



UNITED STATES AIR FORCE
CENTER FOR STRATEGIC
DETERRENCE STUDIES

at The Air University



Don't Be Caught In the Dark: *Examining Deterrence Options for a High Altitude Electromagnetic Pulse Limited Nuclear Attack*

By Dr. Lyndon "Kyle" McKown, USAF Civilian

<http://www.airuniversity.af.edu/csds/>

One Second After, an unsettling novel by award winning author William R. Forstchen, details how an attack on the U.S. homeland using a nuclear electromagnetic pulse (EMP) instantaneously transforms this country from the digital age back to the turn of the 20th century.¹ In this doomsday scenario, the United States is literally left in the dark with no electricity, no electronic technology, and a collapsed civilian infrastructure. The results are catastrophic. Over the next year, 90 percent of the U.S. population perishes from the lack of medical care, starvation, and civil unrest. While the likelihood of any nuclear attack is considered low, the consequences are so high that for many years the United States military establishment has been conducting research and taking concrete actions to ensure they are ready for just such an attack.

The problem is, that unfortunately, our government has only recently started to evaluate the potential effects and needed preparations for the civilian infrastructure to survive an EMP attack. While a start, this governmental effort is still fragmented across multiple agencies and unduly handicapped because of the current classification of relevant government research data. All of which has led to a failure to set and implement industry standards to protect the civilian infrastructure from the most potent of the EMP threats. To correct this potentially catastrophic vulnerability and avoid the "*One Second After*" doomsday scenario, stronger governmental leadership, improved transparency, and industry wide federal standards are needed to send a strong signal of preparedness and resilience to deter any potential aggressors.

This research will explore the United States vulnerability to an EMP attack and seek a deterrent solution that may also address a recent U.S. Air Force Headquarters A10 question of interest: "In this era of great power competition, how do adversaries perceive the United States' nuclear posture or policy and their impact on strategic stability?"²

The background for this question talks about deterrence as a function of capability, credibility, and national will or intent. It also questions whether adversaries are most intimidated by mass, technology, or policy (such as preemption, first strike use,

and posturing forces). This background information appears to focus on a type of deterrence referred to as deterrence by punishment. This is problematic because many experts have expressed concern that in the arena of limited nuclear warfare between great powers, and even more so with lesser or non-state aggressors, deterrence by punishment may be difficult to execute and/or less effective than deterrence by denial or a combination of broader tailored deterrence approaches.³ My research will examine this concern, look at the deterrence options against this type of threat and suggest policy recommendations designed to reduce the probability and consequences of such an EMP attack.

As suggested earlier, the scope of this research is bounded to looking only at limited nuclear warfare. Additionally, based on my initial literature review and the numerous aspects and possible capabilities and tactics associated with limited nuclear warfare, this research will focus specifically on how best to deter a limited nuclear attack on the continental United States via a high altitude EMP. Specifically, this research will attempt to answer the question: "What is the best method of deterrence for a limited nuclear attack via a high altitude electromagnetic pulse, deterrence by punishment or deterrence by denial?"

My hypothesis is an adversaries' perception of the United States as being unprepared for attack greatly increases the likelihood of the attack. Without improved resiliency of our civilian infrastructure (primarily the power grid and communications), pure deterrence by punishment may fail because the aggressor will likely conclude a high probability of achieving the negative effects they desire and take their chances on any retaliatory response. Additionally, the aggressor may also doubt the credibility of an American threat to respond to an EMP attack with nuclear weapons and may not sufficiently fear a conventional response enough for deterrence by punishment to be effective. Therefore, deterrence by denial would be the best method of deterrence against an EMP attack against the United States. At the very least it would seem prudent to attempt to utilize some combination of punishment and denial to increase the deterrent and other positive effects and in turn the strategic stability.

Doctor McKown is a student at the Air War College at the Air University, Maxwell Air Force Base, Alabama.

While the scope of this effort was narrowed significantly because of the limited amount of time to complete the research, the results may have broader implications to deterrence theory in general.

— Definition of Terms —

Deterrence — Deterrence is an ancient concept. The Roman adage: “if you want peace, make ready for war” clearly illustrates this point.⁴ A more modern definition is found in the Oxford dictionary as “the action of discouraging an action or event through instilling fear or doubt of the consequences.” There are two basic approaches to deterrence, deterrence by punishment and deterrence by denial.⁵ Both approaches are fundamentally psychological and entail the nuanced shaping of perceptions in the mind of the potential aggressor. In other words, we seek to get inside aggressors’ heads and manipulate their decision making in ways that restrain them from taking the undesired action. This manipulation is possible due to the rational adaptation to the deterrence approaches designed to change their cost-benefit calculus.

Deterrence by punishment approaches are essentially designed to affect the perceived costs associated with an action. This approach threatens to inflict severe penalties as punishment in response to an action. To be most effective, the threat of punishment must come from someone that has the capability, the credibility, and the will to use it, should it be needed. It is also most effective if the punishment is swift, certain and severe. Conversely, deterrence by denial, is a form of deterrence where an action is discouraged because the expected benefit of the attack is negated or the potential success rate appears too low. For example, defensive measures to hold off an incoming attack or increased resilience that limits damage would be considered to reduce the perceived benefits in the mind of the aggressor and thus the likelihood of an attack.

While the concept of deterrence is as old as war, the advent of nuclear weapons was the catalyst that brought the logic of deterrence under the microscopic scholarship of international relations.⁶ Since this time there have been multiple waves of nuclear deterrence theory evolution as the concept evolved in response to the environment in which it operated. Bernard Brodie led the First Wave using deductive theory and theoretical strategizing. Thomas Schelling and Herman Kahn applied tools like game theory to develop the conventional wisdom in the Second Wave. During this period, the deterrence by punishment approach was firmly established by Schelling. On the other hand, Kahn’s advocacy for a broader approach to deterrence to include defensive activities was largely ignored until most recently. The Third Wave was characterized by the use of statistical and case study methods to test Second Wave theory and challenge the rational actor model assumption. Finally, while the first three waves were developed primarily in the Cold War security environment, the current Fourth Wave authors analyze deterrence in a post-9/11 security environment. This post-Cold War change in the security environment context and its effect on the validity of some of deterrence theory’s conventional wisdom assumptions is a central aspect of this research and deserves additional attention.

Thomas Schelling was a Nobel Laureate who used the “rational actor” model of modern economics to develop the punishment approach to deterrence. Schelling recognized that with nuclear weapons, military victory was no longer the “price of admission” for the ability to successfully employ the threat of violence. He asserted, “Deterrence rests today on the threat of

pain and extinction, not just on military defeat.”⁷ His philosophical belief was that actual nuclear warfare was unthinkable and therefore he supported the approach of a balance of terror based upon mutual vulnerability. A strategy of Assured Destruction and later Mutual Assured Destruction (MAD) was officially adopted by the United States for much of the Cold War based on this approach.⁸ His approach called for minimum deterrence, which required only the minimum number of weapons necessary to unleash an unacceptable level of destruction upon the Soviet Union’s infrastructure and civilian population. He advocated maintaining similar force structures to help make the terror “stable.” Conversely, anything such as civil or missile defenses designed to reduce vulnerabilities and protect human resources was seen by Thomas Schelling as inherently destabilizing. Schelling’s approach of deterrence by punishment, was in effect, each side holding the other’s civilian populations as hostages.

Herman Kahn’s philosophical views differed from Schelling’s. First, Kahn cast doubt on the widely accepted theory of a mutual balance of terror. He argued that in order to achieve success the terror had to be mutual and reliable. What if one side thought that, given sufficient preparations, although difficult, they could prevail in a nuclear war. He feared this could result in another Pearl Harbor for the United States. Another stark difference was that while Schelling viewed reducing vulnerabilities and seeking superiority as destabilizing, Kahn favored seeking to limit damage through defensive measures and strategic superiority through an array of offensive capability as more effective and safe deterrents. In taking this approach Herman Kahn was adding “deterrence by denial” to Schelling’s “deterrence by punishment.” Even though this approach seems more robust than Schelling’s, addressing both a potential adversaries’ perception of the cost and benefits in their decision calculus, Kahn was largely ignored until recently.

One of the reasons that Schelling’s deterrence by punishment was so strongly endorsed during the Cold War was that most experts and leadership felt that defending against total war involving nuclear weapons was nearly impossible. They felt that a total nuclear war simply could not be won and therefore must never be fought. Additionally, they assumed that the Soviets shared this same outlook on total war, because anything otherwise would not be rational. The strategy on both sides during the Cold War was that the nuclear threat had to be always ready and credible, but never used because a nuclear war could not be won. While these assumptions may have been valid in the past, there is growing evidence that our adversaries’ strategies may be changing and we must begin to start dealing with some new realities.

Limited Nuclear War — One of these new realities is that the long-held proposition, nuclear wars cannot be won and therefore must not be fought, is fading in the eyes of our potential adversaries. Wes Mitchell in a recent article details how Russia’s and China’s new focus on “limited war” capabilities is challenging our traditional method of deterrence by punishment.⁹ He asserts that there are at least three reasons for it getting harder to punish. First, the sheer number of competitors is increasing. Secondly, the rivals are becoming better armed. Finally, our rivals are developing new tactics designed to evade our retaliatory deterrence. His article is primarily focused on new tactics that try to operate below the threshold of deterrence by punishment to create territorial *faits accompli*.

In another article, John Warden describes similar disturbing trends providing additional evidence that leads one to have

little doubt that our adversaries have formulated a new strategy, namely that nuclear wars can be won because they can be kept limited.¹⁰ One envisioned scenario would be to capitalize on a surprise use of limited nuclear assets to quickly achieve an operational advantage and making it appear too costly for the United States to intervene because of the threat of escalation. This would be in effect an attempt to decouple theater and strategic warfare and challenge the resolve of our extended deterrence.

Another more subtle limited nuclear warfare trend described by Warden, most relevant to this research, is the attempt by adversaries to “distinguish between nuclear use consistent with Law of Armed Conflict traditions and strikes that are far less discriminating.” This approach would be to use nuclear weapons in a way that causes few if any immediate civilian casualties and in doing so hopes to avoid the backlash of transgressing the nuclear taboo. An upper atmosphere nuclear detonation designed to generate an EMP effect is just such an example. The motivation for such an attack could be multifold.

First, a direct nuclear attack on the United States would probably be seen as too escalatory, since the threat of a U.S. retaliation with nuclear weapons would be credible, as it was during the Cold War. However, a limited nuclear EMP attack, while still having the potential to damage and downgrade military operations and civilian infrastructure, could be seen as somewhat reasonable and restrained when compared with mutual assured destruction. Second, the situation could be further complicated because the technology needed for such an attack makes it the perfect asymmetrical threat for a limited nuclear power or a rogue non-state actor with a low yield nuclear device and a modified SCUD missile. Additionally, Warden asserts, “These vulnerabilities might encourage adversary nuclear use, on the belief that they provide an opportunity for significant disruption of United States and Allied operations.”¹¹ He then advises that these vulnerabilities should be mitigated with increased operational resilience. Increased operational resilience requires a thorough understanding of the characteristics and potential effects of an EMP.

EMP Characteristics/Effects — Experts in this field specify an EMP is actually composed of three component pulses designated E1, E2, and E3.¹² The E1 pulse is an almost immediate, brief, and very intense pulse that can induce tremendously high voltages into electronic circuits destroying vital components. It is unique to a nuclear event, has no similar counterpart in nature, and the data on the effects are classified for the most part. The E2 pulse is intermediate in duration and has similar effects to that of a lightning strike. The E3 pulse is much slower and longer lasting with effects similar to that of a solar storm. From the effects of natural solar variation we can predict this E3 effect from an EMP would virtually eliminate the ability to use radio communications (other than line of sight) for an extended period of time because of the absorption of radio waves by the ionized D-layer of the ionosphere.¹³ Although many of the particular details on the potential vulnerabilities to these effects are classified, we know they can be devastating.

Understanding the vulnerabilities in the critical civilian infrastructure from an EMP, specifically the power grid and communications is a central part of this research. A recent *Executive Report to Congress* asserted: “The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm.”¹⁴ This report goes

into great detail about a possible high-altitude nuclear EMP attack that could suppress the U.S. national command authority’s ability to respond and thus negate the deterrence value of assured nuclear retaliation. Additionally, because of the dependence of society on the electrical power system and its vulnerability, this EMP attack could also create long-term, catastrophic consequences for our civilian population. It is reasonable to assume that potential adversaries are also aware of these vulnerabilities and might estimate the benefit of exploiting them to be worth the potential cost of retaliation punishment.

The final part of this research literature review focused on understanding the capabilities, cost, and benefits of reducing vulnerabilities through various technical solutions designed to eliminate or mitigate the adverse EMP effects. There is a wealth of literature available in this area which provides relatively simple technical recommendations to improve resiliency to help prevent or mitigate the adverse EMP effects.¹⁵ Additionally, these experts argue that the costs to address these vulnerabilities are quite modest relative to the potential costs of repairing the damage caused by an EMP. Understanding the capability and potential costs of a deterrence by denial strategy is an important consideration in a decision for implementation since we must also use this data in our own cost-benefit analysis. The key takeaway here is that we have the technical capability to develop a very high quality defense against this threat at a reasonable cost to implement.

— Methodology —

In order to test my hypothesis, there needs to be some way to measure the effectiveness for deterrence by punishment and deterrence by denial and compare the results. Although a direct effectiveness measure would be desirable, measuring deterrence effectiveness quantitatively is problematic since this aspect is not understood very well nor has any direct measure been discovered in my literature review.¹⁶ For this reason, a qualitative approach will be used by looking at the comparison utilizing a simple cognitive model proposed by Paul Davis in a RAND Corporation working paper in conjunction with an adaptation of standard cost and benefit analysis decision making process.¹⁷

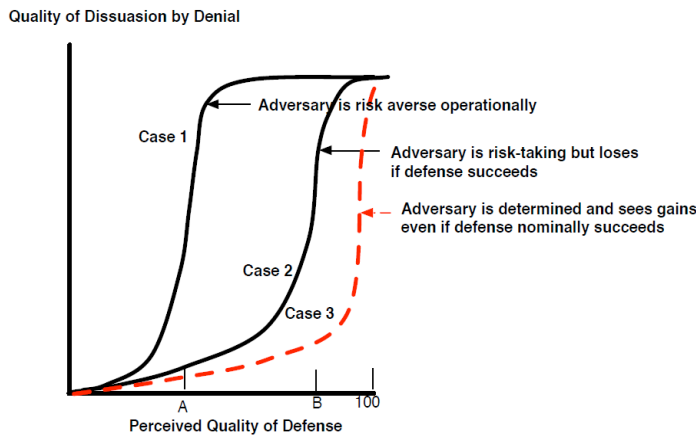
Davis begins his model development by redefining and relabeling Snyder’s original deterrence by denial concept. Concerned that extending the definition of deterrence beyond its threat of punishment meaning confuses effective communication, he renames deterrence by denial to dissuasion by denial and proposes the following definition: “Dissuasion by denial is deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action.”

In examining his definition, it is clear that dissuasion by denial and defense are closely related. In fact, Figure 1 depicts the quality of dissuasion by denial as a function of how good the defense is perceived to be by three notional cases of adversaries.



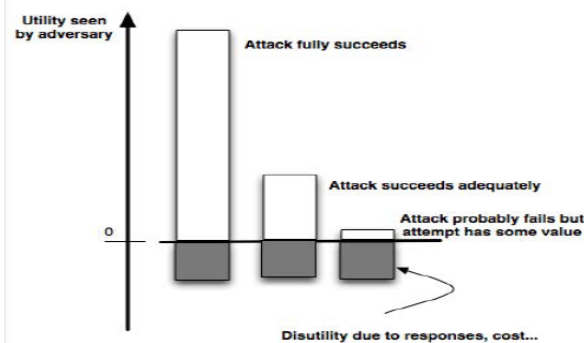
U.S. AIR FORCE

Figure 1 Actual and Perceived Quality of Defense



In Case 1, dissuasion by denial is very effective against an adversary who is operationally risk averse and perceives the defense to be less than perfect, but sufficiently good. Case 2 depicts a more determined and risk-taking adversary that is only dissuaded if the defense is perceived as quite good. Case 3 depicts the most extreme adversaries that may see possible strategic gains even if the defense is near perfect and largely succeeds. In applying these concepts to the research question at hand, we can surmise that the effectiveness of deterrence by denial is directly related to how the adversary perceives the “Quality of Defense” against an EMP attack. Taking this to the extreme, it is arguable that if a perfect defense were possible and acknowledged by an adversary, deterrence by denial alone would suffice. In our particular case, while experts have provided ways to greatly reduce vulnerabilities and thereby increasing the actual quality of defense against an EMP attack, there is no guarantee of an actual perfect defense and there is even less of a possibility that the adversary would perceive it as perfect. Therefore, it follows a comprehensive strategy should also include elements of deterrence by punishment that cause the adversary to evaluate the potential costs associated with an attack in comparison with the potential benefits in an adaptation of cost-benefit analysis as depicted in Figure 2.

Figure 2 Deterrence Depends on Both Positive and Negative Benefits



The basic framework for this approach rests on the rational actor assumption that we can take actions that manipulate the aggressor’s decision making in ways that produce net security benefits. The manipulation is possible due to sensitivity and

rational adaptation to operational risks posed by defensive measures that are designed to change the cost-benefit calculus. From a cost-benefit perspective, classic deterrence by punishment approaches are essentially designed to affect the perceived costs associated with an operation. Conversely, deterrence by denial, is where an operation is dissuaded because the adversary perceives that the potential benefits appear too low. Since sensitivity and rational adaptation will vary depending on the type of potential aggressor and other unique situational factors, I will look at three general cases of potential aggressors: near peer, asymmetrical, and non-state actor to using the methodology described above.

Each case will be analyzed in a notional scenario that portrays the situation in which the adversary could employ a limited nuclear EMP attack against the United States to achieve its desired political aims. While notional, each scenario will be based on reasonable expectations from current trends that could plausibly occur. The intent is heuristic rather than predictive with the intent of illustrating how a limited nuclear EMP might be used and serving as a venue to evaluate the two different approaches to nuclear deterrence in each case.¹⁸ The answer to my research question will be surmised from analyzing the general results in how each one of these three types of aggressors might be affected in a decision to conduct an EMP attack against the United States.

— Case Study Analysis —

Near Peer — The apparent success of the United States’ Cold War nuclear deterrence strategy against the Soviet Union, namely deterrence by punishment, has served to reinforce the mainstream belief that the same basic approach will be sufficient in the current geopolitical situation. However, the United States is no longer in a bipolar environment, but now faces much more complex near peer situations. Russia has nuclear parity with the United States and as detailed earlier, its military doctrine and exercises have increasingly embraced limited nuclear war capabilities and strategies. Similarly, an emerging China is challenging the United States economically, becoming increasingly capable militarily and aggressively pursuing new operational concepts such as unrestricted warfare.¹⁹ Either country could be used in this first scenario, but I will use Russia because it still remains the only country with a nuclear arsenal capable of completely destroying the United States and thus would be our worst-case scenario.

In this scenario, we start with American and NATO troops in the Baltic countries and Russia’s military buildup in neighboring Belarus making this region rife with tension and the stakes for conflict extremely high. Russia uses the excuse of protecting ethnic Russians as the rationale to invade one of the Baltic countries. NATO and Russian troops become embroiled in a conventional conflict that quickly escalates when Russia executes concerted conventional attacks against NATO bases and airfields in northern Europe, as well as a limited nuclear EMP attack against infrastructure and communication networks in Europe and the United States. Russia’s limited nuclear EMP attacks are an attempt to incapacitate the United States and its allies temporarily to gain a regional tactical advantage in the Balkans. In this scenario the United States would have to balance the need to defend itself and its allies against the possibility of further Russian escalation.

So for this scenario, which deterrence option is best suited to counter such a limited nuclear EMP attack? Looking at the deterrence by punishment option, the 2018 *Nuclear Posture*

Review provides the United States' declaratory policy regarding the potential employment of nuclear weapons:²⁰

"The United States would only consider the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners. Extreme circumstances could include significant non-nuclear strategic attacks. Significant non-nuclear strategic attacks include, but are not limited to, attacks on the United States, allied, or partner civilian populations or infrastructure, and attacks on United States or allied nuclear forces, their command and control, or warning and attack assessment capabilities.

"The United States will not use or threaten to use nuclear weapons against non-nuclear weapons states that are party to the Nuclear Non-Proliferation Treaty (NPT) and in compliance with its own nuclear non-proliferation obligations.

"Given the potential of significant non-nuclear strategic attacks, the United States reserves the right to make any adjustment in the assurance that may be warranted by the evolution and proliferation of non-nuclear strategic attack technologies and U.S. capabilities to counter that threat."

So in this scenario, while punishment is still possible, its deterrence effect has already failed. Russia has opted for such an attack because our infrastructure is currently vulnerable, our declaratory policy is vague, and the Russians are gambling the United States will limit or even preclude nuclear punishment in order to avoid possible escalation to total war. In other words, Russia has discounted the "fear of retaliation" costs by rationalizing the "fear of escalation" burden will mitigate or preclude the United States' punitive actions. This is certainly in line with Cimbala's concern that in many cases the idea of deterrence by punishment has become too risky because of the unpredictability of the nuclear escalation process.²¹ Additionally, currently the United States would have few options for punishment beyond conventional weapons and yet short of strategic nuclear weapons because the number of nonstrategic nuclear warheads has declined by approximately 90 percent from September 1991 to September 2009.²² The good news with a near peer adversary is that because they have something to lose, punishment is possible, and in fact has to be applied if there is any hope of reestablishing this type of deterrence in the future. The major problem with the punishment approach is that it can only be demonstrated after it has already failed and in doing so there is a significant risk of escalation.

Turning to deterrence by denial, and referring back to Figure 1, a near peer adversary would probably fall into the Case 1 or Case 2 category because of the risk of mutual destruction if the aggression led to total nuclear war. However, an adversary might be tempted because our current situation of little to no defense is arguably increasing the probability of success of just such an attack. Supporting this line of thought, the *Executive Report to Congress* mentioned earlier concludes with this very powerful statement: "The consequence of continued failure to address the U.S. vulnerability to EMP generated by a high-altitude nuclear weapon invites such an attack."²³ Conversely, if we were to increase our infrastructure's resiliency even moderately, this could provide a very effective deterrence for a peer adversary effectively taking this limited nuclear option off the table. For limited nuclear war in general, many experts recommend a strategy of deterrence by denial, both as an end in itself and as a compliment to deterrence by punishment. This approach presents both a strong defense that will deter low to moderate risk adverse opponents from believing that limited

nuclear warfare will result in any benefit, and in the worst-case scenario still allow the option to impose punitive costs in the case that deterrence by denial fails. So for this scenario, I argue that deterrence by denial is preferable because putting up a strong and obvious defense sends a clear and unambiguous message to the peer aggressor that a limited nuclear EMP attack against the United States could not be effective. Therefore, there would be no benefit in this approach regardless of their calculus on the credibility of the punitive cost we would impose on them if they did attack in this manner.

Asymmetrical — We now shift from a focus on relatively symmetrical situations of mutual deterrence to what may be an even more complicated deterrence challenge from asymmetrical threats. For this case study we will analyze the following notional scenario with North Korea. Ongoing denuclearization talks between the United States and North Korea break down and economic sanctions continue to deprive Kim Jong-un from much needed hard currency. The United States obtains credible intelligence reports that North Korea has negotiated a deal to provide Iran with nuclear material and technology in exchange for oil and cash. Under the authority of a United Nations Security Council Resolution, the United States and its allies launch a maritime interdiction campaign against North Korean merchant ships believed to be carrying the materials. A North Korean ship is fired upon by the United States to disable it, boarded, and a load of centrifuges are discovered. In retaliation for the boarding, North Korea launches a nuclear EMP strike against the continental United States. Because of our current vulnerabilities, the strike is seen as the best use of its limited nuclear assets to cause the maximum damage to the United States.

In the case of an asymmetrical opponent, deterrence by punishment will continue to be an option, but, in the case where the survival of the adversary state is in question, the adversary may feel it has nothing to lose. Nevertheless, in this particular scenario, there is little doubt punishment would be used as retaliation. The only question would be the conventional or nuclear nature of the response. However, since the threat of punishment diminishes because of desperation and the decision-making calculus shifts to the possibility of inflicting maximum damage as a last act of defiance, punishment's deterrence effect is questionable in this case. Alex S. Wilner supports this idea and further suggests, that Cold War-style deterrence (deterrence by punishment) is not likely to be effective against potential aggressors from failing states or trans-national groups.²⁴ So while punishment is always an option after the fact, why take the chance with this reactive and questionable approach when a more proactive approach is available.

From a deterrence by denial perspective, we again refer back to Figure 1, where normally an asymmetrical adversary would probably fall into a Case 1 scenario because of its relative weakness compared to the United States. Therefore, it should be dissuaded from attack by a good defense. Even in the case of a failing state, a good to excellent defense and the associated low probability of success would arguably cause the adversary to rethink the situation and avoid the Case 3 scenario by attacking in some other way deemed more likely to succeed. In this notional scenario, North Korea decided to use an EMP attack on the United States because of the perceived unaddressed infrastructure vulnerabilities and the possibility of putting the entire population in the dark. Under these circumstances, this would be a very effective use of its limited nuclear stockpile. However, addressing our infrastructure vulnerabilities and clearly communicating our defensive efforts would change the

North Korean decision calculus. The North Koreans probably would not use their nuclear weapons for an EMP attack, and most likely decide to attack in another way. What exactly that other attack mode or target will be is one of the central problems inherent in deterrence by denial. It is simply impossible to defend and deny every target. The best one can do is to defend the highest value targets and I assert that our civilian infrastructure should be designated and defended as such. Therefore, for my particular research question, I again argue that defense and deterrence by denial are the more effective approaches.

Non-state Actor — Finally, turning to look at potential non-state adversaries, especially terrorists, we will analyze the following notional scenario. The Islamic State of Iraq and the Levant (ISIL) is able to use propaganda to radicalize key personnel in a nuclear-capable country and with its covert assistance steal a single nuclear weapon. In contemplating how to best use the weapon, the leaders conclude that attempting to smuggle it into the United States for use is too risky. They decide to use a SCUD missile fired from a shipping barge just off the coast of the United States to deliver the weapon. Additionally, they rationalize that while attacking a single city directly would inflict tremendous damage, using an air burst is more effective because it will devastate the entire continental United States' electrical infrastructure because of its current extreme vulnerability. ISIL sleeper cells across the entire country will also be activated to take advantage of the resulting social unrest spreading the uncertainty and panic across the entire nation.

This analysis of deterrence against non-state adversaries is the focus of the Fourth Wave of nuclear deterrence theory. Wilner and Jeffrey Knopf, two prominent Fourth Wave scholars, discuss deterrence for these types of actors and while they both concur that deterrence is still applicable, several aspects must be modified. Both agree that in this type of scenario, deterrence by punishment becomes much more problematic. First, non-state actors and terrorists many times are more focused on the potential benefits of the operation than the costs. Additionally, if punishment is to be applied, there is also still considerable uncertainty about what kind of threatened response is most appropriate because deterrence by punishment requires knowing who the aggressors are and what they value in order to be effective.

Wilner argues that deterrence theory can still be applied to non-state actors, but suggests a much broader definition of deterrence to include denial, defense, and mitigation. From this perspective, making preparations to manage the effects of an EMP attack is critical to reducing the potential benefits to bolster deterrence by denying the aggressor the desired negative effects they seek. From a deterrence by denial perspective, we again refer back to Figure 1, where non-state adversaries would probably fall into a Case 1 or 2 scenario and be dissuaded from attack by a good to excellent defense. Since in this scenario the non-state actor only has a single nuclear weapon, deterrence by denial would be very powerful, because that group would not want to waste its only weapon on an EMP attack that would have little effect. Even if the terrorists fall into a Case 3 scenario where they will carry out their attack in the face of a near perfect defense, deterrence by denial is still beneficial. The logic being that if an attack is inevitable, defense at the very least, minimizes the negative consequence of the attack.

— Conclusion —

Using Davis's cognitive model, I have argued that deterrence by denial is the most effective deterrence approach for preventing a limited nuclear EMP attack against the United States for three main reasons. First, deterrence by punishment relies heavily on many assumptions such as the validity of the rational actor model, speculating on what the potential adversaries value, their perceptions, risk tolerance, decision style and emotional state.²⁵ These pesky deterrence by punishment issues can be eliminated in this special case by focusing on deterrence by denial in the form of pure defense, which doesn't rely as heavily on understanding the complete psychology of the enemy. Increased resiliency for the civilian power grid is strictly technical in nature and it should be easier to credibly signal that our vulnerabilities in this area have been reduced or eliminated and preclude potential adversaries from seriously considering this option. Second, deterrence by denial is proactive versus reactive. In our special case, a good to excellent defense precludes the limited nuclear EMP attack and avoids the necessity to risk escalation in a retaliatory action. Finally, deterrence by denial in this particular case is the more robust option. It provides a complement to deterrence by punishment when the two approaches are to be applied simultaneously. Also, the defense and deterrence by denial approach has additional benefits above and beyond deterrence, such as protection against natural disasters including solar flares or other weather events. Deterrence by denial in this narrow scope of preventing a limited nuclear EMP attack on the United States is clearly preferable. Putting up a strong and obvious defense through increased resiliency in the civilian infrastructure not only protects our population from being left in the dark, but it also sends a clear and unambiguous message to potential peer aggressors that they will accrue no benefits from their efforts.

— Recommendations —

To fully implement a deterrence by denial effort, decisive government leadership in a public-private partnership is needed to foster improved transparency, set and enforce federal resiliency standards and signal to any potential adversaries that our civilian infrastructure has been updated to withstand the perilous threat of an EMP attack. Some might argue that private enterprise always does a better job and that government involvement only means overly bureaucratic standards and regulations, higher costs, and often solutions that are worse than the problems they were intended to correct. In certain areas, I tend to agree, but in areas extremely technical in nature, where the consequences of failure are beyond disastrous, and where there is little monetary incentive for action, the United States government may be the only entity that can effectively get the job done. This is definitely one of those areas.

First, the effects of a nuclear EMP and the protective measures needed in the civilian infrastructure are extremely technical in nature. Additionally, although many of the particular details on the potential consequences of these effects are classified, we know they can be devastating. Finally, due to the distributed, private, and competitive nature of the American electrical enterprise, there is little financial incentive to invest in resilience improvements against this low probability threat. These three circumstances combined preclude private enterprise

from leading this effort and reinforces the need for government leadership in a public-private partnership to meet the EMP attack threat.

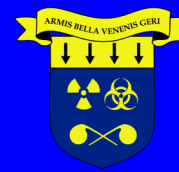
Government leadership needs to start with the designation of a single leader. A leader to focus and bring order to the current fragmented, incomplete, and under-resourced efforts. In a 2017 *Report to Congress*, some of our nation's top experts in this area concurred stating, "The single most important action that requires immediate action to advance the U.S. Security and Survivability is that the President establish an Executive Agent with the authority, accountability, and resources to manage U.S. national infrastructure protection and defense against the existential EMP threat." Only through the designation of an executive agent will this effort have any hope of moving past admiring the problem and get down to the tough business of protecting our civilian infrastructure from the threats of an EMP.

More government transparency is another key area needing improvement. Currently much of what is known about the potential EMP effects to our national infrastructure is extrapolated from classified computer models, and thus, is difficult to share with industry. This difficulty can and must be overcome because the foundation for preparedness against this EMP threat has to be transparent sharing of relevant information between the government and private utilities. This has been the focus of a 2016 joint effort between the Department of Energy and the Electric Power Research Institute to establish a common public-private EMP resilience strategy. This effort seeks to establish a common framework with consistent goals and objectives to guide government and industry activities.

Along these lines, the establishment of federal infrastructure resilience standards should be a top priority. Established and codified standards will not only guide industry investment, but also support a deterrence by denial strategy against any potential adversaries. The thought here is that if potential adversaries know the infrastructure is resilient, then they will probably decide against this type of attack. Just as important, federal standards will mandate investments in resilience that may not happen otherwise because of the competitive nature of this business sector. The good news here is that experts conclude that "protecting and defending the national electric grid and other critical infrastructure from an EMP attack could be accomplished at reasonable cost and minimal disruption."

There is no doubt that Americans have become accustomed to their technology-enhanced lifestyle. In fact, our society has become so dependent on technology that in its absence we run the real risk of a doomsday struggle for survival. Faced with potential adversaries who might try to leverage this vulnerability, we must move beyond admiring the problem and designate a leader, an executive agent, who has the authority and the accountability to take concrete actions to mitigate these vulnerabilities. The agent must be someone who can foster improved transparency and set and enforce federal standards that result in an updated civilian infrastructure to withstand the perilous threat of an EMP attack.

The mission of the U.S. Air Force Center for Strategic Deterrence Studies is to develop Air Force, DoD, and other USG leaders to advance the state of knowledge, policy, and practices within strategic defense issues involving nuclear, biological, and chemical weapons



The Trinity Site Papers present key discussions, ideas, and conclusions that are directly relevant to developing defense policy and strategy relating to countering weapons of mass destruction and developing the nuclear enterprise.

The opinions, conclusions, and recommendations expressed or implied in this article are those of the author and do not necessarily reflect the views of the Air University, Air Force, or Department of Defense.



— Notes —

1. William R. Forstchen, *One Second After*, (New York: Forge, 2009).
2. Aug. 22, 2018, Headquarters, United States Air Force/ A10 Memorandum for Air University Commander, Subject: AY19 Deterrence Research Topics
3. Jeffrey W. Knopf, “The Fourth Wave in Deterrence Research,” *Contemporary Security Policy* 31, No. 1 (2010); Wes A. Mitchell, “The Case for Deterrence by Denial,” *The American Interest*, Aug. 3, 2017; John K. Warden, “Limited Nuclear War: The 21st Century Challenge for the United States,” *Livermore Papers on Global Security*, No. 4 (July 2018); Alex S. Wilner, “Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism,” *The Journal of Strategic Studies*, 34:1 (2011), 3-37.
4. Michael, Quinlan, “Deterrence and Deterrability,” *Contemporary Security Policy* 25/1 (April 2004), 11.
5. Thomas Schelling, *The Strategy of Conflict* (Cambridge, Mass.: Harvard UP 1960), 9, an oft-cited definition presenting deterrence as “persuading a potential enemy that he should in his own interest avoid certain courses of activity.”
6. Alex S. Wilner, “Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism,” *The Journal of Strategic Studies*, 34:1 (2011), 5.
7. Thomas Schelling, *Arms and Influence*, 23.
8. Henry Sokolski, “Getting MAD: Nuclear Mutual Assured Destruction, Its Origins and Practice,” November 2004. Accessed Jan. 20, 2019. <http://strategicstudiesinstitute.army.mil/pdffiles/PUB585.pdf>.
9. Wes A. Mitchell, “The Case for Deterrence by Denial,” *The American Interest*, Aug. 3, 2017, www.the-american-interest.com/2015/08/12/the-case-for-deterrence-by-denial/
10. John K. Warden, “Limited Nuclear War: The 21st Century Challenge for the United States,” *Livermore Papers on Global Security*, No. 4 (July 2018)
11. Ibid.
12. Dennis Bodson, “Electromagnetic Pulse and the Radio Amateur,” *QST* September 1986: 22-26. <http://www.arrl.org/tis/info/pdf/88615.pdf>.
13. George Jacobs, *The NEW Shortwave Propagation Handbook*, Hicksville, N.Y., CQ Communications, Inc. 1995.
14. “Assessing the Threat from Electromagnetic Pulse (EMP), Volume 1: Executive Report.” *DTIC Online*, www.dtic.mil/docs/citations/AD1051492.
15. Barnes, 1994, Bodson, 1986, Kindt, 2006, and TM 5-690. These articles describe a variety of commercially available EMP transient-protection devices such as coaxial line suppressors, miniature gas-tube surge protectors, and metal oxide varistors that can be used in grounding, bonding, and shielding applications.
16. Debra K. Rose, (2011), “Only in the Mind of the Enemy: Can Deterrence Effectiveness be Measured?” Author indicates no direct measurement of deterrence is possible and proposes using intelligence indicators to provide feedback for indirectly measuring effectiveness.
17. P. Davis, (2018). “Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of Adversary to Inform Strategy.” [online] RAND.org. Available at: www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RANDWR1027.pdf [Accessed Nov. 29, 2018]. The RAND policy is that working papers can be quoted and cited without permission of the author, provided the source is clearly referred to as a working paper.
18. This approach is similar to Mahnken’s chapter in *On Limited Nuclear War* and is intended to help the reader step through the logic of the pros/cons of challenge by punishment or denial.
19. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, February 1999), 145-146. Authors advocate going beyond traditional boundaries of warfare using unrestricted strikes on a superior adversary’s critical nodes to include civilian infrastructure that will cause social panic, street riots, and internal political crisis.
20. “2018 - United States Department of Defense, Nuclear Posture Review,” accessed Jan. 22, 2019.
21. Stephen J. Cimbala, *The Past and Future of Nuclear Deterrence*, Westport, Conn.: Praeger, 1998.
22. “Fact Sheet: Increasing Transparency in the U.S. Nuclear Weapons Stockpile,” (Washington, D.C.: Department of Defense, May 3, 2010), Accessed Jan. 22, 2019. <https://fas.org/sgp/othergov/dod/stockpile.pdf>.

— Notes (Continued) —

23. “Assessing the Threat from Electromagnetic Pulse (EMP). Volume 1: Executive Report.” DTIC Online, www.dtic.mil/docs/citations/AD1051492.

24. Alex S. Wilner, “Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism,” *The Journal of Strategic Studies*, 34:1 (2011), 3-37.

25. Arguably, the United States does not understand some current adversaries, such as North Korea and Iran, as well as it understood the Soviet Union. This makes it harder to know what to “hold at risk” in order to deter those adversaries.