials to cover up nuclear power’s risks, fabricating studies on the safety of plants.

**Shrader-Frechette**: Shrader-Frechette, Kristin. O’Neill Family Professor, University of Notre Dame “Answering ‘Scientific Attacks’ on Ethical Imperatives: Wind and Solar Versus Nuclear Solutions to Climate Change.” Ethics and the Environment Volume 18, Number 1, Spring 2013. RP <https://www.jstor.org/stable/10.2979/ethicsenviro.18.1.1#metadata_info_tab_contents>

Part of the answer is military, and part of it is public relations firms and lobbyists, as noted earlier. The Economist (2005) also blames US nuclear-industry campaign contributions. These nuclear-industry donations encourage politicians to do precisely what bankers and investors refuse to do: loan or spend money on reactors. Thus, many members of the public mistakenly believe that nuclear-generated electricity is low-carbon, economical, and desirable because of industry campaign donations, and industry funding of public relations firms and lobbyists. Moreover, **because the nuclear industry controls most emissions/cost/safety data, it either performs or funds virtually all fission-related studies [which are tainted by conflicts of interest]. However**, when one examines the few university, government, and **independent analyses,** as already shown, these studies **virtually always show the flaws in atomic energy**, although the public has little access to such studies. Instead the public often receives the best (nuclear) science money can buy—what Sheldon Krimsky (2003; see Beder 2002) calls “science in the private interest”—alleged **science tainted by conflicts of interest. Because of this “private-interest science” and nuclear cover-up,** most people do not realize that, in most nations, reactors have zero liability for an accident—whose losses ultimately will be borne by its victims. In the US, the legally-mandated liability limit is $11 billion, roughly one to two percent of US-government-calculated losses ($600–700 billion) from an accident like Chernobyl or Fukushima. Yet, since nuclear power began, twenty-four core melts have occurred—including in the US, where four of the melted reactors were actually online. Because one cannot see, hear, feel, touch, or taste ionizing radiation, nuclear core melts can be covered up, as occurred, for instance, in Los Angeles. Industry and government covered up this Santa Susana meltdown, until cancer increases nearby forced release of secret reports (Shrader-Frechette 2011, 110–60; Smith 2006). Similarly, industry and government covered up the fact that epidemiologists agree there was a 64 percent cancer increase, within ten miles, after the 1979 Three Mile Island (TMI), Pennsylvania core melt, and also massive cancer increases downwind—into other states; yet, the official industry position is that no one died as a result of TMI (Hatch 1990; Mangano 2004; Shrader-Frechette 2011). Epidemiologists likewise agree that children are the major victims of nuclear energy and are up to thirtyeight times more sensitive to ionizing radiation than adults, and that children’s cancer rates increase near nuclear plants, because of normal emissions, even without any accidents (Baker and Hoel 2007; Busby and Scott-Cato 1997; Clapp et al 1987; Forman et al 1987; Gardner et al 1990; Guizard et al 2001; Michaelis et al 1992; Kaatsch et al 2008; Mangano 2008, 2006, 2002; Mangano and Sherman 2008, Shrader-Frechette 2011, 110–60). Yet, many people do not know these established scientific facts, just as they do not know the facts about nuclear costs, nuclear emissions, nuclear intermittency, and so on. Once such data are known, there are few roadblocks to following the ethical imperative to use renewable energy.

**Shrader-Frechette continues**. (2013). Answering “Scientific” Attacks on Ethical Imperatives: Wind and Solar Versus Nuclear Solutions to Climate Change. Ethics and the Environment, 18(1), 1. doi:10.2979/ethicsenviro.18.1.1. <http://sci-hub.tw/10.2979/ethicsenviro.18.1.1>

The US Nuclear Regulatory Commission (NRC 2006) warned that, in the five years since 2001, **75 percent of US reactors have violated safety regulations** . The NRC also (2011) recently reported that at least **28 percent of US nuclear operators have covered up, [and] not reported, defective nuclear-plant parts.** Such regulatory failures illustrate why only fleet-lifetime-average—not annual—load factors are reliable. Otherwise, violators inflate load factors by deferring maintenance and causing safety threats. Thus, at best, claims that reactors “operate around the clock”—are not factual. At worst, they presuppose **[which constitutes] regulatory misconduct and potential disaster.**

#### The chance of another Chernobyl is high — replace

Jurica **Dujmovic**, 10-19-20**19**, "Think fossil fuels are bad? Nuclear energy is even worse," MarketWatch, https://www.marketwatch.com/story/think-fossil-fuels-are-bad-nuclear-energy-is-even-worse-2019-10-17

Not long ago, I wrote about nuclear plants and the large number of “incidents” (many of which go under the radar) that occur every year, **despite upgrades,** updates**, technological advancements and research that’s put in nuclear energy.** Researchers from the Swiss Federal Institute of Technology have come up with an unsettling discovery. Using the most complete and up-to-date list of nuclear accidents to predict the likelihood of another nuclear cataclysm, they concluded that **there is a 50% chance of a Chernobyl-like event (or larger) occurring in the next 27 years,** and that we have only 10 years until an event similar to Three Mile Island, also with the same probability. (The Three Mile Island Unit 2 reactor, near Middletown, Pa., partially melted down on March 28, 1979. This was the most serious commercial nuclear-plant accident in the U.S.)

### 2nd is because of Cyberattacks

Alexander **Campbell**, 11-14-201**9**, "Lessons from the cyberattack on India’s largest nuclear power plant," Bulletin of the Atomic Scientists, https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant/

Indian officials acknowledged on October 30th that a cyberattack occurred at the country’s Kudankulam nuclear power plant. An Indian private cybersecurity researcher had tweeted about the breach three days earlier, prompting Indian authorities to initially deny that it had occurred before admitting that the intrusion had been discovered in early September and that efforts were underway to respond to it. According to last Monday’s Washington Post, Kudankulam is India’s biggest nuclear power plant, “equipped with two Russian-designed and supplied VVER pressurized water reactors with a capacity of 1,000 megawatts each. Both reactor units feed India’s southern power grid. The plant is adding four more reactor units of the same capacity, making the Kudankulam Nuclear Power Plant one of the largest collaborations between India and Russia.” While reactor operations at Kudankulam were reportedly unaffected, this incident should serve as yet another wake-up call that the nuclear power industry needs to take cybersecurity more seriously. There are worrying indications that it currently does not: A 2015 report by the British think tank Chatham House found **[there are] pervasive shortcomings in the nuclear power industry’s approach to cybersecurity, from regulation to training to user behavior.** In general, nuclear power plant operators have failed to broaden their cultures of safety and security to include an awareness of cyberthreats. (And by cultures of safety and security, those in the field—such as the Fissile Materials Working Group—refer to a broad, all-embracing approach towards nuclear security, that takes into account the human factor and encompasses programs on personnel reliability and training, illicit trafficking interception, customs and border security, export control, and IT security, to name just a few items. The Hague Communiqué of 2014 listed nuclear security culture as the first of its three pillars of nuclear security, the other two being physical protection and materials accounting.) This laxness might be understandable if last week’s incident were the first of its kind. Instead, **there have been over 20 known cyber incidents at nuclear facilities since 1990.** This number includes relatively minor items such as accidents from software bugs and inadequately tested updates along with deliberate intrusions, but it **demonstrat[ing] that the nuclear sector is not somehow immune to cyber-related threats. Furthermore, as the digitalization of nuclear reactor instrumentation and control systems increases, so does the potential for malicious and accidental cyber incidents alike to cause harm. This record should also disprove the old myth, unfortunately repeated in Kudankulam officials’ remarks, that so-called air-gapping effectively secures operational networks at plants.** Air-gapping refers to separating the plant’s internet-connected business networks from the operational networks that control plant processes; doing so is intended to prevent malware from more easily infected business networks from affecting industrial control systems. The intrusion at Kudankulam so far seems limited to the plant’s business networks, **but air gaps have failed at the Davis-Besse nuclear power plant in Ohio in 2003 and even classified US military systems in 2008. The same report from Chatham House found ample sector-wide evidence of employee behavior that would circumvent air gaps, like charging personal phones via reactor control room USB slots and installing remote access tools for contractors.****The consequences of a cyber-based intrusion at a nuclear power plant could** range from loss of confidential employee or business information to potentially **caus[e]ing a reactor shutdown or physical damage.** The industry must realize that cyberattacks can be the main event, rather than simply a means to enable more traditionally imagined threats like physical intrusions. And regardless of the consequences of a given incident, public statements like those from Indian authorities last week that refuse to even admit the possibility of **cyberattack will undermin[ing] public trust—an existential resource for many nuclear power programs.** One item to note, however, is that the problem’s scale and complexity is only likely to grow as more states join the nuclear power club. And even with years of experience, **no country is immune from succumbing to cyberattack: Last week’s incident occurred in a country whose nuclear power program dates back to the 1950s, and previous cyberattacks have struck nuclear facilities in countries with similarly long-established nuclear power programs, including Japan, France, and the United States.** That they have still fallen victim to breaches bodes ill for prospective newcomers like Jordan, whose national Computer Emergency Response Team is only two years old. One can expect that nuclear newcomers with less indigenous cybersecurity expertise will need more help from international partners, and will face a steeper uphill climb towards maintaining that workforce.

Robert Chen 2/4/20 <https://ctf.redpwn.net/static/drafts/81/8188bfc51cfec2edec1277f2a121a4b2.pdf>

Even if the vulnerabilities don’t get exploited, the presence of additional nuclear reactors could incentivize adversaries to devote more money to offensive cybersecurity programs. Russia and China are nowhere close to their limit on cybersecurity spending: an excuse is all they need to ramp up spending. With juicy targets like nuclear reactors, there might even be a full-fledged cyberwar. Returning to the example of Stuxnet, nuclear energy is one such area that we should take the utmost caution towards. If anything, **building new nuclear reactors will only increase the [number of vulnerable computer systems]** attack surface. It is a common adage that no code is bug free. In fact, Steve McConnell, author of Code Complete, finds that the average codebase has anywhere between 15 to 50 errors per 1000 lines of code. nuclear reactor could increase the size of the codebase by 1.6%. With presumably millions of lines of code per reactor, the conclusion is obvious. There is a need for alarm. Our internal modeling suggests that **for every nuclear reactor built, the probability of a nuclear cyberattack increases by 4%. If the US were to switch entirely to nuclear energy, there would be a 75% chance of a cyberattack before the end of 2020. A cyberattack [causing]** would be devastating, potentially crippling the United States. Coordinated **meltdowns**could trigger an environmental calamity, permanently ruining the environment **and killing millions instantly from radiation poisoning and fallout.** These conditions could quickly become global, decimating populations around the world.

### 3rd is high burn-up fuel, or HBF

Robert **Alvarez 16,** 8-11-2016, "Nuclear power plant? Or storage dump for hot radioactive waste?," Bulletin of the Atomic Scientists, https://thebulletin.org/2016/08/nuclear-power-plant-or-storage-dump-for-hot-radioactive-waste/

In addition to generating electricity, **US nuclear power plants are now major radioactive waste management operations, storing concentrations of radioactivity that dwarf those generated by the country's nuclear weapons program.** Because the proposed Yucca Mountain nuclear waste repository remains in limbo, and other permanent storage plans are in their infancy, these wastes are likely to remain in interim storage at commercial reactor sites for the indefinite future. This reality raises one issue of particular concern—how to store the high-burnup nuclear fuel used by most US utilities. An Energy Department expert panel has raised questions that suggest neither government regulators nor the utilities operating commercial nuclear power plants understand the potential impact of used high-burnup fuel on storage and transport of used nuclear fuel, and, ultimately, on the cost of nuclear waste management.

US commercial nuclear power plants use uranium fuel that has had the percentage of its key fissionable isotope—uranium 235—increased, or enriched, from what is found in most natural uranium ore deposits. In the early decades of commercial operation, the level of enrichment allowed US nuclear power plants to operate for approximately 12 months between refueling. **In recent years,** however**, US utilities have begun using what is called high-burnup fuel [which]. This fuel generally contains a higher percentage of uranium 235,** allowing reactor operators to effectively double the amount of time the fuel can be used, reducing the frequency of costly refueling outages. The switch to high-burnup fuel has been a major contributor to higher capacity factors and lower operating costs in the United States over the past couple of decades.

While this high-burnup trend may have improved the economics of nuclear power, the industry and its regulator, the Nuclear Regulatory Commission (NRC), have taken a questionable leap of faith that could, according to the Electric Power Research Institute, “result in severe economic penalties and in operational limitations to nuclear plant operators.” Evidence is mounting that spent high-burnup fuel poses little-studied challenges to the temporary used-fuel storage plans now in place and to any eventual arrangement for a long-term storage repository.

The NRC and the nuclear industry do not have the necessary information to predict when storage of high-burnup fuel may cause problems. To err on the side of caution, high-burnup fuel might have to be left in cooling pools for 25 years—as opposed to the current three to five years for lower burnup spent fuel— to allow cladding temperatures to drop enough to reduce risks of cladding failure before the fuel is transferred to dry storage. Also, **the cooling pools at US commercial reactors are rapidly filling, with more than 70 percent of the nation's 77,000 metric tons of spent fuel in reactor pools, of which roughly a fourth is high burnup**. So far, a small percentage of high-burnup used fuel assemblies are sprinkled amid lower burnup fuel in dry casks at reactor sites. But **by 2048—**the Energy Department's date for opening a permanent geologic disposal site**—the amount of spent fuel could double, with high burnup waste accounting for as much as 60 percent of the inventory.**

**USNRC 19** <https://www.mass.gov/files/documents/2019/05/30/February%2020%2C%202019%20Pilgrim%20Watch%20Petition%20to%20Intervene%20and%20Hearing%20Request.pdf>

Pilgrim has approximately 35% HBU; yet the NRC is just starting a test to see whether the casks can handle it, with results not in until 2027. Robert Alvarez (https://www.ips-dc.org/ips-authors/robert-alvarez/ ) explains the problems in doing so: **Research shows that under high-burnup conditions, fuel rod cladding may not be relied upon as a key barrier to prevent the [it could cause] escape of radioactivity, especially during prolonged storage** in the "dry casks.**"High-burnup waste reduces the fuel cladding thickness and a hydrogen-based rust forms on the zirconium metal used for the cladding, which can cause the cladding to become brittle and fail**- a costly event. • In addition, under high-burnup conditions, increased pressure between the uranium fuel pellets in a fuel assembly and the inner wall of the cladding that encloses them causes the cladding to thin and elongate. **• And the same research has shown that high burnup fuel temperatures make the used fuel more vulnerable to damage from handling and transport;** cladding can fail when used fuel assemblies are removed from cooling pools, when they are vacuum dried, and when they are placed in storage canisters. • High burnup spent nuclear fuel is proving to be an impediment to the safe storage and disposal of spent nuclear fuel. For more than a decade, evidence of the negative impacts on fuel cladding and pellets from high burnup has increased, while resolution of these problems remains elusive. • NRC Meeting Presentation Slides Dry Storage & Transportation of High Burnup, 9/6/18 meeting, slides 14 & 15: NRC said that storage and transportation of HBU is safe, providing no technical bases, for 60 years – no guarantee for longer storage when fuel may still be onsite.

• 2016 Princeton Study: A major Spent Fuel Pool fire could contaminate as much as 100,000 square kilometers of land (38,610 square miles) and force the evacuation of millions.86 • 2013 NRC Study: **A severe spent fuel pool accident would render an area larger than Massachusetts uninhabitable for decades and displace more than 4 million people.87** • 2006 Massachusetts Attorney General Study: $488 Billion dollars, 24,000 cancers, hundreds of miles uninhabitable88

The GEIS, SEIS and Holtec minimize **the potential consequences of a spent fuel pool fire or a cask rupture. The amount of radiation released likely** would far exceed the EPA’s one rem release limit, and the **result [in]ing off-site damage to property and health would be unimaginable.**  79 Pilgrim’s pool contains approximately 70 million curies.84 Much of the damage from a pool fire or dry cask failure would be caused by the release of Cesium-137. To make the risk meaningful, it is useful to compare the inventory of Cs-137 in Pilgrim’s pool and core with the amount of Cs137 released at Chernobyl.85 Chernobyl - 2,403,000 curies Cs-137; Pilgrim’s pool - more than 44,000,000 curies Cs-137; Pilgrim’s Core - 5,130,000 curies Cs-137. Each cask contains more than half the total amount of Cs-137 released at Chernobyl Studies of the consequences of a spent fuel pool fire show huge, potential consequences, ignored by Holtec and the documents Holtec relies on.

### The first impact is meltdowns

Meltdowns have wide-spread consequences as [Gesellschaft 12](https://www.sciencedaily.com/releases/2012/05/120522134942.htm) finds that

The team in Mainz found that in Western Europe, where the density of reactors is particularly high, the contamination by more than 40 kilobecquerels per square meter is expected to occur once in about every 50 years. It appears that citizens in the densely populated southwestern part of Germany run the worldwide highest risk of radioactive contamination, associated with the numerous nuclear power plants situated near the borders between France, Belgium and Germany, and the dominant westerly wind direction. If a single nuclear meltdown were to occur in Western Europe, around 28 million people on average would be affected by contamination of more than 40 kilobecquerels per square meter. This figure is even higher in southern Asia, due to the dense populations. **A major nuclear accident** there would affect around 34 million people, while **in the** eastern **US**A and in East Asia this **would [affect]** be **14 to 21 million people**. "Germany's exit from the nuclear energy program will reduce the national risk of radioactive contamination. However, an even stronger reduction would result if Germany's neighbours were to switch off their reactors," says Jos Lelieveld. "Not only do we need an in-depth and public analysis of the actual risks of nuclear accidents. In light of [this] our findings I believe an internationally coordinated phasing out of nuclear energy should also be considered ," adds the atmospheric chemist.

These meltdowns are deadly. After accounting for casualties from radiation, [Bertell](http://www.pacificecologist.org/archive/12/behind-the-cover-up.pdf) 06 terminalizes that

Any estimate would be increased by including internal contamination from food and water and conversion of energy deposits to effective collective doses. This very conservative estimate of cancer fatalities in Europe attributable to Chernobyl is 889,336 to 1,778,672. Summary of findings **Using conservative methodology,** I estimate **the eventual death toll from the Chernobyl disaster** will be: • 253 due to direct radiation damage • 904,763 to 1,809,515 due to fatal cancers or • 905,016 to 1,809,768 in total This estimate of **[was]** roughly **1 to 2 million deaths** is conservative for several reasons, firstly, because of the failure of the radiation investigation by UNSCEAR to document the radionuclide variety and the extent of radiation contamination of food; and secondly, because of the use of faulty ICRP (International Commission on Radiation Protection) methodology, and the absence of a comprehensive scientific examination of all deaths among emergency and rescue workers, and disaster witnesses.

### The second impact is mass shutdowns

#### Accidents destroy public support which leads to mass shutdowns

**Cherp 12** [Aleh; Professor of Environmental Sciences and Policy, Central European University; 2012; “Chapter 5 – Energy and Security. In Global Energy Assessment – Toward a Sustainable Future”; Cambridge University Press, Cambridge, UK and New York, NY, USA and the International Institute for Applied Systems Analysis, Laxenburg, Austria; pp. 325-384] [Premier] <https://iiasa.ac.at/web/home/research/Flagship-Projects/Global-Energy-Assessment/GEA_Chapter5_security_lowres.pdf>

As a result, strong government backing is necessary for the development of **nuclear power** (Finon and Roques, 2008 ). Such political backing **depends on** the **public support**of nuclear power, **which** has been very uneven. In particular, public opinion**is swayed by nuclear accidents** such as the ones at Three Mile Island in the United States in 1979, Chernobyl in the USSR in 1986, and Fukushima in Japan in 2011. Each **such change of public opinion** and the resulting change in the government policy **may**affect energy security both in the short term (e.g., as a**result [in] of shutting down nuclear power** plants immediately affected by the accident 9 and those deemed unsafe) and in the longer term (through complicating the investment climate). Unlike other energy sources and electricity-generating technologies, for nuclear energy the risks associated with accidents extend beyond the plant level or national level to the entire nuclear power plant fleet. Thus, nuclear power globally faces the systemic risk of nuclear accidents.w

#### A single accident collapsed the nuclear industry

Kimberly **Amadeo**, 1-31-20**20**, "Did the Three Mile Island Nuclear Accident Help Kill Nuclear Power?," Balance, https://www.thebalance.com/three-mile-island-nuclear-accident-facts-impact-today-3306337

**The Three Mile Island accident** was a meltdown at a nuclear power plant in Middletown, Pennsylvania. It occurred on March 28, 1979. Officially, it caused no deaths. But unofficial investigations and lawsuits claimed there were above-average rates of cancer and birth defects in the surrounding area. The accident **halted the development of the U.S. nuclear power industry for 30 years. During that time, no new nuclear power plants were approved**. Several that were under construction at the time of the accident were completed.

**DON'T READ WALLACE BELOW**

**Which is why Wallace 18 concludes that**

Michael Wallace 2018 Pg 34. <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180714_Wallace_BackFromtheBrink_Web.pdf?XcEEhWkM1msyhBiDvIiTijfpiekw5oBm>

**Another Chernobyl or Fukushima not only would harm countless lives, but risks putting an end to nuclear power around the world.**

****

# Framing

#### CX: xxxxx

# Lay Rhetoric

Cheese Frontline strats: We account, directionality, no warrant, not a turn

# Frontlines

## C1: Renewables

### Extension/Weighing

Using nuclear means you trade something that works for something that doesn’t.

90% of the US’s new energy is coming from renewables like wind and solar but if we expand nuclear we lose renewable power [in two ways].

1. Investment tradeoff - [Karpov and Kanellos] SInce nuclear plants cost billions, once investors fund nuclear plants they won’t have any investment capital to invest in renewables anymore.
2. Lobbying - [Cooper and Lyderson] The nuclear industry lobbies to cut tax incentives for wind and solar which they feel is their biggest competitor, which disincentivizes new renewable construction.

Extend Dvork - states with no nuclear plans have 10x as much renewable energy

Nuclear power isn’t just bad, its counterproductive.

Extend Jacobson - Nuclear power takes 14 years to build while wind and solar take just 2 years - by the time nuclear plants are built it’s too late to stop climate change which is why switching to nuclear would kill 93 million people.

Weighing:

1. We control the IL into their warming arg - renewables are the only source that can be built in time to stop warming
2. o/w mag - 93 m lives lost > [xyz]
3. o/w tf - ??

### Frontlines

#### FL: Nuclear backups renewables

1. Don’t need to build more reactors if we r just using as a backup - existing is sufficient - delinks the aff
2. Renewables don’t need nuclear in the first place, it’s way better-- aff causes tradeoff tho

#### FL: Fossil fuel switch

1. Doesn’t answer the links - investment and lobbying
2. EIA/ 90% of new energy is renewable - that’s the most likely, also postdates conca by 3 years which is by 2016 - times are changing

#### FL: Intermittency

1. Kline 18 - Lithium ion batteries solve - tesla has massive ones already and battery tech is rapidly improving
2. Kline 18 - Co-location - combine solar, wind, diff sources together to cover gaps- for example while solar is stronger mid-day, wind is stronger in the evenings

#### FL: Not enough Land

1. They can’t tell u how much land we need - MIT- we only need 12k square kilometers which isnt a lot since we spend 10k km on golf courses
2. Most are either offshore or in the Mojave Desert in like nevada where nobody lives- we have plenty of land

#### FL: Innovation is faster

1. Double bind: Cutting regulations would allow companies to skimp more on safety standards which is a new independent link into our C2 about meltdowns
2. Hutner 20 - innovation itself takes time (designs, small-scale testing) so it takes even longer

#### FL: Emissions inc.

1. Ev is short term before renewables are built - this is otherwise nonsensical since solar panels dont emit co2

#### FL: Nuclear is cheaper

1. Proctor 18 - the most recent reactor the Vogtle plant had cost overruns of 900% - nuclear industry intentionally and chronically underestimates costs to win contracts but in reality it costs way more

### FL Cards

Darrell Proctor 18, 9-24-2018, "How the Vogtle Nuclear Expansion’s Costs Escalated," POWER Magazine, https://www.powermag.com/how-the-vogtle-nuclear-expansions-costs-escalated/

Units 1 and 2 at Plant Vogtle, which is located about 25 miles south of Augusta, Georgia, consist of Westinghouse four-loop pressurized water reactors (PWRs) rated at 1,109 and 1,127 MW respectively. Unit 1 began commercial operation in 1987; Unit 2 followed in 1989. Original estimates for Vogtle reactors 1 and 2 were under $1 billion each, but final costs skyrocketed to nearly $9 billion.

Heidi Hutner 20, 2020, "Nuclear power is not the answer in a time of climate change – Heidi Hutner &amp; Erica Cirino," Aeon, https://aeon.co/ideas/nuclear-power-is-not-the-answer-in-a-time-of-climate-change

Lassiter and several other energy experts advocate for the new, Generation IV nuclear power plants that are supposedly designed to deliver high levels of nuclear power at the lowest cost and with the lowest safety risks. But other experts say that the benefits even here remain unclear. The biggest critique of the Generation IV nuclear reactors is that they are in the design phase, and we don’t have time to wait for their implementation. Climate abatement action is needed immediately.

<https://www.starenergypartners.com/blog/renewable-energy/how-much-land-does-renewable-energy-require/>

According to a study from MIT, powering the entire U.S. electricity demand in 2050 with solar technology would require roughly 33,000 square kilometers of land, or roughly 8 million acres if evenly spread out. However, if the nation concentrates their solar panels to the sunniest parts of the country, it would only require 12,000 square kilometers of land–roughly 3 million acres.

This is certainly a lot of land! However, it starts to look a little smaller when compared to statistics about U.S. land usage. For example, the U.S. uses roughly 10,000 square kilometers of land for golf courses, and our nation has 20,000 square kilometers of rooftops and 49,000 square kilometers of major roadways. So, while the amount of land that would be required to power the nation on solar energy seems large, it really isn’t all that much in the grand scheme of things.

Tom Kline 18, 5-4-2018, "The keys to solving renewable intermittency," New Energy Solar, https://www.newenergysolar.com.au/renewable-insights/renewable-energy/the-keys-to-solving-renewable-intermittency

Storing excess renewable power (or buying and storing when prices are cheap) for use when electricity demand exceeds supply is one way to resolve the intermittent nature of renewable energy. While energy storage comes in many forms, including pumped hydro, hydrogen and flywheels, batteries are the most common solution to renewable intermittency. There are a range of batteries that are currently in use and many more under development that could be combined with renewable generation. **Lithium ion batteries are one of the common types of rechargeable storage devices. This technology is not new and has been in commercial use for almost 30 years.** Australia has been an early adopter of large-scale lithium ion technology combined with renewable generation, and a prime example is the 100 MW Tesla battery in South Australia.10 This battery will be used for a number of purposes, the most important of which is to help prevent load shedding blackouts, and Tesla estimates that at full capacity, it could be capable of powering approximately 50,000 homes for more than an hour.11 According to the Australian Energy Market Operator (AEMO), Tesla’s battery has outperformed coal and gas generators on a number of key metrics.12 On 18 December 2017, a coal generator supplying 689 MW to the South Australian market tripped without warning and within seconds, the Tesla battery was able to respond to discharge electricity to the grid.13 According to AEMO, a steam turbine or gas generator would have taken significantly longer to respond to the shortfall and provide electricity to the market.14 Tesla’s lithium battery also appears to have lowered costs borne by electricity consumers in South Australia. Due to the state’s high penetration of wind farms, AEMO is required to source “frequency control” or “back-up” power generation from gas-fired power stations.15 Sourcing electricity from gas-fired power stations can be very expensive with costs flowing down to consumers.16 However, sourcing back-up power from the battery at a lower cost has enabled the South Australian energy market to avoid the significant price spikes of the previous summer.17 **Another solution to renewable intermittency is the co-location of renewable assets. Australia has** pioneered co-located developments with the Gullen wind and solar project.18 Located in the southern tablelands of NSW, Gullen combines a 10 megawatt (MW) solar farm with 73 wind turbines.19 The Gullen project’s **wind and solar plants complement one another, with solar producing more electricity during the summer and wind generating more in the winter.2**0 F**urthermore, the generation profile of solar and wind are complementary, with solar peaking in the middle of the day and wind generation generally climaxing in the afternoon.**21 The complementary generation profile of wind and solar enables projects to produce electricity almost continuously.22

## C2: Meltdowns

### Extension/Weighing

Expanding nuclear energy causes disaster because of

1. Coverups - due to corruption in the nuclear industry,[frechette finds] 75% of reactors are violating safety regulations and 28% covered up dangerous and defective parts which is why [dujmovic concludes] there’s a 50% chance of another chernobyl-like meltdown in the next 27 years.
2. Cyberattacks - [campbell finds] the nuclear industry is grossly incompetent at defending against cyberattacks, which is why there’s been 20 attacks on reactors since 1990. [Chen finds that] since new reactors means more vulnerable computer systems, each reactor built increases the chance of nuclear cyberattack by 4%, concluding that the total probability of a cyberattack is 75% which leads to meltdowns.
3. HBF - [alverez USNRC] reactors are switching to a new type of fuel called high burnup fuel and its usage is going to double by 2048 -- but it’s high uranium-235 content makes it ultra-hot and highly dangerous and unstable-- that causes spontaneous burnups during transportation and storage that quickly spiral out of control into meltdowns that would make an area the size of massachusetts uninhabitable.

Meltdowns lead to disaster

1. [Gesellschaft and Bertell] find that it would affect 21 million people and kill 2 million from toxic radiation release, just like chernobyl - vote here off the cleanest link to lives in the round.
2. More importantly - [cherp and amadeo] empirically find that accidents cause politicians and the public to turn against and shut down all nuclear reactors in the country- after three mile island and fukushima, nuclear plants were permanently closed around the world.
	1. This outweighs and prereqs the aff- we only need to win that one meltdown happens for all nuclear plants to be banned -- this means the aff has zero chance to solve for warming.

## Frontlines

### Link 1: Coverups

#### FL: Russia China exports worse

1. Turn - Hunkele/ china is actually much better - rapidly improving regulations and now meets international standards - meanwhile US reactors engage and coverups and safety violations

#### FL: US regulations good

1. We’ve subsidized for a long time and it’s still super unsafe
2. Gilinsky 20- Price Anderson act means that the government takes on all liability which removes any incentives for prioritizing safety
3. Ross 11- regulations are super lax ineffective and get circumvented

### Link 2: Cyber

#### FL: No cyberattacks -- Reactors are isolated/airgapped

1. USNRC 19 - a hack on the electrical grid would shut down the safety systems that protect reactors
2. Sovacool 8- new reactors are untested and have vulns
3. Shah 19 - air gapping fails, nothing more than a temp barrier: US airgapped systems have been hacked before
4. [Van Dine 16](https://media.nti.org/documents/IAEA_Conf_2016_Outpacing_Cyber_Threats_Van_Dine.pdf)-already attacks in Japan Ukraine Germany Korea - he concludes cyberattacks probably inevitable
5. As reactors modernize they use more vulnerable computer systems
6. Cybercriminals are getting more sophisticated - rogue nations (iran), or terrorist groups

#### FL: Cyber is alt to physical conflict

1. They don’t have physical mil capacity anyways to beat the US
2. they feel it’s less likely to escalate

#### FL: Should have seen cyberattacks already

1. Yeah there’s been 20, many almost caused meltdowns
2. Chen in case - every plant we build inc hack probability by 4% since more vulnerable systems
3. Chen 20 - enemy nations will pay more attention and inc spending on cyberattacks when we have more reactors b/c we’re seen as a bigger target

### Link 3: HBF

Misc cards: [NEG High Burn-up fuel](https://docs.google.com/document/d/1Ge5Cs-ubIz3qOHyhuPcyBvlmhG_pTOP1Iv3ysIPQ3hw/edit)

#### FL: store it somewhere/dump in new mexico

1. Can’t contain - ev in case says its too hot
2. USNRC/Accidents happen during transportation since it’s unstable
3. USNRC/HBF destabilizes these storage sites - you just move the meltdown somewhere else

#### FL: reprocessing solves

1. Turn: Mikhail 19 - it just transforms it into a different form of even more toxic and dangerous waste and still needs a waste storage site

#### FL: HBF is safe

1. USNRC/ nobody knows about long term safety: studies don’t come out until 2027 and evidence is building that its super dangerous

### Impact

#### FL: New Reactors better/Passive safety measures

1. Maucione 20 - it does not protect against severe accidents or intentional attacks - he’s the director of the national nuclear security project so he’s the more qualified source here
2. Turn: Nuclear Power Org - new reactors use even higher burnup fuels

#### FL: won’t shut down

1. Gillinsky 20 - after fukushima japan shut down all their reactors

2. Mitchel 18 - Germany shut all their reactors down too right after

#### FL: Japan restarted reactors

1. Harding 19 - They got shut down again b/c of public opinion and safety regulations they couldn’t meet

#### FL: No accidents yet

1. Empirically false - just look at fukushima, three mile island, and chernobyl - the risk grows as coverups increase
2. Dujmovic 19 - already seen 56 accidents that resulted in deaths or major property damage, many were covered up but had the risk of meltdowns and nuclear explosions.

#### FL: Fossil Fuels kill more ppl/few ppl actually die

1. Bertell in case- other reports significantly undercounted, didn’t take into account LT radiation deaths - 2 mil total

### FL Cards

Robin Harding 19, 4-25-2019, "Japan’s nuclear reactors face new near-total shutdown," No Publication, https://www.ft.com/content/1b2c395e-6724-11e9-9adc-98bf1d35a056

Japan is heading towards another near-total shutdown of its nuclear reactors after regulators refused to extend deadlines for completing antiterrorism measures.

The Nuclear Regulation Authority said it would enforce deadlines that expired next summer for many operating reactors. Electricity companies have said there was almost no chance they would be ready on time.

Japan has struggled to restart its reactors in the face of strong public opposition and many are still offline. As of March 15, nine out of Japan’s 57 reactors had restarted. Several others have restarted only to shut down again because of injunctions issued by local courts.

Johannes Mikhail 19, 7-8-2019, "Recycle everything, America—except your nuclear waste," Bulletin of the Atomic Scientists, https://thebulletin.org/2019/07/recycle-everything-america-except-your-nuclear-waste/

Now that Americans are “woke” about waste in general, they may turn to the specific kind produced by the nuclear energy industry. Plans to revitalize US nuclear power, which is in dire economic straits, depend on the potential for new, “advanced” reactors to reduce and recycle the waste they produce. **Unfortunately, as they “burn” some kinds of nuclear wastes, these plants will create other kinds that also require disposal. A**t the same time, these “advanced” reactors—many of which are actually reprises of past efforts—increase security and nuclear weapons proliferation risks and ultimately do nothing to break down the political and societal resistance to finding real solutions to nuclear waste disposal. The current nuclear dream is really no different from previous ones of the last 70 years: the next generation of reactors, nuclear power advocates insist, will be safer, cheaper, more reliable, less prone to produce nuclear bomb-making material, and more versatile (producing electricity, heat, and perhaps hydrogen), without creating the wastes that have proved almost impossible to deal with in the United States. The Nuclear Energy Innovation and Modernization Act specifically describes the advanced reactors it seeks to support as having all those positive characteristics. This newest burst of enthusiasm for advanced reactors is, however, largely fueled by the idea that they will burn some of their long-lived radioisotopes, thereby becoming nuclear incinerators for some of their own waste. Many of these “advanced” reactors are actually repackaged designs from 70 years ago. If the United States, France, the UK, Germany, Japan, Russia, and others could not make these reactors economically viable power producers in that time, despite spending more than $60 billion, what is different now? **Moreover, all of the “advanced” designs under discussion now are simply “PowerPoint” reactors: They have not been built at scale, and, as a result, we don’t really know all the waste streams that they will produce.** It’s tempting to believe that having new nuclear power plants that serve, to some degree, as nuclear garbage disposals means there is no need for a nuclear garbage dump, but this isn’t really the case. Even in an optimistic assessment, **these new plants will still produce significant amounts of high-level, long-lived waste. What’s more, new fuel forms used in some of these advanced reactors could pose waste disposal challenges not seen to date. Some of these new reactors would use molten salt-based fuels that, when exposed to water, form highly corrosive hydrofluoric acid. Therefore, reprocessing (or some form of “conditioning”) the waste will likely be required for safety reasons before disposal.** Sodium-cooled fast reactors—a “new” technology proposed to be used in some advanced reactors, including the Bill Gates-funded TerraPower reactors—face their own disposal challenges. These include dealing with the metallic uranium fuel which is pyrophoric (that is, prone to spontaneous combustion) and would need to be reprocessed into a safer form for disposal. Unconventional reactors may reduce the level of some nuclear isotopes in the spent fuel they produce, but that won’t change what really drives requirements for our future nuclear waste repository: the heat production of spent fuel and amount of long-lived radionuclides in the waste. To put it another way, **the new reactors will still need a waste repository, and it will likely need to be just as large as a repository for the waste produced by the current crop of conventional reactors.** Recycling and minimizing—even eliminating—the waste streams that many industries produce is responsible and prudent behavior. But in the context of nuclear energy, recycling is expensive, dirty, and ultimately dangerous. **Reprocessing spent nuclear fuel—which some advanced reactor designs require for safety reasons—actually produces fissile material that could be used to power nuclear weapons. This is precisely why the United States has avoided the reprocessing of spent nuclear fuel for the last four decades, despite having the world’s largest number of commercial nuclear power plants.**

#### FL: new reactors better - SMRs use even higher burnups

Nuclear Power xx, xx-xx-xxxx, "Fuel Burnup," https://www.nuclear-power.net/nuclear-power/reactor-physics/reactor-operation/fuel-burnup/

Current light water reactors are typically designed to achieve burnup about 50 GWd/tU. With newer fuel technology, and particularly the use of advanced burnable absorbers, these same reactors are now capable of achieving up to 60 GWd/tU. Some studies shows that in the near future, even with the present enrichment limit (5 wt %), fuel burnup could be extended near to 70 MWd/kg. Further increase in fuel burnup is impossible without the relaxation of the present enrichment limit (5%).

#### **2. regulations are ineffective and get circumvented**

Ross shows: Ross, Timothy J. Professor of Civil Engineering, University of New Mexico “Avoiding Apocalypse: Congress Should Ban Nuclear Power.” UB Law, Fall 2011. RP

Currently, the NRC is the primary regulatory agency for issues related to nuclear power in the United States.128 Other agencies and offices involved with the regulation of various specific activities related to nuclear power include (but may not be limited to) the DOE, EPA, The NRC’s regulations regarding nuclear power are codified in 10 C.F.R.130 Some key provisions cover licensing and relicensing of power plants,131 disposal and storage of waste,132 and safety and security of nuclear power plants.133 There have, over the years, been a wide array of complaints regarding both the efficacy of the regulations and the NRC’s commitment (or lack thereof) to enforcing them. One major complaint, in so many terms, is that the process of relicensing reactors that have outlived their original licenses is a farce. 134 In a recent Associated Press report, the NRC and the nuclear power industry came under fire for doubling back on the long-standing notion that nuclear power reactors were only supposed to operate for a maximum of forty years.135 According to that article, that forty year limit on the life of nuclear power reactors was “unequivocal . . . ”136 The article refers to the current relicensing process as resembling “nothing more than an elaborate rubber stamp,”137 and states that, often, the NRC’s licensing paperwork looks like a carbon copy of industry applications for relicensing.138 The article also asserts that the NRC has yet to decline a single application for relicensing.139 Another common argument is that safety protocols for nuclear power plants are inadequate to deal with an event like that in Fukushima.140 Current regulations and policies regarding unexpected natural disasters of that sort are based on unrealistic assumptions about the length of time that plants may be blacked out in the event of a power failure.141 Charlie Miller, the head of a recent task force formed to evaluate current regulations in this area, stated that risk studies had never analyzed the risk of simultaneous loss of both grid and backup generator power.142 Yet another issue is the arguably lax enforcement of existing regulations by the NRC. According to one report, the NRC has investigated and discovered twenty-four failures to report faulty equipment and, in the last eight years, has not penalized any plant operators for failure to report these types of risks.143 The same article also mentioned the continued leak at Indian Point (mentioned above), along with several other lapses in enforcement.144 The article also discusses the issue of “capture” and the notion that the NRC, working so closely with the nuclear power industry, often acts more in the interest of the industry than that of the general public.1

#### **3.Gilinsky 20- Price Anderson act removes incentive for prioritizing safety**

Victor Gilinsky, 2-26-2020, "The US government insurance scheme for nuclear power plant accidents no longer makes sense," Bulletin of the Atomic Scientists, https://thebulletin.org/2020/02/the-us-government-insurance-scheme-for-nuclear-power-plant-accidents-no-longer-makes-sense/

To return to the Price-Anderson Act: As we’ve seen, a catastrophic accident would render the US self-insurance scheme for nuclear power plants pretty much irrelevant. **But the indemnification of all industry participants would remain highly relevant: The industry would be free of any liability for offsite death or damage, whereas the victims would have to go hat in hand to Congress for restitution.** This is an enormous subsidy—consider, again, the $750 billion and counting tab for Fukushima—that the federal government provides the nuclear industry, one without which not a single US nuclear power plant would or could operate. **Freedom from liability also has had a perverse effect on nuclear safety. Without the liability protection of Price-Anderson, industry incentives to develop nuclear designs safer than light water reactors would surely have been higher.** Freedom from liability was put into law in the 1950s to get the US commercial nuclear power industry off the ground. It was meant to be temporary, until industry and insurers got some experience with the new technology. But even as time went on, industrial organizations like General Electric and Westinghouse would not participate in the civilian nuclear program if they risked responsibility for offsite damage from a nuclear plant accident.This government guarantee was an understandable demand at the outset of the nuclear age, when the risks of nuclear power were unclear and maybe a little scary. But it’s now half a century later, and the NRC commissioners tell us that probabilistic risk assessment is a highly developed tool. They urge their staff to make greater use of it in making regulatory decisions. **Yet the vendors continue to maintain their insistence on freedom from liability for offsite consequences.** If you accept the NRC accident estimates, the risk the vendors would run without an exemption from liability would be very small, and likely a lot smaller than other corporate risks they routinely run. **What is clear is that the nuclear firms—the largest of which possess an understanding of nuclear safety far beyond that of the public—do not believe the NRC safety conclusions that the risk of a catastrophic nuclear accident is infinitesmal.** Nor do they accept that probable risk—probability of an accident times the consequences, were one to occur—as the right measure of risk to their companies. They don’t want to risk their companies, period. Such new designs would eliminate the current dilemma of a federal nuclear self-insurance scheme that cannot, as a practical matter, cover the financial consequences to the public of catastrophic nuclear power plant accidents. But how to get there? **One of the disincentives is the Price-Anderson Act’s limitations on industry liability for offsite accident consequences. That should get phased out.**

Dean Hunkele 19, 12-6-2019, "And the prize for global nuclear security goes to... China," Bulletin of the Atomic Scientists, https://thebulletin.org/2019/12/and-the-prize-for-global-nuclear-security-goes-to-china/

In fact, when it comes to nuclear security policies and practices, as well as laws, regulations, management, monitoring, and the structure of emergency response, the country is unusually transparent—and readily meets international standards. As a result, China is poised to play a leading role in global nuclear risk reduction efforts in the coming decades, at home and abroad. This trend can be seen by China’s many commitments within the Nuclear Security Summit process, its cooperation in bilateral nuclear security structures with the United States, and its efforts to remove highly enriched uranium from a Nigerian research reactor (that China itself played a role in building).

But what do recent Chinese nuclear security efforts reveal about how China will approach setting the agenda for the future? And how is China’s approach likely to evolve in the coming decades as arms control becomes less prominent, China becomes a larger exporter of nuclear technology and materials, and China asserts its own priorities in other forums?

China’s approach to nuclear risk reduction. Chinese participation in the Nuclear Security Summits has played into China’s long-standing self-perception as the most responsible of the major nuclear powers. Indeed, China has joined nearly all international legal instruments relevant to nuclear security, and the obligation to fulfill the many requirements of these instruments has been the major driver of improvements to Chinese nuclear security capabilities. Since the first Nuclear Security Summit in 2010, China has drafted a relatively complete set of nuclear security policies, implemented a series of domestic laws and regulations, and established a fairly complete system for nuclear security management, monitoring, and emergency response.

Scott Maucione 20, 3-5-2020, "Lord: DoD wants mini nuclear reactors on bases and for transport," Federal News Network, https://federalnewsnetwork.com/defense-main/2020/03/lord-dod-wants-mini-nuclear-reactors-on-bases-and-for-transport/

“Passive safety cannot eliminate every pathway by which the reactor fuel could be damaged and release radioactivity. If a severe accident or sabotage attack were to induce more extreme conditions than the reactor was designed to withstand, all bets are off,” Edwin Lyman, senior scientist and acting director of the Nuclear Safety Project at the Union of Concerned Scientists wrote in the Bulletin of the Atomic Scientists.

[Van Dine 16](https://media.nti.org/documents/IAEA_Conf_2016_Outpacing_Cyber_Threats_Van_Dine.pdf) concludes that

**. It may only be a matter of time before the world experiences a catastrophic event**—whether a theft of nuclear material, or the sabotage of a nuclear facility—facilitated **by a cyber-attack** deployed by a[n] determined, well-resourced adversary. Those responsible for security, from policymakers to regulators to industry leaders to facility operators, face the significant challenge of getting ahead of the fast-moving threat.

 Aaron Esau and Robert Chen 2/4/20 <https://ctf.redpwn.net/static/drafts/81/8188bfc51cfec2edec1277f2a121a4b2.pdf>

Even if the vulnerabilities don’t get exploited, the presence of additional nuclear reactors could incentivize adversaries to devote more money to offensive cybersecurity programs. Russia and China are nowhere close to their limit on cybersecurity spending: an excuse is all they need to ramp up spending. With juicy targets like nuclear reactors, there might even be a full-fledged cyberwar.

Returning to the example of Stuxnet, nuclear energy is one such area that we should take the utmost caution towards. If anything, building new nuclear reactors will only increase the attack surface. It is a common adage that no code is bug free. In fact, Steve McConnell, author of Code Complete, finds that the average codebase has anywhere between 15 to 50 errors per 1000 lines of code. nuclear reactor could increase the size of the codebase by 1.6%. With presumably millions of lines of code per reactor, the conclusion is obvious.

There is a need for alarm. Our internal modeling suggests that for every nuclear reactor built, the probability of a nuclear cyberattack increases by 4%. If the US were to switch entirely to nuclear energy, there would be a 75% chance of a cyberattack before the end of 2020. A cyberattack would be devastating, potentially crippling the United States. Coordinated meltdowns could trigger an environmental calamity, permanently ruining the environment and killing millions instantly from radiation poisoning and fallout. These conditions could quickly become global, decimating populations around the world.

Risks are magnified due to the new wave of nuclear technology. [Sovacool 08](https://www.academia.edu/40232917/NUCLEAR_NONSENSE_WHY_NUCLEAR_POWER_IS_NO_ANSWER_TO_CLIMATE_CHANGE_AND_THE_WORLD_S_POST-KYOTO_ENERGY_CHALLENGES) finds that

Although the incident at Three Mile Island avoided this nightmare scenario, barely, it brought about sweeping changes to the industry and forced the permanent closure and decommissioning of TMI Unit 2.498 After the accident, emergency response planning, reactor operator training, human factors engineering, radiation protection, and many other areas of nuclear power plant operations in the U.S. were radically reformed. Newer Reactors are the Riskiest Unfortunately, **safety risks** such as those at Chernobyl and Three Mile Island **are** only **amplified with new** generations of **nuclear systems**. Nuclear engineer David Lochbaum has noted that **[as] almost all serious** nuclear **accidents occurred with recent technology**, making newer systems the riskiest.5" In 1959, the Sodium Research Experiment reactor in California experienced a partial meltdown fourteen months after opening." 1 In 1961, the S1-1 Reactor in Idaho was slightly more than two years old before a fatal accident killed everyone at the site.50 2 The Fermi Unit 1 reactor began commercial operation in August 1966, but had a partial meltdown only two months after opening.50 3 The St. Laurent des Eaux Al Reactor in France started in June 1969, but an online refueling machine malfunc- tioned and melted 400 pounds of fuel four months later."4 The Browns Ferry Unit 1 reactor in Alabama began commercial operation in August 1974 but experienced a fire severely damaging control equipment six months later.5 Three Mile Island Unit 2 began commercial operation in December 1978 but had a partial meltdown three months after it started.0 6 Chernobyl Unit 4 started up in August 1984, and suffered the worst nuclear disaster in history on April 26, 1986 before the two-year anniversary of its operation.0 7 Safety risks may be especially acute for new reactors in the U.S. for three reasons. First**, the pressure to build new generators on existing sites** to avoid complex issues associated with finding new locations only **increases the risk of catastrophe**, **because there is a greater chance that one accident can affect multiple reactors**. Second, Generation IV [Furthermore,] researchers continue to pursue breeder reactor designs that use liquid sodium as coolant[s].5" Liquid sodium, however, can be dangerous, since it [which] can immediately catch fire when exposed to water.510 Third, the domestic nuclear industry lacks qualified and experienced staff and is losing much of the expertise that it does have to retirement, attrition and death.5 '

[Van Dine 16](https://media.nti.org/documents/IAEA_Conf_2016_Outpacing_Cyber_Threats_Van_Dine.pdf) finds that

The past decade has seen unprecedented progress in the security of nuclear materials and facilities. As key improvements to physical security have been implemented, however, a potentially more dangerous threat is undermining these gains: the cyber threat. **Cyber-attacks could be used** to facilitate the theft of nuclear materials or **[as]an act of sabotage resulting in radiological release**. A successful attack could have consequences that CN-244-64 2 reverberate around the world and undermine global confidence in civilian nuclear power as a safe and reliable energy source. Given the risk and the stakes, governments and industry must now increase focus on the cyber threat. Nuclear operators and a range of national and international organizations have recognized the challenge and have begun to accelerate their efforts to strengthen cyber security at nuclear facilities. However, the rapidly evolving cyber threat, combined with the proliferation of digital systems, makes it difficult to get ahead of the threat. Case after case—from the Stuxnet attacks on the Natanz uranium enrichment facility in Iran, to the hack of Korea Hydro and Nuclear Power in South Korea, to disturbing revelations of malware seeking login credentials found on systems at a German nuclear power plant—demonstrates that the current approach to cyber security at nuclear facilities is falling short, and will soon be insufficient. Crafting a strategy that protects facilities from the dynamic, evolving cyber threats they now face requires a fresh, unconstrained examination of the overarching framework that guides their cyber security. **Recent history is filled with examples demonstrating that** critical infrastructure and even **nuclear facilities are vulnerable, including attacks in**—both to untargeted malware and targeted cyber-attacks. As is now well known, the Natanz uranium enrichment facility in Iran was attacked with the Stuxnet virus between 2009 and 2010, damaging centrifuges and delaying enrichment activities. [3] This case is particularly notable as the facility was described as well-defended and isolated from the internet. Since news of Stuxnet broke, revelations of malware found in nuclear facilities and critical infrastructure have only increased in frequency. In 2014 alone, a cyber-attack against a German steel mill caused massive physical damage, malware was introduced into the control room at **Japan’s** Monju nuclear power plant, and systems associated with the **Korea** Hydro and Nuclear Power in South Korea was hacked. The Japanese and South Korean cases resulted in the release of technical data online. [4] [5] [6] The year 2015 saw a sophisticated, troubling cyber-attack—one that it is not hard to imagine being used against a nuclear facility—against the **Ukrain[e]ian** power grid that turned out the lights in portions of that country for between three and six hours. [7] [8] And in 2016, a **[and] German[y]** nuclear power plant , and a Japanese facility that handles plutonium and other nuclear materials revealed that they had discovered malware in its systems. [9] [10]**. It may only be a matter of time before the world experiences a catastrophic event**—whether a theft of nuclear material, or the sabotage of a nuclear facility—facilitated **by a cyber-attack** deployed by a[n] determined, well-resourced adversary. Those responsible for security, from policymakers to regulators to industry leaders to facility operators, face the significant challenge of getting ahead of the fast-moving threat.

####

#### Chernobyl was bad

Bertell of the PEI http://www.pacificecologist.org/archive/12/behind-the-cover-up.pdf

The Chernobyl disaster occurred in 1986, and now 20 years after the event, there is as yet no comprehensive systematic report on the casualties. This article presents an attempt to extend the sketchy information given in the 2000 report of the United Nations Committee on the Effects of Atomic Radiation. (UNSCEAR): “Sources and Effects of Ionizing Radiation.” This report, as Part III, gives the official U.N. agency’s information on the Chernobyl accident, the release of radionuclides, exposure to individuals and health effects, as gathered by the International Atomic Energy Agency (I.A.E.A.) over the past twenty years.1 **The 2000 report omitted to assess the entire population at risk and failed to estimate fatalities due to radiation damage to tissue and/or its ability to initiate a fatal cancer**

Poor records and methodology, omissions, and the failure of various committees to consider all health issues resulting from the Chernobyl nuclear power plant disaster in 1986, have meant **the real consequences for the many millions of affected people have been hidden from public scrutiny**, DR. ROSALIE BERTELL reports. Using a report from a U.N. science committee in 2000, **Dr Bertell identifies the many omissions and makes a very conservative, preliminary estimate of the eventual death toll from the Chernobyl disaster to be 1 to 2 million.**

Mitchel 18, 11-24-2018, "Germany's Nuclear Power Phase-Out Post-Fukushima," No Publication, http://large.stanford.edu/courses/2018/ph240/mitchel2/

The nuclear disaster in Fukushima, Japan, in March 2011 came at a time when leaders across the world were embracing the idea of nuclear power as an alternative to fossil fuel energy production. [2] The Fukushima disaster involved the meltdown of three nuclear reactors as a result of a tsunami triggered by an earthquake. [3] **After the disaster, there was a major shift in Germany's attitude towards nuclear power. [3] In the wake of the Fukushima disaster, over 40,000 people protested against nuclear power across Germany. By June 2011, Merkel decided to shut down eight of Germany's seventeen reactors. Furthermore, the remaining plants would be shut down altogether by 2022.** This aggressive action against nuclear power was supported by politicians across parties and the general public. By 2016, of Germany's electricity production of 651 TWh, only 85 TWh came from nuclear power. [1]

#### Accidents lead to mass shutdowns - Fukushima proves

Victor Gilinsky, 2-26-2020, "The US government insurance scheme for nuclear power plant accidents no longer makes sense," Bulletin of the Atomic Scientists, https://thebulletin.org/2020/02/the-us-government-insurance-scheme-for-nuclear-power-plant-accidents-no-longer-makes-sense/

The main public risk of nuclear power plants comes from rare but devastating nuclear accidents. Because data on such accidents is sparse, the probability of their occurrence has to be calculated on the basis of a model, rather than obtained from experience. Moreover, the extent of an accident and its monetary consequences are postulated on the basis of models that are limited by analysts’ imagination. Who would have imagined, for example, that **the Fukushima accident would involve several reactors? Or that Japan would subsequently shut down all its other nuclear power plants?**

Jurica Dujmovic, 7-2-2019, "HBO’s ‘Chernobyl’ is a scary reminder that there are constant nuclear-safety violations," MarketWatch, https://www.marketwatch.com/story/hbos-chernobyl-is-a-scary-reminder-that-there-are-constant-nuclear-safety-violations-2019-07-02

Between 2001 and 2006, the U.S. Government Accountability Office (GAO) reported more than 150 incidents of nuclear plants not performing within acceptable safety guidelines**. According to a survey of energy accidents from 2010, there have been at least 56 accidents at nuclear reactors in the U.S., resulting in loss of human life and/or more than $50,000 of property damage. These accidents included meltdowns, fires** and coolant-related problems. They were nothing to scoff at. **Many of them might have had the potential to turn into something catastrophic**, but none were as serious as the Three Mile Island accident in 1979 and the one at the Davis-Besse Nuclear Power Station in 2002 The Three Mile Island accident occurred because of a cooling malfunction, which caused a part of the core to melt. This resulted in a radiation leak and counts as the most significant accident for any U.S. commercial nuclear power plant. While the crisis was subdued in a timely manner, and the radiation released into the environment wasn’t significant, it **was a close call**: **In a worst-case scenario, the nuclear fuel would have melted and burned through the vessel** and the reactor basement right into the soil. **The result would have been a steam explosion spewing vast amounts of radiation.**

USNRC 19

<https://www.mass.gov/files/documents/2019/05/30/February%2020%2C%202019%20Pilgrim%20Watch%20Petition%20to%20Intervene%20and%20Hearing%20Request.pdf>

The GEIS and SEIS both ignore the escalating terrorist threat with US infrastructure, including nuclear reactors as targets. Both predate awareness of an increased threat from cyber-attacks,70 drones, and electromagnetic attacks.71 For example, while reactor safety systems are more or less isolated from an outside cyberattack, a hack knocking out the electrical grid system would shut down power to all reactor safety systems. On-site emergency power generators are then vulnerable to insider and armed assault seeking to cause a meltdown. Loss of electric grid may disenable security cameras.

#### India attack last year

Alexander Campbell, 11-14-2019, "Lessons from the cyberattack on India’s largest nuclear power plant," Bulletin of the Atomic Scientists, https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant/

**Indian officials acknowledged on October 30th that a cyberattack occurred at the country’s Kudankulam nuclear power plant.** An Indian private cybersecurity researcher had tweeted about the breach three days earlier, prompting Indian authorities to initially deny that it had occurred before admitting that the intrusion had been discovered in early September and that efforts were underway to respond to it. According to last Monday’s Washington Post, Kudankulam is India’s biggest nuclear power plant, “equipped with two Russian-designed and supplied VVER pressurized water reactors with a capacity of 1,000 megawatts each. Both reactor units feed India’s southern power grid. The plant is adding four more reactor units of the same capacity, making the Kudankulam Nuclear Power Plant one of the largest collaborations between India and Russia.” While reactor operations at Kudankulam were reportedly unaffected, this incident should serve as yet another wake-up call that **the nuclear power industry needs to take cybersecurity more seriously. There are worrying indications that it currently does not: A 2015 report by the British think tank Chatham House found pervasive shortcomings in the nuclear power industry’s approach to cybersecurity, from regulation to training to user behavior. In general, nuclear power plant operators have failed to broaden their cultures of safety and security to include an awareness of cyberthreats.** (And by cultures of safety and security, those in the field—such as the Fissile Materials Working Group—refer to a broad, all-embracing approach towards nuclear security, that takes into account the human factor and encompasses programs on personnel reliability and training, illicit trafficking interception, customs and border security, export control, and IT security, to name just a few items. The Hague Communiqué of 2014 listed nuclear security culture as the first of its three pillars of nuclear security, the other two being physical protection and materials accounting.) This laxness might be understandable if last week’s incident were the first of its kind. **Instead, there have been over 20 known cyber incidents at nuclear facilities since 1990.** This number includes relatively minor items such as accidents from software bugs and inadequately tested updates along with deliberate intrusions, but **it demonstrates that the nuclear sector is not somehow immune to cyber-related threats. Furthermore, as the digitalization of nuclear reactor instrumentation and control systems increases, so does the potential for malicious and accidental cyber incidents alike to cause harm. This record should also disprove the old myth, unfortunately repeated in Kudankulam officials’ remarks, that so-called air-gapping effectively secures operational networks at plants.** Air-gapping refers to separating the plant’s internet-connected business networks from the operational networks that control plant processes; doing so is intended to prevent malware from more easily infected business networks from affecting industrial control systems. The intrusion at Kudankulam so far seems limited to the plant’s business networks, **but air gaps have failed at the Davis-Besse nuclear power plant in Ohio in 2003 and even classified US military systems in 2008. The same report from Chatham House found ample sector-wide evidence of employee behavior that would circumvent air gaps, like charging personal phones via reactor control room USB slots and installing remote access tools for contractors.** **The consequences of a cyber-based intrusion at a nuclear power plant could** range from loss of confidential employee or business information to potentially **causing a reactor shutdown or physical damage.** The industry must realize that cyberattacks can be the main event, rather than simply a means to enable more traditionally imagined threats like physical intrusions. And regardless of the consequences of a given incident, public statements like those from Indian authorities last week that refuse to even admit the possibility of **cyberattack will undermine public trust—an existential resource for many nuclear power programs.** One item to note, however, is that the problem’s scale and complexity is only likely to grow as more states join the nuclear power club. And even with years of experience, **no country is immune from succumbing to cyberattack: Last week’s incident occurred in a country whose nuclear power program dates back to the 1950s, and previous cyberattacks have struck nuclear facilities in countries with similarly long-established nuclear power programs, including Japan, France, and the United States.** That they have still fallen victim to breaches bodes ill for prospective newcomers like Jordan, whose national Computer Emergency Response Team is only two years old. One can expect that nuclear newcomers with less indigenous cybersecurity expertise will need more help from international partners, and will face a steeper uphill climb towards maintaining that workforce.

####

####

#### State and non-state actors will cyber aĴack vulnerable nuclear power plants – terrorists can easily develop the means and cyber defenses are low.

Pompera and Tarinib, 17 Miles A. Pompera (Senior Fellow, James Martin Center for Nonproliferation Studies) and Gabrielle Tarinib (Research Associate, James Martin Center for Nonproliferation Studies), “Nuclear Terrorism – Threat or Not?”, AIP Conference Proceedings 1898, 050001 (2017); hĴps://doi.org/10.1063/1.5009230, accessed 2-3-2020, VBI

 **Finally, cyber-aĴacks are an emerging vulnerability for nuclear power plants. Several notable cyberaĴacks have already occurred at nuclear facilities, including the Stuxnet virus that damaged Iran’s Natanz centrifuge facility, the placement of a virus into the computers of the Ignalia nuclear power plant in Lithuania in 1992, and the hacking of the computer systems of KHNP, South Korea’s nuclear operator by presumably North Korea.**47 AĴackers could use cyber techniques to undermine security at nuclear reactors to facilitate, on one end of the spectrum, the theft of confidential or proprietary information, or the release of radiation on the other. According to a 2015 report published by Chatham House, “An adversary with sufficient technical knowledge and adequate resources could mount an aĴack on a nuclear power plant that could trigger the release of ionizing radiation. All nuclear power plants need offsite power to operate safely and all have a standby generator which is designed to be activated when a loss of main power occurs. AĴacks on the offsite power supply and on the on-site backup system could create some of the effects that occurred following the 2011 earthquake and tsunami at Fukushima Daiichi, although multiple failures of the many safety features at modern nuclear power plants could also need to occur at the same time as that loss to offsite power and the disruption of standby generators.”48 While the concern of radiation release is remote, even a small-scale cyber incident at a nuclear facility would likely have a disproportionate effect on the public’s opinion of nuclear energy and nuclear industry. Although terrorists are not currently believed to possess an advanced cyber capability, groups like the Islamic State of Iraq and Syria (ISIS) have developed a sophisticated strategy of online recruitment, which utilizes not only Facebook and TwiĴer but also encrypted platforms on mobile devices.49 Moreover**, it is not implausible that a group’s desire to cause damage at a nuclear facility could lead them to develop the necessary skills or employ a profit-motivated cyber-criminal group to do this.50** Cyber defense of nuclear power plants requires a significant financial and intellectual investment on the part of states. According to the NTI Nuclear Security Index, many countries require virtually no cyber security measures at nuclear facilities and do not have a legal framework for these requirements.51

#### Airgaps don’t solve against determined adversaries or new threats

Stoutland, 18 Page Stoutland (PhD, Vice President, Scientific and Technical Affairs at NTI), ”CyberaĴacks on Nuclear Power Plants: How Worried Should We Be?”, 3-19-2018, Nuclear Threat Initiative, hĴps://www.nti.org/analysis/atomic-pulse/cyberaĴacks-nuclearpower-plants-how-worried-should-we-be/, accessed 2-4-2020, VBI

 As recent aĴacks have confirmed, cyberaĴacks are geĴing increasingly sophisticated. Complex aĴacks are no longer just the purview of nations but can now be conducted by smaller groups. Furthermore, systems which may have been analog at one time are increasingly digital and increasingly complex. The growing Internet-of-Things will present additional challenges. Responding to this growing threat is not easy**. Airgaps, originally designed to counter untargeted aĴacks, are not effective against a determined adversary. Existing safety systems may not be effective against cyberaĴacks that can lead to failures that would never occur naturally.** Furthermore, threats do not just arise from the internet—defenders must consider supply chain risks and the potential for insider threat.

#### Airgaps don’t solve – tech exists to penetrate air-gapped nuclear facilities.

Shah, 19 Syed Sadam Hussain Shah (a research assistant at the Center for International Strategic Studies in Islamabad, he has published in leading journals such as the Bulletin of Atomic Scientists (“Estimating India’s nuclear weapon producing capacity”) and CISS Insight. He recently presented and published a paper (“Indian Strategic Thought”) at Karadeniz Teknik University, Turkey. His forthcoming paper is “Artificial Intelligence, Hacking, and Nuclear Weapons.”) “Offensive Cyber Operations and Nuclear Weapons,” March 2019, Center for Strategic and International Studies, hĴps://csisprod.s3.amazonaws.com/s3fs-public/190313\_Shah\_OffensiveCyber\_pageproofs2.pdf,

Organizations struggle to protect the confidentiality and integrity of their networks and data. They invest a lot of money in securing their networks by using defensive cyber security measures such as purchasing expensive firewalls, tasking dummy networks to confuse the aĴacker, and investing in honeynet traps. But all of these measures are vulnerable and insufficien**t. Therefore, military and nuclear organizations rely heavily on air-gapped networks (“a network that is not connected to the internet, no wireless, no modem, and protected by gates and guards, and considered as hack-proof”)4 . But airgapped networks are still vulnerable to cyberaĴacks. For example, the U.S. Department of Homeland Security believes that Russian hackers have infiltrated U.S. critical infrastructure, which was air gapped**.5 Speaking to a Black Hat conference in Amsterdam, Shamir Adi—a professor of applied mathematics at the Weizmann Institute of Science and co-developer of RSA algorithm—elaborated how air-gapped network can be compromised. He described how a vulnerability that he called “Scangate” could allow malware to “infiltrate and exfiltrate data from air-gapped networks, using a long-distance laser to send data into the environment and the video camera on a drone to get it out.”**6 System-level access in an air-gapped network at a nuclear facility could allow a hacker to cause a radiological accident or crash the reactor process by raising or lowering pressure, resulting in mass causalities and loss of the facility. Nuclear organizations require thousands of computers for their operations, and even a single vulnerability can lead to severe consequences.** Missile guidance systems, communications systems, nuclear submarines, and many other critical C3 systems are connected to computers and thus vulnerable to cyberaĴack, which may result in an inadvertent escalation.

#### F2: Nuclear Encryption

1. **Futter of Arms Control Association-** finds that although there have bee move to bolster defense of US nuclear systems, they will never manage to fill in all the holes.

[Andrew Futter, , Arms Control Association, "The Dangers of Using Cyberattacks to Counter Nuclear Threats | Arms Control Association," July/August 2016, https://www.armscontrol.org/act/2016-07/features/dangers-using-cyberattacks-counter-nuclear-threats]

Thomas D’Agostino, head of the Department of Energy’s National Nuclear Security Administration, revealed that U.S. nuclear weapons and associated systems “are under constant attack” from a “full spectrum of hackers.”2**0 Although recent moves to bolster the defense of U.S. nuclear systems against cyberattacks**,21 as well as the establishment of in-house hacker teams at the Pentagon,22 should be welcomed, they **are unlikely to be foolproof.** This is particularly true **in light of the ongoing development of technologies to “jump” the air gap** and widespread attempts by U.S. adversaries to use cyberespionage to steal sensitive nuclear-related secrets about these systems from U.S. government agencies, research laboratories, and contractors, possibly as a precursor to future attack.

####

#### Nuclear cyberattack inevitable

https://media.nti.org/documents/IAEA\_Conf\_2016\_Outpacing\_Cyber\_Threats\_Van\_Dine.pdf

The past decade has seen unprecedented progress in the security of nuclear materials and facilities. As key improvements to physical security have been implemented, however, **a potentially more dangerous threat is undermining these gains: the cyber threat. Cyber-attacks could be used to facilitate the theft of nuclear materials or an act of sabotage resulting in radiological release. A successful attack could have consequences that CN-244-64 2 reverberate around the world and undermine global confidence in civilian nuclear power as a safe and reliable energy source**. Given the risk and the stakes, governments and industry must now increase focus on the cyber threat. Nuclear operators and a range of national and international organizations have recognized the challenge and have begun to accelerate their efforts to strengthen cyber security at nuclear facilities. However, the rapidly evolving cyber threat, combined with the proliferation of digital systems, makes it difficult to get ahead of the threat. Case after case—from the Stuxnet attacks on the Natanz uranium enrichment facility in Iran, to the hack of Korea Hydro and Nuclear Power in South Korea, to disturbing revelations of malware seeking login credentials found on systems at a German nuclear power plant—demonstrates that the current approach to cyber security at nuclear facilities is falling short, and will soon be insufficient. Crafting a strategy that protects facilities from the dynamic, evolving cyber threats they now face requires a fresh, unconstrained examination of the overarching framework that guides their cyber security.

**Recent history is filled with examples demonstrating that critical infrastructure and even nuclear facilities are vulnerable—both to untargeted malware and targeted cyber-attacks. As is now well known, the Natanz uranium enrichment facility in Iran was attacked with the Stuxnet virus between 2009 and 2010, damaging centrifuges and delaying enrichment activities. [3] This case is particularly notable as the facility was described as well-defended and isolated from the internet. Since news of Stuxnet broke, revelations of malware found in nuclear facilities and critical infrastructure have only increased in frequency. In 2014 alone, a cyber-attack against a German steel mill caused massive physical damage, malware was introduced into the control room at Japan’s Monju nuclear power plant, and systems associated with the Korea Hydro and Nuclear Power in South Korea was hacked. The Japanese and South Korean cases resulted in the release of technical data online. [4] [5] [6] The year 2015 saw a sophisticated, troubling cyber-attack—one that it is not hard to imagine being used against a nuclear facility—against the Ukrainian power grid that turned out the lights in portions of that country for between three and six hours. [7] [8] And in 2016, a German nuclear power plant** , and a Japanese facility that handles plutonium and other nuclear materials revealed that they had discovered malware in its systems. [9] [10]**. It may only be a matter of time before the world experiences a catastrophic event—whether a theft of nuclear material, or the sabotage of a nuclear facility—facilitated by a cyber-attack deployed by a determined, well-resourced adversary.** Those responsible for security, from policymakers to regulators to industry leaders to facility operators, face the significant challenge of getting ahead of the fast-moving threat.

#### Cyberattacks on our grids are inevitable—Ukraine proves.

**Morgan 16** Steve (Steve Morgan is the Founder and CEO at Cybersecurity Ventures and Editor-In-Chief of the Cybersecurity Market Report. The Cybersecurity Market Report is published quarterly and covers the business of cybersecurity, including global market sizing and industry forecasts from consolidated research by IT analyst firms, emerging trends, employment, the federal sector, hot companies to watch, notable M&A, investment and IPO activity, and more) “Major Cyber Attack On U.S. Power Grid Is Likely” Forbes February 7th 2016 <http://www.forbes.com/sites/stevemorgan/2016/02/07/campaign-2016-major-cyber-attack-on-u-s-power-grid-is-likely/#5339e6a6610f>. JW

In his New York Times bestselling investigation, Koppel reveals that **a major cyberattack on America’s power grid is** not only possible but **likely**, that it would be **devastating**, **and** that **the United States is shockingly unprepared**. U.S. investigators recently found proof that a cyber attack can take down a power grid. **A destructive malware app** known as ‘BlackEnergy’ **caused a power outage on the Ukranian power grid** this past December, **resulting in a blackout for hundreds of thousands** of people. Ukranian officials have blamed Russia for the cyber attack. A CNN article states **that U.S. systems aren’t any more protected** than those breached in Ukraine.

#### The threat of cyber-attack is real – multiple countries and terrorists are acquiring capabilities

**Habiger 10** (Eugue, Retired Air Force General, Cyberwarfare and Cyberterrorism, The Cyber Security Institute, 2/1, p. 11-19)

However, there are reasons to believe that what is going on now amounts to a fundamental shift as opposed to business as usual. Today’s network exploitation or information operation trespasses possess a number of characteristics that suggest that the line between espionage and conflict has been, or is close to being, crossed. (What that suggests for the proper response is a different matter.) First, the number of cyberattacks we are facing is **growing significantly**. Andrew Palowitch, a former CIA official now consulting with the US Strategic Command (STRATCOM), which oversees the Defense Department’s Joint Task Force‐Global Network Operations, recently told a meeting of experts that the Defense Department has experienced **almost 80,000 computer attacks**, and some number of these assaults have actually “reduced” the military’s “**operational capabilities**.”20 Second, the nature of these attacks is starting to shift from penetration attempts aimed at gathering intelligence (cyber spying) **to offensive efforts** aimed at taking down systems (cyberattacks). Palowitch put this in stark terms last November, “We are currently in a cyberwar and war is going on today.”21 Third, these recent attacks need to be taken in a broader strategic context. Both Russia and China have stepped up their offensive efforts and taken a **much more aggressive cyberwarfare posture**. The Chinese have developed an openly discussed cyberwar strategy aimed at achieving electronic dominance over the U.S. and its allies by 2050. In 2007 the Department of Defense reported that for the first time China has developed **first strike viruses**, marking a **major shift** from prior investments in defensive measures.22 And in the intervening period China has launched a series of offensive cyber operations against U.S. government and private sector networks and infrastructure. In 2007, Gen. James Cartwright, the former head of STRATCOM and now the Vice Chairman of the Joint Chiefs of Staff, told the US‐China Economic and Security Review Commission that China’s ability to launch “denial of service” attacks to overwhelm an IT system is of particular concern. 23 Russia also has already begun to wage offensive cyberwar. At the outset of the recent hostilities with Georgia, Russian assets launched a series of cyberattacks against the Georgian government and its critical infrastructure systems, including media, banking and transportation sites.24 In 2007, cyberattacks that many experts attribute, directly or indirectly, **to Russia shut down the Estonia government’s IT systems**. Fourth, the current geopolitical context must also be factored into any effort to gauge the degree of threat of cyberwar. The start of the new Obama Administration has begun to help reduce tensions between the United States and other nations. And, the new administration has taken initial steps to improve bilateral relations specifically with both China and Russia. However, it must be said that over the last few years the posture of both the Chinese and Russian governments toward America has clearly become **more assertive, and** at times even **aggressive**. Some commentators have talked about the prospects of a cyber Pearl Harbor, and the pattern of Chinese and Russian behavior to date **gives reason for concern** along these lines: both nations have offensive cyberwarfare strategies in place; both nations have taken the cyber equivalent of building up their forces; both nations now regularly probe our cyber defenses looking for gaps to be exploited; both nations have begun taking actions that cross the line from cyberespionage to cyberaggression; and, our bilateral relations with both nations are increasingly **fractious and complicated by** areas of marked, direct **competition**. Clearly, there a sharp differences between current U.S. relations with these two nations and relations between the US and Japan just prior to World War II. However, from a strategic defense perspective, there are enough warning signs to warrant preparation. In addition to the threat of cyberwar, the limited resources required to carry out even a large scale cyberattack also makes **likely the potential for a significant cyberterror attack** against the United States. However, the lack of a long list of specific incidences of cyberterrorism should provide no comfort. There is **strong evidence** to suggest that al Qaeda has the ability to conduct cyberterror attacks against the United States and its allies. Al Qaeda and other terrorist organizations are extremely active in cyberspace, using these technologies to communicate among themselves and others, carry out logistics, recruit members, and wage information warfare. For example, al Qaeda leaders used email to communicate with the 9‐11 terrorists and the 9‐11 terrorists used the Internet to make travel plans and book flights. Osama bin Laden and other al Qaeda members routinely post videos and other messages to online sites to communicate. Moreover, there is evidence of efforts that al Qaeda and other terrorist organizations are **actively developing cyberterrorism capabilities** and seeking to carry out cyberterrorist attacks. For example, the Washington Post has reported that “U.S. investigators have found evidence in the logs that mark a browser's path through the Internet that al Qaeda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transport and communications grids. In some interrogations . . . al Qaeda prisoners have described intentions, in general terms, to use those tools.”25 Similarly, a 2002 CIA report on the cyberterror threat to a member of the Senate stated that al Qaeda and Hezbollah have become "more adept at using the internet and computer technologies.”26 The FBI has issued bulletins stating that, “U. S. law enforcement and intelligence agencies have received indications that Al Qaeda members have sought information on Supervisory Control And Data Acquisition (SCADA) systems available on multiple SCADA‐related web sites.”27 In addition a number of jihadist websites, such as 7hj.7hj.com, teach computer attack and hacking skills in the service of Islam.28 While al Qaeda may lack the cyber‐attack capability of nations like Russia and China, there is every reason to believe its operatives, and those of its ilk, are as capable as the cyber criminals and hackers who routinely effect great harm on the world’s digital infrastructure generally and American assets specifically. In fact, perhaps, the most troubling indication of the level of the cyberterrorist threat is the countless, serious non‐terrorist cyberattacks routinely carried out by criminals, hackers, disgruntled insiders, crime syndicates and the like. If run‐of‐the‐mill criminals and hackers can threaten powergrids, hack vital military networks, steal vast sums of money, take down a city’s of traffic lights, compromise the Federal Aviation Administration’s air traffic control systems, among other attacks, it is **overwhelmingly likely** that terrorists can carry out similar, if not more malicious attacks. Moreover, even if the world’s terrorists are unable to breed these skills, they can certainly buy them. There are untold numbers of cybermercenaries around the world—sophisticated hackers with advanced training who would be willing to offer their services for the right price. Finally, given the nature of our understanding of cyber threats, there is always the possibility that we have already been the victim or a cyberterrorist attack, or such an attack has already been set but not yet effectuated, and we don’t know it yet. Instead, a well‐designed cyberattack has the capacity **cause widespread chaos**, sow societal unrest, undermine national governments, spread paralyzing fear and anxiety, and create a state of utter turmoil, all without taking a single life. A sophisticated cyberattack could throw a nation’s banking and finance system into chaos **causing markets to crash**, prompting runs on banks, **degrading confidence in markets**, perhaps even putting the nation’s currency in play and making the government look helpless and hapless. In today’s difficult economy, imagine how Americans would react if vast sums of money were taken from their accounts and their supporting financial records were destroyed. A truly nefarious cyberattacker could carry out an attack in such a way (akin to Robin Hood) as to engender populist support and deepen rifts within our society, thereby making efforts to restore the system all the more difficult. A modestly advanced enemy could use a cyberattack to shut down (if not physically damage) one or more regional power grids. An entire region could be cast into total darkness, power‐dependent systems could be shutdown. An attack on one or more regional power grids could also cause **cascading effects that could jeopardize our entire national grid**. When word leaks that the blackout was caused by a cyberattack, the specter of a foreign enemy capable of sending the entire nation into darkness would only **increase the fear, turmoil and unrest**. While the finance and energy sectors are considered prime targets for a cyberattack, an attack on any of the 17 delineated critical infrastructure sectors could have a major impact on the United States. For example, our healthcare system is already technologically driven and the Obama Administration’s e‐health efforts will only increase that dependency. A cyberattack on the U.S. e‐health infrastructure could send our healthcare system into chaos and put countless of lives at risk. Imagine if emergency room physicians and surgeons were suddenly no longer able to access vital patient information. A cyberattack on our nation’s water systems could likewise cause **widespread disruption**. An attack on the control systems for one or more dams could put entire communities at risk of being inundated, and could **create ripple effects across the water, agriculture, and energy sectors**. Similar water control system attacks could be used to at least temporarily **deny water to** otherwise **arid regions**, impacting everything from the quality of life in these areas to agriculture. In 2007, the U.S. Cyber Consequences Unit determined that the destruction from a single wave of cyberattacks on critical infrastructures could exceed $700 billion, which would be the rough equivalent of 50 Katrina‐esque hurricanes hitting the United States all at the same time.29 Similarly, one IT security source has estimated that the impact of a single day cyberwar attack that focused on and disrupted U.S. credit and debit card transactions would be approximately $35 billion.30 Another way to gauge the potential for harm is in comparison to other similar noncyberattack infrastructure failures. For example, the August 2003 regional power grid blackout is estimated to have cost the U.S. economy up to $10 billion, or roughly .1 percent of the nation’s GDP. 31 That said, a cyberattack of the exact same magnitude would most certainly have a much larger impact. The origin of the 2003 blackout was almost immediately disclosed as an atypical system failure having nothing to do with terrorism. This made the event both less threatening and likely a single time occurrence. Had it been disclosed that the event was the result of an attack that could readily be repeated the impacts would likely have grown substantially, if not exponentially. Additionally, a cyberattack could also be used to **disrupt our nation’s defenses or distract our** national **leaders** in advance of a more traditional conventional or strategic attack. Many military leaders actually believe that such a disruptive cyber pre‐offensive is the most effective use of offensive cyber capabilities. This is, in fact, the way Russia utilized cyberattackers—whether government assets, governmentdirected/ coordinated assets, or allied cyber irregulars—in advance of the invasion of Georgia. Widespread distributed denial of service (DDOS) attacks were launched on the Georgian governments IT systems. Roughly a day later Russian armor **rolled into Georgian territory**. The cyberattacks were used to prepare the battlefield; they denied the Georgian government a critical communications tool isolating it from its citizens and degrading its command and control capabilities precisely at the time of attack. In this way, these attacks were the functional equivalent of conventional air and/or missile strikes on a nation’s communications infrastructure.32 One interesting element of the Georgian cyberattacks has been generally overlooked: On July 20th, weeks before the August cyberattack, the website of Georgian President Mikheil Saakashvili was overwhelmed by a more narrowly focused, but technologically similar DDOS attack.33 This should be particularly chilling to American national security experts as our systems undergo the same sorts of focused, probing attacks on a constant basis. The ability of an enemy to use a cyberattack to counter our offensive capabilities or **soften our defenses for a wider offensive** against the United States is **much more than mere speculation**. In fact, in Iraq it is already happening. Iraq insurgents are now using off‐the‐shelf software (costing just $26) to hack U.S. drones (costing $4.5 million each), allowing them to intercept the video feed from these drones.34 By hacking these drones the insurgents have succeeded in greatly reducing **one of our most valuable sources of real‐time intelligence** and situational awareness. If our enemies in Iraq are capable of such an effective cyberattack against one of our more sophisticated systems, consider what a more technologically advanced enemy could do. At the strategic level, in 2008, as the United States Central Command was leading wars in both Iraq and Afghanistan, a cyber intruder compromised the security of the Command and sat within its IT systems, monitoring everything the Command was doing. 35 This time the attacker simply gathered vast amounts of intelligence. However, it is clear that the attacker could have used this access to wage cyberwar—**altering information, disrupting the flow of information, destroying information, taking down systems**—against the United States forces already at war. Similarly, during 2003 as the United States prepared for and began the War in Iraq, the IT networks of the Department of Defense were hacked 294 times.36 By August of 2004, with America at war, these ongoing attacks compelled then‐Deputy Secretary of Defense Paul Wolfowitz to write in a memo that, "Recent exploits have **reduced operational capabilities on our networks**."37 This wasn’t the first time that our national security IT infrastructure was penetrated immediately in advance of a U.S. military option.38 In February of 1998 the Solar Sunrise attacks systematically compromised a series of Department of Defense networks. What is often overlooked is that these attacks occurred during the ramp up period ahead of potential military action against Iraq. The attackers were able to obtain vast amounts of sensitive information—information that would have certainly been of value to an enemy’s military leaders. There is no way to prove that these actions were purposefully launched with the specific intent to distract American military assets or degrade our capabilities. However, such ambiguities—the inability to specifically attribute actions and motives to actors—are the very nature of cyberspace. Perhaps, these repeated patterns of behavior were mere coincidence, or perhaps they weren’t. The potential that an enemy might use a cyberattack to soften physical defenses, increase the gravity of harms from kinetic attacks, or both, significantly increases the potential harms from a cyberattack. Consider the gravity of the threat and risk if an enemy, rightly or wrongly, believed that it could use a cyberattack to degrade our strategic weapons capabilities. Such an enemy might be convinced that **it could win a war**—conventional or **even nuclear**—against the United States. The effect of this would be to **undermine our deterrence**‐based defenses, making us **significantly more at risk of a major war**.

#### Cyberattack causes nuclear reactor failure and is the largest existential threat. Grids are vulnerable now.

**Huff 14** Ethan (staff writer for Natural News) “Nuclear power + grid down event = global extinction for humanity” August 12th 2014 Natural News [http://www.naturalnews.com/046429\_nuclear\_power\_electric\_grid\_global\_extinction.html#](http://www.naturalnews.com/046429_nuclear_power_electric_grid_global_extinction.html) JW

If you think the Fukushima situation is bad, consider the fact that **the U**nited **S**tates **is vulnerable to** the exact same **meltdown** situation, **except at 124 separate nuclear reactors throughout the country. If anything should happen to our nation's poorly protected electric power grid, these reactors have a high likelihood of failure**, say experts, **a** catastrophic **scenario that would most likely lead to the destruction of all life** on our planet, **including humans**. Though they obviously generate power themselves, **nuclear power plants** also **rely on an extensive system of power backups** **that ensure** the constant **flow of cooling water** to reactor cores. In the event of an electromagnetic pulse (EMP), for instance, diesel-powered backup generators are designed to immediately engage, ensuring that fuel rods and reactor cores don't overheat and melt, causing unmitigated destruction. But most **of these generators were only designed to operate for** a maximum period of about **24 hours or less**, meaning **they are** exceptionally **temporary** in nature. **In a real emergency situation, such as** one that might be caused by **a systematic attack on the power grid**, **it could take days or even weeks to bring control systems back online**. At this point, **all those backup generators would have already run out of fuel, leaving nuclear reactors** everywhere **prone to meltdowns**. Cost to retrofit power grid minimal, but government won't do it According to Dave Hodges from The Common Sense Show, it would only cost taxpayers about $2 billion to update the power grid and protect it from attack or shutdown. This is roughly the same price as a single B-1 Stealth Bomber, or the annual sum that the government pays American farmers not to grow crops. In other words, it is a mere drop in the bucket compared to everything else the government spends money on. And yet nothing is being done to protect the power grid against failure or, worse yet, an attack by domestic or foreign enemies. Investment guru Paul Singer warned about this, noting that **an electromagnetic surge is the "most significant danger" facing the world today**. "**Even horrendous nuclear war,** except in its most extreme form, **can [be] a relatively localized issue**," said Singer, "and the threat from asteroids can (possibly) be mitigated."

# Extra Cards

#### Problematically,

**Gilmore San Onofre Organization** High Burnup Fuel Fact Sheet Posted on January 8, 2014 by Donna Gilmore High Burnup Nuclear Fuel Pushing the Safety Envelope by Marvin Resnikoff 1 and Donna Gilmore 2 January 2014 <https://sanonofresafety.org/2014/01/08/high-burnup-fuel-fact-sheet-2/> Donna Gilmore is the founder of San Onofre Safety, an organization that provides factual government and scientific information on the serious safety issues found at the San Onofre Nuclear Generating Station in Southern California. Since the closure of the nuclear reactors, the focus of the organization has turned from operational safety issues to issues of nuclear spent fuel storage at San Onofre and other California and U.S. locations. The San Onofre Safety website (sanonofresafety.org) is used around the world by journalists, engineers, elected officials, regulators and the general public for creditable sourced information on nuclear safety issues. Gilmore was part of local efforts to educate the public on the San Onofre steam generator problems. The reactors are permanently shut down. However, the 1680 metric tons of highly radioactive nuclear waste at the plant are still very active. Recent papers by Gilmore include: High Burnup Nuclear Fuel – Pushing the Safety Envelope (co‐authored with nuclear physicist Dr. Marvin Resnikoff), Diablo Canyon: Conditions for Stress Corrosion Cracking in Two Years, Reasons to Buy Thick Nuclear Waste Dry Storage Casks, and Myths About Nuclear Waste Storage. Gilmore has made presentations on nuclear waste storage issues at national, state and local venues, including the 2014 NRC Annual Spent Fuel Management Regulatory Conference, the 2015 California Democratic Convention (Environmental Caucus), the Malibu Democratic Club, the California Energy Commission, and California Coastal Commission, the Sierra Club and other NGO venues. Gilmore also educates federal, state and local regulators and elected officials and activists on critical nuclear waste storage issues. Gilmore has effectively advocated for improved nuclear waste storage safety evaluations in federal and state regulatory proceedings. She is an intervener in the CPUC $4.3 billon San Onofre Decommissioning proceeding, which may likely determine the future of nuclear waste storage at San Onofre. Gilmore has over 30 years experience in systems analysis and information technology project management including the design and implementation of major technology systems for the State of California and the management of a large engineering data center.

 As commercial reactor economics have declined, utilities, with the acquiescence of the Nuclear Regulatory Commission (NRC), have burned nuclear fuel longer and crammed more of it into storage containers. This experiment **[HBF] has unresolved serious safety issues** for storage, transportation and disposal of this highly radioactive waste; issues **that have been essentially overlooked by nuclear regulators and the general public. For high burnup fuel (HBF), the [container shielding] cladding surrounding nuclear fuel, is thinner, more brittle, with additional cracks. In a transportation accident, the cladding could shatter and a large inventory of radioactivity, particularly cesium, could be released.**  The NRC should stop use of HBF and make solving HBF storage problems one of its highest priorities. High Burnup Fuel Problems Almost all commercial reactors have HBF. Since the 1990’s almost all spent nuclear fuel (SNF) being loaded into dry casks is HBF.[3] HBF is low-enriched uranium that has burned in the reactor for more than 45 GWd/MTU (GigaWatt days per Metric Ton of Uranium).[4] Many Pressurized-Water Reactors have fuel with projected burnup greater than 60 GWd/MTU.[5] Cross Section Fuel Rod Significant Radial Hydride Orientation DE-NE-0000593 Fig. 1. Cladding cracks The only issue NRC staff consider is the highest heat within a storage cask, but this ignores the fact that the cladding of HBF is thinner, more brittle, with additional cracks, as shown in Fig. 1. Longer cooling time will not solve these problems. Uranium fuel pellets, stacked within long thin tubes called cladding, are struck by neutrons and fission, producing heat. A collection of these tubes is called a nuclear fuel assembly, shown in Fig. 2. After 3 to 4 years, extremely radioactive and thermally hot fuel assemblies are removed from the reactor and stored underwater in a fuel pool. Following a cooling period of 7 to 20 years, 24 to 32 fuel assemblies are removed from the fuel pool and inserted into a fuel canister, which are then pushed into a concrete overpack shown in Fig. 3. Because of the poor economics of nuclear power, utilities are pushing the limits for how long fuel remains in reactors with dire consequences. Here are the high burnup fuel issues: **HBF is dangerously unpredictable and unstable in storage – even short-term. HBF is [and] over twice as radioactive and over twice as hot [as other fuels]. The higher the burnup rate and the higher the uranium enrichment, the more radioactive, hotter and unstable fuel and cladding become.** Fig. 4 shows the increase of heat output of fuel assemblies as a function of burnup.