SANDIA REPORT
SAND201X-XXXX
Printed Month and Year

External Threat Risk Assessment Algorithm (ExTRAA)

Troy C. Powell

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

SAND201X-XXXX
Printed August 2017

External Threat Risk Assessment Algorithm (ExTRAA)

Troy C. Powell
Mechanical Systems and Design
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS0790

Abstract

Two risk assessment algorithms and philosophies have been augmented and combined to form a new algorithm, the External Threat Risk Assessment Algorithm (ExTRAA), that allows for effective and statistically sound analysis of external threat sources in relation to individual attack methods. In addition to the attack method use probability and the attack method employment consequence, the concept of defining threat sources is added to the risk assessment process. Sample data is tabulated and depicted in radar plots and bar graphs for algorithm demonstration purposes. The largest success of ExTRAA is its ability to visualize the kind of risk posed in a given situation using the radar plot method.

ACKNOWLEDGMENTS

I would like to express my deepest appreciation to my Senior Manager Roberto Mata for the opportunity to perform this analysis and contribute to “an exceptional service in the national interest.” A special gratitude goes out to my Manager Mark Soo Hoo for providing special insights and useful perspective along the way. I also thank Mark Snell greatly for his added insights and resources that allowed me to verify and improve the risk rating algorithm.

TABLE OF CONTENTS

FIGURES

TABLES

1. INTRODUCTION

Principal protection is a globally important topic. The principal can be anything from money, to the U.S. President, to special nuclear material. When the principal is stationary, high degrees of security are possible. However, when the principal is transported on the ground to and from sites (office buildings, banks, conventions, etc.) specific vulnerabilities come into play (Garcia, 2008). Therefore, the problem at hand is to provide a reproducible, effective, and relatively simple algorithm for risk assessment of ground transportation of principal assets (specifically over-the-road and not railway or water transportation). However, this does not exclude the applicability of the following work to other forms of principal protection. It should be noted, however, that those other forms may require some creative adaptive measures of the algorithm.

The perspective of this research takes on that purely of an outsider. That is to say, the analysis cannot take into account the effectiveness of physical protection system defenses against any attack whatsoever. Estimations based on statistical evidence, open-source literature, and the opinions of subject matter experts (SME) can be made, but definitive system effectiveness is unknown. The goal then is that, in any given attack scenario, effective risk analysis can be performed without an insider perspective. The advantages here are twofold. Firstly, this eliminates insider analyst bias – the effect of knowing how a system operates, and thus trying to exploit the vulnerabilities perceived by the analyst. Many threats are external, and will not have this knowledge. This perspective, by eliminating the insider analyst bias, provides a realistic approach to analyzing the risk of external threats. Secondly, if the physical protection systems themselves are classified or restricted in any way, effective risk analysis can still be performed by those without access to the systems. The analyst does not need to use the time of others and his/her own time to be trained on the physical protection systems and/or go through the lengthy process of any governmental clearance requests or lifting of special information restrictions. This offers the ability of streamlining the risk analysis process and the possibility of the process becoming more cost effective.

The above goals and qualifications of the research combine to form the External Threat Risk Analysis Algorithm (ExTRAA). In the following work, it is applied to the movement disruption of principal transportation specifically (not theft/sabotage of cargo), but is not limited to principal transportation scenarios.

2. RISK RATING ALGORITHM

In an effort to fully illuminate external threats, approaches from two different sources were augmented and combined. The first is the Open Web Application Security Project (OWASP). This approach was geared towards analyzing risk in the event of a cyber-attack on a company. OWASP split risk factors into two categories: likelihood and impact (OWASP, 2016). Within the likelihood category, OWASP corrals threat agent parameters (such as capability, size, motivation, and tactics), or what will later become known in this work as threat definition. There is a problem inherent to this grouping. The same method performed by various threat agents will have different impacts and likelihoods. The approach to define a threat agent in the OWASP algorithm is taking the threat agent that would have the most success with a method. In that case, every attack would be carried out by highly trained professionals that know best how to use that attack method. For example, an attack using airborne drones would be best carried out by professional drone racers who can manipulate the drones into tight, potentially vulnerable places. Of course, this cannot be the case. Therefore, this research postulates that the threat be defined based upon what adversary is most likely to use a particular method and then separately qualify the threat source from the other factors so that it may be analyzed independently. For example, a VBIED is a favorite among terror groups while a cyber-attack is most probably carried out by hacktivists. But a group of hackers is not likely to employ a VBIED.

Mary Lynn Garcia (Garcia, 2008) thoroughly explained threat definition. This approach takes into consideration (in a broad sense) motivation and capabilities of the adversary. Again, this research augments this style by splitting the capabilities (number, weapons, equipment and tools, transportation, technical experience, and insider assistance) of an adversary and then consolidating them into capability, size, and tactics, which are fully explained in section 2.2.1. While in the previous paragraph it seems that this research is dedicated to fleshing out every minor detail, the philosophy for the consolidation is simple. Threat sources are not particularly homogenous. Some terrorist organizations have different capabilities than others. “So-called” Islamic State has access to better hardware than most other terror groups. On the other hand, Hezbollah is made influential in the Western Hemisphere due to their networking with cartels. So is a separate threat definition to be made for every criminal organization? No. This would be too complex and ultimately such a list is useless in analyzing risk. Consolidating the factors takes a broad threat surface and shrinks it to something manageable that allows for comparing various threat sources.

2.1. Factorization and Value Averaging

Three factors contribute to the determination of the overall risk of a method: threat definition, use probability, and employment consequence. Defining a threat is to assess potential adversaries in a given scenario, determining which type of adversary is most probable, and then quantifying the threat posed by that adversary. This is done by evaluating four discrete parameters of threat definition (TD): capability, motive, tactics, and size. These and the following parameters under the other two factors are thoroughly and individually explained in the following sections. The parameters that comprise the use probability (UP) factor are as follows: use ease, build ease, covertness, method propensity, and speculated transport vulnerability. In addition to how likely a method is to occur, it is necessary for risk assessment to consider how consequential to transportation systems an employed method will be. This is introduced by the employment consequence (EC) factor. Similarly to UP and TD, EC is calculated in a similar manner with four parameters: defense personnel endangerment, equipment endangerment, loss of integrity, and atmospherics. Each parameter will be assigned a value on a scale from zero to nine. After calculating and tabulating the EC values, they are multiplied with the UP and TD values to enumerate the overall risk. (Both Garcia's and OWASP risk assessment methods use multiplication to enumerate risk from their versions of EC and UP, but in different ways. So multiplying the three factors in ExTRAA together is a logical step.) The relationship between the factors and the overall risk is as follows:

$$R = TD * UP * EC$$

Each parameter, P_n, comprises a factor, F, using the following relationship:

$$F = \frac{1}{N}\sum_{n} P_n$$

where N is the number of total parameters and each factor is either Threat Definition, Use Probability, or Employment Consequence.

OWASP developed an algorithm similar to this. Whereas OWASP took a two-dimensional approach to risk, this research will be dedicated to a three-dimensional factorization, adapted from the OWASP algorithm. The added dimension (namely Threat Definition) comes from Garcia's work on risk assessment (Garcia, 2008). Garcia's approach was not used in its entirety because it required an insider perspective, which is not included in this research. Regardless, Garcia's insights into Property Protection Systems have proven to be central to this algorithm.

The 3-factor approach does not unnecessarily complicate things, indeed quite the opposite. Each factor further explains the individual effects of a method, gearing itself towards a more statistically sound approach. This creates a much more stable environment for risk analysis because it reduces the inaccuracies caused by heuristics and biases (Kahneman, 2011). In his work, Daniel Kahneman explains how arbitrary factors such as a cool breeze, an annoying coworker, and national media can influence perspective and bias towards decision-making processes in adverse ways. Kahnemann goes on to explain as well how heuristic shortcuts, though they may seem logical, can swing perspective away from the truth. Instead, Kahnemann offers a statistical approach to decision making that will reduce or eliminate uncertainty in a decision. In this approach, he recommends basing decisions on statistical data instead of a gut-feeling. Thus, three measures can be taken in the effort to reduce arbitrary bias and heuristic inaccuracy. The first is to gather all available open-source information, statistical data, and any subject matter expert's opinions on a given topic, compile it all, and base parameter values on that information. Secondly, the parameter values themselves are based on a consistent rating system. The consistent use of a rating system, not necessarily the accuracy of the system, is key to the process of reducing logical inconsistencies. As research on each parameter is conducted, the value of the parameter in question is chosen based on a descriptive value list. The values ranged from 0-9, as described above, and a meaningful spectrum was used. To get an idea of descriptive value lists, after each parameter list are the exact tables that are used to select parameter values. When using these tables, the blank spaces may be used. The cells with values serve as pegging values that were assigned their descriptions by mimicking the style of the OWASP descriptive value lists.

The third measure taken to reduce bias and heuristics is the averaging of the parameters so that they are all equally weighted. This is done in hopes that any errors will balance themselves out. Another topic in Kahneman's book is the idea that a "back-of-an-envelope" estimation is often just as good as a multiple regression analysis (in other words, weighting each parameter according to importance), which may take ten times as long. Thus, the averaging of the parameters is a quick and viable approach to eliminating inconsistencies.

2.2. Threat Definition

Testing of security systems is best accomplished through physical situation simulation. The key is situational accuracy. What is likely to happen? Who is likely to do it? How effective will the attack be? These questions are not independent of one another. A small terrorist plot would be financially limited but radically motivated; they would not be deterred by loss of life, even their own. A tactical strike force would have more sophisticated, clean, well-oiled methods. A terrorist would not mind a public, metropolitan setting - especially if it involved collateral damage to an enemy populace. Not wanting to be met by opposition, the strike force would be more inclined to a remote setting in which the operation might go unnoticed by law enforcement for as long as possible. Defining threat is the first step towards situational accuracy. Thus it is important to understand the expected adversary. In the case of multiple adversary possibilities, it is important to consider in which environment each adversary is most likely to be encountered. The first question that needs answering, though, is, "Why?". Why would the bad guy want to do this bad thing? Outsider threats may hold ideological motivations, economic motivations, or personal motivations (Garcia, 2008). Whoever the "bad guy" is, his reason will vary depending on with whom he associates and from where he obtains his motivation.

Attack method does not change how capable, how large, what motivation, or what type of tactics an adversary has. Thus, threat definition will be defined separately for each adversary. For each attack mode the question will be asked: what entity is *most likely* to carry out this attack? Once that question is answered, the use probability and employment consequence (defined in the following section) parameters will be based off of the "most probable" adversary for the given attack mode. This makes risk assessment much easier and adds a level of consonance to the algorithm.

A useful technique to save time and provide even better consonance to the analysis is to predefine any threats. In order to do this, a threat will need to be analyzed and results recorded for each threat source. For example, an organized crime entity (OCE), a terrorist group, and a hacktivist group may be predefined. Then, once analysis of the other factors (Use Probability and Employment Consequence) begins, the most likely threat source need only be selected and the parameter values copied. This is particularly handy when there is a broad range of attack modes to be analyzed. Many of the attacks will come from the same threat source. So this could cut analysis time down by about a third – only two of the three factors needs to be analyzed per each attack method.

2.2.1. Threat Definition Parameters

Capability – Education, skill, and training are central to the severity of the threat posed by a particular adversary. The capability parameter takes into account these qualities of an adversary. For example, a terrorist organization will have a different skill set than your typical hacker. This will show their aptitude, which most often reflects their chances at successfully disrupting transportation. If the adversary has been trained, how extensively have they been trained, and how effective/pertinent is that training?

Motive – Every adversary has a reason for attacking. The motive parameter will evaluate what that motive is and how influential that motive is. An ideologically motivated activist can be extremely stubborn in how they respond to opposition because they view it as the "right thing to do". Terrorists max out this scale with a do-and-die mentality for their cause.

Tactics – Two things that go hand-in-hand are the hardware available to a malicious party and how well they can use that hardware. The tactics parameter takes into account the level of equipment instead of the capability parameter for this reason. How an adversary prepares and attacks is crucial to their success. A coordinated threat source will use their resources wisely, attack at an appropriate time/location, and ensure they have hardware to optimize their success. An uncoordinated one will put together a rag-tag clan to haphazardly assault a transport with less-than-substantial weapons at the time/location when it best suits them. The distinction between these types of adversaries is the tactics parameter's objective.

Size – It is not necessarily the case that the size of the dog in the fight determines the outcome, but big dogs are often harder to stop. Size will take into account the expected number of people in an attack.

Table 1. Threat Definition Parameter Values

Value	Capability	Motive	Tactics	Size
0	▨	▨	Disorganized, No Tools	▨
1	No Technical Skills	Low or No Reward	▨	▨
2	▨	▨	▨	2 Person Attack
3	Some Technical Skills	▨	▨	▨
4	▨	Possible Reward	Somewhat Coordinated, Access to Small Arms and Basic Tools	▨
5	Good Technical Skills	▨	▨	Large Group
6		Financially Motivated	▨	Crowd
7	Educated Adversary	▨	Coordinated, Access to Heavy Machinery and Light Weapons	▨
8	▨	▨	▨	▨
9	Espionage Agents	Ideologically Motivated	Massive Strategy, Heavy Machinery and Heavy Weapons Available	Small Army

2.3. Use Probability

How probable a method is to be used (not how likely it is to succeed) is the best way to analyze likelihood. Key factors in what may deter, prevent, or encourage an adversary to use a particular method need to be considered. Using a high-energy laser would have a high likelihood of success. But there is little reason to use such bulky and expensive technology in an ambush scenario. Therefore, a different approach needs to be taken to determine the "likelihood" of a scenario. (When speaking about to "likelihood", this refers to the likelihood factor used in the OWASP algorithm.) This will be called use probability, and it consists of five parameters: ease of use, ease of build, covertness, method propensity, and speculated transport vulnerability.

2.3.1. *Use Probability Parameters*

Ease of Use – Once the attack apparatus is built and/or the attack scenario set-up, this parameter serves as a metric for how easy it would be for the defined adversary to "pull off" an attack. For example, throwing a paper airplane at the transporter is extremely easy (it will be shown later that this is countered by the Employment Consequence parameters). How much technical knowledge needed to perform the attack is also taken into account. Is the method point-and-shoot, or something more complicated?

Ease of Build/Acquisition – This parameter takes into account the research, time, facilities, materials, knowledge, skills, and abilities required to prepare an attack or build an apparatus. Sticking with the paper plane example, it is extremely easy to build. A high-energy laser, on the other hand, requires extensive time, facilities, research, etc. to build the system. Additionally, the relative ease of buying an attack apparatus will be taken into account.

Covertness – If an attack is extremely noticeable, it often does not bode well for the attackers. If the attack can be foreseen and/or the attacking party easily identified, then there is a chance that the defense personnel (couriers, bodyguards, etc.) may be able to prepare themselves, employ evasive maneuvers, and fight back in an attempt to thwart the attack. Thus, measuring covertness gives an insight to how well an attack may proceed for the adversary.

Method Propensity – Understanding how often a particular method is used by the defined threat sheds light on just how likely it is for the adversary to use it for themselves. Mortar bombardment may be popular for deterring an army, but it is not often used in an attack on moving principal transportation. Also, given a particular adversary, are they likely to use this method over something else? Method propensity answers this question, giving an idea of how probable a method is.

Speculated Transport Vulnerability – Suppose that in a blog online, somebody claiming to have insider knowledge speaks about a vulnerability on a specific device on the transport. Whether the vulnerability exists or not is irrelevant. If an adversary thinks it is there, they might just go for it. So this parameter is supposed to weight the use probability factor according to perceived vulnerabilities in transports. Some adversaries are much more prone to fact-checking, and that will be accounted for in the discussion. For example, in a hacking scenario, there is definitive evidence that some vehicles can be controlled through their CAN-bus, which can be accessed through cellular fleet tracking networks. So an adversary may think that this vulnerability will exist on a presidential motorcade. Whether layers of encryption have been put on these connections is not clear, but logic would have it that any government network is going to have several layers of encryption. The idea is that a speculated vulnerability will still generate interest in the method and incite an attack.

Table 2. Use Probability Parameter Values

Value	Ease of Use	Ease of Build	Covertness	Method Propensity	Speculated Transport Vulnerability
0	▨	▨	▨	▨	▨
1	Practically impossible	Theoretical	Publicly Declared Threat	Not Practical	No vulnerability
2	▨	▨	▨	▨	▨
3	Difficult	Difficult	▨	Used Rarely	▨
4	▨	▨	Obvious	▨	Small vulnerability potential
5	▨	Easy	▨	Used Sometimes	▨
6	▨	▨	Miss at first glance	▨	▨
7	Easy	▨	▨	Used Frequently	Large vulnerability potential
8	▨	▨	▨	▨	▨
9	Automated tools available	Automated tools available	Completely Covert	Used Consistently	Massive exposed vulnerability

2.4. Employment Consequence

The effects of a successful attack (worst-case scenario) in a particular method is paramount to understanding just how much risk a particular attack method poses. Just because throwing a paper airplane at a transportation system is easy to use, build, etc. does not mean it is going to have any ill effects (outside of poking someone in the eye) and therefore does not pose a risk.

The parameters related to employment consequence make a few assumptions for the purposes of the specific application of this research to transportation systems. The first is that there are defense personnel in harm’s way. In the event of an attack on a stationary location (such as a bank), this may not always be the case. An attacker may wait for a guard to leave or a shift change before trying to engage the physical protection systems. In the case particular to this research, however, the defense personnel present play a vital role in defending the principal and are always present, so their survivability needs to be considered. The second assumption to make about a transportation system is that an attack may occur in a remote place where outside help (say from law enforcement) is delayed for an extended period of time. This eliminates the need to consider a timeline for response and focuses the analysis on the attack itself.

2.4.1. Employment Consequence Parameters

Defense Personnel Endangerment – Simply put, this is a metric for how heavy any sustained casualties will be. Armoring of the transportation system, ballistics, and convoy positioning will be taken into account. If the method does not aim to kill defense personnel and only impair them, then this will be a measure of how impaired they will be, especially the driver of the transport.

Loss of Integrity – Post-attack operability of the transport is important in understanding how effective the attack actually is. If the transport is dead in the water, then this parameter is high. If the transport can shrug off an attack and escape, then this parameter is low. Additionally, if a specific system is under attack (such as electronics during an EMP), this parameter gives weight to the significance of that system's role in ensuring security. Loss of integrity will be rated on the assumption that the method is as successful as can be on its own.

Equipment Endangerment – Physical deformity sustained to the transport needs to be discussed. If structural integrity is compromised, then it becomes easier to maliciously interact with the principal, and is therefore desired by the adversary. Sustained damage is measured to be macro-physical – that is, discrete (non-composite) systems, software, and electronics are to be collectively considered. This parameter also serves as a weighting agent to the "Loss of Integrity" rating. In assessing some complex physical protection systems, emphasis can be placed on the physical aspects of the systems instead of the people guarding them. This balances the effects of a bomb, which does not target a specific system, against that of a CAN-bus hack, which targets the transport in only one way.

Atmospherics – This is a metric of how much or how little defense personnel can do against an attack, what advantages are given to the adversary by the location and method, and what social or political consequences might exist in the scenario that could help the adversary or hinder the defense personnel, based on the probable location of the attack. The probable location of an attack is dependent on various factors and has interesting consequences. Firstly, the probable location depends on the type of adversary who is probable to utilize the attack method. Terrorists, wanting to spread terror, would feel urged to act in a populated environment. Hacktivists might prefer to act when the transport is on the road when the vehicle is running, possibly allowing them more control. Secondly, the probable location depends on the attack itself and its inherent limitations. With cellular communications, a CAN-bus hack may be possible anywhere. For a VBIED, stationary or on-the-road location can be proven to be irrelevant – a VBIED is equally effective in either scenario. Ultimately, the probable location lends the most consequences to the "Employment Consequence" realm in the way of atmospherics, and should be discussed in each method prior to and in support of the atmospherics rating.

Table 3. Employment Consequence Parameter Values

Value	Defense Personnel Endangerment	Loss of Integrity	Equipment Endangerment	Atmospherics
0	▨	▨	▨	▨
1	No Casualties	Little to no loss of functionality	Little to no equipment damage	High Defense Personnel Advantage
2	▨	▨	▨	▨
3	▨	Minimal loss of functionality	▨	▨
4	Small Potential for Harm	▨	▨	Moderate Defense Personnel Advantage/ Low Adversary Advantage
5	▨	Moderate functionality loss	Light damage to vehicle	▨
6	▨	▨	▨	▨
7	Multiple Casualties	Severe functionality loss	Heavy Sustained Damage	Low Defense Personnel Advantage/ Moderate Adversary Advantage
8	▨	▨	▨	▨
9	Catastrophic Loss	Loss of all functionality	Vehicle(s) totally destroyed	High Adversary Advantage

3. BINNED ANALYSIS PROCEDURE

Categorizing attack modes into separate bins (e.g. stand-off attack, directed energy weapons, explosives, etc.) before analyzing them according to the ExTRAA methodology is what is meant by performing a binned analysis of the attack methods. Binned analysis helps focus on one type of attack at a time by organizing each method and putting it under an umbrella with other similar methods. Aside from being a more organized analysis, this also allows the analyst to compare attacks with better relative accuracy by keeping any and all effects and side-effects of the method in mind. This section should constitute a verbal defense of the tables in the Results section, which holds the numerical portion of the risk analysis. They simply should be a compilation of evidence and explanations for the numerical assessments (assigning parameter values). It is best for each subsection to discuss the factors and parameters in the following fashion:

Method – Method Description

- ➔ Threat Definition
  - o Pick the most likely threat source and defend why it is the most likely.
- ➔ Use Probability
  - o Ease of Use; Ease of Build; Covertness; Method Propensity; Speculated Transport Vulnerability
- ➔ Employment Consequence
  - o Defense Personnel Endangerment; Equipment Endangerment; Loss of Integrity; Atmospherics

3.1. Assigning Parameter Values

Gaining the opinion of Subject Matter Experts (SMEs) is crucial to assigning parameter values. This can be done by gathering SMEs and conducting a poll. Say one wants to analyze the threat definition factor based on a domestic terrorist threat. The FBI would be an excellent resource for SME opinions.

Additionally, the FBI has a number of open-source literature on domestic terrorism. Parameter values can also be selected based on research conducted on open-source literature. In this regard, it is also necessary to do some serious critical thinking. Being honest about any information the analyst may find and not allowing his or her own biases and heuristics to come into play is vital in this process. Published research on the topic is the only acceptable form of literature to use. This will provide a stable foundation from which to select parameter values.

4. RESULTS

4.1. Tabulated Results

All results from the verbal analysis need to be reported and tabulated. This is important for explicit reporting of results in an organized fashion. Sample tables with example data are given below. Each row represents one method (e.g. bomb scenario, chemical weapons attack, directed energy attack, etc.), however for the purposes of just being an example, they are named in the following tables according to their risk. Each factor (i.e. TD, UP, EC) is assigned a value that will be explained later. The values of the parameters under each factor (e.g. in Threat Definition: Capability, Motive, Tactics, and Size) are simply given random values that average out to the desired factor value. Once again, this is just an example, so all the values are for demonstration purposes. This should still give an idea as to how the results should look.

Table 4. Threat Definition Results

Each method listed was assigned a threat definition (e.g. terrorist, activist, etc.) and the threat definition parameters for each method were then tabulated.

Method	Capability	Motive	Tactics	Size	TD
Low	1	1	1	1	1
Moderate	3	3	5	5	4
High	8	6	6	4	6
Critical	9	9	9	9	9

Table 5. Use Probability Results

The tabulated results of the use probability analysis for each method.

Method	Use Ease	Build Ease	Covertness	Method Propensity	Speculated Transport Vulnerability	UP
Low	3	4	5	6	7	5
Moderate	9	8	7	8	8	8
High	7	6	5	4	3	5
Critical	9	7	8	7	9	8

Table 6. Employment Consequence Results

The tabulated results of the employment consequence analysis for each method.

Method	Defense Personnel Endangerment	Loss of Integrity	Equipment Endangerment	Atmospherics	EC
Low	0	3	3	6	3
Moderate	2	3	4	3	3
High	9	8	7	8	8
Critical	7	9	8	8	8

4.2. Bin Radar Plots

Visualizing the above results is important to understand them. It is hardly informative to stare at tables of numbers. This is probably one reason for the invention of calculus and computers – tables of numbers are not terribly qualitative or interpretive. Using radar plots to visualize individual bins allows one to actually see in which way they are effective or ineffective. The values are plotted on axes of threat definition, employment consequence, and use probability. Higher values of threat definition implies the threat source is more formidable. Higher values of employment consequence means that the method, if employed successfully, will pose a more dire disruption. Higher values of use probability will imply that the threat source is more likely to use that method.

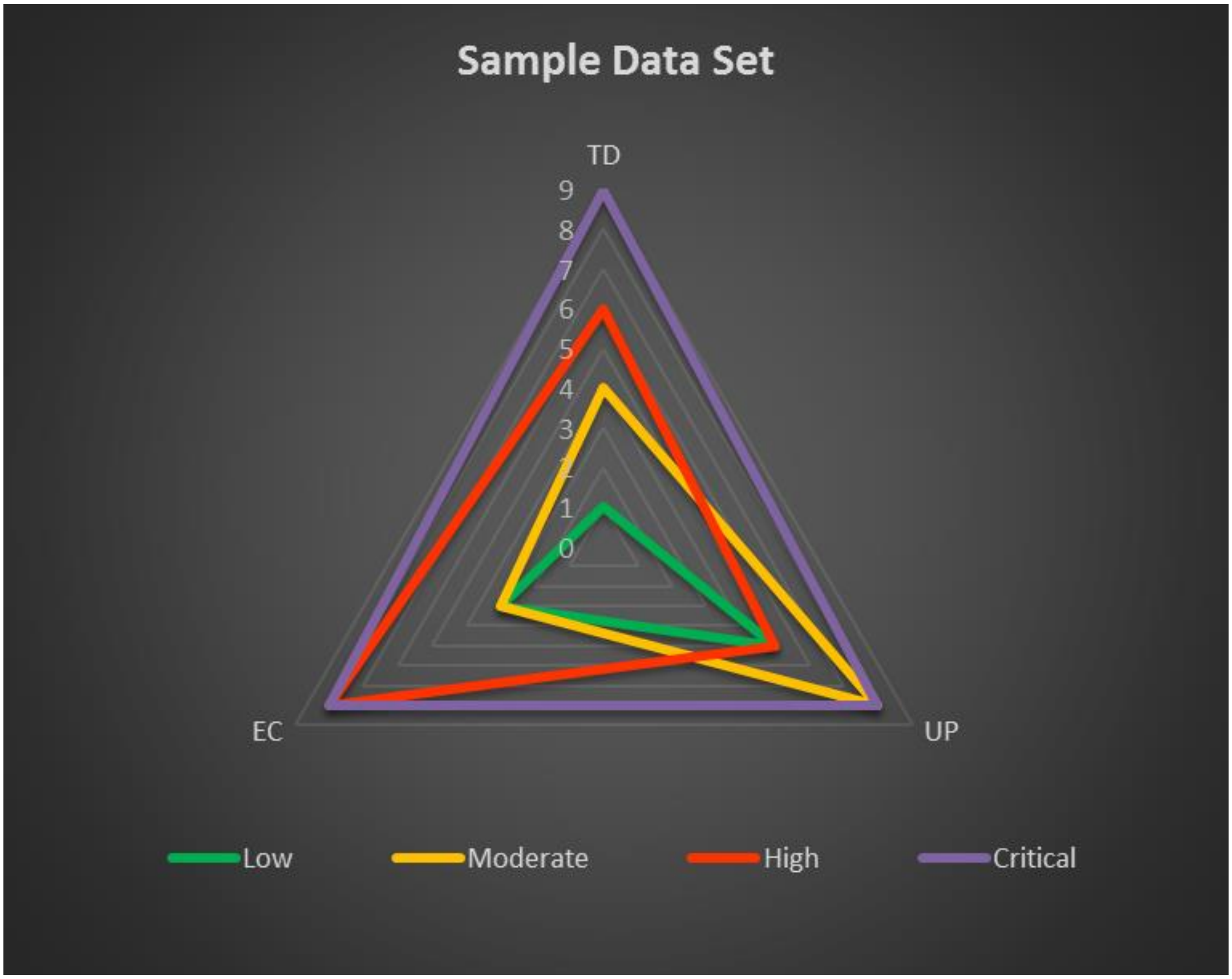


Figure 1: Sample Data Radar Plot

4.3. Final Risk Results

Multiplying the factor values (TD, UP, and EC) gives the overall risk of a method. This section showcases the final risk results in both tabular and graphical formats. Fig. 2 shows the risk classification spectrum formulated for this research.

Table 7. Final Risk Results

The tabulated results of the employment consequence analysis for each method.

Method	Threat Definition	Use Probability	Employment Consequence	Risk
Low	1	5	3	15
Moderate	4	8	3	96
High	6	5	8	240
Critical	9	8	8	576

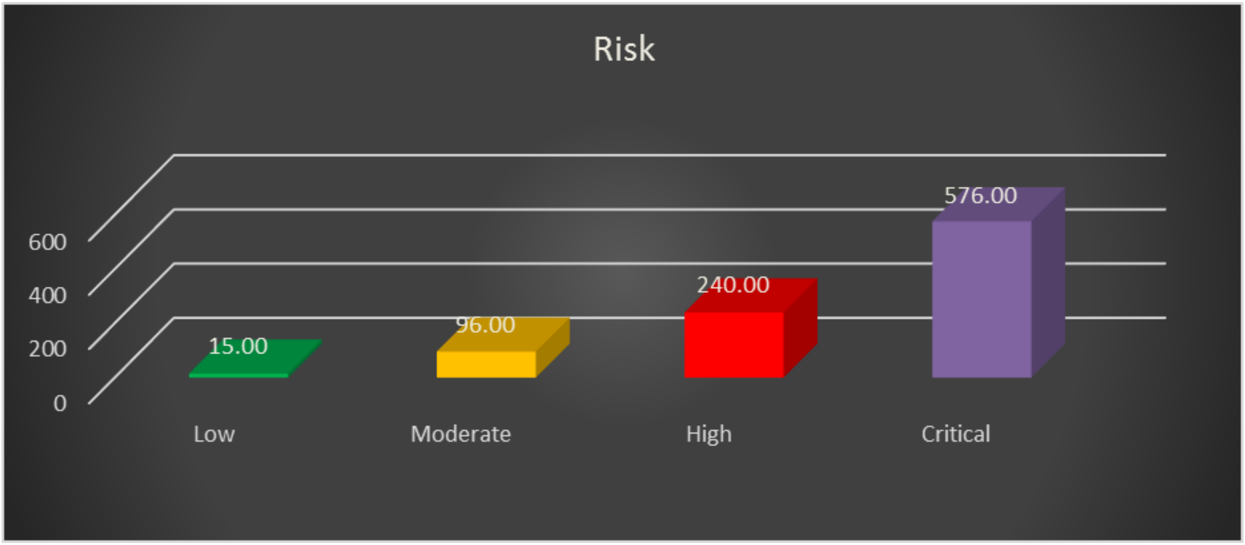
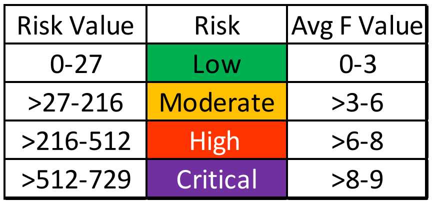


Figure 2: Overall Risk Bar Graph Plot



Risk Value	Risk	Avg F Value
0-27	Low	0-3
>27-216	Moderate	>3-6
>216-512	High	>6-8
>512-729	Critical	>8-9

Figure 3: Risk Rating Spectrum

5. DISCUSSION

5.1. Algorithm Discussion

The radar plots demonstrate clearly the ways in which each method are risky. In the case of the "moderate" method, the high UP value indicates that the method is highly likely to be used by the defined threat. Moreover, the low EC value indicates that the method will not be particularly harmful to the transportation system; the moderate TD value demonstrates that the threat source is not a particular worry in this case – perhaps this is because they have little access to tools and equipment or for some other reason.

Conclusions from the radar plot representation can also be drawn about method similarities. Depending on what the analyst wants to know about a particular attack method, a grouping of triangle points can be a quick way of pointing out the desired information. For example, say the analyst wants to find the most probable type of attack to be used in a given scenario. All that needs to be done is to pick out those methods that are grouped high on the UP scale.

Scaling of the overall risk rating value cannot be linear. Since the three factors all have range 0-9 and are multiplied together, the overall risk rating value increases as the cube of factor values. This can be seen in Fig. 2. Thus for a risk rating scale, there needs to be a spectrum that is both telling of risk severity and is numerically sound. Luckily, there is a simple solution. First, the factor values were split into low, moderate, high, and critical ranges by use of boundary values in the following fashion: 0-3, >3-6, >6-8, >8-9, respectively. To obtain the overall risk values, each of these bounding numbers was simply cubed.

Much like looking at an analog clock for a spatial awareness of what time it is, a quick look at a radar plot will also give one a glimpse of relativity insofar as overall risk. If the area of one triangle is larger than another, then the risk of that method will indeed be greater. With that in mind, it becomes apparent that "low" method is lower in risk than the "high" method almost immediately. However, to actually determine the riskiness of one method against another, it is advised to use the bar graph plot. Two triangles that look to have similar areas may have vastly different risk ratings, especially due to the cubing effect discussed above.

Lastly, ExTRAA lends itself to be used in a simple, handy spreadsheet format. Questions can be coded into a spreadsheet that will take the answer to the questions and turn them into parameter values. The questions can be simple: "How capable is the adversary?" or "How easy is building or acquiring the necessary hardware for this attack?" The descriptive parameter value tables can be coded into dropdown menus that make answering the questions and populating the data tables immediate.

REFERENCES

D'Alfonso, S. (2014, September 04). Why Organized Crime and Terror Groups are Converging. Retrieved from Security Intelligence: https://www.securityintelligence.com

Garcia, M. L. (2008). The Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann.

Kahneman, D. (2011). Thinking, Fast and Slow. New York: Farrar, Strauss and Giroux.

OWASP. (2016). OWASP Risk Rating Methodology. December 22. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood.

DISTRIBUTION LIST

1	MS0768	Roberto Mata Jr.	6620
2	MS0789	Mark Snell	6835
3	MS0790	Mark Soo Hoo	6623
4	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories