University of Nebraska Omaha

Space and Defense

Volume 12
Number 3 *Volume 12 Issue 2 (Summer 2021)*

Article 9

June 2021

Deterring Terroists Organizations in Times of a Global Pandemic: An arguement for an indirect approach to deterring terrorism

Grant Van Robays
University of Nebraska at Omaha, grant.vanrobays@edu.edu

Recommended Citation

Van Robays, Grant (2021) "Deterring Terroists Organizations in Times of a Global Pandemic: An arguement for an indirect approach to deterring terrorism," *Space and Defense*: Vol. 12: No. 3, Article 9.
DOI: 10.32873/uno.dc.sd.12.02.1076
Available at: https://digitalcommons.unomaha.edu/spaceanddefense/vol12/iss3/9

Deterring Terrorist Organizations in Times of a Global Pandemic: An argument for an indirect approach to deterring terrorism

Grant Van Robays*

Introduction

The COVID-19 pandemic has disrupted nearly every facet of life across the world. While the United States is the world's social, economic, and political powerhouse, it is no exception to the indiscriminate virus. The U.S. faces economic volatility, social unrest, political polarization, and a devastating loss of American life due to the pandemic. To make matters worse, these crises leave the U.S. vulnerable to opportunist terrorist organizations at home and abroad, who may seek to take advantage of these vulnerabilities, whether perceived or real. While the pandemic appears to be slowing down both in the U.S. and abroad, the vulnerabilities to the economy and social and political arenas can persist long after the last positive COVID test. History shows that pandemics are not merely a one-time occurrence, meaning there will almost surely be another in the future. When this occurs, vulnerabilities will again present themselves and open doors for opportunist terrorist organizations to attack. Thus, it is imperative to explore new terrorist deterrence strategies, particularly strategies catered towards global pandemics and the chaos they invite. To explore the question of "Can we deter terrorists from exploiting the pandemic?" this paper first asks, "Do vulnerabilities in an established regime brought on by pandemics invite circumstances of opportunity for terrorist organizations? If so, how can a power like the U.S. deter terrorists from taking advantage of these vulnerabilities?

Objectives and Hypotheses

This paper investigates these research questions in pursuit of three main objectives. First, the paper will establish that vulnerabilities brought on by global pandemics invite circumstances of opportunity for terrorist organizations. It will also explore deterrence strategies against terrorists that may be applicable to times of global health crises. Thirdly, this paper will argue in favor of a more indirect approach to terrorist deterrence; one that emphasizes the maintenance of resilient health, governmental, and economic institutions to minimize the exploitable vulnerabilities in the U.S. sociopolitical system. I hypothesize that if the U.S. practices this resiliency, terrorist organizations will have fewer opportunities to act on perceived vulnerabilities during times of global pandemics.

Procedure

This paper will rely on open-source information such as academic literature and

publications to investigate the research question and hypothesis. I will draw on research regarding terrorism, counterterrorism, and the logic of terrorist organizations to establish that terrorists may seek to capitalize on vulnerabilities in U.S. society because of the pandemic. To establish that these vulnerabilities exist, I will explore economic data from U.S. publications or nongovernmental financial institutions. To provide support for my hypothesis, I will rely on available deterrence literature to build a framework from which I will expand my argument. This paper looks at the United States' current situation in the pandemic through a lens that asks, "What vulnerabilities exist?" and "What are some ways our government can fix them?" to best protect the American people. In short, I will use available qualitative resources rather than a statistical analysis to construct a unique, theoretical strategy to terrorist deterrence during pandemics.

Potential Vulnerabilities Wrought by the Pandemic

The COVID-19 pandemic has ravaged virtually every country in the world, regardless of wealth, development, or government type. At the time of writing, the global death toll sits at nearly 2.7 million out of 121 million infections.[1] The impact on the United States is nothing short of devastating, amounting to over 537,000 deaths out of nearly 30 million cases.[2] The sheer loss of life from this pandemic is incalculable. However, as crippling as this pandemic has been on the U.S. and around the world, this does not preclude extremists or terrorist groups from taking advantage of the vulnerabilities wrought by the pandemic. This paper must first define vulnerability. In simple terms, vulnerability is the state or quality of being vulnerable.[3] Vulnerable, a derivation from the Latin "vulnus," meaning wound, originally meant capable of being physically wounded, but can be used figuratively to suggest a defenselessness against non-physical attacks.[4] Altogether, a vulnerability can be conceptualized as the state of being at susceptible to attack or wounding. The wound can be physical, emotional, psychological, economic, political, or social. This paper will consider vulnerability in this broad sense, considering the weaknesses, tangible or otherwise, created or exacerbated by the global pandemic.

The pandemic has contributed to a drastic economic downturn. As the pandemic spread, many businesses shuttered and had to reduce staff to cut their losses, while other jobs were moved online when applicable. According to a May 2020 publication by the Congressional Budget Office (CBO), the social distancing measures taken to curtail the spread of the COVID-19 virus have "widely disrupted economic activity, causing a wave of job losses and ending the longest expansion since World War II."[5] The unemployment rate skyrocketed from 3.8 percent in February 2020 to 14.4 percent in April 2020, as nearly 14 million Americans lost their jobs.[6] These figures surpass the Great Recession of 2007-2009, which pushed the unemployment rate to nearly 11 percent.[7] However, the labor market is projected to improve gradually throughout 2021 as vaccination rollout improves,

hiring rebounds, and job losses drop significantly, according to the CBO.[8] These improvements will not be large enough to make up for earlier losses, though, as the 2021 real GDP is projected to be 1.6 percent lower and the unemployment rate 5 percent higher in the fourth quarter than their respective values in 2019.[9] Recent projections from the Congressional Budget Office show a comparatively more positive economic outlook. Real GDP will return to its previous peak level in mid-2021 and will continue to expand at a 2.5 percent annual rate until 2025 due to a strong rebound in consumer spending and reinvestment in business hurt by the pandemic.[10] The CBO projects consumer spending to grow at an average annual rate of 2.8 percent until 2025; however, this projection is inhibited by lasting effects of unemployment, reduced labor income and lasting caution by consumers.[11] The unemployment rate is projected to decline gradually to below the natural rate of unemployment in 2024 and reach 4 percent by 2025, which is on par with the pre-pandemic unemployment rate.[12] However, the CBO notes that their projections contain a substantial degree of uncertainty due to government policies, vaccine distribution/efficacy, and consumer attitudes and behaviors. Additionally, a virulent variant of COVID-19 can manifest and reinforce social distancing measures and more economic disruption.[13] There is also the possibility that economic output may decline and stall the recovery process. The pandemic has had disparate effects on different industries and populations, which provides uncertainty for long-term productivity projections.[14] Finally, the increase in domestic and global debt in turn increases the risk that financial instability in only a couple countries can severely impact many countries due to the globalization of markets.[15]

The U.S. economy has rebounded well to the initially devastating economic impacts of COVID-19, as the CBO projections indicate. By their estimates, the U.S. economy and labor force will approach pre-pandemic figures by the year 2025. This paper does not aim to argue that the U.S. economy is in shambles or that it is not able to recover from the pandemic. Rather, it argues that the uncertainty within the U.S. economy serves as a potential source of vulnerability, perhaps an exploitable one. According to the CBO projections, the economy may not reach pre-pandemic figures in respect to unemployment and real GDP growth until a year or two from now, which may contribute to a wide sense of economic uncertainty. Economic uncertainty and an ever-expanding federal and global debt can be a source of vulnerability on behalf of consumers and the national economy. It is unclear if this economic uncertainty and vulnerability significantly heighten the risk for terrorist attacks. A 2018 analysis of terrorism in Tunisia by Nurunnabi and Sghaier, researching the socioeconomic determinants of terrorism, found that a 1% increase in the unemployment rate increases the number of terrorist attacks by .24 percent. Nurunnabi and Sghaier also found that a 1 percent increase in political instability increases the number of terrorist attacks by 1.02 percent.[16] The rationale behind these results is that politically unstable countries may offer favorable conditions for

the spread of terrorism.[17]

The results of Nurunnabi and Sghaier's analysis share commonalities with those of Staub, who found that higher unemployment rates lead to an increase in terrorist attacks.[18] Their findings also indicate that increases in GDP per capita have a negative impact on terrorism.[19] This notion contrasts to the findings of Piazza,[20] who discovered that the level of economic development (operationalized by gross national income and the Human Development Index) has a significantly positive impact on domestic terrorism, suggesting that more modernized countries offer more targets for terrorists and more means to plan and act.[21] This finding align with the results of Estrada et al., who revealed a positive relationship between GDPs per capita and terrorism. Ismail and Amjad found that unemployment, inequality, and political repression have insignificant impacts on terrorist activity in the long term.[22] [23] Thus, the actual relationship between economic growth and unemployment remains gray, with evidence that both supports and disproves the notion that economic growth decreases the risk of terrorism. This paper does not intend to present new evidence in favor of either side but intends to explore the relationship between the economy and threats of terrorism to identify threats to the U.S. during the pandemic. However, an uncertain economy compounded by political and social division can result in serious instability, and the resulting vulnerability is significant and must be considered.

The pandemic has become a highly politicized and polarized issue in the U.S. Since the early days of the pandemic, Republican Party officials have tended to downplay the severity of the virus, whereas Democratic leaders have urged more caution.[24] Republicans generally engaged in less social distancing compared to Democrats, according to GPS data on smartphones.[25] Media outlets on each side of the political spectrum have also sent divergent messages on the pandemic and its severity, following a pattern of a hyper-partisan media.[26] After a tumultuous election cycle in 2020, partisanship has hardly subsided. The 2020 election results were highly contested by the incumbent Republican president and certain Republican members of Congress. This partisanship culminated in a siege at Capitol Hill on 6 January, 2021 by domestic terrorists and supporters of the former president.[27] An unclassified summary from the Office of the Director of National Intelligence has also indicated that domestic violent extremists motivated by a range of ideologies are likely to be galvanized by political and societal events from this past year.[28] Thus, hyper-partisanship and polarization are not a new phenomenon, rather one that has deepened in the recent months and years and may continue to deepen. Public opinion surveys attest to this, as the share of Americans from both parties who view members of the other party as "cold" on a feeling thermometer has risen from about 60 percent in 2016 to a little over 80 percent in 2019.[29] Survey results have shown that people from opposing parties increasingly view the other party as close-minded and unpatriotic.[30] The global health crisis and the 2020 election have

exacerbated existing political and social tensions in the United States, posing a significant vulnerability to the country. Domestic terrorist and extremist groups may, as the ODNI assessed, escalate their plans and attacks to take advantage of a polarized climate. International extremist groups may also take advantage of a divided United States, as their weakening social structures and trust in government may present an opportunity too rife to pass up.

Another domain in which the U.S. may be vulnerable to attack is cyber. As the pandemic spread across the country, countless shutdowns and closures took place in response. Jobs, education, and businesses moved online when possible, providing more opportunities for cybercriminals to take advantage of increased security vulnerability. An INTERPOL assessment reported an uptick in cybercrime activities, with over 900,000 spam messages, 737 incidents related to malware, and 48,000 malicious URLs all related to COVID-19 between January and April of 2020.[31] INTERPOL projected an increase in cybercrime in the future because vulnerabilities related to working at home and the potential for increased financial benefit will motivate cybercriminals.[32] As COVID-19 case numbers decrease with an increased distribution of vaccines, INTERPOL assesses that there will be another spike in phishing related to these medical products.[33] Put simply, the fear and uncertainty created by the pandemic provide a golden opportunity for cybercriminals to exploit.

There are many ways in which cybercriminals have utilized the online domain for personal gain during the pandemic. The same INTERPOL assessment addressed five different strategies deployed by cybercriminals. Online scams and phishing are the most common and consist of actors impersonating government and health authorities to entice victims into providing their personal data. Cybercriminals are also using more disruptive malware against critical infrastructure, government, and healthcare institutions. Cyberattacks and disruptive malware against critical infrastructure have a high impact and significant financial benefit for the hacker.[34] The U.S. healthcare system is not immune to these attacks by any means, as an estimated 26 million patient records were exposed to unauthorized parties in the U.S. in 2020, with about 24.1 percent of those resulting from healthcare cyberattacks.[35] Cybercriminals also have deployed data-harvesting malware and spyware, in which criminals use COVID-19 information as a lure to infiltrate and compromise networks and steal personal data. There has also been a significant increase in malicious domain usage, whereby criminals use fraudulent websites with COVID to attack victims, who are then subject to a variety of malicious activities like malware deployment and phishing. The INTERPOL assessment reported a 569 percent growth in malicious registrations from February to March 2020, and a 788 percent growth in high-risk registrations in the same time period.[36] Finally, cybercriminals can easily spread unverified misinformation about the virus and vaccines.

The INTERPOL assessment on cybercrime during the pandemic and the hacks on U.S. healthcare infrastructure highlight a significant vulnerability and opportunity for cybercriminals, both at home and abroad. The importance of this vulnerability and the need for a secure cyberspace cannot be understated, as cybersecurity is an essential component of a safe and secure society. The U.S. Department of Homeland Security reiterates this message and has stated on its website that "our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace."[37] While there has yet to be a cyberterrorist attack or insurgency through cyberspace, the U.S. must consider the possibility that they can and will happen. As society continues to work and learn online for the duration of the pandemic, cybercriminals and organizations with expanding capabilities can feasibly jump the opportunity to attack critical infrastructure in the U.S. or spread misinformation or disinformation. The reality of the latter is already well-documented, as recent reports show online platforms directed by Russian intelligence are spreading disinformation about COVID-19 vaccines used in the U.S.[38]

Perhaps one of the most logical and dangerous targets for cybercriminals is the U.S. power grid. All 16 sectors of the U.S. economy that make up the country's critical infrastructure rely on access to electricity.[39] Disabling the power grid would therefore be extremely serious and could impact basic government and social services and institutions. While an attack on the grid would require intensive planning and capabilities that many criminal or terrorist organizations simply do not have, the possibility of an attack cannot be entirely ruled out, especially after a cyberattack in Ukraine. In December 2015, a synchronized and expertly executed cyberattack caused a six-hour blackout for hundreds of thousands of people in and around Kiev.[40] Forensic evidence and geopolitical circumstances tied the attack to Russian hackers from a group called Sandstorm.[41] During the outage, hackers took control of the computers of Ukraine's main power companies, disabled backup power supplies, sabotaged operator workstations, and implemented malware that wiped out essential files.[42] The "BlackEnergy" malware used in this case has been used by Sandstorm in their targeted attacks against industrial control systems in Ukraine, the U.S., and NATO.[43] Sandstorm has been active since 2010 and has used BlackEnergy malware to disrupt operations at major businesses and government officials since 2011 with the knowledge or consent of the Russian government.[44] U.S. Navy Admiral Michael S. Rogers stated that the probable goal of the large-scale 2015 attack was to watch the response and learn how to slow it down in the future.[45] In other words, this cyberattack was a well-executed trial run.

This cyberattack was not a one-off or a profit-driven plot, rather an act of coordinated destruction. Coordinated destruction, as defined by Tilly, is when persons or organizations that specialize in coercive means undertake a program of damage to persons/objects.[46] The Sandstorm cyberattack on Ukraine fits this

definition because the hacker collective specializes in coercive, albeit unconventional, means of inflicting damage through cyberspace. Cyberspace has few rules of operation or oversight, allowing Sandstorm and other political entrepreneurs to activate boundaries (Russia-Ukraine, in this case) and coordinate an attack. This cyberattack may also fall under a sub-category of coordinated destruction called conspiratorial terror. This is when a small, well-organized set of actors begin attacking more powerful targets by clandestine means.[47]As a group, Sandstorm is vastly less powerful than Ukraine or other targets, yet their skill and support by allies in the Russian government allow them to compensate for this power differential. The result in Ukraine was a mass power outage that lasted for hours. A larger-scale attack on the United States would surely do more damage. The ubiquity and relative anonymity of cyberspace makes this threat more severe.

Russia is not the only power with cyber capabilities, either, as Admiral Rogers noted in 2014 that China likely has the capability to shut down the U.S. power grid, and that Iran could acquire this capability, too.[48] After the Ukraine attack, the U.S. Department of Energy reported that the U.S. faced imminent dangers from cyberattacks, and that a widespread disruption of electric service could undermine U.S. lifeline networks, critical defense infrastructure, and a significant portion of the economy, in addition to endangering the health and safety of millions of Americans.[49] The complexity of a cyberattack on this scale makes it doubtful that current terrorist networks could plan and execute an attack on the power grid. However, as the Ukraine attack shows, they are technologically possible. According to a simulation by the University of Cambridge's Centre for Risk Studies, an extreme blackout caused by a team of highly skilled personnel with many months of planning and operational implementation could feasibly take control of 50 generators in the U.S. power grid and cause them to overload.[50] The result of this scenario would plunge 15 states into darkness and leave up to 93 million without power, while disrupting water supplies and transport networks.[51] The shift to online work and education during the pandemic also provides more opportunities for criminal groups to execute cyberattacks, which exacerbates the need for increased cybersecurity measures.

Threat of Opportunist Terrorist Organizations

Thus far, this paper has addressed potential vulnerabilities in the U.S. due to the havoc wrought by the global pandemic. Namely, the weakened and uncertain economy, political polarization and social unrest, and vulnerable cyber infrastructure have coalesced into a nexus of crises and opportunity for motivated threat groups. The next portion of this paper explores why such groups, namely terrorist organizations, threaten the U.S. now, amid a global health crisis, and how they could be deterred. For the sake of this paper, terrorism is broadly defined as a method used by insurgents to seize power from an existing government, manifesting in acts of

socially unacceptable violence meant to create a psychological effect on certain groups.[52] This paper also considers domestic, foreign, and even cyber terrorist groups in order to paint in broad strokes the threat of terrorism in and against the U.S. during this global health crisis.

Social science research tends to support the claim that terrorists and their respective organizations consist of rational actors.[53] That is to say, terrorists aim to maximize their utility by weighing the costs and benefits of a certain action when given information and choices.[54] Violence against a certain population or a symbolic representation of such is thus a strategy that the group collectively selects as a course of action that maximizes benefits over costs.[55] Terrorist organizations are also heavily influenced by recent changes in motives and opportunities.[56] This is because terrorists are impatient for action and highly sensitive to time constraints, which may be rooted in their calculations of ends and means.[57] When vulnerabilities in government manifest, terrorist organizations may rationally decide to take the chance to compensate for its inferiority and execute an attack.[58] In other words, when the balance of power between the terrorist organization and the regime they oppose is disrupted in the favor of the former, it is in the best interest of the organization to capitalize.

Martha Crenshaw describes two forms of vulnerabilities that make an established regime, such as the United States, vulnerable to challenge. The first vulnerability is when the regime's ability to respond effectively, efficiently repress dissent, or protect its own citizens is weakened.[59] In 1983, for example, a terrorist attack on U.S. Marines barracks in Beirut killed over 240 U.S. servicemen, an attack in which lax security in and around the barracks played a crucial role in leaving American troops vulnerable to attack.[60] Currently, the U.S. has its hands full in dealing with the virus and distributing vaccines. With the world's largest number of COVID-19 cases and deaths, the U.S. may appear to be unable to protect its citizens. A preliminary assessment on the impact of COVID-19 on Salafi-jihadist and far-right extremists has shown that members of such groups have greeted the global health crisis with enthusiasm because it has crippled the U.S. and other western nations, perhaps vindicating their respective ideologies and objectives.[61] An ISIS editorial article in the al-Naba' Magzine included a call to action for Muslims to capitalize on the paralysis of western governments, stating that, "The Mujahedeen should show no mercy towards the suffering West."[62] The pandemic diverts resources and assets from security and counterterrorism duties, which further exacerbates the vulnerability to an opportunist attack. As of March 2021, the Department of Defense identified more than 6,000 active-duty service members to support vaccination centers.[63] The economic and financial crises may also inhibit the United States' ability to defend itself from external threats, as these matters may divert the attention of policymakers from vital national security threats.

The second type of vulnerability that makes the regime an attractive target for terrorist organizations manifests when the regime makes itself morally or politically vulnerable by increasing the likelihood that terrorists will gain popular support.[64] If a government is overly repressive, they will provoke backlash and lose public support, support which then could be diverted to insurgent or extremist groups. The current sociopolitical climate in the U.S., one driven by polarization and partisanship, could present such vulnerability and lend legitimacy to anti-government extremist groups. The contested election of President Joe Biden over the incumbent Donald Trump was a breeding ground for conspiracy theories and charges of election fraud. Former President Trump was a major source of misinformation regarding the election and tweeted over 200 inaccurate messages about unsubstantiated claims of voter fraud, with a particular emphasis on mail-in ballots.[65] Effectively, only 61 percent of Republicans believed Biden rightfully won the election, according to a Northeastern University poll taken one month after the election.[66] Political division and uncertainty came to a head in the January 6 Capitol riot, in which hundreds of pro-Trump and far-right domestic extremist protesters gathered and eventually infiltrated the Capitol to contest Biden's Electoral College victory.[67] This event sparked international condemnation by world leaders from the UK, Germany, France, and even Russia, as the U.S. took a big hit to its international legitimacy and democracy.[68]

The backlash from this riot may further motivate foreign terrorist organizations to attack while the U.S. is vulnerable or as its legitimacy is in turmoil. However, the threat of domestic terrorism may be more severe. Far-right extremist groups are likely to be emboldened by the Capitol riot, as the ODNI report suggested.[69] If the U.S. response to these groups is viewed as too harsh by the groups themselves and their supporters, they may be encouraged to increase the scale of their attacks in retaliation. These extremists may do so with the perception that their public support is broad, and there is some evidence to support this. For instance, 58 percent of Trump voters said they viewed the January 6 events as "mostly an antifa-inspired attack that only involved a few Trump supporters."[70] There is no evidence that any anti-fascist movement was present at the Capitol, yet the perception that leftist provocateurs continue to pervade right-wing media.[71] To be fair, most Americans do believe it is important to prosecute people who breached the Capitol on January 6; however, this is also a partisan point, with less Republicans deeming prosecution of these criminals as important.[72] The fact is that America is a deeply divided country, and potential areas for unity like the pandemic and domestic extremist attack have only exacerbated the divide. This could potentially make the U.S. look morally weak or illegitimate from the perspective of foreign terrorist groups, but also illegitimate by millions of Americans who feel the current political regime is fraudulent. This may broaden support for anti-government attacks and thus is a significant vulnerability.

Deterring Terrorism

This paper has so far laid out sources of vulnerability that the U.S. currently faces either as a direct result, or byproduct of, the pandemic. The threats posed from opportunity-seeking terrorist organizations, foreign and domestic, are real and must not be overlooked, despite the many other pressing matters the government faces. How, then, should the government go about deterring these threats? Deterrence can first be conceptualized as "a strategic interaction in which an actor prevents an adversary from taking an action that the adversary otherwise would have taken by convincing the adversary that the cost of taking that action will outweigh any potential gains."[73] In other words, an actor must persuade the adversary that a certain action will not produce the expected benefits of said action, and that the action should not be taken. Broadly, there are two types of deterrence strategy with terrorism: deterrence-by-retaliation and deterrence-by- denial.

Deterrence-by-retaliation strategies seek to deter terrorists by threatening to impose unacceptable costs on an adversary if they take a particular course of action.[74] For example, if a jihadist group makes threats against the U.S. homeland about an imminent attack, the U.S. could try to deter the attack by imposing a high cost to the group. The costs could be in the form of sanctions or a coordinated military response. The cost imposed must be great enough to deter the terrorist from pursuing their attack. Deterrence-by-denial strategies, on the other hand, threaten to deny an adversary the benefits of a particular course of action.[75] An actor must convince the adversary that they will not succeed or reap benefits from an action. In their analysis of terrorist deterrence strategies, Kroenig and Pavel also differentiate between direct and indirect approaches to deterrence. Direct approaches aim to deter adversaries by threatening to retaliate against the adversary, whereas indirect response strategies are those that deter by threatening to retaliate against something the terrorists value, like their assets or communities.[76] These different deterrent strategies are featured in **Table 1**, borrowing from examples from Kroenig and Pavel.[77]

TABLE 1

	Cost Imposition	Denial of Benefits
Direct Approach	Threaten to retaliate against terrorists	Threaten to deny the terrorists a tactical success
Indirect Approach	Threaten to respond against terrorist's assets/things they value	Threaten to deny the terrorists strategic success (keeping forces in their community, for example)

Frey also provides a thorough overview of terrorism response and deterrence strategies that include and extend those discussed by Kroenig and Pavel.[78] Frey distinguishes soft and hard responses, the former aiming to address the root causes of terrorism while the latter imposes immediate and strong retribution.[79] Conciliatory responses may consist of accommodating the demands of terrorists, but also includes addressing the grievances of the terrorists without dealing with them directly.[80] Deterrent responses consist of applying criminal justice, by means of prosecution and ultimately conviction.[81] Frey also differentiates between short- and long-run responses to terrorism, where the short run deals with immediate problems created by terrorists, while the long run is directed at long-term reform and prevention.[82] Finally, Frey identifies reactive and proactive responses, the former, of course, referring to actions taken in response to a terrorist incident and the latter consisting of steps taken to identify and prevent terrorist activity before it occurs.[83]

Potential Solutions to Shore Up Vulnerabilities

Now that the main facets of terrorist deterrence have been broadly explained, this paper will present a strategy that borrows a little from each in hopes of creating a holistic terrorist deterrent strategy that catered to the threats to the U.S., both internal and external, that have been magnified by the global health crisis. This strategy is indirect in the sense that the response does not initiate contact nor threaten foreign or domestic terrorist organizations. Rather, it aims to address and resolve the vulnerabilities created by the pandemic, lest they be exploited by opportunist threat groups. The strategy is applicable in both the long and short term and is proactive instead of reactive. By shoring up the vulnerabilities in the American economy, political, social, and cyber arenas, opportunist terrorist organizations will lack exploitable opportunities to strike the U.S. with its back turned. The first vulnerability that must be addressed is the economy, which has been in turmoil because of the social distancing measures, business closures, and job losses provoked by the pandemic. Economic turmoil begets uncertainty, which could provide motivate criminal networks to take drastic steps to rectify their economic deprivation. Furthermore, the United States' back may be turned to these threats as it works to stimulate the economy, leaving it vulnerable to threats, internal and external. This paper argues that if the U.S. can build a resilient post-pandemic economy, it will effectively minimize these vulnerabilities. The matter becomes, then, how does the U.S. minimize the vulnerability to the economy and build a resilient economy, one that can withhold the tensions created by global health crises? This paper explores possible policy actions in pursuit of this question.

The United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) interviewed economic policy experts on how to build a resilient

post-COVID economy. The experts reached a consensus on a set of broad themes. The U.S. is more economically developed than most countries in the Asia and Pacific region, but the input of ESCAP is relevant because the pandemic has shown that even the mighty U.S. is susceptible to pandemic-induced economic fallout. The commission emphasizes that strong and sustained macroeconomic policy is essential to shorten the post-pandemic recession and minimize long-term scars to the economy.[84] In other words, the U.S. should not be afraid to sustain relief and stimulus packages for the foreseeable future, as this could help prevent an unequal recovery. The pandemic has disproportionately impacted the economically vulnerable, such as the less educated and low earning. Of the U.S. jobs deemed "vulnerable" to pay cuts and layoffs, 86 percent are held by those earning under $40,000 a year, compared to one percent of jobs held by earners of over $70,000.[85] Additionally, U.S. billionaires also expanded their wealth by 20 percent between March and June 2020, while millions of Americans and small business owners continue to grapple with lost wages and unemployment.[83] Put simply, the economic stimulus must not forget the most vulnerable. The U.S. cannot sacrifice Americans jobs and lives for a growth in GDP.

ESCAP also urges governments to explore unconventional financing mechanisms like catastrophe risk insurance and multilateral financial safety nets to enhance the fiscal buffer for future shocks.[87] The commission also emphasizes the need for governments to make economies more inclusive and environmentally sustainable by focusing on strengthening health and social protection systems and closing the digital divide, which has been deepened since the pandemic forced jobs and education fully online.[88] U.S. policymakers should also diversify the economy in ways that make them better at withstanding market volatility and invest in innovation. This means building and strengthening research and development, entrepreneurship, and commercialization from the local to national levels.[89] Leaders should commit to long-term investments in the American people, regardless of race, ethnicity, gender, or wealth, as equity-enhancing measures can boost economic growth in the long run. According to one estimate, achieving gender equality could add up to $4 trillion to the U.S. economy by 2025.[90] In short, the U.S. must invest in the American people, in both the short and long term. These investments are key for resilient economies and resilient countries. While investments and economic innovations of this scale are daunting, the benefits surely outweigh the costs. With a more resilient, human-centered economy, the vulnerabilities in the economy will be greatly minimized.

The next vulnerability that must be shored up is social and political polarization, which has been a significant source of conflict before and during the pandemic. Polarization and a sense of distrust in the "other" or the government at large is a dangerous threat to the American political system and way of life, as evidenced by the Capitol Hill storming. If the U.S. can work to increase unity, understanding, and

empathy, then the threat of domestic extremists who oppose the current political system will be minimized. There is no quick fix to reverse the deep animus Americans have towards members of the opposing political party, but small steps combined with bold ideas can set the U.S. on the right path. As of 2019, 77 percent of Americans believed that their differences with the opposing party are not so great that they cannot come together.[99] While it may be more challenging for Americans to come together after this divisive and tumultuous year, it is far from impossible with constructive intergroup contact and responsive government.

Americans on each side of the political spectrum take cues from party leaders and media influencers, which heavily influence voting behavior and other political choices.[92] When these influencers and political elites speak on political, social, or cultural issues, their followers listen, even if the information they provide is not always an accurate representation of reality. With the proliferation of social media, these messages are available at all hours of the day and are not vetted thoroughly, which exacerbates the divide. This has been especially apparent during the pandemic, with conspiracy theories about the virus, vaccines, and the election spreading across the country instantaneously. This fuels partisanship and outgroup hostility. Constructive intergroup interactions and contact can help minimize this hostility by bringing people from opposing political beliefs together. Intergroup contact is beneficial because it allows people to learn about members of the social outgroup and reduces anxiety about intergroup interactions, as well as increase empathy with members of the outgroup.[93] Intergroup contact must be facilitated carefully to prevent further polarization and intergroup hostility. One example of a model of intergroup contact is "Citizen Assemblies," in which citizens are brought together to deliberate over pertinent social and political issues.[94] If the U.S. gives its people a forum for constructive deliberation and understanding, the country could develop a stronger sense of unity and empathy. And because Americans take cues from their party leaders, members of Congress and the Executive must lead by example. Senator Mitt Romney has reiterated this very point when asked about the polarization of America and has suggested the reinstitution of weekly meetings for Republican and Democratic senators.[95] Media at all levels must take fact-checking seriously in order to present the truth on matters of national importance, such as a pandemic. Misinformation in all levels of media can foment hate and deepen division, and those that stoke these flames should be held accountable. Those who do not acquiesce to intergroup contact and unity, namely domestic violent extremists, should be prosecuted to the extent that they commit a crime, such as those committed at the Capitol. However, the U.S. should welcome regretters, those who once participated in domestic extremist groups, and offer support if they renounce their activities and reintegrate them into society.[96] A policy of reintegration embodies the unity and empathy the country must practice, as well provides the regretters a sense of belonging and acceptance that may have driven them to

extremism in the first place.

At the individual level, there are many simple practices Americans could adopt to shore up their defense against opportunist cybercriminal networks. For starters, they should back up important files and store them independently from their system. Individuals should regularly check their software and systems and install the latest anti-virus software. They must be vigilant, check and update their privacy settings, and update passwords and ensure that they are strong.[97] At the macro level, the U.S. should consider investing in microgrids to combat the threat of a cyberattack on the U.S. power grid. Microgrids are decentralized, local energy grids that can disconnect from the traditional grid and can thus operate autonomously.[98] "Campus style" microgrids are currently used at military installations, hospitals, colleges, data centers, and other private and public properties that highly value uninterrupted power supplies.[99] Microgrids have proven to be lifesaving during severe storms like Superstorm Sandy in 2012. Millions of residential and commercial customers lost power when Sandy hit, and many critical facilities like water treatment centers, police stations, and hospitals had to rely on standby generators or were completely shut down. One hospital was disconnected from the main grid for two weeks, yet it remained operational with a microgrid.[100] College campuses in the area also used microgrids throughout the duration of the storm and subsequent recovery process.[101] Despite these successes, microgrids only provide less than .2 percent of U.S. electricity, mainly in Alaska, California, New York, Texas, Maryland, Georgia, and Oklahoma.[102] This is mostly due to technical, economic, and regulatory barriers. To begin with, microgrids and similar distributed energy resources are not designed for resiliency, meaning they cannot operate as a standalone power source in cases of an outage. Economically, research and development for microgrids are expensive for residential and commercial use, and the government often must provide tax incentives and funding for such projects. Due to the polarization of renewable energy and climate change-related services, this is a significant struggle. Microgrids still provide a reliable power source in cases of emergency, and the growing cyberthreat should pressure the U.S. government to invest in alterative power sources such as these to maintain resilient cyber and power structures.

Conclusion

The threat of terrorism, either from domestic, foreign, or cyber threats can easily be overlooked in the middle of a global health crisis. Testing and vaccination logistics are complicated matters and demand attention from U.S. leaders, as does the economic fallout from yearlong disruptions in commerce and employment. Government leaders must not sleep on the vulnerabilities revealed by the pandemic, though. Rather, by addressing and working to rectify the flaws and vulnerabilities in the current U.S. government, economy, and society, terrorist groups are effectively deterred by not giving them any opportunities to attack. This strategy may seem

idealistic, too broad, or too unrelated to the terrorism, and to a degree this is true. Large economic policy changes, human-centered investments, sociopolitical unity and bipartisanship, and beefed-up cyber and energy sectors are daunting tasks that take a considerable amount of time and money. Moreover, terrorism is a multifaceted issue with differing methods, objectives, ideologies, and motivations, meaning an effective deterrent strategy must be comparatively multifaceted and complex to effectively counter the threat. However, many big problems require bold solutions, and there is hardly any problem bigger than the threat of opportunity-seeking terrorist groups combined with the threats and vulnerabilities imposed by a pandemic. Resiliency is at the heart of this unique, albeit indirect approach to deterring and preventing terrorism in the United States. By focusing on creating and maintaining policies and institutions at all levels of government and the economy, vulnerabilities will be minimized, and so too the threats posed by opportunist terror groups who threaten the United States.

*Grant Van Robays is a senior and honors student majoring in Political Science with a minor in Sociology and Human Rights Studies at the University of Nebraska at Omaha. He is an intern at the National Counterterrorism Innovation, Technology and Education (NCITE) Center, which is a Center of Excellence for the Department of Homeland Security (DHS). His research interests include intelligence analysis, counterterrorism, deterrence, and international and national security. Mr. Van Robays aspires to graduate and enter the workforce as an analyst in the intelligence community, security field, or public service.

Notes

1. The New York Times. "Coronavirus in the U.S.: Latest Map and Case Count." The New York Times. The New York Times, March 3, 2020. https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html?action=click&module=Top+Stories&pgtype= Homepage.

2. Ibid.

3. Merriam-Webster, "Vulnerable." Merriam-Webster. Merriam-Webster. Accessed March 20, 2021.https://www.merriam-webster.com/dictionary/vulnerable.

4. Ibid.

5. Congressional Budget Office, "Interim Economic Projections for 2020 and 2021." Congressional Budget Office, 2020. https://www.cbo.gov/publication/56368#:~:text=The%20unemploymaboent%20rate%20is%20projected, 2019%2C%20before%20the%20pandemic%20began.

6. Kochhar, Rakesh, "Unemployment Rose Higher in Three Months of COVID-19 than It Did in Two Years of the Great Recession." Pew Research Center. Pew Research Center, August 26, 2020. https://www.pewresearch.org/fact-tank/2020/06/11/unemployment-rose-higher-in-three-months-of-covid-19-than-it-did-in-two-years-of-the-great-recession/.

7. Ibid.

8. Congressional Budget Office, "Interim Economic Projections for 2020 and 2021."

9. Congressional Budget Office, "Interim Economic Projections for 2020 and 2021."

10. Congressional Budget Office, "Additional Information About the Economic Outlook: 2021 to 2031," Congressional Budget Office, 2021. https://www.cbo.gov/publication/57014#_idTextAnchor051.

11. Congressional Budget Office, "Additional Information About the Economic Outlook: 2021 to 2031."

12. Ibid.

13. Ibid.

14. Ibid.

15. Ibid.

16. Nurunnabi, Mohammad and Asma Sghaier, 2018, "Socioeconomic Determinants of Terrorism," DOMES: Digest of Middle East Studies 27 (2): 278–302. doi:10.1111/dome.12139.

17. Nurunnabi, Mohammad and Asma Sghaier, "Socioeconomic Determinants of Terrorism."

18. Staub, Ervin. 2007, "Preventing Violence and Terrorism and Promoting Positive Relations Between Dutch and Muslim Communities in Amsterdam." Peace & Conflict 13 (3): 333–60. doi:10.1080/10781910701471397.

19. Nurunnabi, Mohammad and Asma Sghaier, "Socioeconomic Determinants of Terrorism."

20. Piazza, James A. 2011, "Poverty, Minority Economic Discrimination, and Domestic Terrorism," Journal of Peace Research 48 (3): 339–53. doi:10.1177/0022343310397404.

21. Piazza, James A, "Poverty, Minority Economic Discrimination, and Domestic Terrorism."

22. Estrada, Mario Arturo Ruiz, Donghyun Park, Jung Suk Kim, and Alam Khan. 2015. "The Economic Impact of Terrorism: A New Model and Its Application to Pakistan." Journal of Policy Modeling 37 (6): 1065–80. doi:10.1016/j.jpolmod.2015.08.004.

23. Ismail, A., & Amjad, S. (2014). Determinants of terrorism in Pakistan: an empirical investigation. Economic Modelling, 37, 320–331.

24. McCarthy, Ti,. "Disunited States of America: Responses to Coronavirus Shaped by Hyper-Partisan Politics," The Guardian, Guardian News and Media, March 29, 2020. https://www.theguardian.com/us-news/2020/mar/29/america-states-coronavirus-red-blue-different-approaches

25. Allcott, Hunt, Levi Boxell, Jacob Conway, Matthew Gentzkow, Michael Thaler, and David Yang,"Polarization and public health: Partisan differences in social distancing during the coronavirus pandemic," Journal of Public Economics 191 (2020): 104254.

26. Ibid.

27. Wilber, Quentin, "FBI Director Says Capitol Riot Was 'Domestic Terrorism'," Los Angeles Times. Los Angeles Times, March 20, 2021. https://www.latimes.com/politics/story/2021-03-02/fbi-wray-testify-congress-capitol-siege.

28. Office of the Director of National Intelligence.*Domestic Violent Extremism Poses Heightened Threat in 2021*.Office of the Director of National Intelligence, 2021.https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf Accessed 20 March 2021.

29. Pew Research Center, "Partisan Antipathy: More Intense, More Personal," Pew Research Center - U.S. Politics & Policy, Pew Research Center, August 17, 2020. https://www.pewresearch.org/politics/2019/10/10/partisan-antipathy-more-intense-more-personal/?utm_source=link_newsv9&utm_campaign=item_268982&utm_medium=copy.

30. Ibid.

31. INTERPOL, "COVID-19 Cyberthreats," INTERPOL, April 2, 2020. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

32. Ibid.

33. Ibid.

34. Ibid.

35. Ikeda, Scott, "Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the U.S. Impacted," CPO Magazine, February 26, 2021. https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/#:~:text=The%20total%20count%20of%20US,%2C%20an%20increase%20of%2055.1%25.&text=However%2C%20in%20terms%20of%20impact,to%20these%20healthcare%20cyber%20attacks.

36. INTERPOL, "COVID-19 Cyberthreats."

37. "Cybersecurity." Department of Homeland Security, March 1, 2021 .https://www.dhs.gov/topic/cybersecurity.

38. Hansler, Jennifer, Pamela Brown, and Devan Cole, "Russian Disinformation Campaign Working to Undermine Confidence in Covid-19 Vaccines Used in US," CNN, Cable News Network, March 8, 2021 .https://www.cnn.com/2021/03/07/politics/russian-disinformation-pfizer-vaccines/index.html.

39. Knake, Robert K., Report, Council on Foreign Relations, 2017. Accessed 23 March 2021.http://www.jstor.org/stable/resrep05652.

40. Sullivan, Julia E., and Dmitriy Kamensky. 2017, "How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid," Electricity Journal 30 (3): 30–35. doi:10.1016/j.tej.2017.02.006.

41. Knake, Robert K., Report, Council on Foreign Relations.

42. Sullivan, Julia E., and Dmitriy Kamensky, "How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid."

43. Hultquist, John, "Sandworm Team and the Ukrainian Power Authority Attacks," FireEye, January 8, 2016.https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html.

44. Ibid.

45. Sullivan, Julia E., and Dmitriy Kamensky, "How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid."

46. Tilly, Charles, 2003, "The Politics of Collective Violence" [VitalSource Bookshelf], Retrieved fromhttps://bookshelf.vitalsource.com/#/books/9781107485976/

47. Ibid.

48. Knake, Robert K., Report, Council on Foreign Relations

49. Sullivan, Julia E., and Dmitriy Kamensky, "How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid."

50. Ruffle, Simon & Leverett, Eireann & Coburn, Andrew & Copic, Jennifer & Kelly, Scott & Evan, Tamara, 2015, Business Blackout The insurance implications of a cyber attack on the US power grid. 10.13140/RG.2.1.1565.5528.

51. Ibid.

52. Crenshaw, Martha, 2011,*Explaining Terrorism: Causes, Processes and Consequences*London: Routledge.

53. Abrahms, Max, and Karolina Lula, "Why Terrorists Overestimate the Odds of Victory," Perspectives on Terrorism 6, no. 4/5 (2012): 46-62. Accessed 20 March 2021.http://www.jstor.org/stable/26296876.

54. Ibid.

55. Crenshaw, Martha,*Explaining Terrorism: Causes, Processes and Consequences,*112.

56. Waterman, Harvey, "Reasons and Reason: Collective Political Activity in Comparative and Historical Perspective," *World Politics*33, no. 4 (1981): 554-89. Accessed 28 February 2021. doi:10.2307/2010135.

57. Crenshaw, Martha,*Explaining Terrorism: Causes, Processes and Consequences,*115.

58. Ibid.

59. Ibid.

60. Dalesio, Emery P., and Allen G. Breed, "30 Years Later, Survivors Recall Beirut Blast," AP NEWS. Associated Press, October 23, 2013.https://apnews.com/article/lebanon-jacksonville-bombings-civil-wars-terrorist-attacks-e0917018dda942cc8bededede033742c9d.

61. Wither, James K., "The COVID-19 Pandemic: A Preliminary Assessment of the Impact on Terrorism in Western States," George C. Marshall European Center For Security Studies, April 2020.https://www.marshallcenter.org/en/publications/occasional-papers/covid-19-pandemic-preliminary-assessment-impact-terrorism-western-states.

62. Norlen, Tova C,"The Impact of COVID-19 on Salafi-Jihadi Terrorism." Connections (18121098) 19 (2): 11–24, 2020, doi:10.11610/Connections.19.2.01.

63. Lopez, C. Todd, "DOD Identifies More Troops to Help Administer COVID-19 Vaccine," U.S. DEPARTMENT OF DEFENSE, March 6, 2021.https://www.defense.gov/Explore/News/Article/Article/2526831/dod-identifies-more-troops-to-help-administer-covid-19-vaccine/.

64. Crenshaw, Martha,*Explaining Terrorism: Causes, Processes and Consequences,*115.

65. Spangler, Todd, "Twitter Has Flagged 200 of Trump's Posts as 'Disputed' or Misleading Since Election Day. Does It Make a Difference?" Variety, November 27, 2020.https://variety.com/2020/digital/news/twitter-trump-200-disputed-misleading-claims-election-1234841137/.

66. Ramjug, Peter, "Many Republicans Don't Believe the Election Results, a New Survey Says," News Northeastern Many Republicans dont believe the election results a new survey says Comments, December 11, 2020.https://news.northeastern.edu/2020/12/11/who-won-the-2020-presidential-election-joe-biden-or-donald-trump-depends-whom-you-ask/.

67. Anderson, Meg, "Antifa Didn't Storm The Capitol. Just Ask The Rioters," NPR, March 2, 2021.https://www.npr.org/2021/03/02/972564176/antifa-didnt-storm-the-capitol-just-ask-the-rioters.

68. BBC News, "US Capitol Riots: World Leaders React to 'Horrifying' Scenes in Washington," BBC News, BBC, January 7, 2021.https://www.bbc.com/news/world-us-canada-55568613.

69. Office of the Director of National Intelligence,*Domestic Violent Extremism Poses Heightened Threat in 2021.*

70. Anderson, Meg, “Antifa Didn't Storm The Capitol. Just Ask The Rioters,”

71. Ibid.

72. “Most Americans Say Prosecuting Capitol Rioters Is 'Very Important',” Pew Research Center - U.S. Politics & Policy, Pew Research Center, March 18, 2021.https://www.pewresearch.org/politics/2021/03/18/large-majority-of-the-public-views-prosecution-of-capitol-rioters-as-very-important/.

73. Kroenig, Matthew, and Barry Pavel, “How to Deter Terrorism,” Washington Quarterly 35 (2): 21–36, 2021, doi:10.1080/0163660X.2012.665339.

74. Ibid.

75. Ibid.

76. Ibid.

77. Ibid.

78. Frey, Bruno S., "Countering Terrorism: Deterrence vs More Effective Alternatives,"*Open Economics*1, no. 1, 2018: 30-35.

79. Ibid.

80. Ibid.

81. Ibid.

82. Ibid.

83. Ibid.

84. Saxena, Sweta, “Building a Post-COVID-19 Resilient Economy,” United Nations ESCAP, November 27, 2020. https://www.unescap.org/blog/building-post-covid-19-resilient-economy.

85. Cheng , Wan-Lae, Andre Dua, Zoe Jacobs, Mike Kerlin, Jonathan Law, Ben Safran, Jorg Schubert, Chun Ying Wang, Qi Xu, and Ammanuel Zegeye,“Reimagining the Postpandemic Economic Future,” McKinsey & Company. McKinsey & Company, December 4, 2020.https://www.mckinsey.com/industries/public-and-social-sector/our-insights/reimagining-the-postpandemic-economic-future.

86. Ibid.

87. Saxena, Sweta, “Building a Post-COVID-19 Resilient Economy,”

88. Ibid.

89. Cheng , Wan-Lae, Andre Dua, Zoe Jacobs, Mike Kerlin, Jonathan Law, Ben Safran, Jorg Schubert, Chun Ying Wang, Qi Xu, and Ammanuel Zegeye,“Reimagining the Postpandemic Economic Future.”

90. Ellingrud, Kweilin, Anu Madgavkar, James Manyika, Jonathan Woetzel, Vivian Riefberg, Mekala Krishnan, and Mili Seoni, “The Power of Parity: Advancing Women's Equality in the United States,” McKinsey & Company. McKinsey & Company, April 7, 2016.https://www.mckinsey.com/featured-insights/employment-and-growth/the-power-of-parity-advancing-womens-equality-in-the-united-states

91. Hawkins, Stephen, Daniel Yudkin, Míriam Juan-Torres, and Tim Dixon, “Hidden Tribes: A Study of America’s Polarized Landscape,” More in Common, More in Common,

2018.https://hiddentribes.us/media/qfpekz4g/hidden_tribes_report.pdf.

92. Iyengar, Shanto, and Sean J. Westwood, "Fear and Loathing across Party Lines: New Evidence on Group Polarization," American Journal of Political Science 59, no. 3 (2015): 690-707, Accessed 21 March 2021.http://www.jstor.org/stable/24583091.

93. Hewstone, M., & Swart, H., Fifty-odd years of inter-group contact: From hypothesis to integrated theory, British Journal of Social Psychology, 50, 374–386, 2011, doi:10.1111/j.2044-8309.2011. 02047.x

94. de-Wit, Lee, Sander van der Linden, and Cameron Brick, "What Are the Solutions to Political Polarization?" Greater Good, July 2, 2019.https://greatergood.berkeley.edu/article/item/what_are_the_solutions_to_political_polarization.

[95. "Idea: Bring Back Weekly Bipartisan Senate Meetings," POLITICO. POLITICO, 2019.https://www.politico.com/interactives/2019/how-to-fix-politics-in-america/polarization/bring-back-weekly-bipartisan-senate-meetings/.

96. Frey, Bruno S., "Countering Terrorism: Deterrence vs More Effective Alternatives."

97. "COVID-19 Cyberthreats." INTERPOL. INTERPOL, April 2, 2020.https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

98. "How Microgrids Work," Energy.gov, June 17, 2014.https://www.energy.gov/articles/how-microgrids-work.

99. Sullivan, Julia E., and Dmitriy Kamensky, "How Cyber-Attacks in Ukraine Show the Vulnerability of the U.S. Power Grid."

100. Ibid.

101. Ibid.

102. "Microgrids," Center for Climate and Energy Solutions, October 25, 2017. https://www.c2es.org/content/microgrids/#:~:text=Microgrids%20provide%20less%20than%200.2,York%2C%20Oklahoma%2C%20and%20Texas.