### D---Grid---Meltdowns---1NC

#### Blackouts no longer cause meltdowns, which aren’t existential anyway.

Stockton 16 – Science Reporter at WIRED, M.A. in Journalism from NYU

Nick Stockton, “Nuclear Power Is Too Safe to Save the World From Climate Change,” WIRED, April 3, 2016, https://www.wired.com/2016/04/nuclear-power-safe-save-world-climate-change/.

But you aren't afraid of routine releases. You're terrified of another Three Mile Island, Fukushima, or Chernobyl.

These disasters were the result of a meltdown, which occurs when something impedes a reactor's ability to cool the fuel. The US, where nearly 20 percent of electricity comes from 99 nuclear plants, uses uranium. Older reactors—which is every reactor in the US, including Watts Bar Unit 2—use electric pumps to move water through the system. The Fukushima disaster showed what happens if you have pumps but no power to use them. Newer generations rely on gravity instead, draining cooling water from elevated storage tanks to send it through the reactor core.

Those updates mean serious nuclear accidents are becoming ever more rare. Since Three Mile Island in 1979, the Nuclear Regulatory Commission found that the rate of shut-down-the-reactor-level problems has dropped from 2.5 per plant per year to around 0.1 (One such happened on March 29 in Washington). Even Three Mile Island wasn't the disaster it could have been, because of that plant's layers of redundant protection.

In terms of full blown nuclear disaster, there is really only one data point: Chernobyl. Which was horrifying. But in terms of real risk? The World Health Organization estimates the disaster will claim 4,000 lives, a figure that includes everything from direct victims to people born with genetic mutations well after the meltdown in 1986. By comparison, particulate matter from coal power plants kills about 7,500 people in the US every year. Radiation is the shark attack of environmental danger: An awful way to go, but far less likely than, say, a car wreck.

#### No grid collapse from cyberattacks.

Mueller 22 – Professor of Political Science, Ohio State University, and Senior Fellow, the Cato Institute

John Mueller, Ph.D. & M.A. in Political Science, UCLA, and A.B., UChicago, “The Cyber-Delusion: Digital Threats are Manageable, Not Existential,” *Foreign Affairs*, 22 March 2022, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion

When Russian forces launched their invasion of Ukraine last month, governments and experts worldwide warned about the danger of catastrophic cyberattacks. Indeed, in the days leading up to Moscow’s invasion, hackers defaced Ukrainian websites, unleashed malware on government systems, and targeted the country’s banking system—albeit with limited effect. Although no cyber-Armageddon has materialized, officials increasingly fear that Russia might eventually step up its efforts and even target the United States.

Russia’s invasion is no doubt catastrophic. But in reacting to it and preparing for what comes next, leaders in Washington and elsewhere should eschew the alarmism that has long warped cybersecurity policy. Mike Mullen, then chairman of the Joint Chiefs of Staff, claimed in 2011 that “the single biggest existential threat out there, I think, is cyber.” The following year, his successor, Martin Dempsey, noted that “a cyberattack could stop our society in its tracks.” Former Defense Secretary Leon Panetta sternly warned in 2012 of an impending “digital Pearl Harbor.” Nicole Perlroth, a cybersecurity reporter at The New York Times, has routinely asked insiders when “a cyber-enabled cataclysmic boom will take us down” and has always been told “18 to 24 months.” She began her survey well over 100 months ago.

This contemporary approach to cyberthreats resembles the aftermath of 9/11, when almost all experts believed an even larger terrorist attack would soon take place. Then, as now, the threat is overblown. Although occasionally dramatic, cyberattacks have turned out to be a comparatively minor and manageable threat. Far too much discussion around the issue focuses on worst-case scenarios, fails to contextualize the problem, and neglects to weigh the costs of cyberattacks against the enormous value of the Internet and artificial intelligence. Most commentary, moreover, does not fully appreciate the ability of the business sector—by far the most tempting of targets for malevolent hackers—to develop effective countermeasures.

CYBERWAR

Over the past decade, the global obsession with digital threats has taken various forms, with a particular focus on the potential military implications of emerging cyber-capabilities. To be sure, the military needs to worry about keeping its communications and command and control [C3] operations secure from hostile attackers. Any disruptions, however, are more likely to be instrumental or tactical than strategic.

Despite statements to the contrary, the U.S. military itself seems to have recognized this reality. When Panetta proclaimed in 2013 that cyber was “without question, the battlefield for the future,” political scientist Micah Zenko observed at the time that the Pentagon was spending less than one percent of its budget on cybersecurity, and an assessment from 2019 suggests it may be more like one-tenth of one percent. If those funds prove adequate for the challenge, it would be something of a bargain.

Cyber also supposedly enhances a state’s ability to carry out such ancient endeavors as espionage, propaganda dissemination, and sabotage. Analysts have even coined a new term, “hybrid warfare,” that usually includes these three enterprises—although, since the term does not include direct armed conflict, it might more plausibly be called “denatured warfare.” Cyber’s contribution to these three areas, however, is relatively limited.

Should invading hackers engage in digital espionage against the United States, for instance, they are likely to find that most of what they come across is already well known, and that much of the rest is not worth knowing in the first place. Wikileaks’ 2010 publication of thousands of classified U.S. government documents demonstrated the degree to which governments worldwide have fallen victim to over-classification. When Bill Keller, the editor in charge of poring over the documents at The New York Times, was asked whether the reporting team found anything they didn’t already know, he responded “no” without hesitation.

Much the same holds for concerns over the theft of intellectual property. Not only is this practice centuries old, but systematic stealing has often proved unwise because it distracts governments from homegrown innovation. Cyber-propaganda efforts, in turn, are more likely to increase the overall amount of available information and disinformation—an age-old problem in warfare—than to provide a decisive advantage.

The achievements of cyber-sabotage have also been quite modest. The United States and Israel famously used a computer virus known as Stuxnet to hamper Iran’s progress toward developing a nuclear weapon. Although observers hailed the operation as a dangerous new development in modern conflict, the damage proved temporary. Iran quickly rebuilt its centrifuges, and the attack actually proved counterproductive, as it encouraged Tehran to accelerate its nuclear program. There have also been efforts by the United States to physically interfere with missile development in North Korea. Yet, much like the Iranians, Pyongyang eventually solved whatever the problem was, and the attacks had little long-term effect on their program.

Cyber-alarmists have also warned about hackers disabling major infrastructure such as power grids—potentially crippling entire countries. Grids do go down occasionally, but the culprits are typically squirrels and lightning. Regardless of the source, such disruptions are usually brief and bearable, and engineers are increasingly designing systems that are resilient to such threats. Estonia, for instance, the victim of a major and oft-discussed cyberattack in 2007, is now the home of NATO’s Cooperative Cyber Defence Centre of Excellence.

CYBERTERRORISM

Fears that terrorist groups could inflict damage through cyberspace have been around for many years. And although cyber played no direct role in the execution of the 9/11 terrorist, the event stirred anxiety about the issue. In 2002, for instance, The Washington Post published a lengthy front-page article conveying the views of “government experts” that “terrorists are at the threshold of using the Internet as a direct instrument of bloodshed.”

To date, however, no terrorist group has launched a successful cyberattack. And even if it becomes possible for hackers to shed blood, shootings and bombings are likely to accomplish the same goal far more reliably. Still, cyber has undoubtedly proved to be a relatively convenient method for terrorist groups to recruit and communicate. Rather than creating a paradigm shift, however, this technique has simply replaced or embellished older methods. Even comparatively savvy groups such as the Islamic State (also known as ISIS) tend to comically fail when using the Internet to stir up violence and instruct potential sympathizers. In one case, an ISIS handler connected his eager American charge to a prospective collaborator who happened to be an FBI operative.

For the most part, any virtual terrorist army in the United States has, as terrorism expert Brian Jenkins puts it, remained exactly that: virtual. “Talking about jihad, boasting of what one will do, and offering diabolical schemes egging each other on is usually as far as it goes,” he noted. Indeed, the foolish willingness of would-be terrorists to describe their aspirations and often-childish fantasies on the Internet has often helped police seeking to track them down.

ELECTION MEDDLING

Election interference also features prominently in alarmist discourse on cyberthreats. During the 2016 U.S. presidential election, for instance, the United States highlighted apparent attempts by Russian hackers to undermine Hillary Clinton’s campaign. Although Clinton still handily won the popular vote, many analysts argued that digital interlopers sought to undermine the integrity of U.S. elections and perhaps democracy itself.

These warnings are exaggerated and—coming from U.S. policymakers—arguably hypocritical. It is worth noting that the United States has intervened in foreign elections for decades. Moreover, the idea that elections and voters are easily manipulated is suspect. If extensive promotion could guarantee success, Americans would all be driving Edsels and drinking New Coke—legendary marketing failures in 1958 and 1985 by two of the most successful businesses in history: the Ford Motor Company and Coca-Cola. In any capitalist society, people are regularly deluged by advertising and marketing campaigns. In all cases, those petitioned remain free to ignore the ads, and most become quite good at it. In fact, studies have shown that campaign information rarely changes many votes. As political scientist Diana Mutz points out, the impact of campaign advertising “is marginal at most.”

Political campaigns, as anyone who has suffered through one knows, are also rife with falsehoods: incumbents strategically distort their record, and challengers do the same in reverse. The 2016 Russian contribution to this flood of misinformation was tiny. On Facebook, where most of the manipulation supposedly took place, Moscow’s intervention totaled perhaps a fractio of one percent of the content on the platform’s news feed. Much of this was also wasted because the people who embraced it were already committed to a particular party or lived in states that went solidly for one or the other candidate. Russia’s efforts, moreover, proved wildly counterproductive. Instead of weakening U.S. policy, Moscow generated bipartisan support for anti-Russian sanctions when the two U.S. political parties could agree on little else.

CYBERCRIME

Despite the overheated rhetoric about war, terrorism, election interference, and critical infrastructure, most cyberattacks target the private sector, seeking to steal or extort money from businesses and their customers. The record here, however, is rather encouraging, and it likely has broader relevance. To be sure, cybercriminals have stolen and extorted billions of dollars from businesses and individuals, but firms have done well at limiting the damage by closing software holes, maintaining backups, and safeguarding sensitive material.

A central issue for potential hackers is the profitability of their enterprise. A report by the cybersecurity firm Symantec estimates that 978 million people were affected by cybercrime in 2017, losing $172 billion in total. That number—regardless of how hackers divvy up the profits—is actually remarkably small compared to losses from other forms of illegal activity. Personal and property crimes in 2017, for instance, cost Americans $2.6 trillion.

Businesses are also learning to adapt. Andrew Odlyzko, former head of the University of Minnesota’s Digital Technology Center, points out that many firms have realized they can readily mitigate the most damaging effects of cybercrime through minor and incremental alterations to their business practices. Banks, for instance, increasingly require customers to verify large or suspicious transactions through voice calls or texts. And even though criminals routinely capture millions of credit card numbers through compromised databases, the overall damage is limited and often dominated by the cost of providing replacement cards. Businesses have also made it easy for consumers to recover from fraud.

RESILIENCE AND PEARL HARBOR

Despite Panetta’s 2012 analogy, the value of adaptation and resilience are illustrated, not shattered, by the Japanese attack on Pearl Harbor. From a strictly military standpoint, the assault proved to be more of an inconvenience than a disaster. The U.S. Navy quickly made repairs and the result was a loss of two aged ships. All the planes lost could be replaced by new and better models within three days at eventual 1942 production rates. The loss of life was, of course, tragic, but the flood of outraged men who deluged recruiting stations in the following days almost instantly compensated for the casualties.

The Pearl Harbor experience, then, does not support alarmism. In fact, it shows that if a system is resilient, even successful, dramatic, and dastardly surprise attacks can be managed.

#### Robust studies show countries don’t escalate cyber conflict.

Jensen 19 – Director of the CSIS Futures Lab, Frank E. Petersen Chair at the Marine Corps University School of Advanced Warfighting

Benjamin Jensen, “What a U.S. Operation in Russia Shows About the Limits of Coercion in Cyber Space,” War on the Rocks, 06-20-2019, https://warontherocks.com/2019/06/what-a-u-s-operation-in-russia-shows-about-the-limits-of-coercion-in-cyber-space/

As social scientists start using larger data sets and experiments to analyze cyber operations, they are casting doubt on whether coercion in this new domain works at all. Wargame experiments analyzing cyber attacks against critical infrastructure reveal difficulties coordinating responses between private industry and the national security establishment, as well as a reluctance to escalate when a cyber incident might cause significant economic damage. Other experiments and simulations similarly demonstrate that players, including national security experts, are unlikely to escalate in response to cyber acts alone. Players seem reluctant to risk World War III over hacking. This hesitation likely is due to the covert character of cyber campaigns and the fact that any predicted coercive effects, to include deterrence, are expectations about the future. Because cyber operations occur in the shadows, politicians can hide the fallout in the short term and avoid public pressure to respond.

There are real concerns about whether cyber operations are a sufficiently costly signal or even the right instrument of power to coerce rivals. Previous studies have found cyber operations can compel rivals, but only when used in conjunction with other instruments of power. It is also unclear whether cyber operations achieve demonstrable battlefield effects. A recent study by Nadiya Kostyuk and Yuri Zhukov finds cyber attacks in Syria and Ukraine did not change combatant behavior. These findings echo earlier studies questioning the efficacy and very concept of cyber war.