## AT: Cyber Impacts

### AT: Cyber Impacts

#### Zero risk of *existential* or escalating cyber-attacks.

Mueller '22 - Political Scientist at the Ohio State University [John, 3/22/2022, "The Cyber-Delusion Digital Threats Are Manageable, Not Existential, 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 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.

### AT: Cyber-terror

#### No impact to cyber-terror.

Mueller '22 - Political Scientist at the Ohio State University [John, 3/22/2022, "The Cyber-Delusion Digital Threats Are Manageable, Not Existential, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion]

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.

### AT: Election Meddling

#### No impact to election meddling.

Mueller '22 - Political Scientist at the Ohio State University [John, 3/22/2022, "The Cyber-Delusion Digital Threats Are Manageable, Not Existential, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion]

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 fraction 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.

### AT: Cybercrime

#### No impact to cybercrime.

Mueller '22 - Political Scientist at the Ohio State University [John, 3/22/2022, "The Cyber-Delusion Digital Threats Are Manageable, Not Existential, https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion]

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.

### Ext – @Cybersquirrel1

#### No impact to grid collapse

@CyberSquirrel1 2016 – tracks grid outages and responds to outlandish claims  
"The Threat to America’s Electrical Grid Is Much Bigger Than You Can Possibly Imagine," Jul 31, foreignpolicy.com/2016/07/31/the-threat-to-americas-electrical-grid-is-much-bigger-than-you-can-possibly-imagine-cyberwar-squirrels-rodents-hackers/amp/

We are everywhere, and yet almost impossible to find. There are other events that have impacted critical infrastructure: a water pump failure in Illinois, power outages in Brazil, a pipeline explosion in Turkey, a cyberattack on a dam in New York; even a blast furnace in a German steel plant was supposedly put into an uncontrolled shutdown from a cyberattack. In each case, the initial cause for the failure was blamed on cyberattacks — but in each case, once the evidence was actually examined, hackers were nowhere to be found. Still, that lack of evidence hasn’t stopped the cyberwar hawks from pointing to these analog events as examples of the coming digital doom. When that doesn’t work, the threatmongers and profiteers point to previous widespread blackouts, known as “black swan” events because of their rarity, such as the Northeast blackout of 2003 or the Southwest blackout of 2011. In both cases, a string of unlikely events occurred, including human error, before the lights went out. In both cases, most of the power was restored in just a few hours. There were no riots, no financial meltdowns, and democracy continued unabated. Then there’s what we affectionately call the “nine substation problem.” After a bunch of armed assailants opened fire on a substation outside of Metcalf, California, in 2013, the Federal Energy Regulatory Commission (FERC) conducted a study of the national power grid and found that if just nine substations were attacked in a similar manner as the one in Metcalf, the entire United States would be without power for over 18 months. Are you freaked out yet? Good. But the problem is: This scenario is extremely unlikely. First, that FERC study only looked at physical damage to the transformers, which are usually custom-built for each location, and are only manufactured by a few companies — meaning a substation could take months to replace. Second, the study only looked at physical damage, which in the event of a cyberattack is extremely unlikely. But still, the prophets of doom ask, what if hackers had guns? Didn’t you see Skyfall?! No, we didn’t. We’re squirrels. Look, even for our billion-strong army of small rodents — in the United States alone — the “attack surface” for the U.S. electric grid is absolutely huge. There are over 7,000 power plants in the United States run by over 3,000 companies. There are over 55,000 substations and over 450,000 miles of high-voltage transmission lines. We squirrels have a hard enough time trying to take out small sections of it, let alone nine substations at once. Anyone attempting to conduct a major coordinated effort to turn out power over a large region for a long period of time is going to find it a rather difficult task. Not that we’re not trying. As of July of this year we squirrels (and our fellow animal operatives) have conducted over 1,400 unclassified operations that have resulted in aggregate of more than 67 days without power, affecting over 3.6 million people. That works out to the entire population of the state of Connecticut losing electricity for more than two months. And remember: Our unclassified ops are just a fraction of the total. On average, we cause dozens of outages every day impacting about 5,000 people each for around two hours. Compare that with the number of outages caused by cyberattack, which in the United States is exactly zero. And yet we get no respect. We’ve hit the NASDAQ stock exchange twice, as well as the Large Hadron Collider in Geneva. We’ve hit 64 schools, 30 universities, 13 hospitals, six government buildings, four airports, and even two military bases. And yes, our unclassified operations have caused seven confirmed deaths. Despite that carnage, your policy officials still just worry about massive cyberattacks directed by Beijing and Moscow. (Oh, don’t worry: We’ve got agents there too.) Look, cyberwar in one form or another has been prophesied for over 35 years. But if things got so bad China and Russia were to intentionally cause a widespread, long-term power outage, you’ve got to believe the United States — and the world — would have much greater things to worry about at that point. The ICBMs would already be flying. Minor threat actors such as North Korea, hacktivists, or the Islamic State lack the time, money, and coordination to pull off a black swan event. Not that they lack the skill, mind you. Let’s face it: The cybersecurity of the U.S. electrical grid is absolutely pitiful. It wouldn’t take a team of geniuses to cut off the power to any large city. However, simply causing an electricity outage and keeping the power offline are two different things. In Ukraine, for example, linemen drove out to each substation and switched them back to manual control; power was back on in just a few hours. Yes, there is a risk to the electric grid from a cyberattack, but that threat is nowhere near the levels of fear, uncertainty, and doubt being peddled by policymakers, threat reduction firms, and cyberwar hawks. If you really want to stop the ongoing, constant attacks on the U.S. electrical grid, there’s an easy way: call Orkin. Until then, we are anonymous, we are legion, we are your unfriendly neighborhood squirrels.

## AT: OCOs

### AT: Nadesan 14

#### This card comes out of left field – control F their internal link to this scenario, it literally doesn’t say the word meltdown once in the entire card also the quals on this card are absolute dog water

Van Zandt 20 – D. Van Zandt, 10-31-2020, "The Millennium Report," Media Bias/Fact Check, https://mediabiasfactcheck.com/the-millennium-report/KK

Reasoning: Extreme Right, Propaganda, Conspiracy, Fake News, Lack of Transparency Country: USA World Press Freedom Rank: USA 45/180 History Founded in 2014 and according to their about page “The Millennium Report provides the most important news during these times of meteoric change and pervasive upheaval.” The website does not provide information about who owns the site. The domain is registered in the USA. Funded by / Ownership The Millennium Report does not disclose ownership. There does not appear to be a source of revenue for this website. Analysis / Bias In review, The Millennium Report is an extreme right biased website that promotes pro-Russia and pro-Assad propaganda. Throughout the website, there is significant anti-Clinton rhetoric with the term “Lock Her Up” used frequently. There is significant use of loaded words in headlines and articles such as this: “Here’s the proven Deep State conspiracy that will hang ’em all!” The primary source of information for this website is State of the Nation 2012, which is another extreme-right conspiracy site that occasionally publishes fake news. Mostly the Millennium Report is a tin foil hat conspiracy website with themes running from Pizzagate, the New World Order to the Deep State conspiracy. They have also failed fact checks. Did the U.S. government finally admit to conducting chemical geoengineering using chemtrail operations? – FALSE Was the Virginia Beach mass shooting a “false flag” attached ordered by the “Deep State” to distract attention away from the investigation of “SPYgate”? – FALSE Overall, we rate The Millennium Report Questionable based on extreme right bias and promotion of propaganda and conspiracy theories.

Table

Description automatically generated

### AT: Aldanova 22

#### Aldanova goes neg! Recut gives multiple reasons why cyberattacks are non-UQ, the squo solves, and why Russia will never attack

1AC Aldanova 22 - *Master’s Candidate at Georgetown University’s Eurasian, Russian, and East European Studies Program* (Dina, May 30, 2022, National Interest, “Will Russia Launch a New Cyber Attack on America?,” <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/will-russia-launch-new-cyber-attack>)recut//KH

Policy circles in Washington are now debating how Vladimir Putin might respond to a major contraction of the Russian economy and clear signs that Moscow is losing the war in Ukraine. Some posit that a cornered president, furious and facing a near defeat, might indeed respond brutally—moving the proxy confrontation of a new Cold War front to a cyber battlefield, where Russia has a greater advantage, and launching a massive cyberattack against the United States. However, several key factors call this thesis into question.

Similar to Iran and North Korea, Russia is known to be responsible for some of the most aggressive, large-scale cyberattacks. However, these cyber tactics have played a rather peripheral role, either in supporting conventional warfare or through disinformation campaigns that serve to spread chaos and panic among targeted societies. For the first time, a known state-backed attack occurred in 2007 and lasted for twenty-two days when the Russian military intelligence unit, the GRU, targeted Estonian commercial, government, and Domain Name System (DNS) servers, and online banking systems. The attacks fell under the Denial of Service (DoS) and Distributed Denial of Service (DDoS) categories that include methods such as ping flooding, spam distribution, botnets, and phishing emails. In 2008, as a part of hybrid warfare amid the occupation of Abkhazia and South Ossetia, Russia defaced Georgian state websites. In 2015, following the annexation of Crimea and the occupation of eastern Ukraine, a GRU proxy group named Sandworm attacked the Ukrainian power grid and deprived more than 200,000 people of electricity for six hours. In 2017, the NotPetya malware attack directed at Ukraine had an unprecedented impact hitting major Western companies in Europe and the United States such as Mondelez International and Maersk, and even striking back at Russian oil company Rosneft. It paralyzed thousands of networks. The global cost the malware had provoked reached $10 billion—encapsulating the most consequential cyber attack in history. In addition, just a month ago, Russia unsuccessfully attempted to attack the Ukrainian power grid with advanced malware classified as a wiper. Overseas, a Russian group of hackers called FancyBear meddled with the United States 2015 presidential campaigns and 2016 federal elections at the county level. To this point, while the Russian cyber tactics are common and multifarious, they represent a secondary function in hybrid warfare that Moscow conducts along with disinformation campaigns and conventional military operations.

Nevertheless, cybersecurity experts speculate on a range of consequences in a worst-case cyber scenario: Russia might attempt to attack U.S. critical infrastructure, turn off the lights, target the operation of ATMs and credit card systems, attack Amazon’s cloud, disrupt the transportation and supply of clean water, and target pharmaceuticals companies’ manufacturing facilities, power grids, and colonial pipelines. But will such a threat manifest?

Not only would a cyberattack against the United States contradict the historically peripheral nature of Russian cyber warfare, but Russia’s cyber capacity would be insufficient for the task. For the past several years, the West has largely overestimated Russian military capabilities in conventional warfare. U.S. intelligence agencies predicted the 2022 war in Ukraine would be the most destructive the European continent has seen since the end of World War II, expecting the fall of Kyiv to come within days. However, the still ongoing, drawn-out war has revealed weaknesses in the Russian armed forces, its military arsenal, and strategic leadership. Russian officials, for their part, underestimated the strength of the Ukrainian resistance and the united position of the international community. Spending slightly more than 4 percent of the country’s GDP on the military, the Russian president mobilizes domestic support for the military budget by articulating the external threat of NATO. In a relatively undigitized society like Russia, lobbying to spend more on the cyber budget would prove less effective. Taking this into account, it seems possible the West could be overestimating Russian cyber competence as well.

Furthermore, Russia is unlikely to wage a cyberattack on the United States due to fear of retaliation on multiple fronts. Russian society is already experiencing the consequences that the war has wrought: an economic crisis and the psychological pressure of being cast as a global pariah. In case of a Russian cyberattack, the consequences of U.S. cyber retaliation would hit the public first. Given current conditions, depriving people of water and electricity could trigger public discontent on an unprecedented scale. Decades of increasingly authoritarian leadership have undoubtedly engendered public grievances hidden deep within society. At some point, this simmering disgruntlement can boil over into outrage. Putin can ill afford to front further domestic unrest now.

Current U.S. cyber capabilities could also contribute to the fear of retaliation. For the past few years, the United States has developed an impressive cyberinfrastructure, restructured its system of governance, and invested in cyber training and education. As Richard Clarke and Robert Knake emphasize in their book, The Fifth Domain, following the Cold War strategy of deterrence and containment, the United States has largely restrained itself from involvement in cyber counter activities. Although for a long time America has focused on defensive cyber policy, today, the U.S. Cyber Command prioritizes offensive measures. As such, in 2019, the United States successfully targeted the Iranian intelligence service and missile launch system as a response to an Iranian strike against an American drone and U.S. oil tankers. Earlier in 2012, the Stuxnet computer worm, designed in cooperation with Israel, successfully infiltrated nuclear facilities in Iran.

In addition to an offensive preference, **a more consolidated system of governance and a set of regulations have advanced U.S. cybersecurity**. A **clear allocation of roles and responsibilities** between the Department of Homeland Security and U.S. Cyber Command and the relevant leadership improved the system of reporting incidents and information sharing. It facilitated communication within federal agencies and between the government, the private sector, and the public. U.S. private enterprises now spend billions of dollars on cybersecurity, employee training, and encrypted channels. The United States also takes a leading role in collaborating with strategic allies on sharing best practices, detecting flaws in networks, and promoting cyber hygiene.

**[their card begins here]**

### AT: Russia Attacks

#### **Russia won’t attack the US – they’re cyber capabilities are outdated and aren’t a cause for escalation**

Wolff 22 JOSEPHINE WOLFF (Wolff is associate professor of cybersecurity policy at The Fletcher School at Tufts University), 3-2-2022, "Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine," Time, https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/

But as the invasion continues with few signs of any sophisticated cyber conflict, it seems less and less likely that Russia has significant cyber capabilities in reserve, ready to deploy if needed. Instead, it begins to **look like Russia’s much vaunted cyber capabilities have been neglected in recent years,** in favor of developing less expensive, less effective cyber weapons that cause less widespread damage and are considerably easier to contain and defend against. For instance, many of the cyberattacks directed at Ukraine in the past month have been relatively basic distributed denial-of-service attacks, in which hackers bombard Ukrainian government websites and servers with so much online traffic that those servers cannot respond to legitimate users and are forced offline for some period of time. Denial-of-service attacks can be effective for short-term disruptions but they’re **hardly a new or impressive cyber capability**—in fact, they’re what Russia used to target Estonia more than a decade ago in 2007. Moreover, launching these types of attacks requires no sophisticated technical capabilities or discovery of new vulnerabilities, and they typically have fairly contained impacts on the specific, targeted computers. Similarly, recent reports that Belarusian hackers are trying to phish European officials using compromised accounts belonging to Ukrainian armed services members suggests that not only are these efforts relying on fairly basic tactics like phishing emails, they are not even being carried out by Russian military hackers directly.

### AT: National Interest

#### The National Interest is a Nixon-created think tank and the card is cut from a BLOG!

Media Bias Check ND (Media Bias, No date, "National Interest," Media Bias/Fact Check, https://mediabiasfactcheck.com/national-interest/)//KH

History

Founded in 1985 by conservative thinker Irving Kristol, The National Interest (TNI) is an American bi-monthly international affairs magazine published by the Center for the National Interest, which we have rated as right-center biased. It is associated with the realist school of foreign policy thought, which contradicts the liberal thought of cooperation. The current executive editor is Harry Kazianis. In general, this is a foreign policy magazine that also touches on politics and other current events of our time. You can view their Masthead here.

Funded by / Ownership

The National Interest is owned by the Center for the National Interest, a right-leaning think tank **created by President Richard Nixon** in 1994. Advertising and subscription fees fund the magazine.

### AT: EMPs

#### EMP’s unlikely – too widescale and require untenable power

Gault 19 – *The National Interest is an extremely un-biased and factual news source funded by an established think tank* (Matthew Gault, 11-10-2019, "The World Won't End: The Danger of an EMP Attack Is More Fantasy Than Fact," National Interest, https://nationalinterest.org/blog/buzz/world-wont-end-danger-emp-attack-more-fantasy-fact-94681)//KH

Key point: A nuclear war is scarier and besides it isn't so easy to generate a really large EMP burst.

Few weapons are as scary as those that exist only in our minds.

A few years ago when the Republican Party released its platform to the public in the run-up to its national convention at the tail end of a section titled “America Resurgent,” GOP leaders detailed what they felt is a looming threat of America — electromagnetic pulses.

“A single nuclear weapon detonated at high altitude over this country would collapse our electrical grid and other critical infrastructures and endanger the lives of millions,” the platform stated. “With North Korea in possession of nuclear missiles and Iran close to having them, an EMP is no longer a theoretical concern — it is a real threat.”

**But it’s not.**

The problem with fear over electromagnetic weapons is that it forgets two simple facts. First, generating enough juice to cause a significant amount of damage is really hard. Second, a country dealing with busted electronics after an EMP assault is a country fighting a nuclear war.

“EMP is the new test case of seriousness in national security,” cyber security expert Peter W. Singer tweeted after reading the platform. “But not in the way advocates not in on the joke think.”

I reached out to Singer and, after a brief pause to make sure I was serious, he pounced. “There’s this irony of the people who think it’s serious not realizing that they’re the joke,” he explained. “When you walk through the actual scenarios of use, it doesn’t pass the logic test.”

An electromagnetic pulse following a nuclear blast is a real thing. The problem is that the process of creating an EMP big enough without the devastation of a nuclear warhead is expensive, absurd and not worth the effort. That’s if it even works.

For that, we can’t recommend enough a 2010 series of articles in The Space Review by Yousaf M. Butt, a physicist currently serving as a foreign affairs officer in the State Department’s Space and Advanced Technology office.

“For a large device (greater than 100 kilotons) …. the whole region on the Earth’s surface which is within line-of-sight to the high-altitude explosion will experience the EMP pulse,” he wrote.

Which sounds scary, but there are several important caveats. The higher you detonate a nuclear device, the greater the blast radius. However, the effect of the EMP will be less. Likewise, the smaller the explosive yield, the smaller the EMP and the closer the blast will need to be to the ground to be effective.

Finding that detonation sweet-spot in the Earth’s atmosphere will take countless tests … which no one has done.

The blast Butt described above, one that knocks out the entire electrical system on roughly half the Earth’s surface, could only come from a high-yield thermonuclear warhead attached to an ICBM. So, engaging in the fantasist view, a nuke from Russia or China.

Setting aside the geopolitical gymnastics that must occur to lead to that kind of exchange, if a foreign power detonated a 100 or more kiloton in an electromagnetic attack on America, then the world is at war and there’s little strategic benefit for the aggressor to not just go ahead and nuke a city.

“It doesn’t mean it can’t happen,” Singer told me. “But if the other side is using EMPs we’re moving into thermonuclear war.”

“A weapon of mass destruction is preferable to a weapon of mass disruption,” Butt explained. “A state would be highly unlikely to launch an EMP strike from their own territory because the rocket could be traced to the country of origin and would probably result in nuclear or massive conventional retaliation by the U.S.”

Let’s say the EMP does go off in space above North America. According to the worst case scenario, the attack would fry the Pentagon’s electronics, leaving the U.S. military unable to retaliate.

However, we don’t know what the effects of an EMP might be. Studies conducted by both the Soviet Union and the United States during the Cold War produced dramatically different results every time.

An electromagnetic pulse is a highly unpredictable side effect of a predictably horrifying weapon. “It’s not a weapon we’ve seen past use of. Ever. Literally ever. Nor tests of,” Singer said.

Some countries have attempted to weaponize EMPs in fits and starts, but it remains a byproduct of other weapons systems, including cruise missiles as well as nukes. The idea of North Korea or Iran using a small-yield nuclear device in low atmosphere fails for the same reasons. North Korea can barely manage to cobble together a crude one-kiloton bomb, let alone a device large enough to do significant damage to U.S. infrastructure.

“Serious long-lasting consequences of a one-kiloton EMP strike would likely be limited to a state-sized region of the country,” Butt explained.

“Although grid outages in this region may have cascading knock-on effects in more distant parts of the country, the electronic devices in those further regions would not have suffered direct damage, and the associated power systems far from the EMP exposed region could be re-started.”

## AT: Undersea Cables

### 1NC/2AC

#### Redundancy solves

Hinck 2018 - PhD Student @ Columbia Garrett, "Evaluating the Russian Threat to Undersea Cables," Mar 15, https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables

Hundreds of cables criss-cross the oceans. They provide the connectivity that allows Microsoft to keep major data centers in Ireland and to have that data nearly instantly accessible to U.S. customers. Although each undersea cable transmits huge quantities of data, the cable network has significant redundancy capacity. Rupturing one cable can cause temporary disruptions but does not cut off service. When a major cable to Vietnam failed last year, customers in Ho Chi Minh City briefly lost connectivity. Because internet routing protocols direct data around points of failure, traffic flows adjust to the lost connection and send data over other cables to the same endpoint. Wayward anchors and storms regularly cause cable faults, about 200 a year; repair ships are readily available to mend broken lines. Cutting the United States off from the rest of the world would require severing a large number of cables: at least 18 in the North Atlantic alone, according to Telegeography’s cable map, and many more connecting the U.S. to Latin America and Asia.

#### Russia won’t snip cables – and they can be repaired quickly

Matsakis 2018 - Louise, "What Would Really Happen If Russia Attacked Undersea Internet Cables," Jan 5, https://www.wired.com/story/russia-undersea-internet-cables/

Because faults happen so frequently, cable repair ships patrol nearly all of the world’s waters. Even if Russia did start snipping, there are crews equipped to rapidly repair them. Besides, Russia’s epic hypothetical cable attack would primarily harm its own people, as another Telegeography analyst pointed out in a video. “It would hurt the Russians perhaps even more than it would hurt [Americans]. They’re far more dependent on international networks than we are, because so much of our content is stored locally” says senior analyst Jonathan Hjembo.

#### Their impact is too old to assume Starlink – it removes the need for cables

Isberto 2020 - Michael, "Why Internet Satellites Will Replace Subsea Cable Technology," Mar 4, https://www.colocationamerica.com/blog/internet-satellites-will-rebuild-the-internet

There are some obvious disadvantages to this old system of submarine cables. The underwater cable installation is very slow, tedious, and expensive. Underwater creatures including sharks have been seen chewing on the cables. Underwater cables have vulnerabilities including boat anchors, natural disasters, etc. Underwater cables are also not easy to repair if repairs are needed. Some of these cables are 6,500 feet underwater making it difficult to reach. Lastly, underwater cables have a life expectancy of 25 years, and then they will need to be replaced. All of these disadvantages are pushing companies like SpaceX to rebuild the internet.

Rebuilding the Internet in Space

Underwater cables seem like outdated technology. Many people think that we transfer data through satellites, but this isn’t the norm, at least not yet. Last year, Elon Musk revealed his plan to surround the world with low Earth orbit satellites. The project, Starlink, will bring satellite broadband internet service to the world.

The United States Federal Communications Commission (FCC) has already authorized SpaceX to fly 12,000 satellites, and eventually as many as 30,000. There are about 2,000 satellites currently in orbit. It seems as though the FCC is on board with this new idea of rebuilding the internet in space.

Starlink’s first 60 satellites were launched on May 23, 2019, by SpaceX’s Falcon 9 rocket. The way these satellites work is by beaming information through the vacuum of space instead of sending the internet signals through electric cables. Information traveling through satellites is transmitted 47% faster than the standard fiber optic cables.

Current satellite internet works using a large spacecraft that orbits 22,236 miles above the earth. Because it’s orbiting a lot higher and is only above a specific spot on earth, there are substantial time delays from sending and receiving data. Starlink’s network would cover the entirety of Earth and would be orbiting a lot lower making it faster and more reliable connection.

SpaceX has launched the second batch of satellites in November 2019, and more recently the third batch this past January 2020. They expect to begin broadband service by the end of 2020.

Multiple companies are looking into creating low Earth Orbit (LEO) satellite services besides SpaceX. These competitors include OneWeb, Telesat, and LeoSat. All are hoping to deliver services better than existing fiber-optic connections. Although SpaceX is ahead of the competition, OneWeb expects to have enough satellites in space for testing sometime in 2020 with hopes to have global coverage by 2021.

Data Centers in Space Could be Reality

A network of data centers orbiting the earth sounds like a farfetched idea—or is it? Data centers powered by the sun and cooled by the -454.75-degree Fahrenheit temperature of outer space might be the perfect scenario for data center operations. Last year, SpaceX launched a Tesla Roadster into space to show the possibilities. But for this to be a feasible idea, they will need to find a way to make it more affordable.

Based on SpaceX’s pricing of $90 million per 8000kgs, it would cost $330 million to put a 30,000kg, 96kW, 12-rack container data center (with IT) into orbit. If they could somehow make this idea more affordable, the possibilities could be endless.

Several startup companies are looking into creating a business model for why the next frontier for data centers should be in space. Some of these companies include ConnectX and Laser Light Communications.

Once one of these companies figures out a way to lower the cost of these projects of sending a data center into space, many companies would most likely be on board. Many companies including Apple, Amazon, Target, Walmart, and Google are already looking to renewable energy data center options, and one that is powered by the sun and cooled by the temperatures of outer space is as renewable as it can get.

Conclusion

Technology is changing the world and making it smaller and more connected. Rebuilding the internet in space is already happening and will most likely be in use by the end of 2020. Having data centers located in space could be the next achievement for the industry. Not only will it improve on old technology that started in the 1800s, but it could also perhaps be the solution to renewable energy that the data center industry is looking for. With all of the data the world is producing and sharing currently, this is a much-needed upgrade.

### 1AR – L/T

#### Focusing NATO’s output on force plans and strategy best improves interoperability and cohesion---otherwise, spending is meaningless.

Cappello 8-13-18, a former B-1B pilot, served as the Air Force Attaché to the U.S. Embassies in Belgrade and Tel Aviv, and is currently a senior fellow at the Foundation for Defense of Democracies, (John, August 13th, 2018, “NATO’s Two Percent and Burden Sharing”, https://www.realcleardefense.com/articles/2018/08/13/natos\_two\_percent\_and\_burden\_sharing\_113713.html?utm\_campaign=755f44acff-EMAIL\_CAMPAIGN\_2018\_08\_12\_12\_56&utm\_medium=email&utm\_source=RC%20Defense%20Morning%20Recon&utm\_term=0\_694f73a8dc-755f44acff-81835773)

NATO Secretary General Jens Stoltenberg, however, noted how all allies have halted cuts to their defense budgets and have begun implementing plans to [increase](https://warontherocks.com/2017/05/clearing-the-air-on-transatlantic-burden-sharing-part-1-whats-going-on-here/) their defense budgets to two percent of their respective GDPs, with a majority planning to reach that goal by [2024](https://www.rferl.org/a/fifteen-of-29-nato-members-meet-defense-spending-goal-2-percent-gdp-by-2024-stoltenberg-says-mattis-pressure-brussels-meeting/29038749.html). While Stoltenberg credited President Trump with delivering a “clear message” on burden sharing, this debate misses an important point. Simply spending more does not equate with actual burden sharing.

According to NATO’s [Strategic Concept](https://www.nato.int/cps/en/natohq/topics_49137.htm), collective defense, crisis management, and collective security are the alliance’s core tasks. These missions require capable, mobile, and interoperable forces. Real burden sharing would require every ally to contribute forces ready to deploy for such missions.

[Defense expenditure](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170629_170629-pr2017-111-en.pdf) alone fails to measure real military capability, let alone its use on the alliance’s behalf. Take the cases of [Denmark](https://www.defenseone.com/ideas/2017/10/benchmark-blinding-us-nato-members-contributions/141736/) and Greece. In [2017](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_06/20170629_170629-pr2017-111-en.pdf), Greece spent 2.32 percent of its GDP on defense, while Denmark spent only 1.17 percent. Using the 2 percent goal as a benchmark, one would, therefore, conclude that Greece is a model NATO partner while Denmark is a free rider “taking advantage of the United States.” These numbers, however, do not accurately illustrate how these two nations actually share the burden.

From [Mali](https://www.defenseone.com/ideas/2017/10/benchmark-blinding-us-nato-members-contributions/141736/) to [Libya](http://carnegieeurope.eu/strategiceurope/59767) and Afghanistan to Iraq, the Danish military is actively deployed in support of NATO’s out-of-area missions. Although it spends more than 2 percent of its GDP on defense, Greece contributed none of its 21,500 [deployable troops](https://eda.europa.eu/docs/default-source/documents/eda-national-defence-data-2013-2014-(2015-est)5397973fa4d264cfa776ff000087ef0f.pdf) to NATO missions ([according to 2014 European Defense Agency data](https://eda.europa.eu/docs/default-source/documents/eda-national-defence-data-2013-2014-(2015-est)5397973fa4d264cfa776ff000087ef0f.pdf)).

The Danish and Greek militaries are not outliers—additional [data](https://www.defenseone.com/ideas/2017/10/benchmark-blinding-us-nato-members-contributions/141736/) shows similar discrepancies among other nations as well. The point is, NATO’s needs are not met by spending 2 percent of GDP alone. Members’ contributions to NATO missions of capable, ready, and deployable forces are what actually matter.

This was made clear once again, when three Czech soldiers serving with NATO's Resolute Support mission were killed in Afghanistan by a suicide bomber. The Czech Republic had recently approved a [plan](https://www.npr.org/2018/08/05/635741406/3-czech-nato-service-members-killed-in-afghanistan) to deploy 390 soldiers in Afghanistan through 2020, up from the current 230. While the Czech Republic has not yet met the two percent of GDP spending goal, it does participate in NATO missions fighting, dying and [sharing](http://carnegieeurope.eu/strategiceurope/59767) the risk alongside their deployed counterparts.

While allies should meet their two percent of GDP commitment, they should also spend that money more wisely, focusing on concrete investments to eliminate capability shortfalls. For example, meeting the related pledge to spend 20 percent of defense budgets on equipment (as opposed to salaries or operations) will facilitate the development of cutting-edge weapon systems that are capable, deployable and interoperable.

#### Arctic presence is counter-productive for NATO

Auerswald 2020 - professor of security studies at the U.S. National War College  
"NATO IN THE ARCTIC: KEEP ITS ROLE LIMITED, FOR NOW," Oct 12, https://warontherocks.com/2020/10/nato-in-the-arctic-keep-its-role-limited-for-now/

While NATO members are facing several challenges to their interests in the Arctic, developing a common policy within the alliance on what to do about this is incredibly difficult. NATO decisions depend on consensus, or at least on members withholding a veto of a pending initiative. Just because there are five NATO members in the Arctic does not mean that each supports a greater NATO role in the Arctic. Canada’s Arctic and Northern Policy Framework, for instance, repeatedly emphasizes “Canada’s enduring Arctic sovereignty,” and the need to “enhance Canada’s military presence” and “Canada’s domain awareness” (emphasis added), with some references to bilateral security cooperation but no mention of NATO. Canada is not the only country that might object to a stronger alliance role in the Arctic. Alliance members in Southern and Eastern Europe might see an increased Arctic focus as syphoning away NATO resources from security challenges in the eastern Mediterranean, the Balkans, Ukraine, or the Baltic Sea. In short, a greater alliance role in the Arctic requires convincing skeptical allies, and doing that might not be worth the diplomatic effort.

### 1AR – AT: Interoperability

#### Their Article 5 cards are about Active Endeavor – that’s in the Mediterranean – no reason the plan disrupts that.

NATO 2016 - https://www.nato.int/cps/en/natolive/topics\_7932.htm

Under Operation Active Endeavour, NATO ships patrolled the Mediterranean and monitored shipping to help deter, defend, disrupt and protect against terrorist activity. The operation evolved out of NATO’s immediate response to the terrorist attacks against the United States of 11 September 2001.

### 1AR – Redundancy

#### Steps are in place now

Roblin 18, [Sébastien Roblin holds a master’s degree in conflict resolution from Georgetown University and served as a university instructor for the Peace Corps in China, Russian Spy Submarines Are Tampering with Undersea Cables That Make the Internet Work. Should We Be Worried?, https://nationalinterest.org/blog/buzz/russian-spy-submarines-are-tampering-undersea-cables-make-internet-work-should-we-be]

The U.S. has begun responding to the threat, with 2018 defense budget authorizing construction of a second cable-laying/repair ship costing $250 million to supplement the only one currently in U.S. military service, the USS Zeus. Sanctions imposed on Russia in June 2018 have targeted a Russian mini-submarine builder associated with cable-tampering operations. A newly formed joint-U.S./Europe Atlantic Command will also strengthen NATO’s ability to monitor submarine activities. A logical additional step would be to strengthen international law around cables to make the act of cutting them more transgressive in a non-wartime context.

They start cutting Roblin

Generally speaking, fear of a massive cable attack is probably over-hyped at least for a country with as may redundant cables as the United States pitted against a limited number of Russian special operations submarines. Furthermore, spying and attacks on cables have abundant historical precedents.

Nonetheless, the extensive Russian military activity around the submarine cables surely reveals that they are perceived as a valuable avenue for asymmetric attack and intelligence gathering, and a capacity to launch a more targeted attack against selected cables could cause significant disruptions.

### 1AR – AT: Halappanavar

#### Their card is about China – says they fill-in

Halappanavar 20, [Author is Engineering Graduate and a Software professional based in Bangalore, he is a contributor to Diplomatist, Submarine Cable Network: The Global Sovereign Asset, July 3, https://diplomatist.com/2020/07/03/submarine-cable-network-the-global-sovereign-asset/]

The uncertainty around the intentions and track records of countries like Russia and China give rise to policing of strategic interests in the marina. Asia Direct Cable (ADC) Consortium, on 11th June 2020, announced that it is connecting the Philippines, China (Hong Kong and Guangdong Province), Japan, Singapore, Thailand, and Vietnam via a 9,400-kilometer submarine cable through the South China sea. This would act as an enabler for the Chinese to patrol and justify their territorial claims in the disputed regions on grounds of protecting its vital interests at the same time misuse of this network by China would be a concern in the already troubled waters.

Their card strats

The submarine cables will play a great role as leverage to start or end conflicts. With the fifth-generation warfare gaining more attention from the world the road to supremacy in cyberspace will go through these cables. Whichever country secures its cable interests will come out as a major power, as continuity and normalcy of the world rely upon these underwater networks. The potential in these cable networks to cripple any given country’s operational capability will naturally gain more traction from its adversary. These assets naturally become strategic in nature for all major powers thereby giving the cables a tag of sovereignty.

### 1AR – Starlink

#### Starlink solves the entire DA

Southard 2019 - Megan, "Elon Musk is Revolutionizing Internet with his Starlink Service," May 24, https://nocable.org/news/elon-must-revolutionizing-internet-with-his-starlink-service/

Light moves through space 47% faster than fiber-optic glass

Even if fiber-optic cables were pervasive, light moves through them more slowly than it does in the vacuum of space, so the new service would be an improvement. The bulky and costly infrastructure limits existing internet transmissions. It’s simply too expensive, or unrealistic to connect every place on earth with fiber-optic cables that transmit data quickly.

Starlink’s mesh ring of 12,000 low Earth orbit satellites will establish high-speed internet for the first time in remote locations. If the project goes as planned, Starlink satellites will deliver cheap, fast internet to rural areas, airplanes, ships, and even cars.

No other internet-providing satellites can transmit that much data that far at those speeds. Existing satellite internet service is reliable but slow. Current satellites orbit at 22,236 miles above Earth, causing transmissions to lag behind a half-second. It doesn’t sound like much time, but the time delay makes long-distance video conferencing disjointed and annoying.

Starlink’s satellites will rotate with Earth, making data transmission from New York to London 15% faster than fiber-optic. Not only international teleconferencing would benefit – online gaming would be lag-free, too. The financial industry seeks gains from a marginally faster transmission time. Markets move billions of dollars, and any delay can lead to losses.

### AT: Starlink isn’t running

#### Starlink is available now

TomsGuide 3/7 - https://www.tomsguide.com/reviews/starlink

In our initial Starkink review, we found it simple to set up and faster not only than DSL lines but also quicker than what many basic cable packages are actually able to deliver. Certainly as the only option for sparsely populated areas, Starlink could prove to be a godsend, albeit an expensive one. The basic hardware package is $499, plus $99 a month for service.(Shipping and taxes put the initial total at $581.94).

### 1AR – AT: Military

#### New suitcase internet set up solves

McCaney June 5, 2014 (Kevin; Army boosts bandwidth with new suitcase-sized satellite terminals; defensesystems.com/articles/2014/06/05/army-t2c2-high-bandwidth-satellite-terminals.aspx; kdf)

Portable network access for soldiers in the field is about to get a lot faster with the Army’s latest satellite kit in a suitcase. The Transportable Tactical Command Communications, or T2C2, boosts the bandwidth for small detachments and teams connecting to the Army’s battlefield network, thus increasing the situational awareness and functionality of early-entry teams and helping to improve communications throughout the tactical edge, the Army said in a release. T2T2 comes in two flavors: a larger transportable dish that serves company-level operations and the smaller T2C2 Lite, which the Army said is about the size of carry-on luggage and which can be set up and working in about 10 minutes. The small model is similar to the Global Rapid Response Information Package, or GRRIP, which soldiers have been using in Afghanistan, for example, as network infrastructure leaves with the drawdown. But GRIPP uses only the L Band in the satellite communications spectrum, limiting transmission to kilobits per second. T2C2 Lite adds the Ka and X bands, boosting performance to megabits per second and allowing soldiers to use advanced applications. Last month, T2C2 was designated a program of record (GRRIP is not), enabling the Army to institutionalize training on the system. The equipment connects to the Army’s battlefield network, the Warfighter Information Network-Tactical, via the military’s Wideband Global SATCOM constellation, and will work as a companion to the Enroute Mission Command Capability, a WIN-T program that gives rapid-response forces a view of their drop zones and allows for mission planning while in flight. For the Army, the bigger bandwidth, combined with T2C2’s portability, advances the cause of seamless, mobile battlefield communications.

### 1AR – No Internet Crash

#### No Internet collapse

**Dvorak 2007** (John; Will the Internet Collapse?; May 1; www.pcmag.com/article2/0%2c2817%2c2124376%2c00.asp; kdf)

When is the Internet going to collapse? The answer is NEVER. The Internet is amazing for no other reason than that it hasn't simply collapsed, never to be rebooted. Over a decade ago, many pundits were predicting an all-out catastrophic failure, and back then the load was nothing compared with what it is today. So how much more can this network take? Let's look at the basic changes that have occurred since the Net became chat-worthy around 1990. First of all, only a few people were on the Net back in 1990, since it was essentially a carrier for e-mail (spam free!), newsgroups, gopher, and FTP. These capabilities remain. But the e-mail load has grown to phenomenal proportions and become burdened with megatons of spam. In one year, the amount of spam can exceed a decade's worth, say 1990 to 2000, of all Internet traffic. It's actually the astonishing overall growth of the Internet that is amazing. In 1990, the total U.S. backbone throughput of the Internet was 1 terabyte, and in 1991 it doubled to 2TB. Throughput continued to double until 1996, when it jumped to 1,500TB. After that huge jump, it returned to doubling, reaching 80,000 to 140,000TB in 2002. This ridiculous growth rate has continued as more and more services are added to the burden. The jump in 1996 is attributable to the one-two punch of the universal popularization of the Web and the introduction of the MP3 standard and subsequent music file sharing. More recently, the emergence of inane video clips (YouTube and the rest) as universal entertainment has continued to slam the Net with overhead, as has large video file sharing via BitTorrent and other systems. Then VoIP came along, and IPTV is next. All the while, e-mail numbers are in the trillions of messages, and spam has never been more plentiful and bloated. Add blogging, vlogging, and twittering and it just gets worse. According to some expensive studies, the growth rate has begun to slow down to something like 50 percent per year. But that's growth on top of huge numbers. Petabytes. To date, we have to admit that the structure of the Net is robust, to say the least. This is impressive, considering the fact that experts were predicting a collapse in the 1990s. Robust or not, this Internet is a transportation system. It transports data. All transportation systems eventually need upgrading, repair, basic changes, or reinvention. But what needs to be done here? This, to me, has come to be the big question. Does anything at all need to be done, or do we run it into the ground and then fix it later? Is this like a jalopy leaking oil and water about to blow, or an organic perpetual-motion machine that fixes itself somehow? Many believe that the Net has never collapsed because it does tend to fix itself. A decade ago we were going to run out of IP addresses—remember? It righted itself, with rotating addresses and subnets. Many of the Net's improvements are self-improvements. Only spam, viruses, and spyware represent incurable diseases that could kill the organism. I have to conclude that the worst-case scenario for the Net is an outage here or there, if anywhere. After all, the phone system, a more machine-intensive system, never really imploded after years and years of growth, did it? While it has outages, it's actually more reliable than the power grid it sits on. Why should the Internet be any different now that it is essentially run by phone companies who know how to keep networks up? And let's be real here. The Net is being improved daily, with newer routers and better gear being constantly hot-swapped all over the world. This is not the same Internet we had in 1990, nor is it what we had in 2000. While phone companies seem to enjoy nickel-and-diming their customers to death with various petty scams and charges, they could easily charge one flat fee and spend their efforts on quality-of-service issues and improving overall network speed and throughput. That will never happen, and phone companies will forever be loathed. But when all is said and done, it's because of them that the Internet will never collapse. That's the good news. The bad news is they now own the Internet—literally—and they'll continue to play the nickel-and-dime game with us.

### 1AR – Eagleman

#### Eagleman’s a hack and internet won’t save civilization

Mnookin 12

Seth Mnookin teaches science writing at MIT and blogs at the Public Library of Science, Download the Universe, March 23, 2012, "The Frozen Future of Nonfiction", http://www.downloadtheuniverse.com/dtu/2012/03/why-the-net-matters-how-the-internet-will-save-civilization-by-david-eagleman-canongate-books-2010-for-ipad-by-set.html

At least, that’s what I assumed before I read Why The Net Matters, Eagleman’s frustrating 2010 e-book about how and why the Internet will save civilization. (I reviewed the $7.99 iPad version, which is the platform it was designed for; a stripped-down, text-based version is available on the Kindle for the portentous price of $6.66.) The problems start with Eagleman’s premise, which is so vague and broad as to be practically meaningless. There are, he writes, just “a handful of reasons” that civilizations collapse: “disease, poor information flow, natural disasters, political corruption, resource depletion and economic meltdown.” Lucky for us (and Eagleman does offer readers “[c]ongratulations on living in a fortuitous moment in history”), the technology that created the web “obviates many of the threats faced by our ancestors. In other words...[t]he advent of the internet represents a watershed moment in history that just might rescue our future.”

On the other hand, it just might not: In order to make his point, Eagleman either ignores or doesn’t bother to look for any evidence that might undercut it. The first of six “random access” chapters that make up the bulk of Why The Net Matters is devoted to “Sidestepping Epidemics,” like the smallpox outbreak that helped bring down the Aztec Empire. In the future, Eagleman writes, the “protective net,” in the form of telemedicine, telepresence (“the ability to work remotely via computer”), and sophisticated information tracking, will save us from these outbreaks. That all sounds lovely, but what of the fact that we’re currently experiencing a resurgence in vaccine-preventable diseases such as measles...a resurgence which is fueled in no small part by misinformation spread over that very same “protective net”?

A few chapters later, in a section celebrating the benefits of the hive mind, Eagleman invokes Soviet pseudoscientist Trofim Lysenko, a famed quack who took over the U.S.S.R.’s wheat production under Stalin. Because the Soviet Union spanned 13 time zones, Eagleman writes, “central rule-setting was disastrous for wheat production. … Part of the downfall of the USSR can be traced to this centralization of agricultural decisions.” That sounds nice, and might even be true—but it’s not a point that’s supported by Lysenko, whose main shortcoming was not that he believed in a one-size-fits-all approach; it was that he was a fraud.

Moving to the present day, Eagleman addresses wildfires that swept through Southern California in 2007, which, he writes, “brought into relief the relationship between natural disasters and the internet.”

At the beginning of the outbreak in October, Californians were glued to their television screens, hoping to determine if their own homes were in danger. But at some point they stopped watching the televisions and turned to other sources. A common suspicion arose that the news stations were most concerned with the fate of celebrity homes in Malibu and Hollywood; mansions that were consumed by the flames took up airtime in proportion to their square footage, which made for gripping video but a poor information source about which areas were in danger next. So people be­gan to post on Twitter, upload geotagged cell phone photos to Flickr, and update Facebook.

I had been fairly obsessed with the wildfires, and since I didn’t remember this “common suspicion,” I decided to check the article Eagleman cites as the source of this info, which was a Wired blog post titled “Firsthand Reports from California Wildfires Pour Through Twitter.” It contained no references to a celebrity-obsessed news media; instead, the piece described how “the local media [was] overwhelmed.” It also talked about a San Diego resident who was “[a]cting as an ad hoc news aggregator of sorts” by “watching broadcast television news, listening to local radio reports and monitoring streaming video on the web” and then posting information, along with info gleaned from IMs, text messages, and e-mails, to his Twitter account.