NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SOLID-STATE HIGH POWER RADIO FREQUENCY DIRECTED ENERGY SYSTEMS IN SUPPORT OF USMC FORCE PROTECTION OPERATIONS

by

Michael D. Simon

June 2015

Thesis Advisor: Raymond Buettner
Co-Advisor: Jon Alt

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
SOLID-STATE HIGH POWER RADIO FREQUENCY DIRECTED ENERGY SYSTEMS IN SUPPORT OF USMC FORCE PROTECTION OPERATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Michael D. Simon

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Service members are often vulnerable conducting entry control point operations in support of force or critical infrastructure protection. Historical evidence and tests from emerging technology suggest that solid-state high power radio frequency directed energy systems emit enough power to disrupt vehicle electronic systems without costly collateral damage to people or property. This thesis builds on previous research toward adding non-lethal tools, in the form of directed energy systems, for service members to utilize as part of entry control points. A combination of literature review, limited modelling, and field experimentation is used to explore whether directed energy is a viable, non-lethal tool for USMC entry control points. After detailed descriptions of force protection, directed energy, and a thorough system of systems analysis of the contemporary operating environment, this thesis offers an example of an entry control point augmented with a high-power radio frequency array. Further, this research recommends exploration of additional uses for this type of directed energy including counter-piracy and electronic ambush operations that utilize ground, air, and sea-based platforms.

14. SUBJECT TERMS
high power radio frequency, suicide vehicle-borne improvised explosive device, directed energy, force protection, entry control point, vehicle control point, solid state, system of systems analysis

15. NUMBER OF PAGES 115

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SOLID-STATE HIGH POWER RADIO FREQUENCY DIRECTED ENERGY SYSTEMS IN SUPPORT OF USMC FORCE PROTECTION OPERATIONS

Michael D. Simon
Major, United States Marine Corps
B.S., United States Naval Academy, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2015

Author: Michael D. Simon

Approved by: Dr. Raymond Buettner
Thesis Advisor

LTC Jon Alt
Co-Advisor

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Service members are often vulnerable conducting entry control point operations in support of force or critical infrastructure protection. Historical evidence and tests from emerging technology suggest that solid-state high power radio frequency directed energy systems emit enough power to disrupt vehicle electronic systems without costly collateral damage to people or property. This thesis builds on previous research toward adding non-lethal tools, in the form of directed energy systems, for service members to utilize as part of entry control points. A combination of literature review, limited modelling, and field experimentation is used to explore whether directed energy is a viable, non-lethal tool for USMC entry control points. After detailed descriptions of force protection, directed energy, and a thorough system of systems analysis of the contemporary operating environment, this thesis offers an example of an entry control point augmented with a high-power radio frequency array. Further, this research recommends exploration of additional uses for this type of directed energy including counter-piracy and electronic ambush operations that utilize ground, air, and sea-based platforms.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C2	Command and Control
COE	Contemporary Operating Environment
COIL	Chemical, Oxygen, Iodine Laser
COIN	Counter-Insurgency
CPB	Charged Particle Beam
DE	Directed Energy
DEW	Directed Energy Weapon
ECP/VCP	Entry Control Point/Vehicle Control Point
EF 21	Expeditionary Force 21
EM	Electromagnetic
EMP	Electromagnetic Pulse
EMS	Electromagnetic Spectrum
FEL	Free Electron Laser
HPM	High Power Microwave
HPRF	High Power Radio Frequency
IED	Improvised Explosive Device
I MEF	First Marine Expeditionary Force
Laser	Light Amplification by the Stimulated Emission of Radiation
LaWS	Laser Weapon System
MCPP	Marine Corps Planning Process
MDMP	Military Decision Making Process
MIRACL	Mid-Infrared Chemical Laser
NAVAIR	Naval Air Systems Command
NBER	National Bureau of Economic Researchers
PSI	Pounds per Square Inch
Radar	Radio Detection and Ranging
RF	Radio Frequency
RFVS	Radio Frequency Vehicle Stopper
ROE	Rules of Engagement
SoS	Systems of Systems
SVBIED	Suicide Vehicle-borne Improvised Explosive Device
USMC	United States Marine Corps

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Many thanks are in order for Dr. Buettner, LTC Alt, and the directed energy team at NAVAIR.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CONFLICT IN THE INFORMATION AGE

The information age presents new challenges for military leaders as the threats and technologies have grown in complexity, scope, and lethality. Only bold, innovative solutions that seek to create new operational paradigms will be able to combat the age's emerging threats. Advances in processor technology and the proliferation of cyber-attacks have changed the ever-expanding landscape of the modern battlefield. Even in everyday life, most usable infrastructure including vehicles, phones, and many personal electronic devices involve powerful computer processing units that have turned simple mechanical or analog systems into sophisticated electronic systems. Those advances have translated into the lethal battlefields of modern warfare, where uniformed and terrorist units apply deadly force while using equipment that could hardly have been imagined some years ago. Large, well-funded countries may have a monopoly on many systems that involve stealth technology and satellite aided munitions. However, non-state actors have effectively used precision small arms weapons, drones and even modern anti-armor missile systems like those Hezbollah employed against Israel in 2006.[1]

As with the previous example, both enemy and friendly actors with access to advanced weapons have successfully leveraged the electromagnetic spectrum (EMS) in the form of various directed energy (DE) systems. It is no secret that the United States and other nations are capable of jamming communications, targeting, or even destroying targets by directing energy through the EMS. It would be false to assume that the United States is the only country exploring such systems. In fact, Ira Merritt, while Chief of Concepts Identification and Applications Analysis Division at the Army's Space and Missile Defense Command, testified before Congress that there is strong evidence that Ukrainian, Swedish, French, and Australian governments are actively investigating

1 Matt Matthews, *We were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), 18.

technology focused on radio frequency (RF) DE systems.[2] Non-state enemy belligerents, too, have employed weapons that rely on working knowledge of the EMS. Merritt also testified that effective homemade versions of RF weapons could be made for as little as $5,000.[3] This testimony was given in 1998, and one could surmise that the fabrication costs have since decreased while effectiveness has increased. Evidence of this trend is that radio frequency detonation devices and even infrared triggers have all been found on modern battlefields.

Adding to this dilemma, new information mediums such as social media have contributed to the information age's wicked problem. Nefarious actors from state and non-state origins have placed greater emphasis on utilizing these new tools to create and control a narrative that is beneficial to their larger cause. It has become commonplace for attacks or messages from enemy personnel to be published via the Internet within minutes of an influential event. In other words, spreading messages or information has become easier and extremely effective. Many have noticed that groups as new as the Islamic State in Iraq and Syria (ISIS) have been just as effective at using social media as they are at committing atrocities throughout the Levant. Numerous intelligence agencies have marveled at the extremist group's adept implementation of state-of-the-art videos, ground images shot from drones, and multilingual use of Twitter to recruit as many as 2,000 Westerners and countless Middle-Easterners to their cause.[4]

As the enemy continues to export their messages of spectacular attacks through these new conduits, it is evident that they have fully assessed the importance of a stout information operations campaign combined with their offensive campaign. Military planners and national leaders must create methods to combat those campaigns in addition to more traditional military operations if they want to see the United States maintain dominance on modern battlefields. Unfortunately, military organization creates a long

2 William McCarthy, *Directed Energy and Fleet Defense* (Air University Maxwell Air Force Base Montgomery, AL: Center for Strategy and Technology, 2000), 12.

3 Ibid.

4 Scott Shane and Ben Hubbard, "ISIS Displaying a Deft Command of Varied-Media," *New York Times*, August 30, 2014. http://www.nytimes.com/2014/08/31/world/middleeast/isis-displaying-a-deft-command-of-varied-media.html?_r=0.

decision making process relative to what the enemy can achieve. Deep staff structures, nebulous command relationships, and highly compartmented authority result in friendly messages that are strictly reactionary. Some though, have decided to take a different approach. Instead of engaging solely on the narrative battle, they have focused on methods that prevent the enemy event from happening in the first place. Before discussing potential solutions, it is more appropriate to dissect a contemporary threat that is at the forefront the overall issue.

B. DEMONSTRATING A PROBLEM

Thus, one could submit that the new millennium has been most profoundly shaped by one new weapon. The suicide vehicle-borne improvised explosive device (SVBIED) has taken many forms and has also proven to be an extremely deadly yet relatively cheap method to attack powerful opponents. Explosive laden vehicles have emerged in three of the world's domains to include sea, air and land. Many times when these SVBIEDs have been used, they have inflicted massive damage and shown that even though the United States is a superpower, it is vulnerable to spectacular attacks. Both, the U.S. Army and Marine Corps has stated that these weapons pose a persistent and devastating threat that impacts unit operations, U.S. policy and public perception.[5]

The first large incident of this century occurred when a small vessel driven by a couple fanatics plunged its explosive payload into the hull of the *USS Cole* (DDG 67) outside of Yemen. Determination, courage and personal heroism saved the Cole from sinking to the bottom of the harbor but the image of one of the most advanced warships on the planet being carried back to the United States reverberated throughout the terror world. Before then, the idea that a few "civilians" willing to give up their lives could neutralize such an immense platform as a U.S. Navy Destroyer was relatively unheard of. As catastrophic as the *Cole* bombing was, it would only foreshadow and even more grotesque SVBIED attack on American interests. The events of September 11, 2001, demonstrated how fewer than two dozen people could transform a few hijacked jetliners

5 Department of the Army, *Improvised Explosive Device Defeat* (FMI 3–34.119 and MCIP 3–17.01) (Washington, DC: Headquarters Department of the Army, U.S. Marine Corps, 2005), v.

into precision cruise missiles. Those SVBIEDs killed more than 3,000 people between New York City, Washington, DC, and rural Pennsylvania, and had part of the world in tears while another part danced in the streets cheering.[6]

The response sent U.S. servicemen to war on two major fronts, in Iraq and Afghanistan. Those theaters of war saw the expansion of SVBIEDs for use attacking dismounted troops with cars, trucks, and motorcycles rigged with bombs. Enemy actors could drive among a relatively passive population to hide in plain sight. The troops on the ground, with almost no indication as to the danger near them could only treat each vehicle as a non-combatant until it proved otherwise. In most instances, the time left to act against a vehicle that revealed itself as a threat was almost zero. In a sobering speech, General John Kelly immortalized two young Marines that experienced one of those moments while serving in Iraq's volatile Anbar Province.

> Two years ago when I was the Commander of all U.S. and Iraqi forces, in fact, the 22nd of April 2008, two Marine infantry battalions, 1/9 "The Walking Dead," and 2/8 were switching out in Ramadi. Two Marines, one from each battalion, were assuming the watch together at the entrance gate of an outpost that contained a makeshift barracks housing 50 Marines. The same broken down ramshackle building was also home to 100 Iraqi police, also my men and our allies in the fight against the terrorists in Ramadi, a city until recently the most dangerous city on earth and owned by Al Qaeda…The mission orders they received from the sergeant squad leader I am sure went something like: "Okay you two clowns, stand this post and let no unauthorized personnel or vehicles pass." "You clear?" They then relieved two other Marines on watch and took up their post at the entry control point of Joint Security Station Nasser, in the Sophia section of Ramadi, al Anbar, Iraq. A few minutes later a large blue truck turned down the alley way—perhaps 60–70 yards in length—and sped its way through the serpentine of concrete jersey walls. The truck stopped just short of where the two were posted and detonated, killing them both catastrophically. Twenty-four brick masonry houses were damaged or destroyed. A mosque 100 yards away collapsed. The truck's engine came to rest two hundred yards away knocking most of a house down before it stopped. Our explosive experts reckoned the blast was made of 2,000

6 "Muslims Celebrating 9/11," YouTube video, 0:38, from a report televised by Fox News on September 12, 2001, posted by "nccanuk," April 12, 2008, www.youtube.com/watch?v=Rmo64fcvKs0.

> pounds of explosives. Two died, and because these two young infantrymen didn't have it in their DNA to run from danger, they saved 150 of their Iraqi and American brothers-in-arms…It took exactly six seconds from when the truck entered the alley until it detonated…You can watch the last six seconds of their young lives. Putting myself in their heads I supposed it took about a second for the two Marines to separately come to the same conclusion about what was going on once the truck came into their view at the far end of the alley. Exactly no time to talk it over, or call the sergeant to ask what they should do. Only enough time to take half an instant and think about what the sergeant told them to do only a few minutes before: " … let no unauthorized personnel or vehicles pass." The two Marines had about five seconds left to live. It took maybe another two seconds for them to present their weapons, take aim, and open up. By this time the truck was half-way through the barriers and gaining speed the whole time…They had three seconds left to live…For about two seconds more, the recording shows the Marines' weapons firing non-stop…the truck's windshield exploding into shards of glass as their rounds take it apart and tore in to the body of the son-of-a-bitch who is trying to get past them to kill their brothers—American and Iraqi—bedded down in the barracks totally unaware of the fact that their lives at that moment depended entirely on two Marines standing their ground. If they had been aware, they would have known they were safe … because two Marines stood between them and a crazed suicide bomber. The recording shows the truck careening to a stop immediately in front of the two Marines. In all of the instantaneous violence Yale and Haerter never hesitated. By all reports and by the recording, they never stepped back. They never even started to step aside. They never even shifted their weight. With their feet spread shoulder width apart, they leaned into the danger, firing as fast as they could work their weapons. They had only one second left to live. The truck explodes. The camera goes blank. Two young men go to their God. Six seconds.[7]

The effects of these weapons are startling. SVBIEDs along with other types of IEDs during the wars in Iraq and Afghanistan have taken an undeniable human toll. Online organizations and newspapers have documented that together, they have caused more than 1,400 American deaths in Afghanistan[8] and more than 2,660 in Iraq.[9] What is more, according to a USA Today report, the Pentagon estimates that the Department of

7 John Kelly, "Untitled" (speech, American Legion Memorial Day Address in St. Louis, MO, November 13, 2010).

8 "IED Fatalities," iCasualties.org, May 7, 2015, http://www.icasualties.org.

9 Mary Hadar, Whitney Fetterhoff, and Magda Jean-Louis, "Faces of the Fallen," *The Washington Post*. May 7, 2015.

Defense has spent upward of $75 billion on new equipment, specialized units, and infrastructure against the deadly weapon systems that plagued U.S. servicemen in the war on terror.[10] The enemy's use of these weapons has obviously proven effective in the amount of resources, in blood and treasure, spent to combat them.

Observers will argue that vehicles used in suicide attempts have been used against the United States in the past. Indeed, there exist some similarities in historical examples of suicides used in combat but there are striking differences as well. As naval battles in the Pacific raged on during World War II, the Japanese shocked the world's conscience by ordering fighter pilots to forgo typical aerial combat tactics and plunge their aircraft into American aircraft carriers instead. The "kamikaze" attacks resulted in towering infernos on U.S. warships with crews scrambling to save the ship and their fellow shipmates. The kamikaze tactic may seem monstrous but, in the Japanese case, it is rooted in the country's culture. The legend of the Divine Wind involves two massive tropical storms that scuttled Kublia Khan's fleet en route to invading Japan in 1274 and again in 1281.[11] Similar to the Mongol threat centuries ago, the U.S. fleet sailed directly toward the Japanese islands and the people reacted by enacting the spirit of a miracle similar to the Divine Wind. The pilots summoned the courage from the Divine Wind to commit their lives to destroy the U.S. fleet. This time, the destruction would be in the form of suicide fighter planes rather than meteorological phenomena.

Similarly, many modern suicide attacks, whether hijacker, SVBIED, et cetera are rooted in culture. Religious extremists frequently speak about the honor of being martyred in the name of Allah before their attacks. The Japanese motivation stemmed from the lore of a 700-plus year weather event while today's suicide bombers' motivation originates from a perverted interpretation of Islam's holy book. The difference in the two examples is the goals of the attacks. The Kamikaze pilots struck the U.S. carriers to sink the fleet's most high-valued asset, to destroy the airplanes aboard, and force the U.S. military into capitulation and defeat. In contrast, the SVBIED and other suicide attacks

10 Greg Zaroya. "How the IED Changed the U.S. Military." *USA Today*, December 18, 2013.

11 Rikihei Inoguchi and Tadashi Nakajima, *"The Divine Wind; Japan's Kamikaze Force in World War II"* (Annapolis, MD: United States Naval Academy Institute, 1958), 213.

conducted today are not meant to directly defeat the U.S. military. Rather, they are a part of a larger information campaign aimed at fear, recruitment, and fund raising to continue jihad not against a military force but unarmed civilians as well. One surviving kamikaze pilot, Atsushi Takutsaka, saw little similarity with the suicide tactics of Japan and those of terrorists when he said, "How could they possibly be thought of as in any way being related when one is a non-discriminatory attack on citizens and the other is a military strategy targeting battleships!"[12] His comments highlight the fact that kamikaze pilots sought to keep the conflict between military foes while terrorist actors' use of SVBIEDs does not exclusively target military targets.

Even as the campaigns in Iraq and Afghanistan wind down, military leaders know that SVBIEDs will be on modern battlefields for many years to come. The Marine Corps' First Marine Expeditionary Force (I MEF) made countering these devices an official focus of effort when it released its Science and Technology Priorities list. It states that resources should be spent to, "create a capability to detect and neutralize suicide bombers including person borne explosive hazard, vehicle borne explosive hazard, and suicide boats."[13] There are too many methods that could help fulfill that priority to discuss in one cohesive paper so this attempts to focus on just one possibility. Before that method is fully introduced, it may prove helpful to review the information environment.

C. DEFINING THE INFORMATION ENVIRONMENT

Before one can define the information environment, it is appropriate to briefly describe the information age. One accepted interpretation is that the information age is the "proliferation of emerging information and communication technologies and the capabilities that those technologies provide and will provide humankind to overcome the barriers imposed on communications by time, distance, and location and the limits and

12 Ryo Manabe and Atsushi Takatsuka, "Divine Wind: An Interview with Atsushi Takutsuka," *The Cabinet*, Winter 2005/2006, no. 20 (2006): 1.

13 John Toolan, I Marine Expeditionary Force Science and Technologies Priorities (Camp Pendleton, CA: I MEF, 2013), 1.

constraints inherent in human capacities to process information and make decisions."[14] Indeed, it is quite a mouthful not only to speak but proves difficult to wrap one's head around as well. Because it is a rather difficult idea to completely understand, the military created a concept that is more manageable: the information environment. The information environment is broken down into three separate dimensions—the informational, cognitive, and physical. For completeness, the first two will be briefly described while the last will be discussed with more depth, as it will be more salient for the remainder of this argument.

1. Information Dimension

The informational dimension can be thought of as the data-centric dimension. According to Joint Publication 3–13 (JP-13), the informational dimension "encompasses where and how information is collected, processed, stored, disseminated, and protected."[15] Put even more simply, the informational dimension is the content and flow of information between parties or among people. Data on a carrier frequency or the code inside a computer is in the informational dimension. Further, the processes that govern how that information moves from one place to another fall within the informational dimension as well.

2. Cognitive Dimension

The cognitive dimension is considered to be the most important dimension within the information environment. It may be helpful to think of the cognitive dimension as the human dimension instead. The joint publication defines this dimension as "the dimension that encompasses the minds of those who transmit, receive, and respond to or act on information."[16] One can see why many consider this to be important as it is central to the decision making process. Keep in mind, this dimension involves everything that goes into

14 M. Alberts, *The Information Age: An Anthology on its Impact and Consequences* (Washington, DC: Command and Control Research Program, 1997), 2, http://www.DODccrp.org/files/Alberts_Anthology_I.pdf.

15 Department of Defense, *Information Operations* (JP 3–13) (Washington, DC: Joint Staff, 2014), I-3.

16 Ibid.

the decision including an individual's culture, experiences, morals, vulnerabilities, etc. Many times, it is the cognitive dimension that is targeted because it is the most influential in military campaigns.

3. Physical Dimension

The physical dimension is the arena that will be stressed for most of this thesis. It is considered to be the tangible part of the information environment. The physical dimension consists of "but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement."[17] One must not put too much emphasis on the word tangible as it may limit what the physical dimension actually encompasses. Instead, the focus should remain on the part of the definition that speaks to empirical measurement. For this reason, it is possible to classify the electromagnetic spectrum (EMS) in the physical dimension. The EMS can be empirically measured by frequency, wavelength and power. Moreover, the EMS is often associated with some type of physical propagation device like an antenna or light source. Now, it should be easier to see how one can place the EMS in the physical dimension of the information environment.

D. USMC FOCUS ON EMS

The Marine Corps has recently recognized the importance of the EMS. The newest service level operating concept entitled "Expeditionary Force 21 (EF 21)" specifically mentions the EMS as a piece of the information environment that must be properly leveraged to ensure mission success across the range of military operations. In EF 21 it states, "freedom of action in cyberspace and the electromagnetic spectrum (EMS) is a key enabler to 21st century military operations."[18] It goes further to say "EMS

17 Ibid., I-2.

18 James Amos , *Expeditionary Force 21* (Washington, DC: United Stated Marine Corps, 2014), 35.

operations will be critical to mission success."[19] The Marine Corps' thinking in this area certainly shows how large of a role the EMS can play in future operations.

As a result of the document, numerous academic and military laboratories have taken the Corps' call to action seriously and began new experiments in earnest. The results have shown exciting progress in regards to advanced science but have yet to adequately match the scientific innovation with modern threats.

E. THESIS FRAMEWORK

Technologies advance everyday yet it is still difficult to apply many of those advances to military problems in a timely and feasible manner. In the case of SVBIEDs, blending concepts from EF 21, I MEF science and technology priorities, and emerging technology could prove to yield promising outcomes. As previously stated, military and private engineers have begun new experiments and improved existing technology. One field of study that has gained significant momentum recently has been focused on high power radio frequency (HPRF) directed energy (DE) systems aimed at disrupting potential SVBIEDs by non-kinetically disrupting the explosive laden vehicle before it reaches its target. Jumping directly to a conclusion would be premature when one considers this complex problem so a deeper analysis of the problem's entire system is required.

First, it is important to describe force protection operations that are similar to the one depicted in General Kelly's speech. Beyond the obvious portrayal of a deadly contemporary problem that needs to be addressed, it shows how dangerous entry control points and vehicle control points (ECP/VCP) can be. The devastating effects of SVBIEDs that target those ECP/VCPs is overly evident but a more thorough analysis of those effects is needed to make more accurate recommendations for possible system requirements.

Second, this thesis will discuss HPRF DE. Listing complicated formulas and modelling difficult physics concepts is not the goal. Instead the analysis will include an

[19] Ibid.

overview of existing DE systems in the U.S. arsenal and emerging technology that is salient to this research. The fact that the electronics involved have become much smaller, less expensive, and more reliable should be apparent. All of those things, in combination, allow for more flexible systems that the military is more apt to use in a wider variety of missions.

Next, a system of systems analysis will be completed to show how all the actors interact. The inspection will not only break down friendly, enemy and neutral actors according to their people/units, equipment and goals, it will identify physical places where they overlap. Those places should incur greater risk similar to the vignette about the two Marines in Iraq. That analysis, with the research concerning force protection and HPRF DE will lead into the development of system design requirements. The research will aim to define requirements and make recommendations for future tests and evaluations. Even during this relatively short, focused explanation it will be evident that utilizing HPRF in force protection operations can help defeat spectacular attacks and prevent enemy combatants from exploiting the opportunity to control and export a damaging narrative.

THIS PAGE INTENTIONALLY LEFT BLANK

II. FORCE PROTECTION

A. WARFIGHTING FUNCTIONS

Military operations consist of numerous separate functions that, when properly integrated together, maximize a unit's warfighting potential in regards to personnel and equipment. Together, those activities are commonly referred to as warfighting functions. Warfighting functions offer planners many advantages. When correctly applied, they increase a commander's capacity to coordinate, control, influence, and synchronize combat power against the enemy while protecting their own units. Planners consider six warfighting functions including Command and Control, Maneuver, Fires, Intelligence, Logistics, and Force Protection while they construct military operations. Even as this section will focus on force protection, it is worthwhile to understand the other five functions.

1. Command and Control

According to MCDP 1–0, Marine Corps Operations, command and control is "the exercise of authority and direction by a properly designated commander over assigned and attached forces to accomplish a mission."[20] As the overarching warfighting function, command and control is more than just arranging and tasking combat power in a battlespace. Command and control allows the commander to project influence over a force and then allow feedback during the operation. The feedback loop mechanism adds flexibility and enables fluid adaptation that is the hallmark of U.S. military operations. Some may incorrectly view command and control as simply as the commander imposing his will on subordinates. Rather, the publication makes it clear that command and control is a mutually supporting system where complementary commanding and controlling

20 United States Marine Corps. *Marine Corps Operations* (MCDP 1–0) (Washington, DC: Department of the Navy, 2011), B-1.

forces interact and make sound adjustments to meet continuously changing battlefield requirements.[21]

2. Maneuver

The next warfighting function to be described is maneuver. Official military dictionaries describe maneuver as "the employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy."[22] Maneuver supports the commander's concept of operation through a combination of distribution or concentration of power. Marine Corps philosophy expands the idea of maneuver to include actions in any dimension, whether it is temporal, psychological, or technological, to gain some advantage over an adversary.

3. Fires

Fires includes more than just the application of lethal force against a target. Instead, fire accounts for lethal and non-lethal measures to harass, suppress, neutralize, or destroy targets that disrupt, delay, limit, persuade, or influence enemy objectives.[23] Normally used in concert with maneuver, fires shape the battlespace for decisive actions that are favorable for friendly units. Effective fires plans coordinate the use of all types lethal weapons, non-lethal methods, and target acquisition systems.

4. Intelligence

Intelligence is vast set of capabilities that supports operations. Further, intelligence provides situational awareness regarding enemy strengths and weaknesses as well as assessments on battlefield effects from friendly or enemy actions. Robust intelligence plans are dynamic processes that aim to refine friendly understanding of the situation and provide accurate depictions of the operational environment.

---

21 Ibid.

22 Department of Defense, *Department of Defense Dictionary of Military and Associated Terms* (JP 1–02) (Washington, DC, Joint Force Development, 2015), 151.

23 United States Marine Corps, *MCDP 1–0*, B-2.

5. Logistics

According to Marine Corps doctrine, logistics encompasses all activities required to move and sustain military forces at the tactical, operational, and strategic levels.[24] For the most part, logistics include elements of arming, fueling, maintenance, transportation, supply, general engineering, and health services.

6. Force Protection

Force protection involves so many different elements that it is difficult to encapsulate in one definition. Each service provides a version of force protection to suit their needs but the Joint Chiefs of Staff offered a holistic approach to define this warfighting function. They defined force protection as "the security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, in all location and situations, accomplished through planned and integrated application of combating terrorisms, physical security, operations security, personal protective services, and supported by intelligence, counterintelligence, and other security programs."[25] Just from that definition, it is evident that force protection is a colossal undertaking. Force protection is not the mission but its importance is often neglected compared to the other warfighting functions.

B. FORCE PROTECTION IN THE CURRENT OPERATING ENVIRONMENT

Force protection remains a key facet to overall mission success but the threats have evolved during in the last few decades. Now, more than ever, force protection operations impact strategic, operational, and tactical goals. That is to say that poor force protection measures taken by small tactical units can have strategic impacts in an entire area of operation not only because of emerging threats but because of increasing U.S. intervention around the globe. The Defense Science Board concluded that intervention

24 Ibid., B-3.

25 Joint Chiefs of Staff, *Commander's Handbook for Antiterrorism Readiness* (CJCS Handbook 5260) (Washington, DC: CJCS), 20.

will increase because places like Somalia Afghanistan will impact the U.S. and its allies.[26] That conclusion forces some to surmise that force protection measures in areas similar to those listed are more important than ever.

Much of the force protection burden rests on tactical units as they will intermingle with new threats on a daily basis. Conventional attacks still pose risks but enemy forces now implement IEDs, car bombs, and other measures that minimize American technology and tactical prowess. The Task Force stated that traditional techniques of hunkering down cede initiative to the enemy and only undermine friendly efforts to interface with the populace.[27] They continued by stating that tactical unit force protection must take the war to the enemy and away from the local populace with all the physical and psychological means available.[28] Tactical units in force protection involve more than just military applications. Military, civilian, and government agencies all require force protection measures carried out by small, dedicated people to secure their installations or critical infrastructure. Examples exist that epitomize the importance of force protection across all three groups; military, civilian, and government.

1. Military Installation Attacks

U.S. military installations span the globe, varying in size, capacity, and scope. Some of the largest military sites house thousands of personnel from numerous units, while others burst at the seams with only a dozen or two service members inside. No matter the size or location of the military base, each one represents a target for enemy actors. The next section describes two instances of attacks on military sites. The attacks on the Marine Barracks in Beirut, Lebanon and *USS Cole* highlight times where enemy combatants exploit less than optimal force protection measures and deal huge blows to U.S. forces.

---

26 Defense Science Board Task Force, Force Protection in Urban and Unconventional Environments (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2006), 10.

27 Ibid., 11

28 Ibid., 13.

a. Attack against Marine Barracks, Beirut, Lebanon

Admiral Robert Long, in his report to a DOD Commission, described the early morning on 23 October 1983. On that morning, a single terrorist driving a Mercedes Benz truck rigged with 12,000 pounds of explosives destroyed the Battalion Landing Team headquarters building in the Marine Amphibious Unit compound at Beirut International Airport. "The truck drove over the barbed and concertina wire obstacle, passed between two Marine guard posts without being engaged by fire, entered an open gate…flattened the Sergeant of the Guard's sandbagged booth at the building's entrance, penetrated the lobby of the building and detonated while the majority of the occupant's slept."[29] The massive explosion caused the building to implode upon itself and kill 241 Marines, Sailors, and soldiers while wounding 100 more.

b. Attack on USS Cole

Sadly, devastating suicide attacks are not relegated to ground based installations. Water-borne threats have stuck military targets as well. Around noon on 12 October 2000, the *USS Cole* was mooring in the port of Aden. While the mighty U.S. warship moored, an explosive laden small boat detonated next to the Aegis Class destroyer. The blast tore a hole approximately 40 by 40 feet in the hull of the ship. Seventeen Sailors were killed with another 39 injured.[30]

These two attacks share similarities even while separated by nearly two decades and occurred in different domains. Both attacks specifically targeted U.S. military interests in contentious areas with suicide bombers. Attackers used few people to inflict serious damage on personnel and infrastructure. Lastly, the two attacks triggered a U.S. withdrawal as the Marines left Lebanon and the Cole had to be towed out of Aden. In this, it is obvious that the attacks aimed to score strategic enemy victories though tactical success exploiting force protection gaps. The previous examples highlight attacks on

29 Robert Long, Admiral, USN (Ret), Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983 (Washington, DC: Department of Defense, 1983), 33.

30 Norman Palomar, "Terrorism Strikes the U.S. Navy," *U.S. Naval Institute Proceedings* 126, no. 11 (November, 2000): 28.

military targets but civilian and government institutions are just as susceptible to terrorist activities.

2. Civilian and Government Infrastructure Attacks

Similar to military installations, buildings that house American civilian entities and government agencies are in almost every corner of the earth. In some cases, one building can hold many different agencies from both the public and private sectors, which is the case for both buildings described in the next section. The World Trade Center and Murrah Federal Building are prime examples of how vehicle-borne explosive devices pose significant threats against massive structures. Save some type of major natural disaster, both buildings seem indestructible because of their size and construction. Attackers though, found a way to slip huge amounts of explosives through force protection measures and inflict damage that is almost impossible to comprehend.

a. Attacks on World Trade Center, 1993 and 2001

The World Trade Center in New York City has been twice attacked using explosively rigged vehicles. The first attack in February 1993 represented the first major terrorist attack in the United States and resulted in six deaths and more than 1,000 injuries.[31] In this case, perpetrators parked a van loaded with 1,500 pounds of explosive in a parking deck underneath the building. The blast caused massive damage including opening a 5,000 square foot hole above the bomb, a 400 square foot crater two stories above the explosion, and nine massive steel beams damaged at ground zero.[32] Unfortunately, the 1993 attack would not be the last or worst attack on the World Trade Center. Seven-and-a-half years later, two hijacked airplanes flew directly into the two main towers causing the structures to collapse and kill thousands of occupants. The two attacks share some characteristics of the attacks on military interests. Both attacks focused on small risk compared to large rewards for the attackers. The attacks also struck at a cornerstone American ideals, the first being U.S. military power projected across the

31 Lim, R. Augustus, *Anti Terrorism and Force Protection Applications in Facilities* (Gainsville, FL: University of Florida Department of Civil and Coastal Engineering, 2003), 37.

32 Ibid., 38.

globe and the second being the epicenter of American capitalism. Again, these attacks show how the enemy uses multiple domains to exploit vulnerabilities in force protection. In this case, the attacks occurred from the land and air. Government agencies share in the misfortune of terrorist attacks too.

b. Attack on Murrah Federal Building

The 1993 attack on the World Trade Center was the first large terrorist attack on U.S. soil, but the April 1995 attack on the Alfred P. Murrah Federal Building was the first attack carried out by domestic terrorists. From a truck bomb loaded with 4,000 pounds of explosives, the attack killed 168 people and injured an additional 500 from the Social Security Agency, Veterans Administration, and Drug Enforcement Agency.[33] Because the truck that detonated was parked only ten feet away from the building, the substantial blast destroyed most of the building and created a crater 28 feet across and more than 6 feet deep.[34] The close proximity of the weapon to the target building shows the difficulty some government sites have in adding enough standoff distance from potential threats.

3. Common Themes

It is evident that military, civilian, and government sites are targets and under constant threat from domestic and international terrorist actors. Each of the attacks above involves asymmetric attacks that are difficult to predict and even more difficult to counter. The proliferation of these attacks compels planners to account for their possibility. Not only must prevalent, ground-based attacks be thwarted, but air and sea-borne attacks as well. Combatting the entire panoply of terrorist attacks involves measures far beyond the scope of this thesis. For this, the ground based threats will remain the focus of effort. The ground based attacks identified all used some type of vehicle-borne explosive with some being suicide missions and others not. Even though the explosive vehicle may or may not have been manned, it did navigate through some type of ECP/VCP to reach their targets. The ECP/VCP remains a vulnerability that the

33 John Prendergast, "Oklahoma City Aftermath," *Civil Engineering* (October 1995), 42.

34 Lim, *Anti Terrorism and Force Protection Applications in Facilities*, 41.

enemy exploits to achieve their objectives. If ECP/VCPs characterize a vulnerability, it is prudent that planners analyze those sites in order to pose solutions to their deficiencies.

C. ENTRY CONTROL POINTS AND VEHICLE CONTROL POINTS

Many times, the first line of physical defense for a unit, base, or piece of critical infrastructure is an ECP/VCP. ECP/VCPs are two types of access control in force protection operations. Concerning entry into a friendly site, ECP/VCPs aim to identify and screen personnel, vehicles, and materials to ensure that only authorized personnel gain entry.[35] Tactical operations among a local populace are a little different. In those cases, the control points should control or maintain the integrity of borders and roadways as well as protect the citizens from criminals and terrorists, and to interdict the flow of contraband and weapons that are injurious to the welfare of citizens.[36] Many think ECP/VCPs amount to little more than a few cones and barriers in front of a guard checking identification credentials. In fact, for correctly constructed ECP/VCPS, much more thought and effort is exerted.

ECP/VCPs exist in a multitude of sizes and shapes. Local geography, time, and resources drive most of aspects of their construction. While each one may look completely dissimilar and be serving a different mission, some characteristics are shared. The next section will discuss the functional zones of an ECP/VCP and then relate those with a few examples that vary in size and scope.

1. Functional Zones

No matter what the mission is, an ECP/VCP should encompass four distinct functional zones that each serves specific purposes. These four zones include the approach zone, access control zone, response zone, and safety zone.[37] Differing threats

35 JFOB Quick Reaction Test, *JFOB Force Protection Handbook* (Alexandria, VA: Office of the Secretary of Defense, Joint Test and Evaluation, 2005), 6–22.

36 Afghan Police Training Mission, *Border Security Company 18 Standard Operating Procedures* (BSC-18, 2011), 2.

37 JFOB Quick Reaction Test, *JFOB Force Protection Handbook*, 6–34.

require adjustments to each zone but all of them must be present in some form to achieve effective entry control and force protection.

a. Approach Zone

The approach zone is the first zone a vehicle will encounter in an ECP/VCP and it serves a few necessary functions. First, the approach zone alerts vehicles to the control point ahead using signs or means. Next, small obstacles slow incoming traffic to ensure the vehicle is unable to defeat the next set of fence, cable, or jersey barrier obstacles in a serpentine. For the obstacles listed, one can assume that it takes 61.9 x 1,000 ft-lbf to breach a fence, 346.8 x 1,000 ft-lbf for a fence supplanted by cable, and 334.4 x 1,000 ft-lbf for a standard jersey barrier.[38] With those figures in mind, it is possible to judge a vehicle's kinetic energy in ft-lbf using standard vehicle weights (W), velocities (V), and the equation: $KE(\text{ft-lbf}) = 0.0334WV^2$. Table 1 illustrates the kinetic energy produced by a vehicle at certain speeds.

Table 1. Kinetic Energy Developed by Vehicle Weight and Speed (1,000 ft-lbf)[39]

	Speed of Vehicle						
Vehicle Weight ↓	10	20	30	40	50	60	70
4,000-lb Vehicle	13	53	120	214	334	481	655
15,000-lb Vehicle	50	200	451	802	1253	1804	2455

The slowed vehicles then make their way through a series of serpentine obstacles designed to restrict a vehicle's movement, further reduce their speed, and provide the first opportunity for early warning of potential threats. Arbitrary placement of serpentine barriers yields an ineffective obstacle that does not achieve any of the identified goals. Planners constructing the serpentine should take curvature radius, friction coefficients, and skid speed into account. It may be common sense that the tighter the curve, the slower a vehicle must travel to negotiate the obstacle. That is true but vehicles that are

38 Lim, *Anti Terrorism and Force Protection Applications in Facilities*, 25.

39 Ibid., Table 6.

unable to pass through the ECP/VCP introduce unnecessary friction and risk into the operation. Table 2 shows accepted skid speeds using two different friction coefficients. The friction coefficient of a dry paved road is 0.6 while 1.0 is used for unknown roads.

Table 2. Skid Speed (mph) vs. Radius of Curve (ft)[40]

	Radius of Curvature (ft)									
Friction Coefficient (μ) ↓	25	50	75	100	125	150	175	200	225	250
0.6	15	21	26	30	33	37	39	42	45	47
1.0	19	27	33	39	43	47	51	55	58	61

The end of the serpentine barriers marks the end of the approach zone and the beginning of the access control zone.

b. Access Control Zone

The access control zone constitutes the main area of an ECP/VCP as it includes guard facilities, inspection areas, and traffic management equipment.[41] Above all, the access control zone should be able to verify personnel credentials, safeguard personnel conducting searches, and provide overwatch in the search area. Obviously, most of the ECP/VCPs personnel will be in the access control zone. That fact forces planners to utilize as many precautions to reduce potential threats in the area while still accomplishing the mission. The threats and precautions will be discussed in more detail in a later section. Immediately following the access control zone is the response zone.

c. Response Zone

The area extending from the end of the access control zone to the final denial barrier into the installation defines the response zone.[42] Just as it sounds, the response zone contains forces and capabilities to react to a threat. In addition, the response zone

40 Ibid., 24, Table 5.

41 JFOB Quick Reaction Test, *JFOB Force Protection Handbook*, 6–34.

42 Ibid., 6–35.

maintains overwatch of the other entire ECP/VCP, protects the reaction forces, and is the command and control node of the ECP/VCP. Similar to the access control zone, the response zone requires thoughtful planning to decrease threats. Those concepts will be discussed with the access control zone precautions. The last zone in the ECP/VCP is the safety zone.

d. Safety Zone

Unlike the other zones, the safety zone does not have a start or endpoint. Instead, the safety zone extends from all passive and active barriers in all directions to protect personnel from explosions or other physical threats.[43] Safety zones comprise of acceptable standoff distances and protective equipment/structures determined from threat assessments or expected weight of explosive charges. In concert, the four zones comprise the make-up of an entire ECP/VCP. As previously stated, ECP/VCPs come in all shapes and sizes so it is appropriate to dissect a few examples.

2. ECP/VCP Examples

While it is impossible to offer an ECP/VCP example that fits every operational scenario, the next section describes three separate ones broken down by size. A small ECP/VCP focuses on tactical units with some support from lift and engineering assets. The medium example involves permanent structures and requires increased time and space to construct. The largest example requires the most space and resources to build but offers the most protection.

a. Small Unit ECP/VCP

The first example is a small unit ECP/VCP taken from the Center for Army Lessons Learned and is illustrated in Figure 1. A few immediate observations include the small number of people required to equip a hasty ECP/VCP. This instance only uses a platoon element, or perhaps less, to operate but does involve barriers and supplies that would require external support. Regarding the four zone, the approach zone

43 Ibid.

is at least 100m before the start of the ECP/VCP. The approach zone is certainly not robust but is enough to alert incoming traffic to the checkpoint ahead while it succeeds in canalizing and slowing the traffic prior to the search area and access control zone.

The access control zone is small in this example but sufficient if it matches the traffic volume and threat analysis of the area. Inside the search area, security personnel check vehicles and their occupants before allowing them to pass the ECP/VCP. True, the fields of fire recommended in this example are atrocious but those types of issues are not the focus of this research. The leaders who constructed this checkpoint incorporated barriers around the search area but those may be insufficient to an oncoming vehicle.

That deficiency is balanced, not because the response zone is located immediately adjacent to the search area, but because of the patrolling effort it provides around the checkpoint. One could assume that the lack of hardened barriers around the response zone results from the small amount of time this ECP/VCP will be active. If needed, those occupying the position could a hasty earthen barrier for added protection. Either way, the response zone accomplishes the tasks previously described in this chapter.

The location of the safety zone for this example is vague but one could surmise it is within support range of its higher headquarters. In this example, the safety zone could contain additional supplies, manpower, etc. for the smaller unit conducting the ECP/VCP.

This example illustrates that ECP/VCPs do not have to be massive undertakings to effectively incorporate all four zones. While it is always nice to have more people, time, and equipment, compromises must be made between all of those and mission accomplishment.

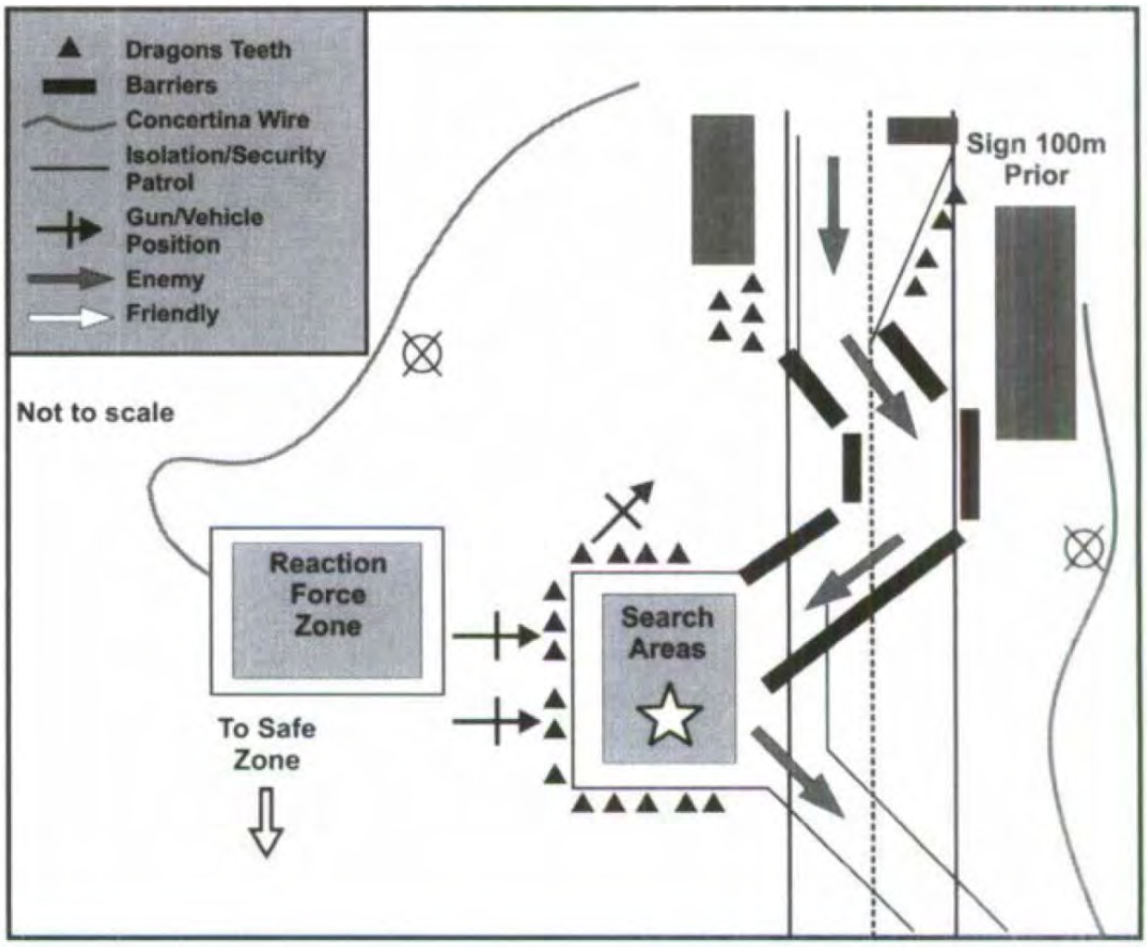

Figure 1. Small Unit ECP/VCP[44]

b. Medium-Sized Permanent ECP/VCP

Unlike the first example, this ECP/VCP design, adapted from the Navy Facilities Engineering Service Center, lends itself to military, government, and civilian use. One can see that the structures and equipment involved are permanent and more robust.

The approach zone for this checkpoint starts before the entrance even though it is not explicitly shown in Figure 2. The slowing and canalizing obstacles lead directly to a guard booth that can pass the traffic through, send to a search area, or immediately reject out of the area. This example demonstrates that the approach zone and access control

44 Matthew Day, John Tien, and Tracy Peacock, "Checkpoint Operations." *in U.S. Army and U.S. Marine Corps Tactics, Techniques, and Procedures for Stability Operations and Support Operations*, ed. Michael Hiemstra (Fort Leavenworth, KS: Center for Army Lessons Learned, 2003), 39, figure unnumbered.

zone can be simultaneous events depending on the situation. The access control zone continues into the search/inspection area the additional structure placed inside the inspection area. That addition combined with the lights and cameras adds more overwatch in the access control zone.

The response and safety zones for this example are less apparent than in the first case. The nature of this ECP/VCP suggests that the response zone is closer to the safety zone and that could be the result of a couple reasons. First, the threat in the area is low and leaders have focused their resources and manpower elsewhere. Second, space may not have been available to construct a proper response zone, this is very likely considering that many buildings are in built-up area or cities. A design that is not constrained by resources or space will be the last example.

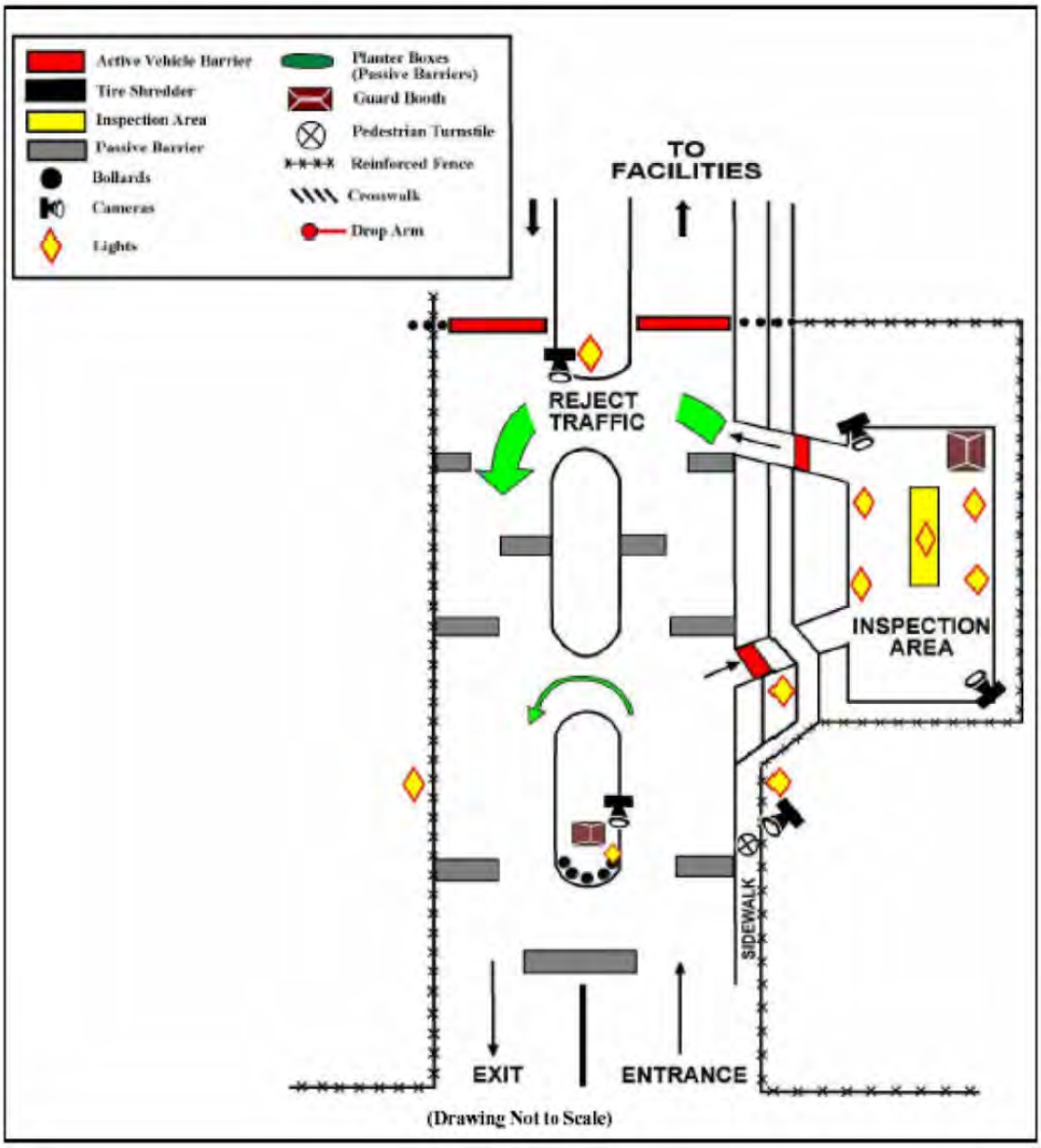

Figure 2. Medium ECP/VCP[45]

c. Unconstrained ECP/VCP Example

The last example shown in Figure 3 is not the largest example that is available but does use the largest space and resources. Similar to the previous examples, the approach

45 Lim, *Anti Terrorism and Force Protection Applications in Facilities*, 60, figure C-1.

zone slows and canalizes traffic but using a series of critical turns instead of serpentine barriers. The critical curves allow security personnel to observe incoming traffic from numerous angles and judge the occupants for a longer period of time. .

The access control zone again occurs in two areas. The first area is located at the initial guard structure that physical barriers protect. That guard can pass that traffic to the facility, force to a subsequent inspection area, or reject it completely. The inspection area includes multiple lanes and another guard structure along with cameras, lights, and physical barriers. Here, personnel pass or reject traffic.

The response zone falls within the access control zones. One can notice that space and physical barriers separate all of the common areas of the checkpoint but are still isolated enough to prevent one attack to attack numerous areas. As a result, response forces from within the ECP/VCP maintain the capability to support each other without the reliance of outside aid. The safety zone extends to areas outside the wire obstacles.

All cases described incorporate sound practices and functional zones for ECP/VCPs but are still vulnerable to violent action from enemy actors. The next section will describe those physical and cognitive vulnerabilities to ECP/VCPs in general.

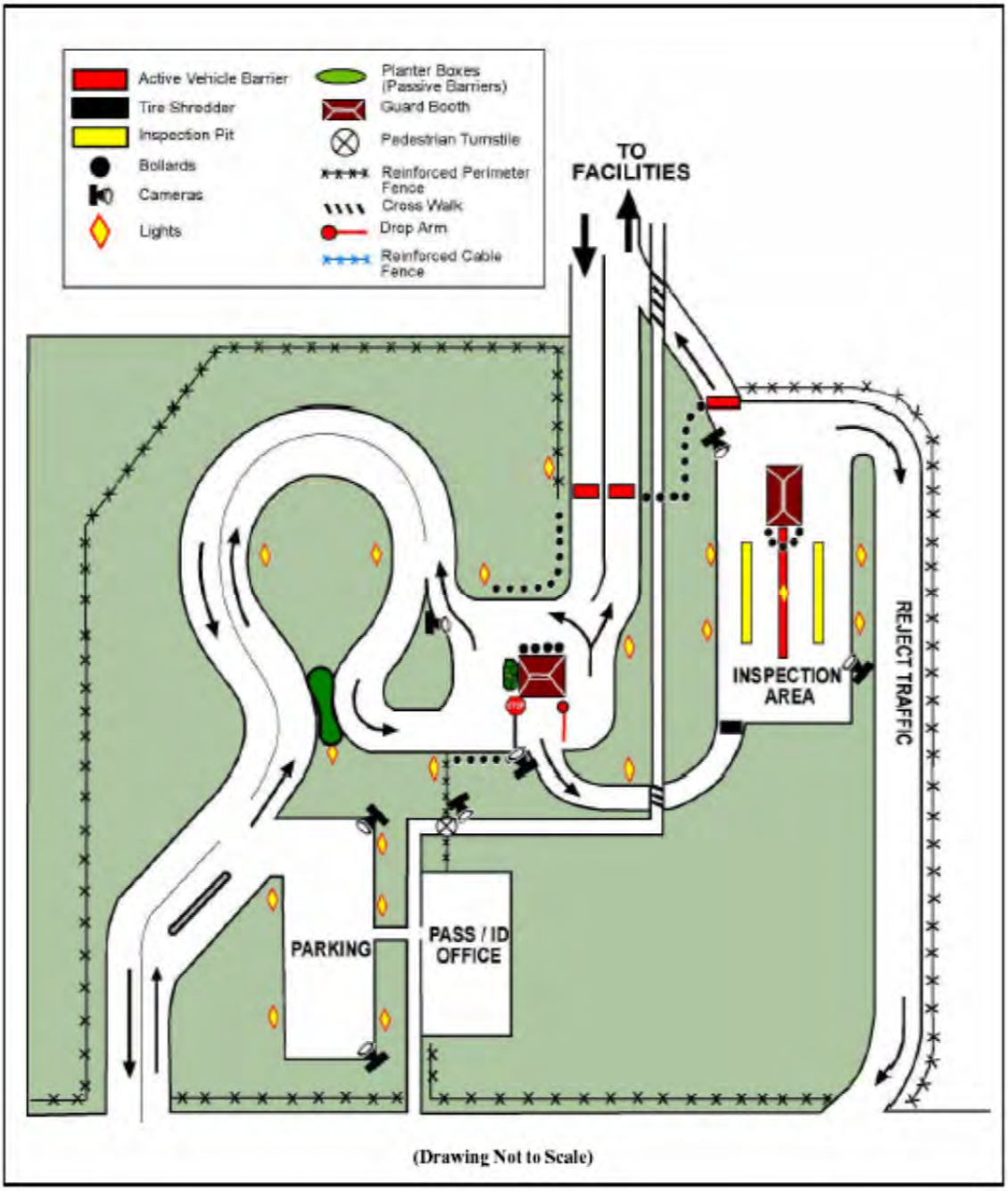

Figure 3. Least Constrained ECP/VCP Example[46]

46 Ibid., 61, figure C-2.

3. Vulnerabilities

Whether inside the United States or amidst some dusty backwater village abroad, enemy combatants actively pursue operations against ECP/VCPs. The first experiment explored to protect the troops in Iraq was to build massive bases where forces could return after each mission. Soon, it became evident that adopting a fortress mentality only isolates the counterinsurgent from the fight.[47] As military commanders pushed smaller tactical units out from larger bases, their time with the local populace increased but also increased their responsibility for force protection as the number of smaller positions grew. Those smaller outposts, along with constant stability operations necessitated frequent if not persistent ECP/VCPs that emerged as a constant target to enemy forces. Enemy forces were quick to identify physical and cognitive vulnerabilities in ECP/VCPs despite their size or construction.

a. Physical Vulnerabilities

There currently exists no panacea that protects troops from large, fragmentation and pressure producing blasts. Mission accomplishment prevents friendly forces from simply "bunkering" themselves into huge, isolated structures but the threshold for pressure and fragmentation related injury is too low to go unaddressed.

Eardrums rupture in 1% of victims at 5 PSI blast overpressure while 99% of eardrums rupture at 45 PSI. Serious lung damage begins around 15 PSI. Overpressure between 35–45 PSI may cause 1% fatalities while 55–65 PSI can cause 99% fatalities.[48] Scaled peak pressure as a function of distance R, and charge weight W looks like the equation $P = W/R^3$. Figure 4 plots out that relationship with four incident pressure curves (5.0, 10.0, 20.0, 50.0 PSI) that would apply on varying charge weights (log scale) and standoff distances.

47 Douglas A. Ollivant and Eric D. Chewning, "Producing Victory: Rethinking Conventional Forces in COIN Operations," *Military Review* 86, no. 4 (July 2006): 54.

48 USMC Regional Command (S), *IED Blast and Fragmentation Distances* (RC(S) C-IED, 2013).

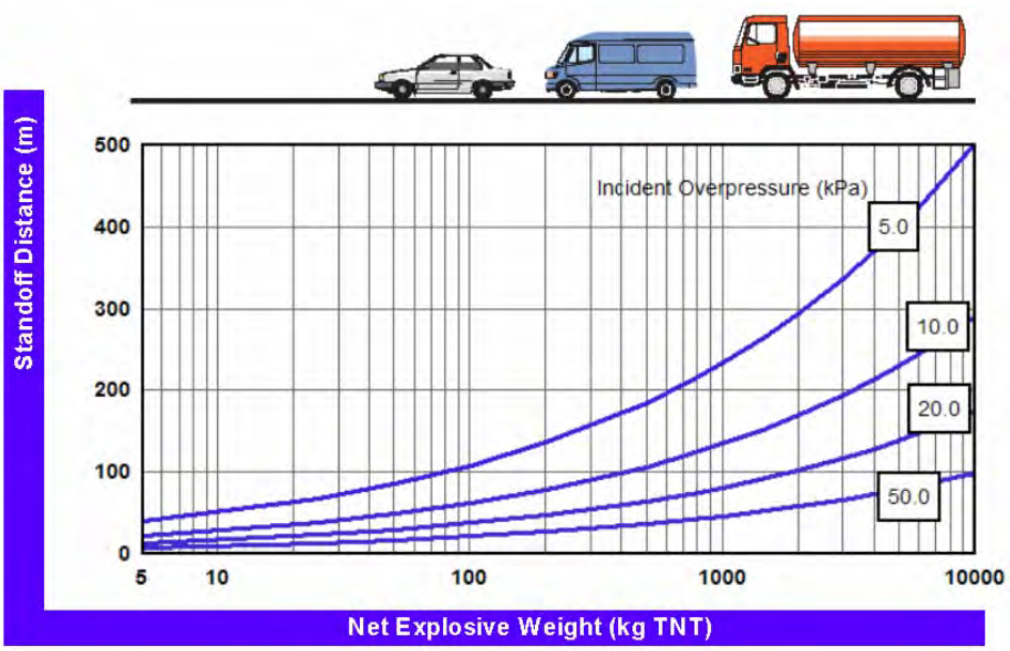

Figure 4. Incident Pressure Related to Stand Off Distance and Charge Weight[49]

When related to personal injury, Table 3 describes what level of trauma is expected compared to the charge weight.

Table 3. Distances to Produce Personal Injury (feet)[50]

Personal Injury Level Expected	50 lbs	220 lbs	500 lbs	1,000 lbs	4,000 lbs
Severe injury or death	33	54	71	90	142
Lung injuries and 20% eardrum rupture	40	66	87	110	174
Serious injuries (Internal bleeding, some organ damage)	66	108	143	180	285
Injury (Lacerations and contusions, no organ damage) and temporary hearing loss	95	151	198	250	396
Injury from debris (Lacerations and contusions)	110	181	238	300	475

49 Alexander Reminnikov and D. Carolan, *Building Vulnerability Design Against Terrorist Attacks* (Wollongong, Australia: University of Wollongong, 2005), 5, Figure 2.

50 Lim, *Anti Terrorism and Force Protection Applications in Facilities*, 10, Table 2.

One may notice that the overpressure reduces by a factor of 8 as the distance doubles and that the risk of injury greatly decreases the further away one is to a blast. The question is, "why not build ECP/VCPs with large amounts of standoff?" First, there is usually not enough space to completely negate blast effects. Second, to properly check occupants and search vehicles, service members must operate at close proximity to the potential threats. That fact is the largest physical vulnerability to the ECP/VCP construct. Security personnel must put themselves in direct danger of bodily harm to accomplish their mission. What is more, enemy actors using SVBIEDs can comply completely with ECP/VCP procedures and go unnoticed until they are next to their targets. Unfortunately, there seems to be plenty of extremists that willing to commit those acts. In an online post, one attacker said, "This is my car bomb, loaded with a ton of explosives so that we can burn and kill these infidels and criminals."[51] Not only does this underscore the physical vulnerability, the powerful language introduces cognitive vulnerabilities as well.

b. Cognitive Vulnerabilities

The enemy frequently targets ECP/VCPs. Successful attacks give the enemy cognitive victories and further their cause for recruiting and fund raising as they consider these SVBIED attacks as grand martyrdom operations that are easy paths to paradise. Terrorist leader Abu-Umar al-Baghdadi stated the following of a SVBIED attacker in a propaganda video posted online. "What is amazing is how that can be true for a lion who rode in the vehicle of death, hurried to pass the crowd, maneuvered like cavaliers, and sang songs of the bridegrooms. He is a lion, who was not confused by the enemy bullets, and the fortifications of the occupiers did not deter him from reaching his target…" Later in the video, he continued to say, "We should propagate their case and deliver it to the Muslims all over the world…We should also raise funds for them and deliver these funds by all means necessary."[52] Suicide attacks cognitively affect U.S. forces too.

51 "Knights of Martyrdom 7," Islamic Al-Fallujah Forums, February 22, 2010, http://202.71.102.68/~alfaloj/vb.

52 "Knights of Martyrdom 6," Islamic Al-Fallujah Forums, August 22, 2009, http://www.al-faloja.info/vb.

The psychological effect resulting from SVBIED attacks on ECP/VCPs is summed up again by al-Bagdadi when he said, "They taught them lessons that still cause them to burn and writhe in pain. These lessons brought their flags to half-staff, shook their roots, and scattered their thoughts, so, that terror took root within them and desperation began to gnaw at their bones."[53] Some argue that those statements amount to nothing more than propaganda from the enemy. Taken alone, that may be true but U.S. leaders have gone on record with equally startling statements. Colonel William Anderson wrote that,

> Few experiences compare with the helplessness felt by those involved in an IED attack. The experience is searing…the combination of these ingredients: helplessness, surprise, calm before chaos, indiscriminate effect, collateral damage, and anonymity of the attacker contribute to tactical anxiety…The strategic power of the IED comes from a non-kinetic source, information.[54]

These statements from enemy and friendly actors capture how vulnerable ECP/VCPs are to cognitive exploitation when attacked by IEDs or SVBIEDs. Vulnerabilities this critical cannot go unnoticed by military leaders. This may represent an opportunity to explore DE systems that reduce those vulnerabilities without adopting a bunker mentality whereby the friendly forces isolate themselves from the populace.

4. Directed Energy in Force Protection

Directed energy seems an unlikely candidate to enhance force protection at ECP/VCPs. The next chapter will expound upon DE capabilities but it is fair to state that DE could help reduce physical and cognitive vulnerabilities previously mentioned.

---

53 "Knights of Martyrdom 3," YouTube video, 41:15, from post by Al-Furqan Media Establishment on July 8, 2008. Posted by "Al Fajr Media Center." July 9, 2008. http://www.youtube.com/watch?v=8Cy6NS7wHfI.

54 William G. Adamson, *An Asymmetric Threat Invokes Strategic Leader Initiative: The Joint Improvised Explosive Device Defeat Organization* (Washington, DC: The Industrial College of the Armed Forces, National Defense University, 2007), 6.

a. Reduce Physical Vulnerabilities

The charts that detailed the standoff distances related to specific charge weights demonstrate how valuable every foot of real estate can be in an ECP/VCP. Non-lethal DE systems designed to stop vehicles could add to the standoff distance between a possible threat and the security personnel staffing the checkpoint. Currently, only intrusive barriers or kinetic measures can be implemented to maintain proper standoff distances. Not only can DE add layers of physical security they could also reduce the cognitive vulnerabilities that were mentioned.

b. Reduce Cognitive Vulnerabilities

Spike strips and other physical barriers that halt vehicle are effective but leave little room for flexibility. Any false assumption could damage an innocent traveler's vehicle and produce damaging cognitive effects with the local populace. Lethal means are always available but the likelihood of collateral damage raises significantly in areas so congested with civilian traffic. DE provides flexibility in ROE constrained areas without losing capabilities required to accomplish the mission. The next chapter will explore DE in order to increase understanding of their capabilities and limitations on the modern battlefield to include ECP/VCP operations.

III. DIRECTED ENERGY

A. BACKGROUND

Directed energy origins trace back millennia when it is said that Hippocrates used burning mirrors to harness the power of the sun. The mirrors directed the sun's rays onto invading ships sails setting them ablaze in 212 BC.[55] While this example may be more lore than fact, the mystery of the electromagnetic spectrum began to be unraveled in the 19th century by scientists like Maxwell and Hertz. Their work enabled further discoveries in the EMS including radio waves, microwaves, infrared, visible light, ultra-violet light, x-rays, and gamma rays.

Work continued in the EMS arena leading up to World War II and led to the discovery of the laser (Light Amplification by the Stimulated Emission of Radiation) and radar (Radio Detection and Ranging). During this period, the British even commissioned scientist Sir Robert Watson-Watt to explore the idea of using radar-like devices to boil pilots blood.[56] This may have been the first foray into leveraging the EMS for defense purposes.

The advent of the nuclear bomb not only demonstrated the weapons destructive capacity but also introduced the power of an electromagnetic pulse; a byproduct of nuclear weapons. The true capabilities of an EMP were not immediately understood until years after the first bombs were developed. In 1962, a one-megaton test nuclear weapon detonated nearly 250 miles above the surface of the Pacific Ocean. As a large imbalance of electrons in the upper atmosphere interacted with the Earth's magnetic field, oscillating electric fields over the Pacific emerged. The fields were so powerful that they damaged electronic equipment in Hawaii, which was more than 1,000 miles away.[57] Military leaders witnessed the utility of EMPs and ordered further study.

---

55 Melissa Olson, "History of Laser Weapon Research," *Leading Edge* 7, no. 4 (2012): 26.

56 P. M. Sforza and H. Zmuda, "Directed Energy," *Journal of Directed Energy* 1, no. 1 (January 2003): 92.

57 Stuart Moran, "Historical Overview of Directed Energy Work at Dahlgren," *Leading Edge* 7, no. 4 (2012): 12.

Unfortunate mistakes also advanced research in directed energy systems. After a devastating fire aboard an aircraft carrier in Vietnam, investigations concluded that high power shipboard radars had set off live bomb fuses loaded on aircraft. In another example, Navy helicopters experienced serious malfunctions when flying too close to high power microwave towers. These events led to consideration that radio frequency or microwaves could be used as weapons against the entire range of enemy electronics or electronically controlled systems.[58] Before diving directly into military application, it is worthwhile to discuss the principles of DE.

B. PRINCIPLES

The next section focuses on a few basic principles of DE. First, several military definitions that are salient to the rest of the thesis are presented to familiarize readers to terms accepted by U.S. forces. The next segment offers a quick comparison between DE systems and conventional systems to show what advantages and limitations users of DE should expect. Lastly, the effects that DE inflicts on targets are explained.

1. Definitions

As is true of any academic discipline, this subject claims its own unique language. The following definitions represent a few important terms that will allow readers to grasp some of the nuances of DE.

Directed Energy (DE): An umbrellas term covering technologies that relate to the production of a beam of concentrated electromagnetic energy or atomic or subatomic particles.[59]

Directed Energy Device: A system using directed energy primarily for a purpose other than as a weapon.[60]

Directed Energy Warfare: Military action involving the use of directed energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy

58 Edward Scannell, *Progress in Directed Energy Weapons Part II: High Power Microwave Weapons* (Alexandria, VA: Weapon Systems Technology Information Analysis Center,2003), 2.

59 Department of Defense. *Department of Defense Dictionary of Military and Associated Terms* (JP 1–02) (Washington, DC: Joint Force Development, 2015), 63.

60 Ibid.

equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption.[61]
Directed Energy Weapon (DEW): A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel.[62]

2. Advantages and Limitations

DE boasts numerous advantages over conventional weapons. That is not saying that DE will completely replace conventional munitions. Rather, DE advantages offer flexibility to the warfighter in circumstances where specific weapons characteristics are required. True to any technology, limitations exist that must be addressed or at least known to the user. Table 4, an author developed table, shows both the advantages and limitations of DEWs.

Table 4. DE Advantages and Limitations

Advantages	**Limitations**
Speed of light engagements	Propagation limited by air breakdown
All-weather capabilities	Legal constraints
Tailored effects (lethal to non-lethal)	Vulnerable to enemy DEWs
Minimizes collateral damage	Sensitive components
Deep magazines	Lethality is statistical
Multiple target engagements	
Difficult to harden assets against DEWs	
Freedom of gravity	
Low operational cost	

The table is not an all-encompassing list of each characteristic but gives a good idea of what DE users can expect. A few of characteristics listed need further explanation though.

61 Ibid.

62 Ibid.

First, the nature of DEWs allow speed of light engagements which provides users extra time to make decisions on whether or not to employ the weapon. Combined with the ability to scale effects from lethal to non-lethal, the flexibility involved with DEWs sets them apart from their conventional counterparts. In addition, DEW's precision minimizes collateral damage that traditional weapons fail to deliver. Lastly, DEWs have deep magazines meaning that they are not constrained with a ready box of ammunition. Energy pulses will last as long as the propagating equipment and power source remain available and functional.

Limits exist with DEWs however. Because air breaks down at approximately 3MV/m, the maximum power transmitted by any one antenna is limited. Beyond 3MV/m, the air simply cannot continue to allow the wave to propagate to the target. Users can reduce the importance of that limitation by implementing an array of antennas. When properly configured, an array of antennas will have additive effects on a target. Another limitation of DEWs goes hand in hand with one of its advantages. While it is useful to friendly units if enemy elements have difficulty hardening their assets against DEWs, it also means that their assets are just as vulnerable to DEW effects. Those DEW effects are the next subject to be addressed.

3. Effects on Targets

Some argue that one of the greatest features of DEWs is that their effects on targets can be tailored to meet lethal and non-lethal requirements depending on the operational situation. In almost all cases, the terms disturb, disrupt, and damage classify DEW effects on targets.

Disturbing a target requires the least amount of DE power. In this case, disturb means that the effect only persists while the DEW is radiating onto the target. After the DEW completes its radiation period, the target immediately reverts to its full capacity.

Disruption needs more DE power but is still non-lethal in nature. Disruption of a target means that the effects persist even after the DEW has ceased radiating onto the target. The target can go back to full capacity but must be restarted.

The last effect, damage, requires the most power from the DEW. Unlike the previous two effects, damaging a target involves maintenance to bring it back to full capacity. If a DEW damaged a target, the target would have to be mechanically or electrically repaired to restore its functionality. In some instances, damaging a target may involve complete destruction of the target. Damaging effects span both lethal and non-lethal tasks but unless the target is a human or human operated vehicle, they can remain non-lethal systems.

With those effects in mind, DEW effects can be further classified as soft-kill and hard-kill.

a. Soft Kills

A soft kill is synonymous with non-lethal effects and are achieved when DEWs temporarily halts the normal operation of a target.[63] Against mechanical systems, a soft kill includes disturbing and disrupting the target. Both effects stop the target's function but only for a short period of time. An example of a soft kill using disturbing or disrupting effect could be the "blue screen of death" on a computer that regains function after the DEW stops propagating on the computer. Another example is a vehicle motor that stops completely because of DEW radiation and has to be restarted when it is out of the path of the propagating wave.

Soft kills affect human targets as well. The U.S.'s Active Denial System is a DEW that uses a 95GHz radar beam against human targets, causing the target's skin to rapidly heat.[64] After the target leaves the path of the beam, or the beam is stopped, the target feels no adverse effects. The DEW aims to keep people out of certain areas but does not want to have long-lasting effects that could be costly to local perceptions. On the other side of the effects spectrum, hard kills seek long-term damage.

63 Bayram Deveci, "Directed Energy Weapons: Invisible and Invincible?" (master's thesis, Naval Postgraduate School 2007), 24.

64 Scannell, *Progress in Directed Energy Weapons Part II: High Power Microwave Weapons*, 8.

b. Hard Kills

Non-lethal effects give flexibility to the user, but some situations still rate physical damage or destruction of a target. Many times, conventional explosive or kinetic energy weapons meet this requirement but DEWs can achieve similar effects at a fraction of the cost.[65] For DEWs, hard kills are achieved when a sufficient amount of energy is delivered onto the target system, such that it is permanently damaged or destroyed.[66] The Defense Science Board Task Force on DEWs suggests that DEWs can be a useful tool for ballistic missile defense in which the DEW would hard kill an enemy missile. The method of the hard kill could be blinding the incoming munition, shorting out electronics, melting components, or any combination of the above.

C. TYPES OF DIRECTED ENERGY WEAPONS

It is obvious that DEWs can provide tailored effects to the warfighters who use them. On one battlefield, a friendly unit can achieve soft and hard kills depending on the ROE and threat. That is a great capability but requires many types of DEWs to guarantee that all effects can be achieved. Lasers, charged particle beams, and high power radio frequency systems typically represent the major categories of serviceable and theoretical DEWs.

1. Lasers

Even though lasers are a relatively new technology, most people in and out of the Armed Forces have seen lasers. Whether being used for munition guidance systems, as harmless pointers during presentations, or vivid streams of light in entertainment events, lasers have been an accepted technology in modern society. The term "laser" is an acronym for light amplification by stimulated emission of radiation and is typically infrared (1mm to 750nm) and visible light (750nm to 400nm).[67] As a comparison,

65 Deveci, "Directed Energy Weapons: Invisible and Invincible?,) 25.

66 Carlo Kopp and Ronald Pose, *The Impact of Electromagnetic Radiation Considerations on Computer System Architecture* (Victoria, Australia: Monash University, undated), 5.

67 Olson, "History of Laser Weapon Research," 26.

microwave frequencies range from millimeters to centimeters and have wavelengths up to 10,000 times longer than lasers.

None of other than Albert Einstein discovered one of the fundamental ideas of laser technology in 1917 when he theorized that when a photon, a quantized packet of energy, interacts with an atom or molecule in an excited state, two photons are produced when the atom or molecules leaves the excited state. Initially, power is introduced to molecules in a ground state to get them into the excited state. Photons pass through those excited molecules thereby creating many additional photons. For a laser, the photons are contained in a chamber and reflected back and forth by a series of mirrors until they reach an output mirror that is only partially reflective. The partially reflective mirror allows some photons to leak through, creating a laser beam.[68] For military purposes, there are four fundamental types of lasers including chemical lasers, solid-state lasers, fiber lasers, and free-electron lasers.[69] Brief descriptions of each will be provided next.

Chemical lasers use chemical reactions to start the process of exciting molecules in the lasing medium.[70] Much recent advancement in laser technology is in this category. One such example is the Mid-Infrared Advanced Chemical Laser (MIRACL) that not only was one of the first megawatt class lasers in the U.S. Navy, the MIRACL has had successful UAV engagements since 1987.[71] Another popular chemical laser, the chemical oxygen, iodine laser (COIL) met a major milestone in 2005 when it reliably ran at power levels and duration necessary to achieve lethal effects on missiles.[72] The chemicals in these systems tend to be expensive and caustic if improperly handled. As a result, alternative methods of laser production were explored. One such method is a solid-state laser.

---

68 Ibid., 27.

69 Defense Science Board Task Force, *Directed Energy Weapons* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2007), 5.

70 Olson, “History of Laser Weapon Research,” 29.

71 William McCarthy, *Directed Energy and Fleet Defense* (Montgomery, AL: Center for Strategy and Technology, 2000), 18.

72 Defense Science Board Task Force, *Directed Energy Weapons*, 5.

As the name suggests, solid-state lasers utilize a solid lasing medium like a rod made of glass, crystal, or a gem combined with an active material like Chromium or titanium. Either a flash lamp, arc lamp, or another laser carries out the excitation process to stimulate the laser beam.[73] At the beginning of their life, solid-state lasers did not garner as much enthusiasm as other laser systems because of their $10–$20 per peak watt power price tag.[74] One could imagine how high the expense would grow with applications requiring 10kW or higher. Recent updates to the technology resulted in reduced prices but not enough to be as viable as other laser systems for weapons purposes. But because of their small size and ruggedness, battery powered solid-state lasers remain a popular laser system for range finding and target designation.

Some consider fiber lasers as a segment of solid-state lasers but this thesis will treat them as a separate entity. Fiber lasers use optical fibers doped with rare earth metals like erbium, ytterbium, or thulium as the gain media.[75] They are powered electrically, which makes them extremely mobile and suitable for battlefield conditions. The most successful fiber lasers damage targets through thermal heating sometimes completely burning through materials. An excellent example of a fiber laser is the Navy Laser Weapon System (LaWS) depicted in Figure 5. In 2009, the LaWS successfully tracked, engaged, and destroyed unmanned aerial vehicles in flight showing its effectiveness against difficult targets.[76]

Free electron lasers (FEL) represent the last type of laser for discussion. While work is ongoing, most researchers view FELs not as a laser weapon but as a device to produce high power microwaves.[77] The payoff in output power from FELs is expected to be in the multi-megawatt class but the equipment required to produce that type of FEL is sensitive and cumbersome. FELs use electron beams (e-beam) generated from a vacuum and an e-beam accelerator. That accelerated e-beam gets injected into an undulator,

73 Olsen, “History of Laser Weapon Research,” 28.

74 McCarthy, *Directed Energy and Fleet Defense,* 16.

75 Olsen, “History of Laser Weapon Research,” 30.

76 Ibid., 33.

77 McCarthy, *Directed Energy and Fleet Defense,* 19.

which consists of a periodic, transverse magnetic field. After further synchronizing the e-beam and electromagnetic field wavelengths, an amplified electromagnetic output is created.[78] The technology is impressive but not user friendly.

Figure 5. Laser Weapon System, LaWS[79]

2. Charged Particle Beams (CPBs)

At this point, CPBs are more theoretical devices than actual weapon systems. Technical and fiscal challenges stifle CPB development but some research is performed today. Unlike lasers or high power radio frequency systems that transmit waves, CPBs transmit matter in the form of atomic or sub-atomic particles.[80] Strong electric fields applied near electron emitting materials produce charged particles that, when accelerated to velocities near the speed of light, can be deposited onto targets with substantial energy.[81] Disadvantages with CPBs include complicated beam control, massive power requirements, line of sight capabilities, altitude constraints, and size/weight problems, which make them unlikely candidates as near term solutions for contemporary problems.[82] High power radio frequency or high power microwave weapons may prove more capable as a solution to the problem posed in this thesis.

78 Defense Science Board Task Force, *Directed Energy Weapons*, 19.

79 Olsen, "History of Laser Weapon Research," 35, Figure 10.

80 Moran, "The Basics of Electric Weapons and Pulsed-Power Technologies," 55.

81 Ibid.

82 Deveci, "Directed Energy Weapons: Invisible and Invincible?,) 16.

3. High Power Radio Frequency

a. Basic Considerations

Essentially, HPRF DEWs and High Power Microwave weapons are synonymous. This research chooses to refer to the umbrella of systems that propagate electromagnetic waves at high power for offensive and defensive purposes as HPRF. Typically, HPM systems generate and deliver EM waves from a frequency band between 100MHz to 100GHz but HPRF utilizes bands less than the microwave range. Figure 6 is a good depiction of which frequencies and wavelengths are involved in HPRF. Concerning power output, most who study the field agree that 100MW peak power is required for high power classification.[83]

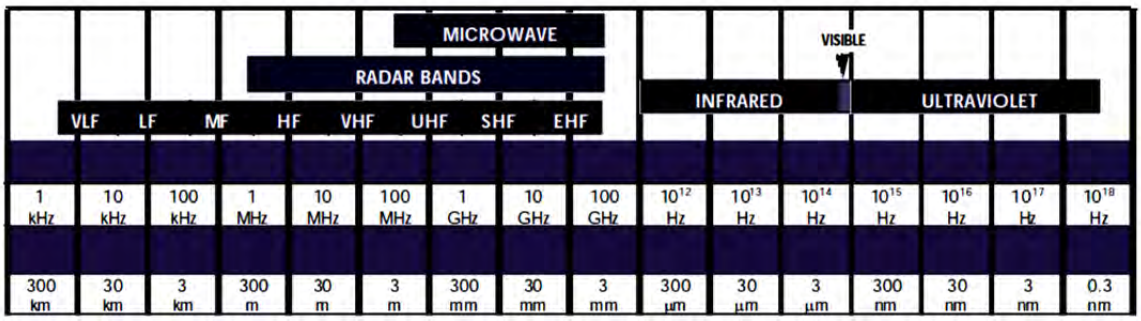

Figure 6. EMS[84]

b. Operating Bands

Many divide HPRF into narrow or wide band systems depending on the pulse length. Narrowband systems produce high peak power but utilize small slivers of frequencies, hence the name.[85] Narrowband systems are effective because of the high power output but one must have a specific frequency range to target.

Wideband systems cover a larger swath of frequencies but do not produce nearly the amount of average power than narrowband systems. Instead, they rely on high peak

83Scannell, "Progress in Directed Energy Weapons Part II: High Power Microwave Weapons," 3.

84 Ibid., 4, Figure 4.

85 Moran, "The Basics of Electric Weapons and Pulsed-Power Technologies," 53.

electric fields to effect targets. Generally, wideband systems produce pulses only nanoseconds long and operate at lower frequencies.[86] Wideband systems interest many researchers because, unlike narrowband systems, they do not require specific knowledge of a target. The frequency needed to effect the target only has to reside somewhere in the wideband system's range. In military parlance, wideband systems are area weapons while narrowband are precision weapons.

c. Components

Whether a HPRF system is narrow or wideband, it is comprised of similar components. HPRF weapons consist of four basic components including power sources, RF source, antenna, and target. Figure 7 is a basic depiction of the HPRF components.

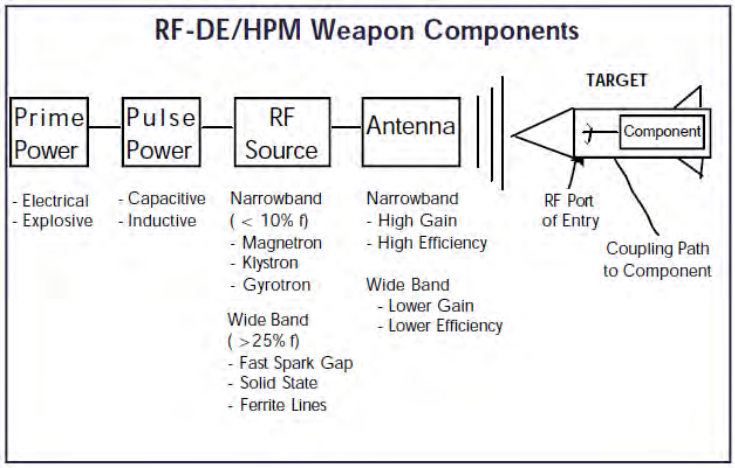

Figure 7. HPRF System Components[87]

Prime power sources initiate the sequence for HPRF systems. As listed, prime power can be derived from electrical or explosive methods but this research will focus on electric means. Pulse power sources generate highly amplified electronic pulses that drive the RF source.

86 Ibid., 53.

87 Scannell, "Progress in Directed Energy Weapons Part II: High Power Microwave Weapons," 6, Figure 12.

The RF source is the beating heart of an HPRF system. Power coming from the original source is converted into a high-powered waved of electromagnetic energy. Narrowband systems rely on traditional devices like magnetrons, klysterons, and gyrotrons. These devices prove effective for producing HPRF waves but, for the most part, are large, bulky systems that prohibit a systems mobility and use. Further, some of them use vacuums or produce powerful magnetic fields that can interfere with friendly electronic systems. Wideband systems have the ability to utilize solid-state technology, electromagnetic pulse-like sources, and transportable sources.[88] Solid-state technology will be discussed in more depth later in this chapter. After a system produces an RF pulse, an antenna propagates it through the air toward a target.

For DEWs, the antenna contributes to a successful system as much as the RF source. The radar range equation,

$$P_{target} = \frac{P_{Source}\, Gain}{4\pi R^2}$$

illustrates a few important factors to take into account. First, antenna gain and source power are on equal footing in directing power onto a target.[89] Next, knowing that if an engineer wants a long range, high gain, and narrow beam weapon, then the antenna's physical area must be large, detailed compromises must be made to between the size of the antenna and the distance from the target. While large antenna arrays are possible, they limit the transportability and flexibility for units constrained by assets to move and operate such a large piece of equipment. Appropriate compromises can lead to a system that meets space, weight, and power requirements, but it still must affect a target.

4. Coupling

HPRF DEWs aim to produce disturbing, disrupting, or damaging effects on targets when high-powered electromagnetic waves propagate through the air and interdict targets by travelling through the exterior layers of structures and coupling energy to

88 Defense Science Board Task Force, *Directed Energy Weapons*, 19.

89 Scannell, "Progress in Directed Energy Weapons Part II: High Power Microwave Weapons," 6.

critical electronic components.[90] Electronic coupling occurs in two general ways; front-door and back-door coupling.

a. Front-Door Coupling

The first method, front-door coupling, directs energy at an antenna or other component on the target that was designed to accept RF energy. Targets are vulnerable to front-door coupling because they are designed to detect and process signals at specific frequencies. Some HPRF systems, particularly narrowband systems, enjoy success in front-door coupling but that success is dependent on the user having comprehensive empirical knowledge of the target system so that the directed energy is the same frequency the target is expecting.[91] That knowledge may not be easily attainable so another coupling method is needed.

b. Back-Door Coupling

Back-door coupling refers to any radiation that follows a path other than the antenna.[92] Paths to back-door coupling are varied and include any cracks, seams, gaps in the targets structure or even exposed wires and exposed conductive materials that lead to vital electronic components. Figure 8 illustrates examples of both types of coupling on a target, which in this case is a missile.

90 Matthew McQuage and Jacob Walker, "Directed Energy Using High-Power Microwave Technology," *Leading Edge* 7, no. 4 (2012), 78.

91 McCarthy, Directed Energy and Fleet Defense, 24.

92 Deveci, "Directed Energy Weapons: Invisible and Invincible?, 55.

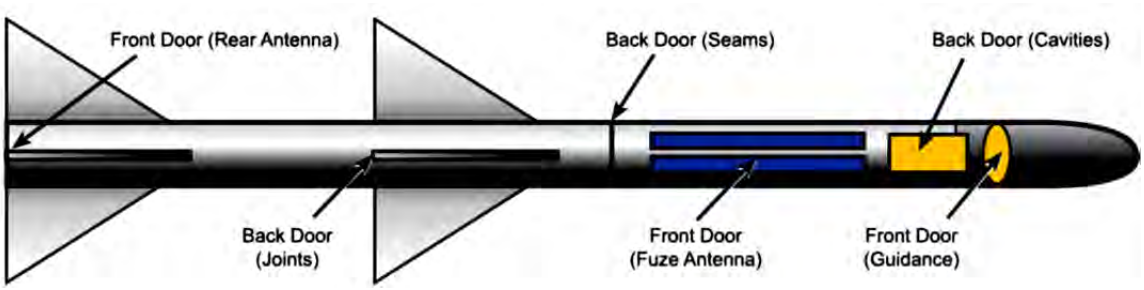

Figure 8. HPRF Coupling Pathways[93]

Each method has obvious advantages and disadvantages. Front-door coupling is a precision engagement needful of detailed target knowledge and a target that does not hop frequencies over a large bandwidth. Back-door coupling is a "brute force" style of engagement that necessitates larger amounts of radiated power.

Both methods, though, need a varying dwell time, that is time on target, to yield desired effects. In each case though, the source-to-target continuum starts at power and RF sources, through an antenna to propagate to a target where the energy penetrates sensitive pathways, couples with electric components, evokes an effect. This research equates targets as vehicles and effects as disruption.

D. HPRF VEHICLE STOPPING CAPABILITY

HPRF systems designed to halt vehicles by corrupting sensitive electrical components is not an unheard of subject. The next section explores that idea by describing some existing and emerging HPRF vehicle stopping technology.

1. Background

SVBIEDs at ECP/VCPs as a contemporary problem to U.S. Forces were discussed in Chapters I and II. Mounting deaths and injuries from SVBIEDs sent military and civilian researchers into frenzy to identify, investigate, and develop technologies that non-lethally stop vehicles in ROE sensitive areas and mitigate blast effects of explosively laden vehicles. One potentially promising technology included the Radio-Frequency Vehicle Stopper (RFVS) developed at the Naval Surface Warfare Center, Dahlgren

93 Moran, "The Basics of Electric Weapons and Pulsed-Power Technologies," 53, Figure 3.

Division. Broadly speaking, this system leverages the EMS to neutralize SVBIEDs, provides friendly forces tools against asymmetric threats, and protects neutral civilians. Those capabilities directly nest with numerous points from two important USMC documents; EF 21 and IMEF S&T.

2. RVFS

The RVFS uses high-power magnetron tubes to generate intense RF pulses that interfere with a vehicle's electronics, rendering them temporarily inoperable.[94] This particular HPRF system creates disruptive effects on vehicles in that the vehicle can be restarted once the RF energy is turned off. Further, the energy deposited onto the vehicle does not harm passengers or render the vehicle so useless that it becomes a burden in the middle of a checkpoint. Prototypes of the RFVS gained notoriety for their success and efficiency.

Despite the successful prototype system, many improvements need to be made for the RFVS or similar HPRF vehicle stopping systems. After quickly observing the RFVS depicted in the Figure 9, planners should notice one glaring detail that will hinder its widespread use throughout the services.

94 Stephen Merryman, "Multifrequency Radio-Frequency Vehicle-Stopping Systems," *Leading Edge* 7, no. 4 (2012), 86.

Figure 9. RFVS Prototype[95]

The size of the system is massive compared to what most units could utilize. Not only is the antenna large and bulky, the structure directly below it contains the power and RF source for the system. No expeditionary unit that counts speed and flexibility as sources of strength could use such a system because it cannot easily be moved and employed in dynamic areas of operation. The disruptive effects without the large, static footprint are the goal and new breakthroughs from Naval Air Systems Command (NAVAIR) may push the technology closer to a battlefield solution.

3. Emerging Solid-State HPRF Technology

For HPRF to be a viable solution for the entire force, it must be smaller and more deployable. For NAVAIR, the answer lies in solid-state technology. Solid-state technology simply refers to rigid hardware compared to hardware based on vacuum tubes. Utilizing solid-state technology creates a few key advantages to existing systems that rely on hardware like magnetrons. Most notably is the overall size and weight of the

95 Ibid., 87, Figure 1.

system. For example, an existing system with vacuum tube technology similar to the RFVS takes up 640 cubic feet of space and weighs in excess of 700 pounds. Compare that to an experimental solid-state system designed by engineers at NAVAIR, and note that the NAVAIR system produces three times more power while using 160 times less space and 29 times less weight.[96] Beyond size, weight, and power, NAVAIR's experimental solid-state HPRF system enjoys many other advantages that make it more amenable to tactical and operational units.

NAVAIR's experimental design has higher RF generating power than conventional microwave tubes, supports higher pulse repetition frequencies, and is modular which supports scalable use. Figure 10 below shows one of NAVAIR's solid-state modules whose volume is around .1 cubic feet and weigh only 6 pounds. Further, there exists no requirement for vacuum tubes, lead shielding, or magnetic fields.[97] That simple comparison demonstrates that HPRF systems can be used in increased roles because they are now more effective and more deployable.

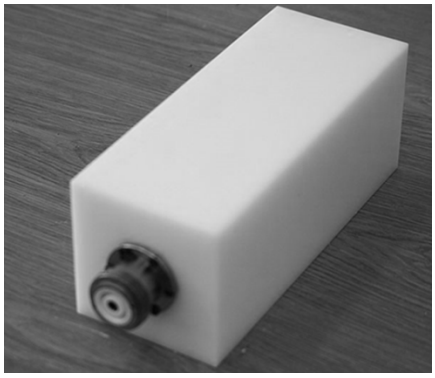

Figure 10. NAVAIR Solid-State HPRF Module[98]

Drawing on knowledge gained from the previous chapter, one should able to see how this type of HPRF technology can be implemented into ECP/VCP operations. Solid-state HPRF vehicle stopping weapons add a much needed non-lethal tool that mitigates

96 Steve Hall, "Solid State RF Sources for Rapid Response," presented at Joint Interagency Field Experiment, Camp Roberts, CA, March 4, 2014.

97 Ibid.

98 Ibid., figure unnumbered.

spectacular attack but protects neutral actors from intrusive barriers or lethal force. In addition, this emerging technology allows units at all levels to benefit. The solid-state system is small enough to use in austere, distributed operations and scalable to use at large fixed sites.

So far in this research, a problem has been identified along with an analysis of the current practices used to counter the problem. A set of technologies was then discussed as a possible alternative to current techniques. Before recommendations or design requirements are suggested, a detailed discussion of the entire system that encompasses the people, equipment, and goals involved in the problem must be completed. The next chapter involves a system of systems analysis of the contemporary operating environment.

IV. SYSTEM OF SYSTEMS ANALYSIS

A. SYSTEMS ENGINEERING PROBLEM SOLVING

The United States military faces a multitude of difficult problems. Each service uses a variety of methods to dissect problems before they begin to define requirements necessary to solve them. Whether it is the Marine Corps' Marine Corps Planning Process (MCPP), the Army's Military Decision Making Process (MDMP), or the joint arena's Joint Operation Planning and Execution system, each strives to provide a repeatable method that planners can utilize to unravel complicated tasks. This case will exit the military arena of decision-making and view the SVBIED problem through the lens of systems engineering.

Systems engineering is "the orderly process of bringing a system into being and the subsequent effective and efficient operation and support that system throughout its projected life cycle."[99] Put differently, systems engineering is a method that aids people toward understanding how many things work together. The term "system" will be used frequently in this section so explaining in it in added depth will help.

A system refers to "a complex combination of resources (in the form of human beings, materials, equipment, software, facilities, data, information, services, etc.), integrated in such a manner as to fulfill a designated need."[100] A system does not have to encompass all of those listed attributes but does include many of them on most occasions. The main idea behind a system is that all of the items within it operate together as a unified whole. Systems can be separated into a variety of categories including; natural and man-made systems, physical and conceptual systems, static and dynamic systems, and closed and open-loop systems. Both are exactly like they sound. A natural process or phenomena like the solar system or river system make a natural system. Man-made systems are the results of human development. Cities, factories, electrical grids, et cetera are examples of man-made systems. A physical system differs from a conceptual system

99 Benjamin Blanchard, *Systems Engineering Management,* ed. Andrew Sage (Hoboken: John Wiley and Sons, 2008), 1.

100 Ibid.

in that the components of a physical system are tangible elements that take up space while conceptual systems are more similar to organizations of ideas. The contrast between static and dynamic systems deals with activity. A shipping company and a warehouse may involve similar structures but the warehouse does not move while the shipping company always has elements in transit. In this simple case, the warehouse is a static system and the shipping company is a dynamic system. Closed and open-loop systems deal with whether or not the system interacts with its environment. Changing environmental effects will have little impact on a closed system but it will on an open-loop system.

There exist instances when the components of a system are distinct systems in and of themselves. A system of systems (SoS) is the term used when this phenomena occurs. SoS is commonly applied to describe highly complex systems within some higher-level structure.[101] In many cases, a SoS may include subsystems from numerous categories that were previously described. Worldwide transportation systems, large investment banks, and advanced military vehicles are excellent examples of a SoS. Figure 11 is a graphic representation of what the SoS analysis for a worldwide transportation system may look like.

101 Ibid., 2.

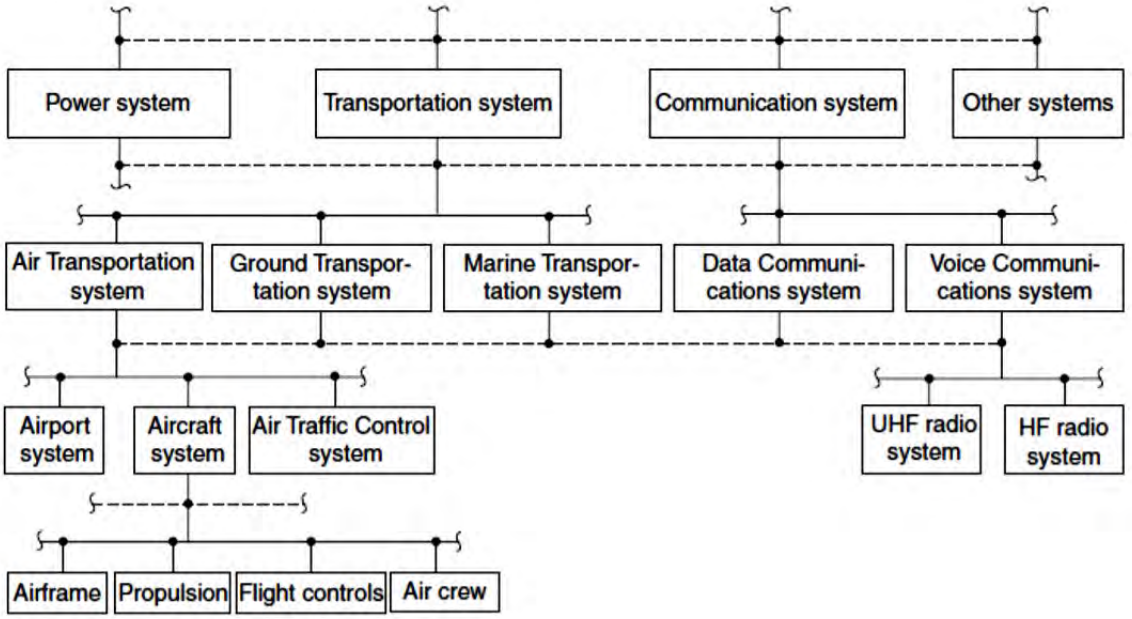

Figure 11. Global Transportation Example[102]

It is evident that each subsystem can be broken down into further subsystems and those subsystems can be separated all way down to the component level. One can imagine how large SoS models become if they are not abridged like this example is. Also, if one were to sever one of the interfaces between the systems, it would cause an avalanche effect and the larger system would fail. Major discrepancies in the propulsion system have no direct linkage to data communications but can still cause the overall mechanism to fail. This short example depicts how efficient a SoS can be if it is well managed but also illustrates how a few disruptions in certain areas or interfaces can have adverse effects.

B. SYSTEM ENGINEERING MODELS

Models often prove to be effective tools as visual aids and systems engineering models are no different. Numerous examples of systems engineering models exist and their usefulness depends solely on the person that is using them. To move forward, it is necessary to offer a few examples that pertain to systems, system development, and

102 Ibid., 8, Figure 1.3.

system of systems. Those three areas will not encompass each area of systems engineering but will be most pertinent to the rest of this thesis's argument. Even though each model is not an all-inclusive solution to every system one can think of, they do represent an accepted set of standard models that academia, military, and government officials use in the course of their respective duties.

The criteria to describe systems range from very straight forward to extremely complicated. For this explanation, two models will be introduced that focus on a system's essential functions and its major elements. As an engineer begins to define a system, they will first identify the vital functions that are required for the system to work properly. Next, classification of the system's inputs by user requirements or consumer is considered. Further, the system's boundaries are outlined as constraints followed by the mechanisms that are available to affect the functions. The product, or output, is the result of inputs, constraints, and mechanisms all working to optimize the essential functions. That description is represented by Figure 12.

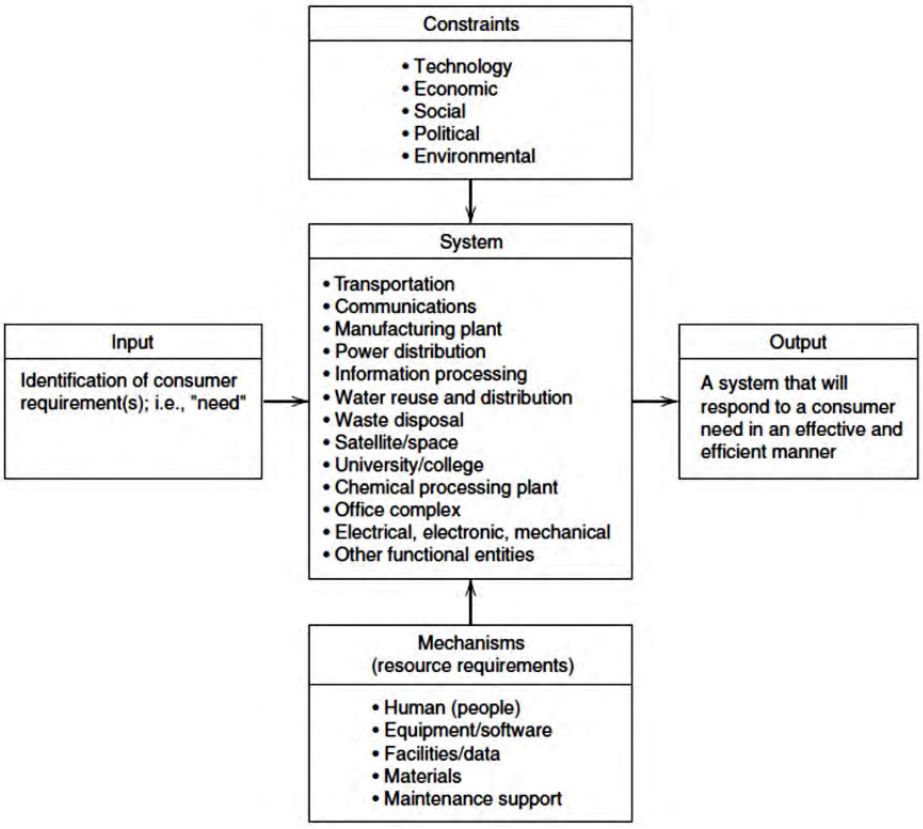

Figure 12. SoS Functionality Focus[103]

An organization working on the same system might frame the system according to its major elements instead of its functions. Rather than an input/output style model above the elements model takes on a classis hub and spoke configuration. The hub, in this case, is the system itself while the spokes are the major elements. Figure 13 shows how simple construction of the model. For a quick snapshot, this model is effective but lacks details that systems engineers require.

103 Ibid., 6, Figure 1.1.

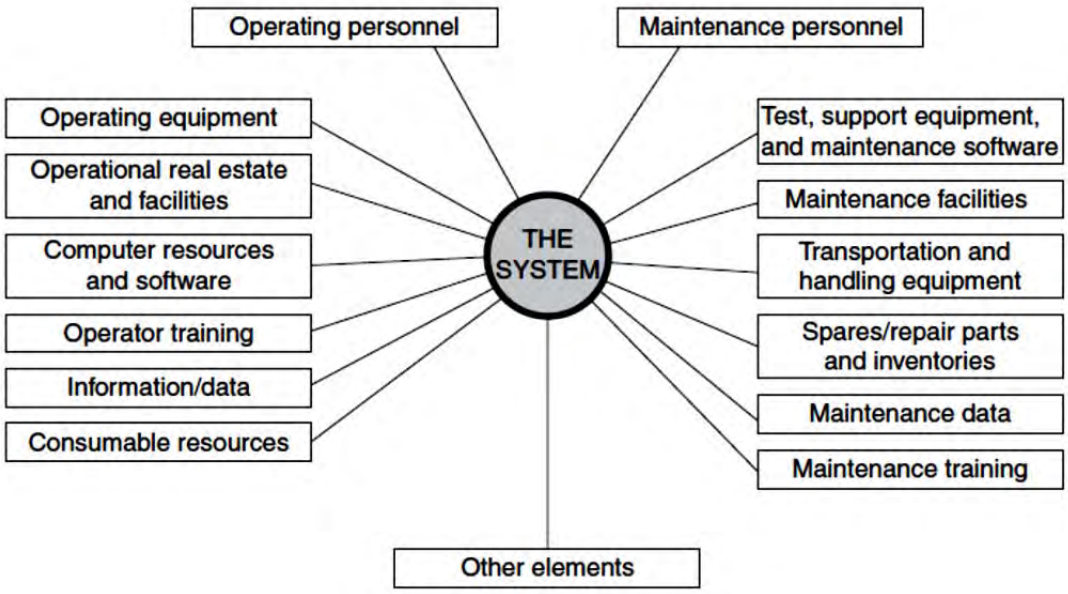

Figure 13. SoS Element Focus[104]

After an organization identifies a system, the next step is to create a method to develop it. Engineers, government institutions, and military acquisition professionals focus a few key models to guide system development. The Defense Acquisition University created a base model for system development that consists of three design process, five realization processes, and eight technical management processes which is depicted in Figure 14.

104 Ibid., 7, Figure 1.2.

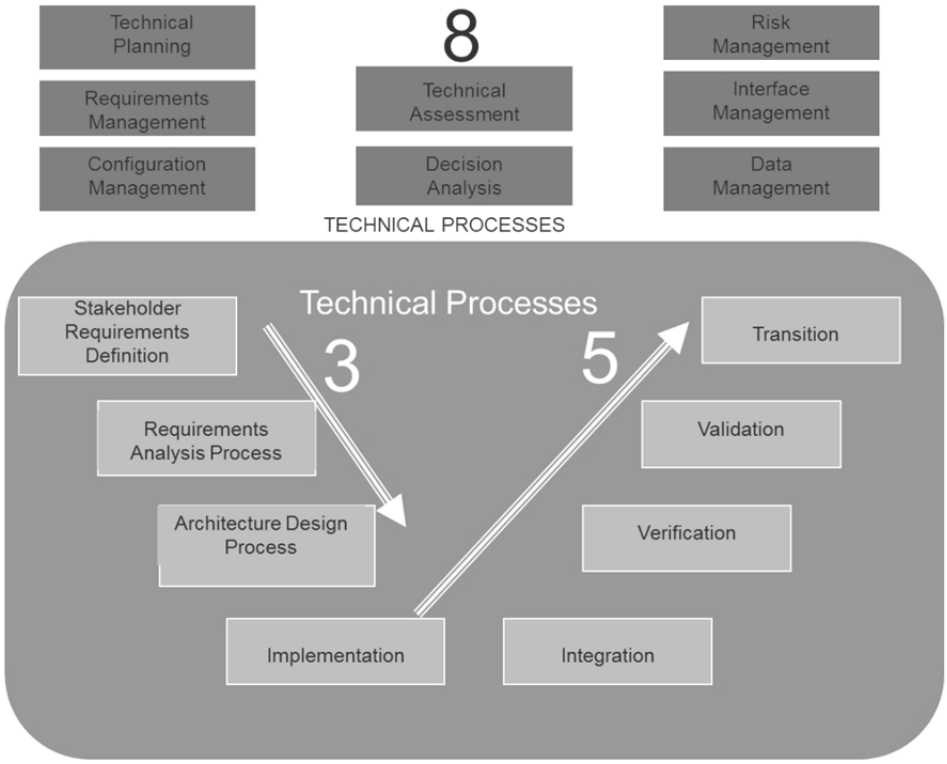

Figure 14. System Development Model[105]

Each technical process, in a phased approach, moves through the realization process through a series of progress reports, tests and evaluations. An example of this process is evident in Figure 15. The example demonstrates a process that has passed to the Engineering and Development phase of the acquisition process. Within the model shows the design processes, realization processes, and all of the reports, trades, and assessments.

105 William Fast, "Systems Engineering Process," presentation at Naval Postgraduate School, Monterey, CA, July 10, 2014, slide 12.

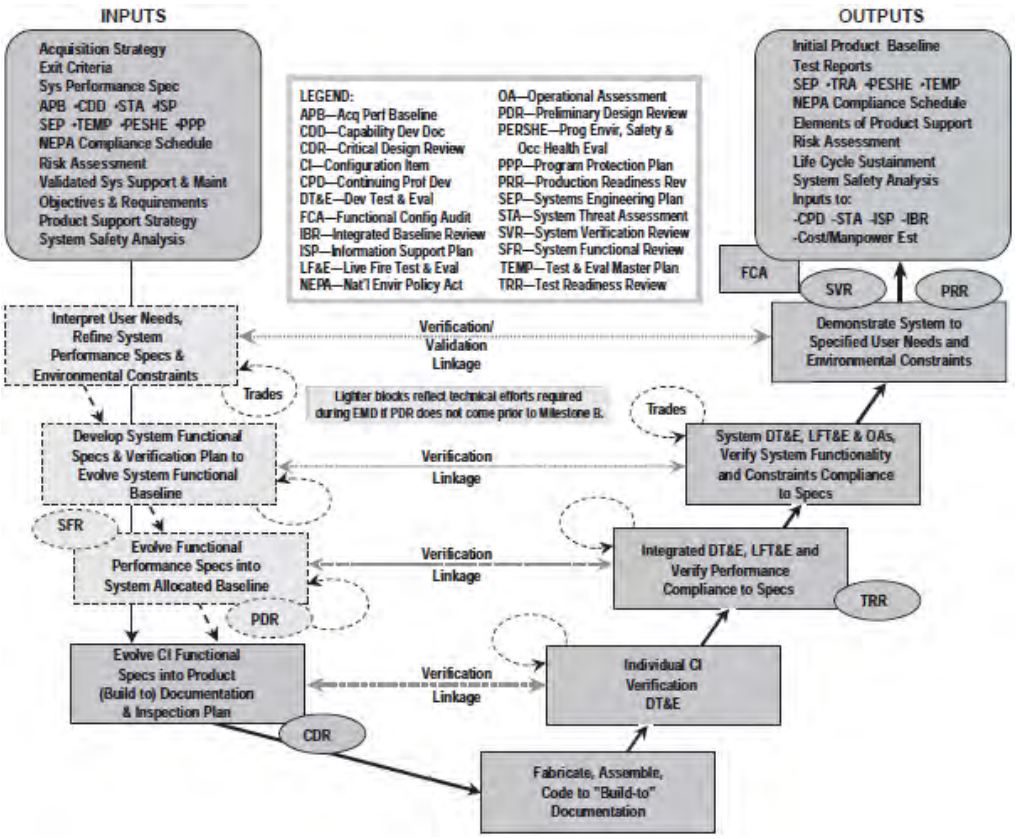

Figure 15. Development Example[106]

Observers notice that the development models get noticeable more detailed than the other system definition models. While true, time, frequent use, and experience alleviate what can appear to be cumbersome methods of systems engineering. Even if someone has mastered those system and development models, working through a system of systems is still a challenge. As a remedy, systems engineers or program managers derive SoS models. The SoS models identify major subsystems, system interfaces, and possible areas of risk. Identifying risk can be arbitrary but some submit that places where subsystems share interfaces represent areas that pose risk. The SoS model in Figure 16 not only shows the major subsystems and system functions but the interfaces between the subsystems.

106 William Fast, "Systems Engineering Process," presentation at Naval Postgraduate School, Monterey, CA, July 10, 2014, slide 60.

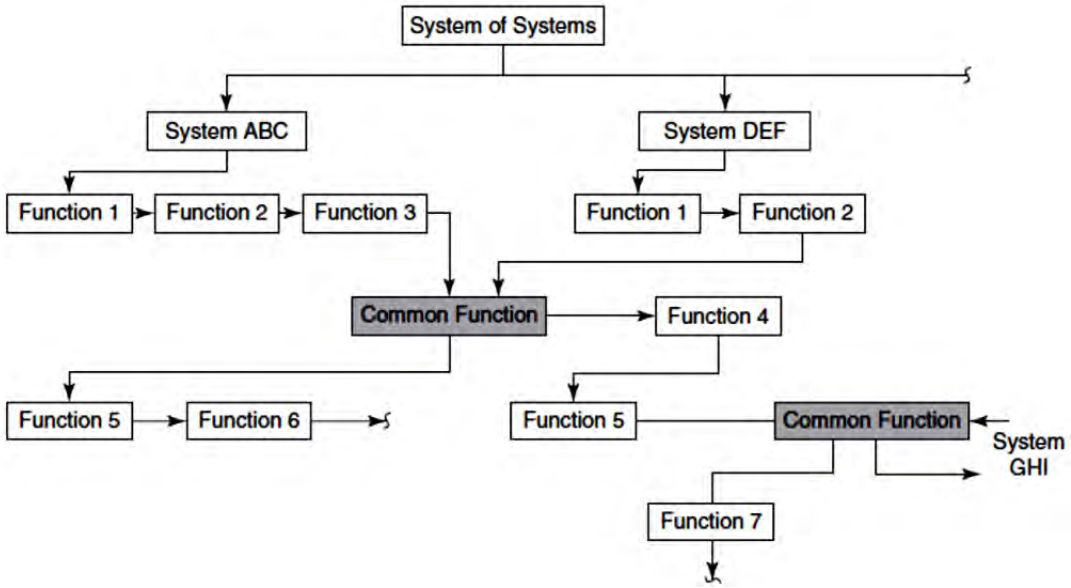

Figure 16. SoS Base Model[107]

Assuming risk is a place of shared interfaces; the common functions should present themselves as places where the systems engineer should target extra attention. Now one sees how each system requires a systems definition model and requisite function models. Moreover, each system progresses through the development models by phase if the SoS is to be effectively produced.

C. COE AS A SYSTEM OF SYSTEMS

For the case of the problem with SVBIEDs and their impact on mission accomplishment, it may be necessary to create a SoS to identify the key systems, functions, and elements of risk so that it may be broken. With the contemporary battlefield as a backdrop, Figure 16, a textbook example, will aid the construction of a SoS with the enemy, friendly, and neutral units serving as subsystems. The remaining SoS models in this chapter were developed by this author and use Figure 16 as a base to create other SoS products.

107 Blanchard, *Systems Engineering Management*, 87, Figure 2.22.

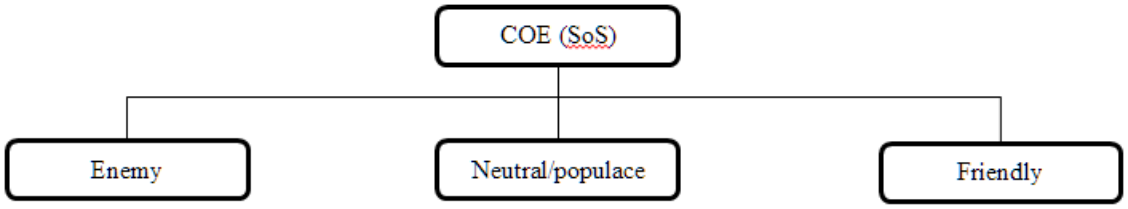

Figure 17. The COE with its Subsystems

1. The Enemy System—First Iteration

The word "enemy" is intentionally vague because it allows flexibility for the construction of subsequent models. Because we used the contemporary operating environment (COE) as the SoS, the enemy is built around groups similar to Al-Qa'ida, Taliban, ISIS, etc. While those groups are well known, any non-state organization that utilizes suicide attacks as a tactic is representative of an enemy unit in the COE. Simple destruction of people and property is not the primary goal of these enemy units. Instead, enemy goals mirror Al-Qa'ida's published strategic mission which involves the overthrow of corrupt and heretical governments of moderate Muslim states, and their replacement with governments based on Sharia Law.[108] Understanding the enemy's goals is noteworthy but identifying the functions and process that the enemy units rely upon to accomplish that goal is just as vital. Many terrorism experts like Bruce Hoffman argue that strategic messaging is their most important enabling activity. Even before the attacks on September 11, 2001, Mr. Hoffman said, "terrorism may be seen as a violent act that is conceived specifically to attract attention and then, through the publicity it generates, to communicate a message.[109] Enemy emphasis on its message compels the model's engineers to treat messages as method to initiate operations and the response of successful operations.

An effective message enables other key enemy functions like recruiting, mobilization, and targeting. The enemy owns the ability to attack when all functions are met with some degree of success. Although attack methods are plentiful, this model will

108 Robert Earl and Emery Norman, "Terrorist Approach to Information Operations" (master's thesis, Naval Postgraduate School, 2003), 71.

109 Bruce Hoffman, *Inside Terrorism* (New York, NY: Columbia University Press, 1998), 131.

focus on the SVBIED. Now, with an idea of the enemy's functions and methods, one can build the first iteration of the enemy system model, which will look like Figure 18.

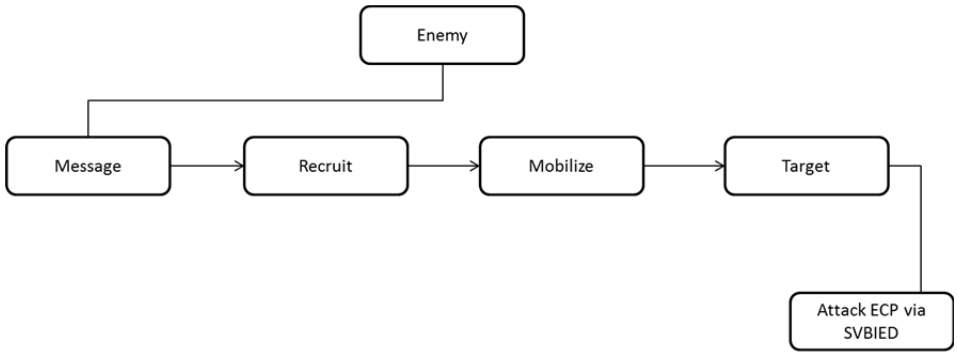

Figure 18. Enemy System—First iteration

2. The Friendly System—First Iteration

Friendly units directly oppose the enemy systems and for this model, can be considered state sponsored militaries or security forces. After initial offensive operations, the friendly system is defensive in nature and must react to enemy actions rather than maintain a tactical initiative. Instead of doctrinal warfighting functions primarily used by U.S. forces, the first iteration of the friendly model will use functions that other security forces commonly share; mobilize, train/equip, plan, and task/act. Mobilization occurs first because some indigenous security forces deploy before any training given by other militaries. In essence, they receive on the job training. Normally, the friendly units' tasks are three-fold and include; provide security, protect the populace, and defeat the enemy. Controlling traffic is one method that friendly units discover meets all three missions. Thus, the first iteration of the friendly system model looks like Figure 19.

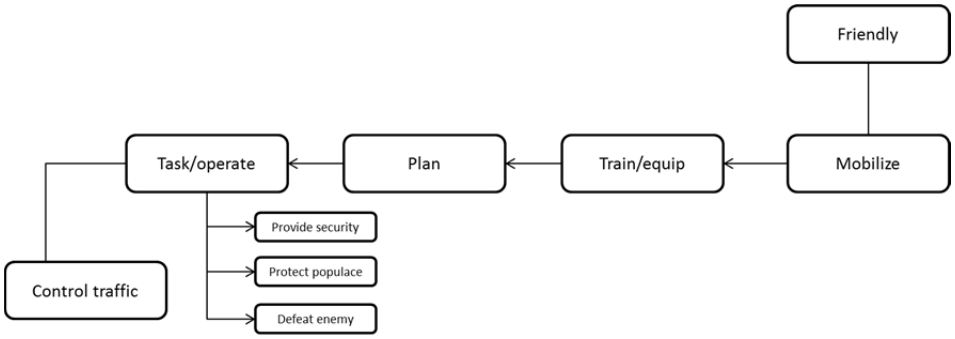

Figure 19. Friendly System—First Iteration

3. Neutral System—First Iteration

Adding the neutral system to the previous two will reveal the interface of all three systems within the COE, which is represented by Figure 20. Essentially, the first overt case of risk comes into view.

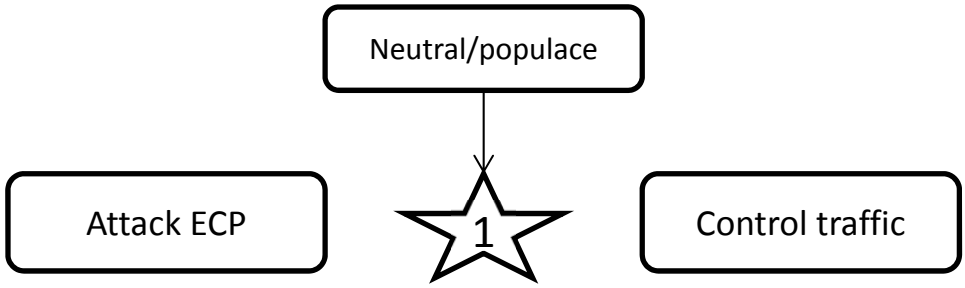

Figure 20. Interface #1

The enemy has judged that traffic control measures offer a suitable target for their immediate goals. They physically target the friendly system through the suicide attack while cognitively targeting the neutral system simultaneously. One argument against this model is that the enemy may harm the neutral system as well. While this is a valid concern, the enemy system puts into practice the theory of "outbidding." Outbidding "suggests that insurgents use suicide bombings to show that they are more committed to the cause of liberation from occupying forces than other groups, because they are willing

to make greater sacrifices for the struggle."[110] Whether or not the attack inflicted damage to the other systems is less significant than the fact that the enemy positioned themselves well to exploit the attack and carry forward a series of powerful messages into the second iteration of the model.

4. Enemy System—Second Iteration

From the enemy's standpoint, a successful action means they do not have to change their base essential functions. Similar to the first iteration, the enemy begins with its messaging. From the enemy's point of view, the message aimed toward the friendly system is that they can inflict destruction to powerful forces at any time. The message that the friendly system cannot protect the populace is aimed at the neutral system. Before the enemy conducts another operation, they learn from the first. While it may take time, enemy units realize the danger of causing harm to the local population. A study done by the Program for Culture and Conflict Studies contends that evidence from enemy statements show they recognize the danger civilian casualties pose towards their public relations campaign. [111] With that in mind, the next logical action for enemy might be to provoke undue harm from the friendly units onto the populace. As such, Figure 21 depicts the second iteration of the enemy system.

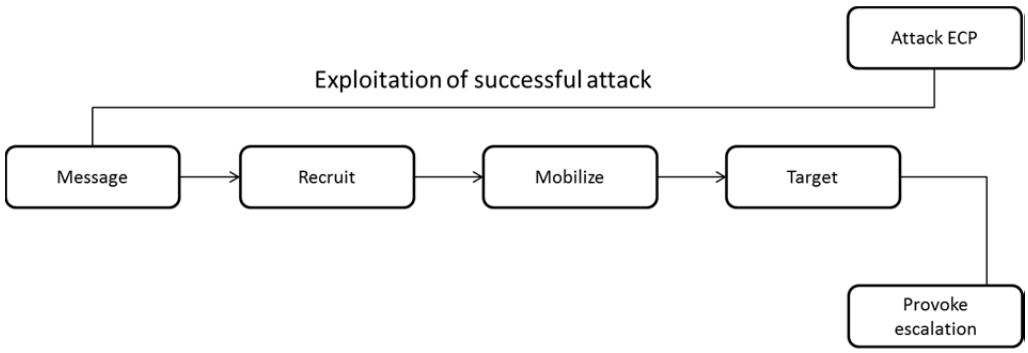

Figure 21. Enemy System—Second Iteration

110 Clark McCauley and Katherine Seifert, "Suicide Bombers in Iraq, 2003–2010: Disaggregating Targets can Reveal Insurgent Motives and Priorities," *Terrorism and Political Violence* 26, no. 5 (February 2014): 805.

111 CCS Research Staff, "Suicide Attacks on the Rise," *The Culture and Conflict Review* 2, no. 2 (March 2008): 9.

At this point, the enemy functions remain the same while the friendly system must change their essential functions because of the successful attack and following message campaign waged by the enemy.

5. Friendly System—Second Iteration

Immediately following the first attack, friendly units react and are forced to reassess their essential functions. In an attempt to quickly guard against deadly SVBIEDs, friendly forces redistribute forces, retrain personnel, increase total forces and then, one again, act. The new functions create negative outcomes inside the friendly system. First, the focus on suicide bombers instills a level of confusion or fear in some of the friendly units. Second, the surprising enemy tactic takes time to properly counter and there exists a natural training deficiency. The deficiency generates poor tactics and techniques at traffic control points that lack proper tools to operate within the constraints of the rules of engagement (ROE). Because of the poor reactions, the second iteration in the friendly system model results in an ROE violation as depicted in Figure 22.

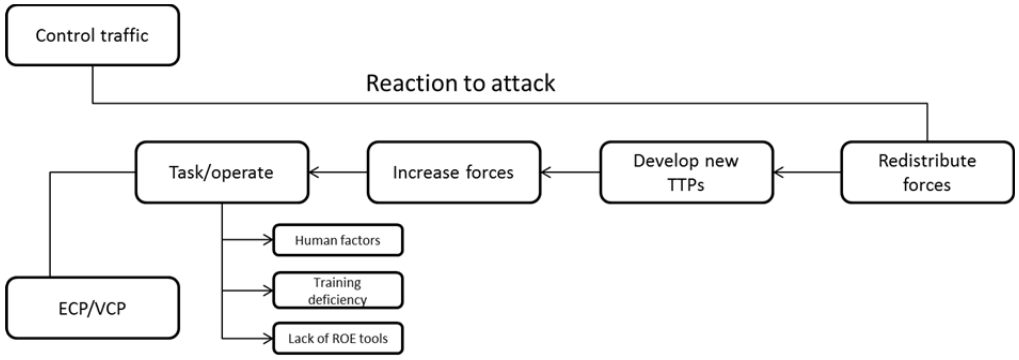

Figure 22. Friendly System—Second Iteration

6. Neutral System—Second Iteration

Adding the neutral system to the second iteration reveals another area of risk. An ROE violation constitutes a victory for the enemy even though they did not conduct an attack. Not only did friendly actors cause harm and disruption to the populace, they handed the enemy more substance for their messaging campaign. Two areas of risk give the enemy obvious advantages. They can attack to inflict damage and show strength in

one area while just threaten violence and exploit friendly mistakes in the second. Figure 23 illustrates both of these risks.

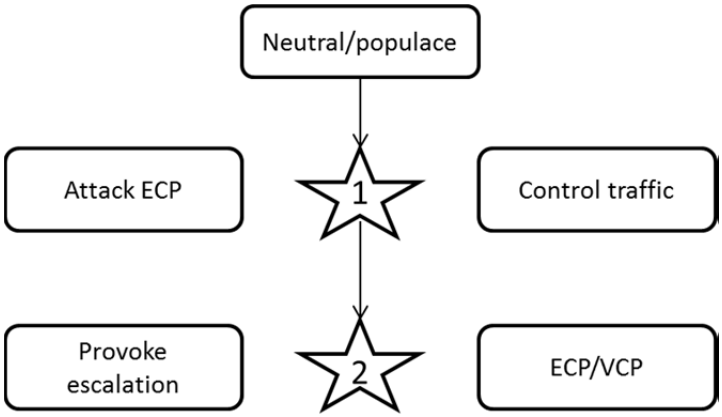

Figure 23. Neutral System—Second Iteration

In addition to the first set of messages the enemy exports to the other systems, they have an opportunity to diversify their themes. One additional message relates directly to the ROE violation at risk area two. The message of "The invaders are here to harm you" would not only thwart friendly efforts to win over the populace but add the "recruiting effect" described by researchers from the National Bureau of Economic Research (NBER).[112] The message to the friendly actors shifts from "We can inflict destruction" to "We choose the time to cause the destruction." At the end of the second iteration of the SoS model, the enemy has maintained its essential functions, caused harm, and crafted effective messages to other systems while the friendly system has only been able to react to enemy operations.

7. Enemy System—Third Iteration

After the gaps in friendly capabilities contributed to ROE violations that may have resulted in civilian casualties, it is clear what message the enemy system will deliver to the neutral populace. Messages focused on civilian casualties plague friendly

112 Luke Condra, Joseph Felter, Radha Iyenga, and Jacob Shapiro, *The Effect of Civilian Casualties in Afghanistan and Iraq* (NBER W16152) (Cambridge, MA: National Bureau of Economic Research, 2010), 6. http://nber.org/papers/w16152.

operations to thwart enemy recruiting efforts. NBER researchers assert the message is so powerful that "the data are consistent with the claim that civilian casualties are affecting future violence through increased recruitment into insurgent groups after a civilian casualty incident."[113] The powerful message allows the enemy system to maintain its key functions and continue its campaign against the friendly system. The third iteration of the model with these points in mind is Figure 24.

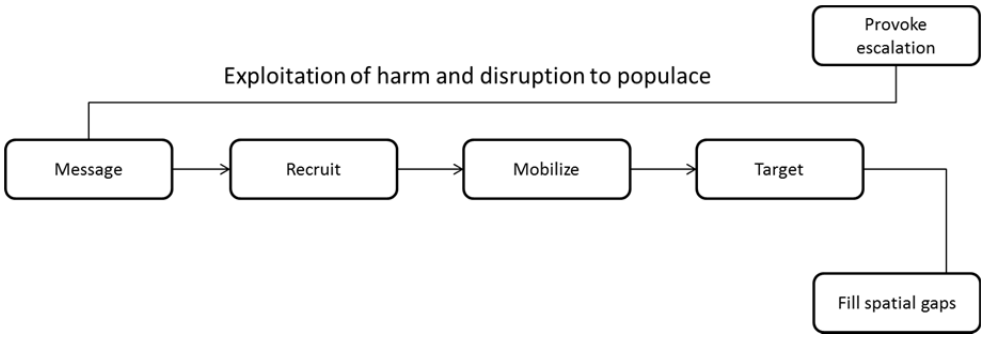

Figure 24. Enemy System—Third Iteration

Before this iteration ends, one expects the enemy to lessen its attacks as it weighs the friendly system's likelihood of causing civilian casualties with the goals of its own future operations. Further, the enemy observes the friendly system move away from population centric operations and focus on force protection and enemy neutralization.

8. Friendly System—Third Iteration

Friendly and civilian casualties from a myriad of sources force the friendly system to again, modify its essential functions. With its focus now centered on enemy weapons/tactics and their destructive effects, the friendly system adjusts by adding more barriers, armor, bases etc. The friendly system, at this point, looks like Figure 25.

113 Ibid., 3.

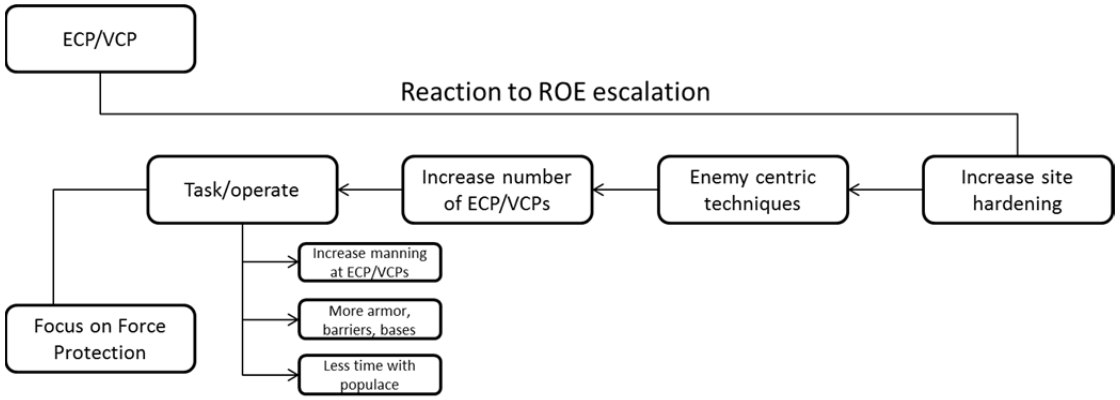

Figure 25. Friendly System—Third Iteration

Increased physical barriers, armor, and static sites lessen the friendly system's maneuverability, add to their overall logistical requirements, and pull units away from the populace. The spatial gap creates yet another area of risk. Fewer friendly units properly interacting with the populace provides the enemy with an opportunity to exploit.

9. Neutral System—Third Iteration

The next neutral model exhibits the numerous areas of risk present in the COE. This next area of risk has less to do with kinetic effects of enemy and friendly weapons and more to do with where each system can be in a geographic sense.

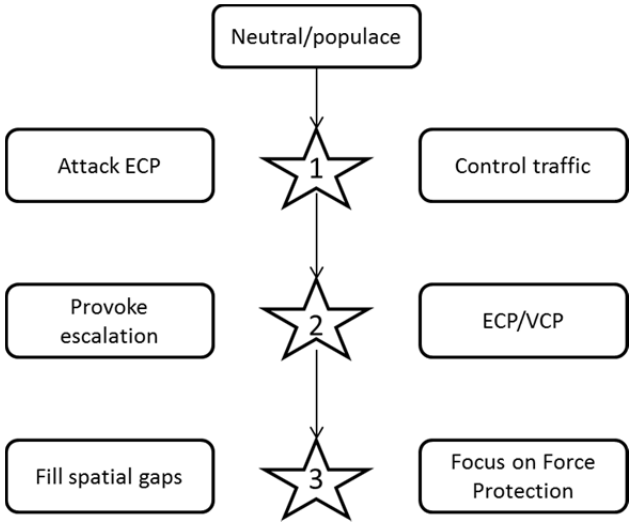

Figure 26. Neutral System—Third Iteration

Figure 26 demonstrates the enemy proves it is strong enough to inflict damage and resolute enough to die for its cause when it attacks an ECP with a SVBIED. They then provoke civilian casualties or damage which gives them at least two advantages. One, they export a message stating that the friendly units only do them harm. Two, the friendly system reacts by building more barriers (physical and psychological) between them and the populace. Enemy actors exploit both barriers.

10. Enemy System—Fourth Iteration

The last iteration of the enemy system revolves around exploit the spatial gap that the friendly system has left near the populace. With friendly actors' interaction with the populace being less frequent, the enemy provides services in attempt to gain more persuasive momentum in the battlespace. They may not abandon other forms of persuasion like violence and intimidation but they shift some of their key functions to meet the populace's needs. Figure 27 depicts their functions as providing security, providing rule of law, and collecting and distributing taxes. The enemy seeks to thoroughly embed themselves into the populace's way of life and eventually compete for overall legitimacy.

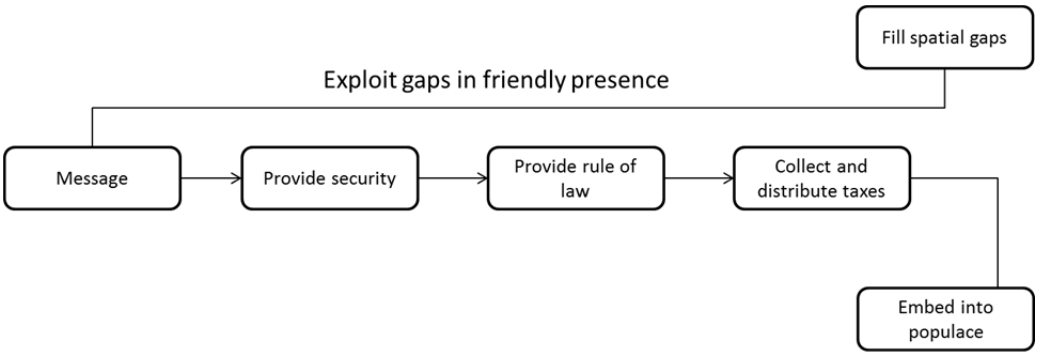

Figure 27. Enemy System—Fourth Iteration

It is false to think that the progression through the enemy system must be measured on a scale of months or years. Even though it could take that long, the enemy system may move on a much quicker timeline. One example involves a respected local police chief and thirteen of his men who were victims of a suicide attack near Kandahar

City. The attack killed a staunch friendly actor, bolstered enemy strength, and forced others to draw back away from the populace. All combined, it left the area vulnerable to prolonged enemy efforts.[114]

11. Friendly System—Fourth Iteration

Compared the enemy, the friendly system within the COE is much slower to adapt to changing conditions required to accomplish its mission but the adaptations do eventually occur. Figure 28 demonstrates the positive changes the friendly system takes combat the enemy's campaign to gain legitimacy. New friendly functions include the application of learned lessons, new training, and a renewed focus on the populace. The friendly actors have more experienced units, specialized equipment, and the realization that they must accept some additional risk to maintain a footprint closer to the populace instead of being safely behind massive barriers or bases. The result is manifested through comprehensive, population-focused COIN operations.

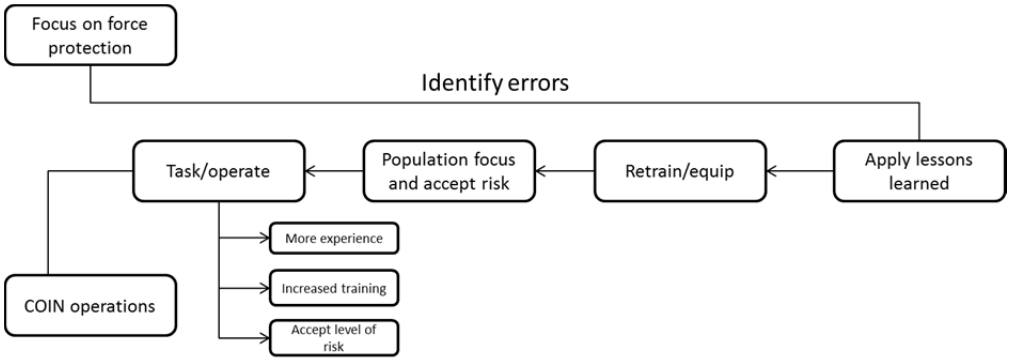

Figure 28. Friendly System—Fourth Iteration

The lines of operation within COIN are similar to the enemy's functions but the methods to carry them out are different. One thing for sure though, is that they aim to gain legitimacy from the populace. Figure 29 shows each iteration with the areas of risk created from the interfaces from each system and how those areas of risk compound to influence legitimacy.

114 CCS Research Staff, "Suicide Attacks on the Rise," 8.

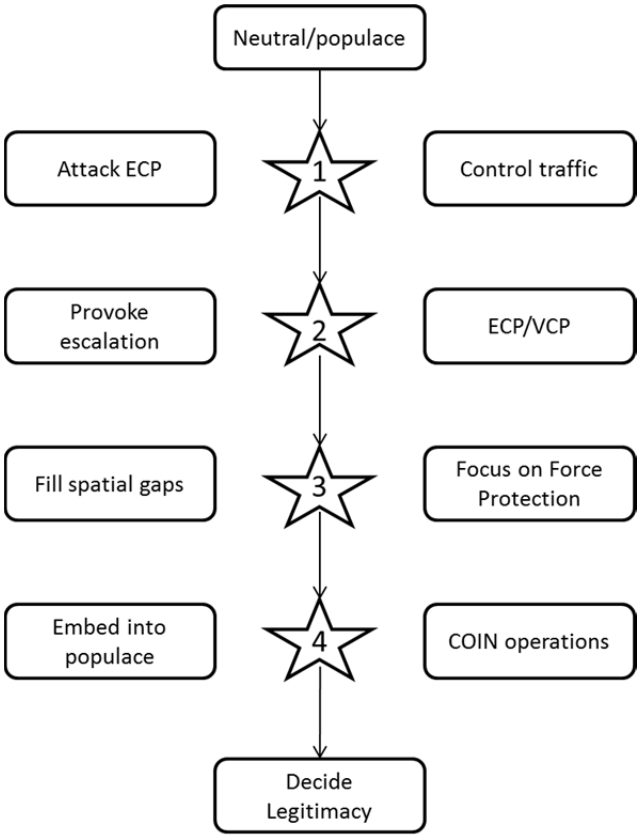

Figure 29. Neutral System Combined

D. LESSONS FROM THE ENTIRE SOS

Figure 30 depicts the entire SoS when each iteration from all actors are put together. Beyond just a conceptual aid for friendly planners to visualize where risk may exist or how the major systems may function, the SoS model hints at points where friendly actions can stem the enemy system's ability to gain legitimacy. The idea is that the friendly system needs to break the link between an enemy action and the subsequent message that perpetuates further operations. If one attempted to build a tool to accomplish this by reducing risk in each highlighted area, at least four things would have to be accomplished. This tool must prevent suicide attacks while not causing undue harm to the local population. Further, it must usable within small units to leave more friendly units to operate among the populace and still add an effective layer of protection for friendly units operating in an ROE constrained environment.

With respect to the specific threat of an SVBIED, a solution entails the ability to stop a vehicle non-kinetically while not causing harm to its occupants, does not require large amounts of space or personnel to operate, and is reliable enough to be a suitable for force protection. Taking no action surely results in more SVBIED attacks. Not expanding non-kinetic tools into the friendly system's arsenal will result in more civilian casualties and the adding further physical barriers only isolates the friendly actors from the populace. Methods that do involve any of those options but still encompass the characteristics needed to break the link between enemy action and enemy message may be closer to realization than some think. Numerous agencies think that HPRF DE systems exemplify a viable solution to this problem. New technology indicates that HPRF DE systems can be made smaller, lighter, and more reliable than ones tested in the past. In addition, the targeted vehicles used by the enemy system consist of electrical components that are more vulnerable to HPRF propagation. An exact solution needs more testing but now that the SoS model helped highlight the objectives to break the enemy system, the HPRF system's requirements can be refined.

No reasonable person would contest the importance of standard military planning processes. They proved repeatable, effective methods to create cohesive plans under difficult circumstances. Unfortunately, the doctrinal planning processes do not always allow the planners a means to fully understand the problem. This paper argued that a system engineering approach to current challenges reveals useful information that can help plan a path to mission accomplishment. With the COE as a SoS, major subsystems with their essential functions were modeled and then combined to identify potential areas of risk. Then, requirements to negate, or at least decrease the risk were extrapolated from the system's linkages. Finally, the argument introduced HPRF as a candidate capable of breaking the action/message linkage the enemy needs to maintain its campaign.

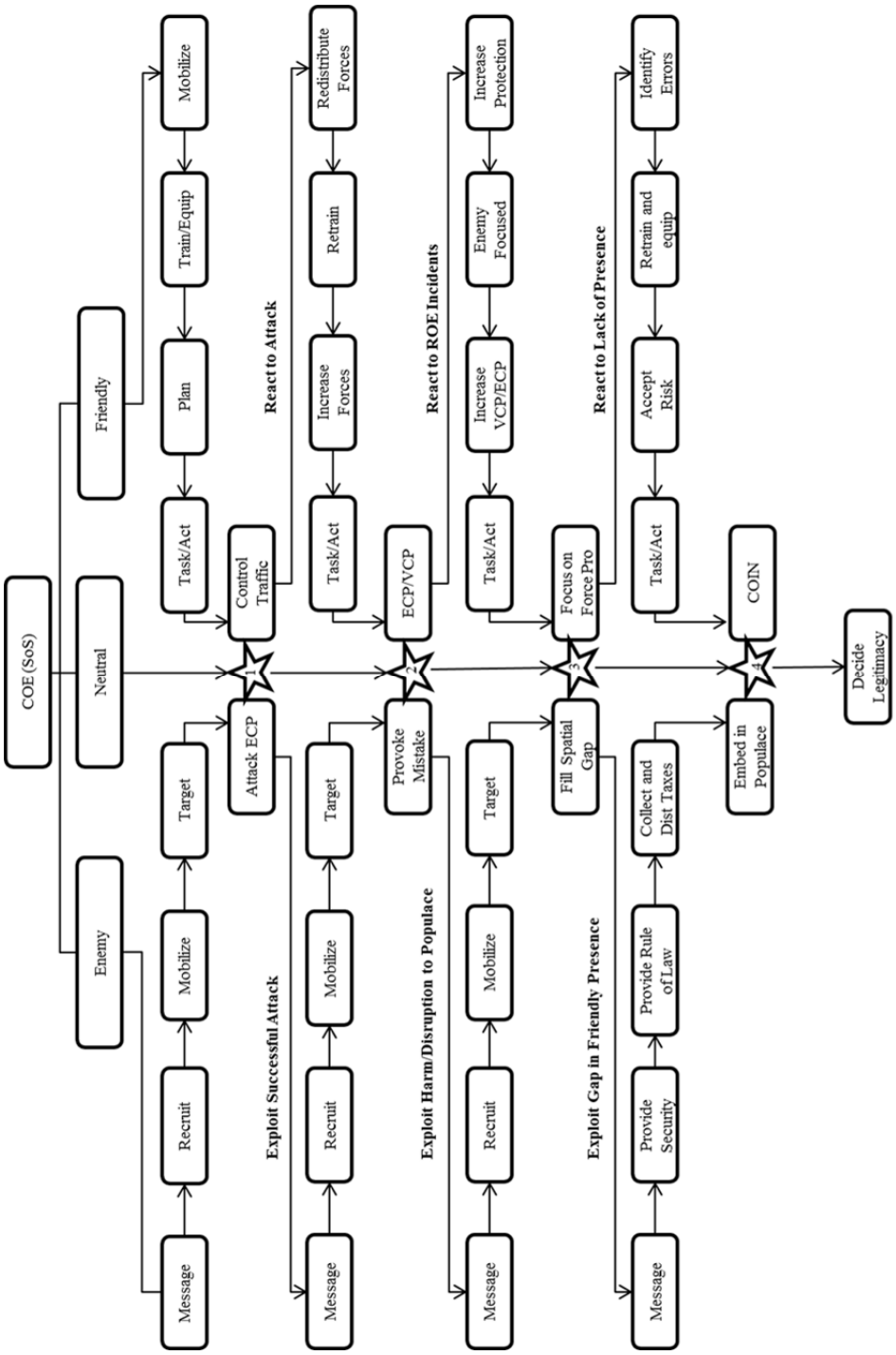

Figure 30. COE (SoS)

V. ANALYSIS OF ALTERNATIVES

A. RESTATE PROBLEM

Throughout this thesis, SVBIEDs served as the root problem that confronts military, government, and civilian agencies across the globe. Their massive payloads guarantee devastating physical destruction, media coverage, and fear. It is not too difficult to think of awful attacks that involved SVBIEDs from WWII to the current war on terror. While 70 years have spanned those two conflicts, some truths remain. One, some enemy combatants will sacrifice their bodies to do the U.S. harm, and two, those tactics are still effective. The difference is that current SVBIEDs target areas where civilians go about their daily routines; places like ECP/VCPs. Efforts intended to protect those civilians and service members have been noble yet feckless. Besides bigger barriers, more intrusive searches, and a few interesting "widgets," ECP/VCPs remain easy targets to inflict maximum damage, export a message of power and resolve, and tear at the fabric of society.

B. REVISIT THESIS MAIN POINTS

To address the problem, this thesis proposed that emerging technology in solid-state HPRF DE augmenting existing ECP/VCP tactics, techniques, and procedures could protect local populations and service members while stifling the enemy's ability to create spectacular attacks meant as a deadly weapon and information tool. Three distinct sections discussed included Force Protection and ECP/VCPs, Directed Energy, and System of Systems Analysis. Before the alternative ECP/VCP is described or other recommendations are made, it is fitting to quickly revisit those three subjects.

1. Force Protection and ECP/VCP

Force protection is a Herculean effort. Not only does this warfighting function encompass protecting service members but also includes civilian employees, families, and equipment. Normally, at the front lines of force protection lays ECP/VCPs.

As demonstrated earlier, ECP/VCPs can vary in size but all should share a few characteristics in their construction. First, an approach zone whose goal is to alert, slow, and canalize incoming traffic is created. The approach zone leads directing in to the access control zone.

The access control zone represents the area of greatest risk inside an ECP/VCP because this is where enemy actors, friendly personnel, and civilians are in closest proximity to each other. One could find search areas, traffic management equipment, and specialized equipment in the access control zone.

The response zone in an ECP/VCP is outside of immediate threats but still close enough to control the site. Reaction forces, command and control, and additional protective measures all fall within the response zone.

Lastly, ECP/VCPs should have a safety zone. Simply, the safety zone is an area well outside the ECP/VCP and only provides support to those staffing the checkpoint. Even if those four zones are constructed perfectly, vulnerabilities still exist in ECP/VCPs. The thesis suggests that directed energy can alleviate some of those vulnerabilities.

2. Directed Energy/HPRF

DE proves an exciting and flexible tool for a myriad of military applications. Typically, most associate lasers, HPRF, and even particle beams with DE. While correct, more attention is given to solid-state HPRF in this thesis. The idea is that properly leveraged HPRF waves bombard and overwhelm the electronic components of vehicles causing them to stop.

Emerging solid-date HPRF technology exponentially reduces the size and weight most traditional HPRF systems are known for. In addition, these new HPRF systems could provide increased flexibility in ECP/VCPs because they are non-lethal systems that protect local civilians, add reaction time for operating units, while still thwarting enemy attempts to attack ECP/VCPs with SVBIEDs.

Some argue that HPRF amounts to little more than another technological breakthrough that only addresses one issue. To guard against exalting HPRF as the next

great military system, a full SoS analysis was completed to surmise if HPRF can affect more than just a vehicle. Perhaps, HPRF's capabilities can play a larger role in defeating an entire SVBIED system and not just the SVBIED vehicle alone.

3. System of Systems Analysis

Problem solving in the military usually comprises a codified set of procedures to distinguish an enemy's strengths, capabilities, requirements, and goals. MDMP, MCPP, and JOPES are just a few of the methods utilized by the services but none of them attempt to understand the inherent linkages between the enemy and the rest of the actors in the operating environment.

For this reason, a thorough SoS analysis using systems engineering models was completed so one could see how each subsystem related to each other. Moreover, the SoS analysis demonstrated places that, if interdicted, would hinder the enemy from advancing their overall goals.

From the friendly perspective, the linkages that connect the enemy's system must be severed to stop their continued successes. The model illustrates that a few ways to halt the enemy system like large obstacles or even lethal measures actually do more to increase the enemy's ability to accomplish its goals. As a result, new tools like HPRF are submitted into the model as a possible candidate to reduce risk to friendly and neutral actors while degrading the enemy system.

C. DESIGN REQUIREMENTS

If HPRF is indeed a capability that services need at ECP/VCPs, design requirements have to be proposed so planners can create a conceptual HPRF augmented ECP/VCP that is an alternative to current ones.

1. HPRF Design Requirements

It is a difficult task to create design requirements for any system let alone one that can be as complicated as an HPRF DE system. To simplify the process, a few considerations from the model in Figure 31 will be addressed.

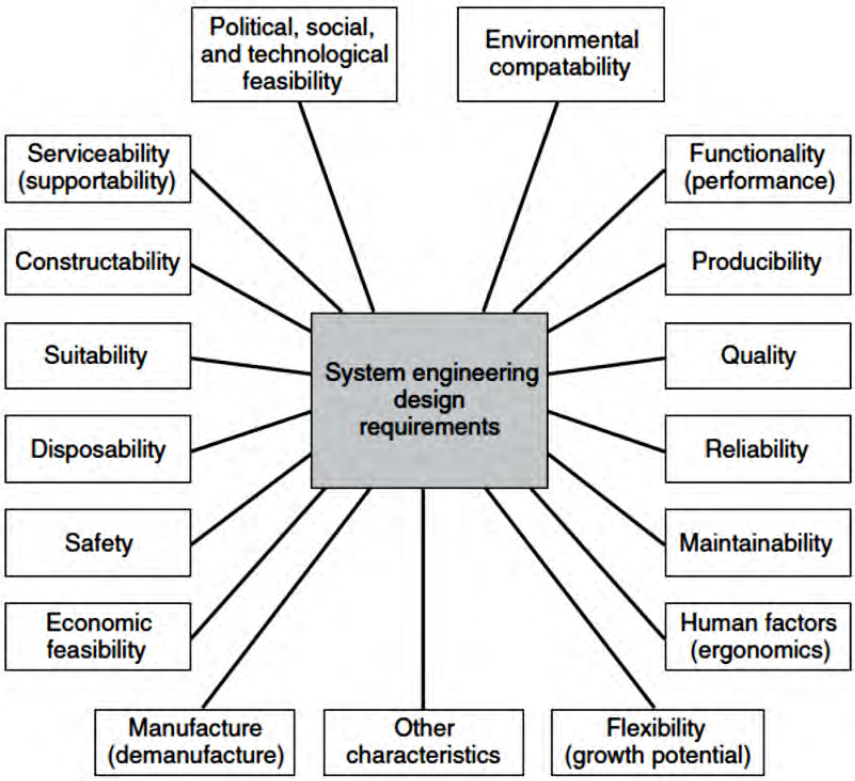

Figure 31. Design Requirements Considerations[115]

Dissecting each consideration is an untenable endeavor for this thesis so this research will focus on four including serviceability (supportability), suitability, functionality, and flexibility. For continuity, their definitions are below.

2. Serviceability/Supportability

Serviceability/supportability is design, technical support data, and maintenance procedures to facilitate detection, isolation, and timely repair and/or replacement of system anomalies.[116] In short, serviceability can equate to ease of use. For the HPRF system augmenting an ECP/VCP, two main requirements fall under serviceability/supportability. First, the system uses only commercial off the shelf power generators. Specialized power generation systems necessitate other special equipment and

115 Blanchard, *Systems Engineering Management*, 104, Figure 2.31.

116 Defense Acquisition University, *Glossary of Terms* (Ft Belvoir, VA: Defense Acquisition University, 2009), B-175.

maintenance materials. Those logistical needs do nest well with small unit expeditionary operations. Next, the solid-state HPRF system requires no subject matter expertise for operation. Only basic knowledge of antenna construction and communications maintenance keeps the system functioning and operational.

3. Suitability

Suitability refers to the ability to accomplish a purpose and comply with the commander's guidance.[117] For this problem, suitability consists of three design requirements. The solid-state HPRF system must smoothly integrate within at least one of the four ECP/VCP zones. Technology must enhance operations instead of forcing operations to fit technology. Next, the system must have remote use capability so operators are outside the minimum safe distance for an SVBIED with 500lb of explosives. Lastly, the system is only non-lethal and does not permanently damage people or their property. It must be a tool for ROE sensitive environments.

4. Functionality

Functionality is the measure of whether or not the system performs as it is designed. Most importantly, the system must demonstrate effectiveness on at least 90% of vehicles ranging from motorcycles to dump trucks. Also, desired effects on targets need to occur within five seconds of the radiation reaching the target. Finally, the wide band frequency has to remain between 60MHz and 66MHz. These frequencies show promise is back door coupling and allow 4–5 element antenna arrays with ½ λ spacing to be small enough to fit in an ECP/VCP but still powerful enough to generate good effects on specified targets.

117 United States Marine Corps, *Marine Corps Planning Process*, (MCDP 5–1) (Washington, DC: Department of the Navy, 2010), 22.

5. Flexibility

Flexibility is the capability for effective reaction with actions appropriate and adaptable to the circumstances existing.[118] The solid-state HPRF system's flexibility lies in its utility in a variety of roles. Those roles will be discussed after the ECP/VCP alternative is presented.

D. ALTERNATIVE ECP/VCP WITH A SOLID-STATE HPRF SYSTEM

Figure 32 represents what an ECP/VCP with a solid-state HPRF system located in the approach zone. A list of a few characteristics and assumptions will help readers understand the ECP/VCP layout.

- Friendly Unit Size—Platoon with Battalion level support, semi-permanent ECP/VCP that can be constructed and demolished is less than 24 hours.
- Enemy Threat—Small to Mid-sized car, 500lb explosive charge.
- Propagating Frequency—60–66MHz. Using basic physics equations, 60MHz yields a ½ λ of 2.5m or 8.2ft. A five element array would be 32.8ft. 66MHz would equate to a 29.8 ft array.
- Turn radius - <50 ft to prevent vehicle speed above 20mph.
- Distance to response zone—Min safe distance based on 500lb explosive charge.
- Distance to safety zone—Min safe distance based on 4,000lb explosive charge.

118 Department of Defense, *Department of Defense Dictionary of Military and Associated Terms,* (JP 1–02), 90.

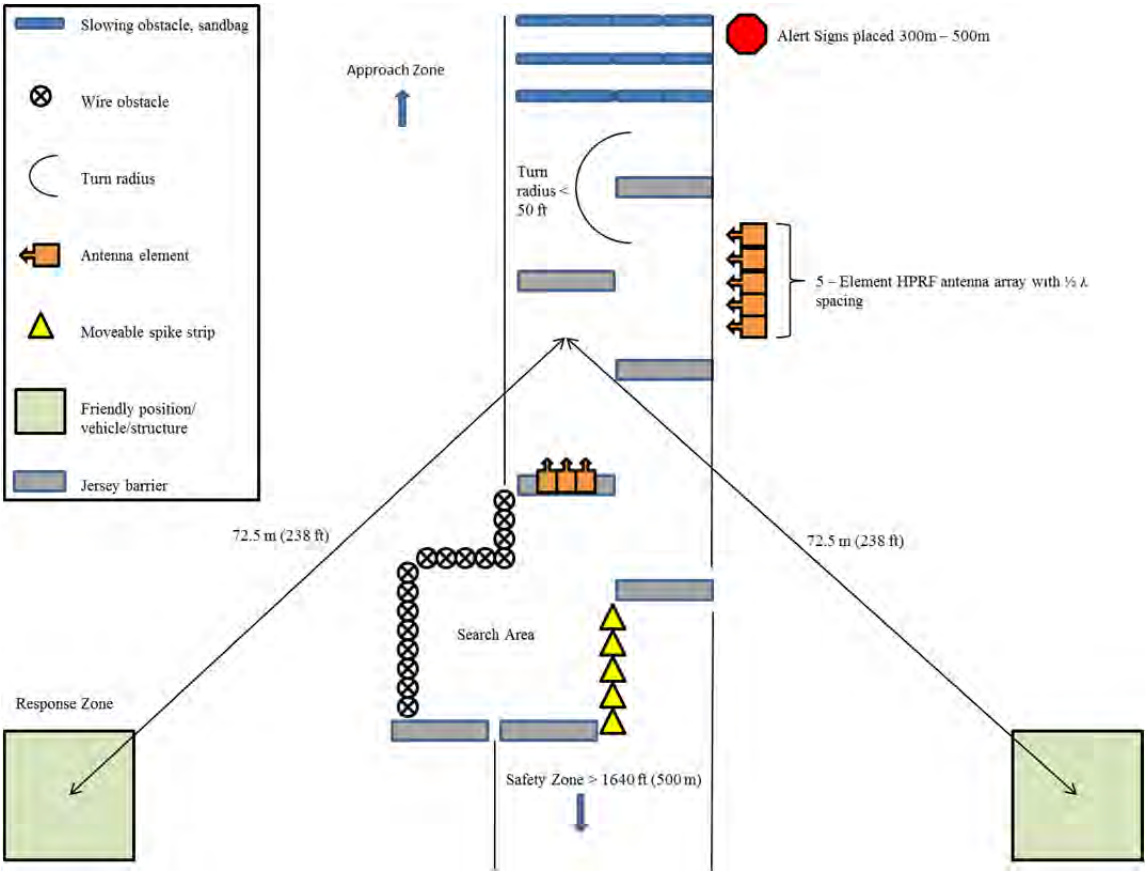

Figure 32. Solid-State HPRF Augmented ECP/VCP

This alternative ECP/VCP is just one method of construction. Leaders still have flexibility to adapt the system to their specific situations and environments. With knowledge from previous chapters and assumptions just provided, one immediately notices that this ECP/VCP has enhanced existing, practical techniques with HPRF technology to meet current threats.

For this ECP/VCP, the HPRF system is best used in the approach zone where it can increase standoff from the vehicles to those operating the checkpoint. After vehicles initially slow from the first set of obstacles, they proceed through a set of serpentine barriers. The turning radius of the serpentine serves a few purposes. First, it slows the vehicles to a point where it cannot build enough kinetic energy to breach the ECP/VCPs obstacles. Tables 1 and 2 in Chapter II showed the relationship of turning radius, skid speed, and kinetic energy. Leaders could utilize that information to adjust the turning

radii of their serpentines based on their environments. Second, it forces the vehicles to further decrease their speed so the operators have enough time to utilize the HPRF system. Lastly, the numerous turns in the serpentine allows the HPRF waves to "attack" the target at multiple aspects, thereby increasing the chances of coupling.

This ECP/VCP contains two separate HPRF arrays. Each operates between 60MHz and 66MHz so the arrays can fit into the ECP/VCP. Some frequencies may prove more effective against vehicles but the main tradeoff is the length of the array. With these frequencies, a 5-element array with ½ λ between elements would have a maximum length of 32.4 feet. If the frequency were 10MHz, the length of the array would be nearly 200 feet, which is much too long to be useful in an ECP. The placement of the arrays serves valuable force protection purposes as well. One, the arrays have been placed at a 90-degree offset to increase the angles at which the target receives radiation. The HPRF will be able to propagate a pulse against a target's front and broadsides. Because each vehicle reacts different to HPRF, it is important to have the ability to vary propagation angles against a target. In addition, the arrays are places at least 72.5 meters away from the response zones. As shown in Chapter II, that distance keeps people reasonably safe from deadly effects of a 500-pound explosive. If an enemy vehicle is successfully halted by HPRF, it still may have the ability to explode so operators in the response zone need standoff. The distance can be scaled depending on the threat analysis of the area of operations. Similarly, the safety zone is at least 500 meters away from the arrays for the same standoff reasons but for a large SVBIED with 4,000 pounds of explosives.

The response zone has sufficient standoff from threats but is also close enough to the site to operate the HRPF via remote or cable conduit, conduct searches, provide overwatch, and respond to events. Again, the distance from the response and safety zones to the rest of the ECP/VCP is scalable depending on the unit's current analysis of the situation and terrain.

Solid-state HPRF is exciting technology that lends well to current operations but more work needs to be done before a usable system can be fielded into the operating forces. While the technology is close, some issues need addressed. Further research, expanded modelling, and designs for other HPRF uses are required.

E. RECOMMENDATIONS FOR RESEARCH

Further research in HPRF systems should occur in two main areas; target vulnerability and antenna array optimization. Increased vulnerability tests on a variety of vehicles would likely be a great place to focus efforts. As vehicles now incorporate numerous electronic components, system developers' comprehension regarding those vulnerabilities is paramount to perfecting solid-state HPRF systems for military purposes. Unfortunately, people who design modern vehicles know that the world is now an invisible sea of EM waves that can affect their car's operation. They have unquestionably hardened those electronic components to guard against normal EM interference. That drives the next recommendation concerning target vulnerability. Hardened components result in difficult coupling so more research is required to determine how much power, pulse duration, or varying frequencies is needed to gain effects against a target set.

Those variables lead to the second area of recommended research, which is focused on antenna array construction. Depending on frequency, space limitations, desired waveform, and many other things, options for antenna arrays is nearly limitless. After vulnerabilities are identified, the results should drive what array fits best within the entire HPRF system. Different types antennas (loop, dipole, etc.) rate active testing. In addition, experimentation on propagation angle may yield further array options. Currently, arrays only propagate on the same plane as targets. Perhaps testing "bottom up" wave propagation so the HPRF system radiates on the bottom of the vehicle targets the vulnerable components more effectively. For that to be an option, antenna arrays that vehicle drive over are needed.

Results from both research topics would then be combined and modelled so system designers could optimize results and visualize potential areas that require trade-offs. Along with power/effects models, frequency/effects models, et cetera, it is recommended that EMS fratricide models be constructed. Different combinations of power, frequency, and array will result in numerous side and back lobes of propagation. Those lobes may be strong enough to adversely affect friendly communication or electronic systems. Detailed models of where the back lobes may be compared to the

EMS threshold of friendly systems will undoubtedly save operators time and frustration with their systems.

F. OTHER USES

HPRF vehicle stopping technology is not constrained to ECP/VCP operations. Naval vessels, aviation elements, and special operations units could all benefit from having a HPRF vehicle stopping asset in their arsenals. The following recommendations represent additional instances where the solid-state HPRF technology shows promise for further exploration.

1. Small-Vessel Interdiction

The idea of stopping cars, motorcycles and trucks with HPRF can be continued into the other domains; namely the sea. "The employment of small vessels to attack merchant ships and other seafaring units has emerged as a significant threat to international navigation and safe operations on the high seas."[119] Pirates, swarming small boats, and terrorists have become all too common in the world's heavily used waterways. Military and civilian ships frequently navigate tightly packed sea lanes with little or no ability to defend themselves from surprise, asymmetric attacks. Physical attempts to stop small vessels using non-lethal methods exist. Propeller entanglement systems, exhaust stack blockers, sea anchor stopping systems (a series of subsurface nets) and "small craft disablers" (spear and fin system) have all been used before but with inconsistent results.[120]

At Dahlgren's Naval Surface Warfare Center Joint Non-Lethal Weapons Directorate engineers began to again investigate if HPRF could be used to curtail small vessel threats in less invasive ways than the physical measures mentioned above. The delivery method is similar to the ground based vehicle stopping system but had its limitations. Shipboard systems are at a serious disadvantage with space and even power generation if they stayed with a high power magnetron to generate the RF pulse. Only

119 J. Walker, "Nonlethal Small-Vessel Stopping with High-Power Microwave Technology," *Leading Edge 4*, no. 7 (2012), 97.

120 Ibid.

large ships that have ample space for a large system could utilize HPRF. That system has been tested with good effects on various types of large outboard motors commonly found on small vessels. The solid state system can be put aboard any size vessel, have similar effects, and still deliver speed of light, non-lethal effects to potentially threatening vessels. One can see that civilian and military personnel could benefit from such flexible systems in environments as dynamic as the world's waterways.

2. Electronic Ambush

The U.S.'s Special Operations Forces frequently complete precision missions where the probability collateral damage or civilian casualties are high. Many times, a successful mission that killed or captured an enemy combatant is overshadowed by the damage or death to the local populace that occurred as a result. HPRF is a tool that can aid planners with this conundrum as well. Airborne platforms, whether human operated or unmanned, along with man-portable ground based systems offer more flexibility for operators tasked with those sensitive missions. Some in the SOF community have voiced a need for an "electronic ambush" capability that can aid in neutralizing enemy actors in congested areas with less likelihood of damage to others.

One method is an airborne array that propagates HPRF downward onto a swath of ground. Figure 33 is a simple depiction of what this may look like. This method of using HPRF entails the power and RF source in an airborne platform. The HPRF propagates downward onto targets whether they are vehicles or other equipment using electronic components. For the case of targeting vehicles, it is easy to see how this type of engagement would be useful for civilian police actions as well. Disastrous endings to high-speed chases are an all too common event. This type of system could potentially end those pursuits quickly and more safely.

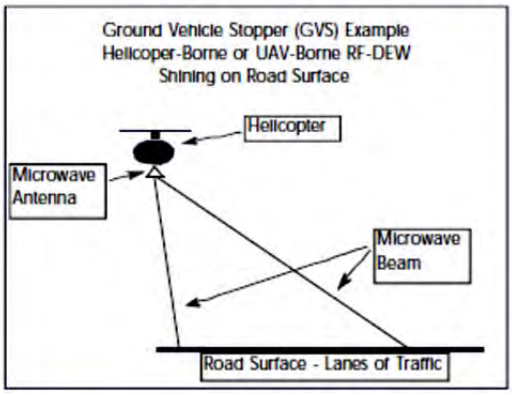

Figure 33. Airborne HPRF engagement[121]

Ground based electronic ambush capability is yet another potential use for HPRF technology. For this to become a reality, a few key components need to be perfected. Most notably, the antenna array and power generation system must be man-portable or even flexible so operators can quickly deploy the system across a road or choke point to interdict targets. This is not to replace deadly weapons but only to add a non-lethal tool if the target is more useful alive or if the target travels with non-combatants.

G. SUMMARY

Deadly SVBIED attacks will continue to plague contemporary operations. While they are effective in their destructiveness they are even more effective as conduits for enemy information campaigns. Scenarios like the one described pertaining to the two Marines fighting against an oncoming SVBIED will replay across the world and span civilian, government, and military personnel. Current TTPs have proven to be inadequate measures to meet this threat.

This research intended to improve those TTPs using HPRF DE technology. First, doctrinal TTPs regarding force protection and ECP/VCPs were discussed. Accepted practices and vulnerabilities were identified which led to the introduction of DE as a method of reducing some of the vulnerabilities.

121 Scannell, "Progress in Directed Energy Weapons Part II: High Power Microwave Weapons," 5, Figure 8.

Under the umbrella of DE, the thesis focused on solid-state HPRF because it afforded more flexibility and suitability than other DE systems. The section on HPRF demonstrated its benefits as a non-lethal tool that can enhance ECP/VCP operations of any size. The next question was whether HPRF solved only one problem or could help resolve an entire system of problems.

A SoS analysis illustrated how the COE encompasses three distinct actors and how their actions affected each other. System engineers use models to make a SoS move more efficiently. This thesis used systems engineering models as a method to target areas where a system can be broken. It became clear that the SVBIED cycle rated friendly targeting and that HPRF could be the instrument to affect it.

Lastly, taking into account current ECP/VCP TTPs, HPRF, and the SoS analysis, an alternative ECP/VCP augmented with HPRF was constructed. That ECP/VCP depicted one way that technology could enhance friendly operations with little negative impact on the operating unit. While it is clear that HPRF is no panacea it most definitely is an excellent candidate to defeat SVBIEDs, disrupt the enemy , and protect friendly and local actors.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adamson, William G. *An Asymmetric Threat Invokes Strategic Leader Initiative: the Joint Improvised Explosive Device Defeat Organization*. Fort McNair, Washington, DC: The Industrial College of the Armed Forces National Defense University, 2007.

Afghan Police Training Mission. Checkpoints (Border Security Company 18 Standard Operating Procedures). BSC-18, 2011.

Alberts, M. *The Information Age: An Anthology on its Impact and Consequences*. Washington, DC: Command and Control Research Program, 1997. http://www.dodccrp.org/files/Alberts_Anthology_I.pdf.

Amos, James. "Focus Areas." In *Expeditionary Force 21*, 35–36. Washington, DC, United Stated Marine Corps, 2014.

Blanchard, Benjamin. *Systems Engineering Management*. In Wiley Series in Systems Engineering Management, edited by Andrew Sage. 4th ed. Hoboken, NJ: John Wiley and Sons, 2008.

Burkebile, Keith. "Using Nonlethal Weapons to Complete the Commander's Toolbox for Fighting Modern Insurgents." Master's Thesis, USMC School of Advanced Warfighting, 2007.

CCS Research Staff. "Suicide Attacks on the Rise." *The Culture and Conflict Review* 2, no. 2 (March 2008): 7-10.

Condra, Luke, Joseph Felter, Radha Iyenga, and Jacob Shapiro. *The Effect of Civilian Casualties in Afghanistan and Iraq*. (NBER W16152). Cambridge, MA: National Bureau of Economic Research, 2010. http://nber.org/papers/w16152.

Day, Matthew, John Tien, and Tracy Peacock. "Checkpoint Operations." In *U.S. Army and U.S. Marine Corps Tactics, Techniques, and Procedures for Stability Operations and Support Operations*, edited by Michael Hiemstra, 36-40. Fort Leavenworth, KS: Center for Army Lessons Learned, 2003

Defense Acquisition University. *Defense Acquisition Guidebook*. Fort Belvoir, VA: Defense Acquisition University, 2013.

———. *Glossary of Terms*. Fort Belvoir, VA: Defense Acquisition University, 2009.

Department of the Army. *Improvised Explosive Device Defeat*. (FMI 3-34.119 and MCIP 3-17.01). Washington, DC: Headquarters Department of the Army, U.S. Marine Corps, 2005.

Department of Defense. *Department of Defense Dictionary of Military and Associated Terms. (JP 1-02).* Washington, DC: Joint Force Development, 2015.

———. *Information Operations.* (JP 3-13). Washington, DC: Joint Staff, Director, 2014.

Defense Science Board Task Force. *Directed Energy Weapons*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2007.

———. *Force Protection in Urban and Unconventional Environments.* Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2006.

Deveci, Bayram. "Directed Energy Weapons: Invisible and Invincible?" Master's Thesis, Naval Postgraduate School, 2007.

Earl, Robert and Emery Norman. "Terrorist Approach to Information Operations." Master's thesis, Naval Postgraduate School, 2003.

Fast, William. "Systems Engineering Process." Lecture, Naval Postgraduate School, Monterey, CA, July 10, 2014.

Hadar, Mary, Whitney Fetterhoff and Magda Jean-Louis. "Faces of the Fallen." *The Washington Post.* May 7, 2015, http://apps.washingtonpost.com/national/fallen/theaters/Iraq.

Hall, Steve. "Solid State RF Sources for Rapid Response." Presentation at Joint Interagency Field Experiment, Camp Roberts, CA, March 4, 2014.

Hoffman, Bruce. *Inside Terrorism*. New York, NY: Columbia University Press: 1998.

iCasualties.org, "IED Fatalities," iCasualties.org, May 7, 2015, http://www.icasualties.org.

Inoguchi, Rikihei and Tadashi Nakajima. *The Divine Wind; Japan's Kamikaze Force in World War II*. Annapolis, MD: United States Naval Academy Institute, 1958.

Islamic Al-Fallujah Forums. "Knights of Martyrdom 6," August 22, 2009, http://www.al-faloja.info/vb.

———. "Knights of Martyrdom 7," February 22, 2010, http://202.71.102.68/~alfaloj/vb.

JFOB Quick Reaction Test. *JFOB Force Protection Handbook*. Alexandria, VA: Office of the Secretary of Defense, Joint Test and Evaluation, 2005.

Joint Chiefs of Staff. *Commander's Handbook for Antiterrorism Readiness*. CJCS Handbook 5260. Washington, DC: 1997.

Kelly, John. "Untitled." Speech. American Legion Memorial Day Address in St. Louis, MO, November 13, 2010.

"Knights of Martyrdom 3." YouTube video, 41:15, from post by Al-Furqan Media Establishment on July 8, 2008. Posted by "Al Fajr Media Center." July 9, 2008. http://www.youtube.com/watch?v=8Cy6NS7wHfI.

Kopp, Carlo and Ronald Pose. *The Impact of Electromagnetic Radiation Considerations on Computer System Architecture*. Victoria, Australia: Monash University, 2014.

Lim, R. Augustus. *Anti Terrorism and Force Protection Applications in Facilities*. Gainsville, FL: University of Florida Department of Civil and Coastal Engineering, 2003.

Long, Robert L. J. Admiral, USN (Ret). *Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983*. Washington, DC: Department of Defense, 1983.

Manabe, Ryo and Atsushi Takatsuka. "Divine Wind: An Interview with Atsushi Takutsuka." *The Cabinet* Winter 2005/2006, no. 20 (2006). www.cabinetmagazine.org/issues/20/manabe.php.

Matthews, Matt. *We were Caught Unprepared: The 2006 Hezbollah-Israeli War*. Fort Leavenworth, KS: Combat Studies Institute Press, 2008.

McCarthy, William. *Directed Energy and Fleet Defense*. Air University Maxwell Air Force Base Montgomery, AL: Center for Strategy and Technology, 2000.

McCauley, Clark and Katherine Seifert. "Suicide Bombers in Iraq, 2003–2010: Disaggregating Targets can Reveal Insurgent Motives and Priorities." *Terrorism and Political Violence* 26, no. 5 (February, 2014): 803–820, DOI: 10.1080/09546553.2013.778198.

McQuage, Matthew and Walker, Jacob. "Directed Energy using High-Power Microwave Technology." *Leading Edge* 7, no. 4 (2012): 78–81.

Merryman, Stephen. "Multifrequency Radio-Frequency Vehicle-Stopping Systems." *Leading Edge* 7, no. 4 (2012): 86–91.

Moran, Stuart. "The Basics of Electric Weapons and Pulsed-Power Technologies." *Leading Edge* 7, no. 4 (2012): 50–57.

———. "Historical Overview of Directed Energy Work at Dahlgren." *Leading Edge* 7, no. 4 (2012): 12–25.

"Muslims Celebrating 9/11." YouTube video, 0:38 From a report televised by Fox News on September 12, 2001. Posted by "nccanuk." April 12, 2008. www.youtube.com/watch?v=Rmo64fcvKs0.

Ollivant, Douglas A. and Eric D. Chewning. "Producing Victory: Rethinking Conventional Forces in COIN Operations." *Military Review* 86, no. 4 (July 2006). 50–59.

Olson, Melissa. "History of Laser Weapon Research." *Leading Edge* 7, no. 4 (2012): 26–35.

Polmar, Norman. "Terrorism Strikes the U.S. Navy." *U.S. Naval Institute Proceedings* 126, no. 11 (November, 2000): 28.

Prendergast, John. "Oklahoma City Aftermath." *Civil Engineering* (October, 1995): 42–45.

Regional Command (S), USMC. *IED Blast and Fragmentation Distances* RC(S) C-IED, 2013.

Reminnikov, Alexander and D. Carolan. *Building Vulnerability Design Against Terrorist Attacks*. Wollongong Australia: University of Wollongong, 2005.

Scannell, Edward. "Progress in Directed Energy Weapons Part II: High Power Microwave Weapons." *Weapon Systems Technology Information Analysis Center* 4, no. 3 (Fall 2003): 1-10.

Sforza, P. M. and H. Zmuda. "Directed Energy." *Journal of Directed Energy* 1, no. 1 (2003): 92.

Shane, Scott and Ben Hubbard. "ISIS Displaying a Deft Command of Varied-Media." *New York Times*, 2014.

Toolan, John. *I Marine Expeditionary Force Science and Technologies Priorities*. Camp Pendleton, CA: I MEF, 2013.

United States Marine Corps. *Marine Corps Operations* (MCDP 1-0). Washington, DC: Department of the Navy, 2011.

———. *Marine Corps Planning Process.* (MCDP 5-1). Washington, DC: Department of the Navy, 2010.

Wagner, Edward S. Jr. *Force Protection: It's Time for a Joint Force Commander for Antiterrorism/Force Protection*. Newport, RI: Naval War College, 2001.

Walker, J. "Nonlethal Small-Vessel Stopping with High-Power Microwave Technology." *Leading Edge* 4, no. 7 (2012): 96–99.

Wilson, Clay. *Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures*. Washington, DC: Congressional Research Service, 2006.

Zoroya, Gregg. “How the IED Changed the U.S. Military.” *USA Today,* December 18, 2013.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California