SANDIA REPORT
SAND2007-5791
Unlimited Release
Printed September 2007

Categorizing Threat

Building and Using a Generic Threat Matrix

David P. Duggan, Sherry R. Thomas, Cynthia K. K. Veitch, and Laura Woodard

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-5791
Unlimited Release
Printed September 2007

Categorizing Threat

Building and Using a Generic Threat Matrix

David P. Duggan
Networked Systems Survivability and Assurance

Sherry R. Thomas, Cynthia K. K. Veitch, and Laura Woodard
Center for Cyber Defenders
Networked Systems Survivability and Assurance

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185

Abstract

The key piece of knowledge necessary for building defenses capable of withstanding or surviving cyber and kinetic attacks is an understanding of the capabilities posed by threats to a government, function, or system. With the number of threats continuing to increase, it is no longer feasible to enumerate the capabilities of all known threats and then build defenses based on those threats that are considered, at the time, to be the most relevant. Exacerbating the problem for critical infrastructure entities is the fact that the majority of detailed threat information for higher-level threats is held in classified status and is not available for general use, such as the design of defenses and the development of mitigation strategies. To reduce the complexity of analyzing threat, the threat space must first be reduced. This is achieved by taking the continuous nature of the threat space and creating an abstraction that allows the entire space to be grouped, based on measurable attributes, into a small number of distinctly different levels. The work documented in this report is an effort to create such an abstraction.

Acknowledgements

We would also like to thank supporters, contributors, reviewers, and others that have inspired us with ideas and constructive criticisms from the Information Assurance and Survivability Business Area at Sandia National Laboratories (SNL), such as John Clem, John Dillinger, Tim Draelos, Bob Hutchinson, Mark Mateski, John Michalski, and Karen Shanklin. The authors would also like to acknowledge the U.S. Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) as part of the National SCADA Test Bed (NSTB) Program for the funding of this work.

Executive Summary

The key piece of knowledge necessary for building defenses capable of withstanding or surviving cyber and kinetic attacks is an understanding of the capabilities posed by threats to a government, function, or system. With the number of threats continuing to increase, it is no longer feasible to enumerate the capabilities of all known threats and then build defenses based on those threats that are considered, at the time, to be the most relevant. Exacerbating the problem for critical infrastructure entities is the fact that the majority of detailed threat information for higher-level threats is held in a classified status and is not available for general use, such as the design of defenses and the development of mitigation strategies. To reduce the complexity of analyzing threat, the threat space must first be reduced. This is achieved by taking the continuous nature of that threat space and creating an abstraction that allows the entire space to be grouped, based on measurable attributes, into a small number of distinctly different levels. The work documented in this report is an effort to create such an abstraction.

The purpose of this threat characterization research and threat matrix development is to aid in the creation of a comprehensive threat analysis framework that enables the objective determination of threat capabilities and supports the ability to identify and prioritize expenditures to mitigate the effects from a class of threats, all in an unclassified venue for use by critical infrastructure providers and utility owners. One of the primary activities necessary to move classified threat information to the unclassified information environment is the development of generic threat profiles that can characterize many different levels of threat without associating a name with a classified ability. This unclassified threat characterization must be able to bin a full spectrum of threat capability to allow analysts from the classified threat environment to map the characterization of an “unnamed” threat to an equivalent bin, or level, of threat in the unclassified threat environment. This will then allow analysts in the unclassified environment to identify potential attack paths that could be supported by the asserted capability and identify proper mitigation steps to thwart attacks.

This work describes a set of generic threat profiles that can be used to identify and characterize the different levels of adversaries and their related capabilities. These profiles enable unclassified actionable threat information to be distributed to potential stakeholders such as critical infrastructure providers and utility owners. The U.S. government and critical infrastructure industries can use the generic threat matrix to communicate about possible threats. Intelligence organizations can categorize each known threat group into a discrete level of the matrix, to communicate the threat to industry. Through this sharing of actionable threat information, critical infrastructure assets will become more secure and utility owners and operators will become more aware of potential vulnerabilities in their related infrastructure.

This report begins with an introduction to the history and significance of threat analysis. Section 2 describes the approach used in this work to identify threat attributes and develop a generic threat matrix. The definition and scale of threat attributes is described in detail in Section 3. In addition, the generic threat matrix is introduced and followed by a discussion of its validity and applicability. The report closes with a conclusion and recommendations for use of the matrix by government organizations and critical infrastructure entities.

This page intentionally left blank

Table of Contents

Table of Figures

Table of Tables

1 Introduction

The key piece of knowledge necessary for building defenses capable of withstanding or surviving cyber and kinetic attacks is an understanding of the capabilities posed by threats to a government, function, or system. With the number of threats continuing to increase, it is no longer feasible to enumerate the capabilities of all known threats and then build defenses based on those threats that are considered, at the time, to be the most relevant. Exacerbating the problem for critical infrastructure providers and utility owners is the fact that the majority of detailed threat information for higher-level threats is held in a classified status and is not available for general use, such as the design of defenses and the development of mitigation strategies. To reduce the complexity of analyzing threat, the complexity of the threat space must first be reduced. This is achieved by taking the continuous nature of that threat space and creating an abstraction that allows the entire space to be grouped, based on measurable capabilities, into a small number of distinctly different levels. The work documented in this report is an effort to create such an abstraction.

1.1 Background

For more than two hundred years, the United States has defended itself from a variety of threats. For each new circumstance, it was required that the capabilities of the unique threat be ascertained and analyzed; the results were then used to develop strategies for, and implementations of, defenses. In those cases where threat capabilities or intent were not adequately identified, the country has had to contend with great losses, such as the events of Pearl Harbor and the terrorist attacks of September 11, 2001. With the number of threats growing on a daily basis, it has become increasingly difficult to catalog the capabilities of each new threat. When cyber methods are considered within the threat space, the complexity of threat characterization becomes even more complex.

1.1.1 Description

Threat can be characterized as one of three types: normal, abnormal, or malevolent. Documents on infrastructure and architectural surety,[1] created from a physical framework perspective, define these categories of threat in the following way:

- **Normal Threat**: An event or condition that affects the reliability of the day-to-day operations; for example, the mean time between failures or inefficient repair and replacement (maintenance) schedules to offset the effects of aging.
- **Abnormal Threat**: A natural disaster, such as hurricane-force winds or earthquakes, resulting in the failure of structural steel frames.
- **Malevolent Threat**: A manmade event or condition; for example, a bombing of a federal facility or the use of chemical and biological agents in terrorist attacks.

Although these definitions were created to address threat to physical structures, all three threat types must be addressed for all systems. Normal and abnormal threats are addressed

[1] Matalucci, R. V., & O'Connor, S. (2000). Infrastructure and Architectural Surety[SM]. *Materials Research Society: When Materials Matter—Analyzing, Predicting and Preventing Disasters. 630,* GG1.3.1-9.

from a safety or functional perspective, whereas malevolent threats must be addressed from a security perspective.

This work specifically addresses only those threats considered to be **malevolent**, whether those threats use cyber, kinetic, or hybrid cyber-kinetic means. For the remainder of this paper, **threat** is defined as a malevolent actor, whether an organization or an individual, with a specific political, social, or personal goal and some level of capability and intention to oppose an established government, a private organization, or an accepted social norm. The **goal** of a threat is considered to be the threat's overall intent, the end-result the threat is trying to achieve (e.g., the overthrow of a leading political party). In contrast, a threat's **objective** is simply a task, such as a specific attack, that must be accomplished to progress toward the goal.

Current threat analysis methods tend to concentrate on more subjective aspects of political and social motivation structures without identifying relevant objective characteristics that may be used to identify attacks each adversary might be able to perform. The method of threat categorization used in this work is not based on the threat's motivation, goal, or objective. Instead, each threat is categorized into a generic threat level profile based on capability attributes, or characteristics, common to all threats. As part of an overall threat analysis framework[2] being developed at Sandia National Laboratories (SNL), these generic profiles allow for actionable, or readily usable, threat information to be determined and distributed to key stakeholders.

1.1.2 Historical Information

With the move into the information age, a new form of weapon has emerged that enables an increased number of individuals and groups to become threats. Attacks are no longer just cyber attacks or kinetic attacks; there is now a hybrid form of attack that integrates both cyber and kinetic components. For example, a kinetic attack could be launched against a supervisory control and data acquisition (SCADA) system that would damage or disable that system's operation of physical processes, potentially endangering the general populace or causing severe economic damage to critical infrastructure assets[3]. In addition, the technological nature of our society and the easy access to diffuse information and communication enables more complex attacks and makes training readily available. There is need for a method of qualifying generic threats to any facility or system, as well as threats specific to cyber systems or physical facilities.

The historical approach to dealing with threat by identifying each unique threat and learning its particular capabilities, then identifying protection mechanisms to be implemented, does not work well as the number of these threats increases. A new method for objective quantification of threat capabilities needs to be developed. This method must allow for the transfer of threat capability information to the unclassified domain in order to be of use to

[2] Duggan, D. P., & Michalski, J. T. (2007). Threat analysis framework report, SAND2007-5792. Sandia National Laboratories.
[3] Stamp, J., Young, W., & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems, SAND2003-1772C. Sandia National Laboratories.

critical infrastructure providers and utility owners, who operate mostly in an unclassified environment.

1.1.3 Significance

It is impractical and inefficient to continue chasing the "threat of the day" as is currently done. As part of an overall framework of threat analysis, the development of generic threat profiles will enable the design of mitigation strategies to simultaneously cover a larger number of threats, both known and unknown, based on threat capabilities. The sharing of these mitigation strategies with utility owners and operators will aid them in securing their critical infrastructure assets by identifying potential vulnerabilities in their related infrastructure.

1.1.4 Literature Review

The approach to threat categorization used for this work has not been found to exist in any prior Department of Energy (DOE) or other literature. However, there is a strong history of this type of approach within SNL. In 1999, shortly following President Clinton's call for the development of a system for identifying and preventing major attacks to critical infrastructure,[4] James Purvis authored a report on the need for a revision of sabotage categories, target types, and consequences and the development of a standardized risk assessment methodology for physical protection at nuclear power plants.[5] Beginning in 2002, SNL researchers started to assess threats to all critical infrastructure assets. Work has been completed on approaches to critical infrastructure security,[6] common vulnerabilities of control systems,[7] threat-group dynamics,[8] threat assessment,[9,10] and information sharing.[11] Most recently, David Duggan has been focusing on developing generic profiles of cyber threats[12] to industrial control systems;[13] this work continues in the current project by extending the threat profiles to include both kinetic and cyber threats to any system.

Similar to the work being performed at SNL, researchers from Lawrence Livermore National Laboratory (LLNL) presented a methodology for vulnerability and risk assessment using the

[4] *The Clinton Administration's policy on critical infrastructure protection: Presidential Decision Directive 63 (NSC-63).* (1998).
[5] Purvis, J. W. (1999). Sabotage at nuclear power plants, SAND99-1850C. Sandia National Laboratories.
[6] Baker, A. B., et al. (2002). A scalable systems approach for critical infrastructure security, SAND2002-0877. Sandia National Laboratories.
[7] Stamp, J., Young, W., & DePoy, J. (2003). Common vulnerabilities in critical infrastructure control systems, SAND2003-1772C. Sandia National Laboratories.
[8] Backus, G.A., & Glass, R. J. (2005). An agent-based model component to a framework for the analysis of terrorist-group dynamics, SAND2006-0860P. Sandia National Laboratories.
[9] Depoy, J., et al. (2006). Critical infrastructure systems of systems assessment methodology, SAND2006-6399. Sandia National Laboratories.
[10] Merkle, P. B. (2006). Extended defense systems: I. Adversary-defender modeling grammar for vulnerability analysis and threat assessment, SAND2006-1484. Sandia National Laboratories.
[11] Hayden, N. K., & Craft, R. L. (2003). The Knowledge Network (KnowNet): Deepening the nation's understanding of terrorist behavior, SAND2004-0476P. Sandia National Laboratories.
[12] Duggan, D. P. (2005). Generic threat profiles, SAND2005-5411. Sandia National Laboratories.
[13] Duggan, D. P. (2006). Generic attack approaches for industrial control systems, SAND2006-0650. Sandia National Laboratories.

Homeland-Defense Operational Planning System (HOPS).[14] However, although this work proposes a matrix for analyzing threat, it addresses facility-specific vulnerabilities rather than communication between industry and government regarding generic threats. In addition to this work by LLNL, researchers at Idaho National Engineering and Environmental Laboratory (INEEL) have proposed the Quantitative Threat-Risk Index Model (QTRIM) to compute a quantitative threat-risk index on a system and component level.[15] While the QTRIM approach may be able to predict the probability of attack on specific facilities, it focuses on a threat's selection of a target, seems to require a great deal of classified information, and does not perform the same information sharing service of which a generic threat profile would be capable.

Additional works were consulted during the process of identifying discrete threat attributes that can be used to establish the capability of a threat; however, each work focused solely on either cyber or kinetic threats and each seemed concerned only with terrorist threat, rather than all types of threat:

- Researchers at LLNL proposed an analytical framework for assessing terrorist intentions by considering organizational structure and capabilities.[16] Threat profiles were linked to specific types of critical infrastructure.
- As part of a counterterrorism project, the RAND Corporation completed research that addressed threat assessment by identifying the character and boundaries of threat and proposed a framework to prioritize the threat of terrorist groups by assessing the intentions and capabilities of each group.[17]
- The United States Army has also committed a great deal of time to the analysis of terrorism and the recognition of terrorist threats to U.S. military forces. A Military Guide to Terrorism in the Twenty-First Century[18] and its supplemental handbooks[19,20] are intended to support military training and education on the Global War on Terrorism. Although these documents focus solely on terrorist threats, they do stand as a strong reference for identifying threat attributes and for case studies of previous terrorist attacks.

Appendix A of this report includes a full bibliography of papers and reports that are relevant to this work.

---

[14] Durling, Jr., R. L., Price, D. E., & Spero, K. K. (2005). Vulnerability and risk assessment using the Homeland-Defense Operational Planning System (HOPS), UCRL-CONF-209028. International Symposium on Systems and Human Science.

[15] Plum, M. M., Gertman, D. I., & Beitel, G.A. (2004). Novel threat-risk index using probabilistic risk assessment and human reliability analysis, INEEL/EXT-03-01117. Idaho National Engineering and Environmental Laboratory.

[16] Ackerman, G., et al. (2007). Assessing terrorist motivations for attacking critical infrastructure, UCRL-TR-227068, Lawrence Livermore National Laboratory.

[17] Cragin, K., & Daly, S. A. (2004). The dynamic terrorist threat: An assessment of group motivations and capabilities in a changing world. RAND, Project AIR FORCE.

[18] *A military guide to terrorism in the twenty-first century, TRADOC DCSINT Handbook No. 1.* Version 3.0. (2005). U.S. Army Training and Doctrine Command.

[19] *Terror operations: Case studies in terrorism, DCSINT Handbook No. 1.01.* (2005). U.S. Army Training and Doctrine Command.

[20] *Cyber operations and cyber terrorism, DCSINT Handbook No. 1.02.* (2005). U.S. Army Training and Doctrine Command.

1.2 Purpose

The purpose of this threat characterization research and threat matrix development is to aid in the creation of a comprehensive threat analysis framework[21] that enables the objective determination of threat capabilities and supports the ability to identify and prioritize expenditures to mitigate the effects from a class of threats, all in an unclassified venue for use by critical infrastructure providers and utility owners. As seen in Figure 1.1, one of the primary activities necessary to move classified threat information to the unclassified information environment is the development of generic threat profiles that can characterize many different levels of threat without associating a name with a classified ability. This unclassified threat characterization must be able to bin a full spectrum of threat capability to allow for analysts from the classified threat environment to map the characterization of an "unnamed" threat to an equivalent bin, or level, of threat in the unclassified threat environment. This will then allow analysts in the unclassified environment to identify potential attack paths that could be supported by the asserted capability and identify proper mitigation steps to thwart attacks.

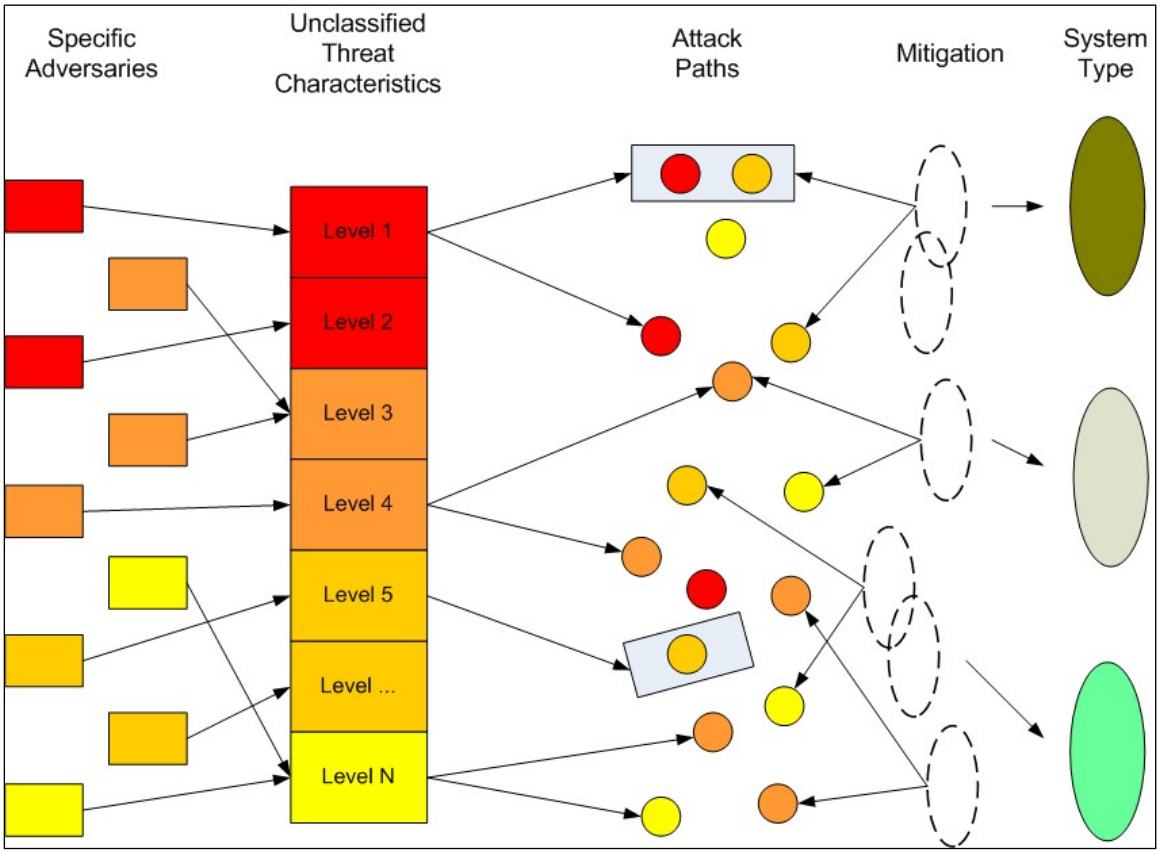

Figure 1.1 Threat Analysis Framework

[21] Duggan, D. P., & Michalski, J. T. (2007). Threat analysis framework report, SAND2007-5792. Sandia National Laboratories.

1.2.1 Reason for Investigation

The reason for this investigation is a combination of historical aspects and the significance of the problem being faced today. Although the "threat of the day" is important to understand, it is not the only issue in place. While looking at only the current threat, the entire picture can become skewed based on assumptions that follow names of organizations due to statements of the media and personal opinion. These assumptions do not allow for the objective differentiation of threats. Creating a generic threat matrix not only removes the assumptions that come with names, but also includes those types of organizations that are not the primary focus of a day, month, year, or decade.

A generic threat matrix also allows for intelligence organizations and other government entities to communicate threat information easily, and without classification issues, by removing the details of a threat, while still capturing its level of commitment and capability. In this way, government entities, such as intelligence organizations, and critical infrastructure entities, such as utility owners, will be able to communicate with fewer barriers and, in the end, be able to provide a more secure and reliable infrastructure than exists today.

1.2.2 Roadmap Challenges

As referenced in the *Roadmap to Secure Control Systems in the Energy Sector*[22] publication, control systems are evolving from isolated operating environments using proprietary software, hardware, and communications technologies toward scalable inter-connected architectures using commercial off-the-shelf (COTS) products and standards-based protocols that provide high levels of interoperability. High connectivity and interoperability comes with a significant security risk. This risk must be managed and, as part of an overall threat analysis framework, threat identification and categorization is an integral part of the overall risk management process.

1.2.3 Audience

This report aims to provide the U.S. Government, including DOE, with a means to communicate to energy-related critical infrastructure providers and utility owners, in a non-classified manner, the dangers they face from potential threats and possible mitigation strategies of those dangers. By applying the generic threat matrix, government entities will be able to inform critical infrastructure entities about which types of threats they should be concerned and what resources (personnel, knowledge, and access) those threats may have at their disposal, without violating the classification of the original information source. This work is designed to be understood by both government and critical infrastructure entities to allow both to communicate with a common vocabulary and the same basic understanding of possible threats.

1.2.4 Desired Response

The primary intention of this report is employment of the generic threat matrix by government entities to share unclassified actionable threat information with critical infrastructure providers and utility owners. In addition to this, the information shared will allow government and critical infrastructure entities to work together to identify possible

[22] Eisenhauer, J., et al. (2006). *Roadmap to secure control systems in the energy sector*. Energetics Incorporated.

attack paths and develop appropriate mitigation strategies for those paths. This will help U.S. critical infrastructure become more secure, as well as enable utility owners and providers to become more aware of potential threats in the future.

To keep this generic threat matrix from becoming obsolete, periodic updates should be applied to the matrix, keeping it in line with the current notion of threat. This may include changing levels of threat or adding new columns to represent a new category of capability. Also, data mining techniques can be used to verify the continued accuracy and relevancy of the threat profiles.

1.3 Scope

To provide an overall threat analysis capability, researchers at SNL are developing a threat analysis framework that employs the important elements necessary to identify, characterize, and mitigate the effects of a threat. As previously demonstrated in Figure 1.1, one of the most important elements needed for unclassified threat analysis is the identification of a threat's capability to carry out a specific type of attack. Current analysis methods tend to concentrate on more subjective aspects of political and social motivation structures without identifying relevant objective characteristics that may be used in identifying attacks each threat might be able to perform. As the focus of this work, which is part of the development of an overall threat analysis framework, a generic set of threat profiles was created to categorize threats. This helps to quantify the threat's ability to conduct both cyber and kinetic operations against a critical infrastructure entity's assets. There is currently no other documented work in the area of threat characterization that is developing generic threat profiles to solve this problem for all systems, whether cyber or physical. Other solutions are reactive in nature, to a specific threat on a specific type of system, while this approach allows the energy-related critical infrastructure provider and utility owner to be proactive.

1.3.1 Extent and Limits of Investigation

For the purposes of this report, the topic will be limited to threats of a malevolent nature only, using generic threat profiles to categorize threats employing cyber, kinetic, and hybrid means against any system, cyber or physical. Although the inputs to this particular work were unclassified open-source materials, previous iterations of the generic threat matrix[23] were validated using a wide variety of source materials.

1.3.2 Goals

The goal of this work is the development of a set of generic threat profiles that can be used to identify and characterize the different levels of adversaries and their related capabilities. These capability profiles allow for unclassified actionable threat information to be distributed to potential stakeholders, such as energy-related critical infrastructure providers and utility owners.

[23] Duggan, D. P. (2005). Generic threat profiles, SAND2005-5411. Sandia National Laboratories.

1.3.3 Objectives

To achieve the goal of this work, the following objectives were accomplished:

- **Identify and define common threat attributes.** This report includes a discussion of each discrete threat attribute and the scale used to determine a threat's profile level.
- Develop the generic threat matrix. This report identifies and characterizes the different levels of adversaries and their capabilities to leverage attacks against critical infrastructure assets.
- Validate the generic threat matrix. This report includes a short discussion of the applicability of threat level profiles to previously occurring events and the discovered or inferred capabilities of the adversary involved.

2 Approach

This work used a qualitative research approach to create the generic threat matrix. That is, the analysis used to determine the nature of the attributes and behavior of the threat being measured was based on professional judgment, not quantitative data. This approach involved background research from open-source material (including literature surveys and case studies), the generation of a matrix of generic threat profiles, and the validation of the matrix against real-world data.

2.1 Methods

The methods employed to create the generic threat matrix included literature surveys and case studies. These sources were used for background research that provided information on the passion and capabilities that have historically been displayed by threat organizations and individuals.

The literature study included papers on threat matrices and threat characterization created by other agencies. Most of these studies focused on the characteristics of executed attacks, but they did provide some knowledge of what capabilities the organization needed to carry out those attacks. Other literature sources were government papers or presentations analyzing specific attacks[24] and generalized organizational capabilities and composition.[25, 26]

Due to the often classified nature of the specific abilities of a threat, case studies were used to develop an in-depth understanding of common threat capabilities. These case studies came from newspaper reports and databases that catalogue terrorist attacks and organizations. The MIPT Terrorism Knowledge Base[25] was a particular asset in gaining information on terrorist threats.

With the knowledge garnered from background research, educated summations were extracted and employed in the creation of the generic threat matrix.

2.2 Assumptions

This investigation involved the following assumptions:

- Current threat analysis focuses on the "threat of the day."
- Analysis of higher-level threats often happens in a classified environment.
- There is need for the communication of unclassified actionable threat information to critical infrastructure providers and utility owners.

[24] "Anatomy of a terrorist attack: An in-depth investigation into the 1998 bombings of the U.S. embassies in Kenya and Tanzania." (2005). The Matthew B. Ridgway Center for International Security Studies at the University of Pittsburgh.
[25] "MIPT Terrorism Knowledge Base (TKB)." (2007). www.tkb.org.
[26] Criminal Intelligence Service Canada. (2006). *2006 Annual Report on Organized Crime in Canada*. Her Majesty the Queen in Right of Canada.

- Advancing technology will boost both cyber and kinetic skills throughout society.
- Threats will continue moving toward hybrid cyber-kinetic attack approaches.
- It is not feasible to catalogue every possible cyber, kinetic, and hybrid threat.

2.3 Procedures

This investigation was completed using the following procedures:

- Identify and define common threat attributes.
  a. Identify discrete threat attributes.
  b. Establish a scale for each attribute that can be used to assign a threat's capability.
- Develop the generic threat matrix.
  a. Use common threat attributes to characterize generic threat profiles.
- Validate the generic threat matrix.
  a. Conduct background research to include literature surveys and case studies.
  b. Determine characteristic levels of threats found during background research.
  c. Verify the applicability of the matrix for categorizing threat.

3 Results and Discussion

This section begins with the definitions and a characterization of the common threat attributes and then presents the generic threat matrix developed by this work. It is important to remember that the matrix includes only attributes of a malevolent threat. Threats of a normal or abnormal nature should be analyzed and mitigated from a functional or safety perspective, rather than a security perspective.

3.1 Threat Attributes

A threat attribute is a discrete characteristic, or distinguishing property, of a threat. The combined characteristics of a threat describe the threat's willingness and ability to pursue its goal. However, both willingness and ability are defined by multiple, separate attributes. The intent of this delineation of attributes is that each defines a distinctive characteristic of a threat and there are no inherent dependencies between any two threat attributes.

There are two families of threat attributes: commitment attributes that describe the threat's willingness and resource attributes that describe the threat's ability.

3.1.1 Commitment Attribute Family

Commitment attributes are the characteristics of a threat that quantify the threat's willingness to pursue its goal. Characteristics of commitment are indicative of a threat's capability because they exemplify the drive of the threat to accomplish its goal. Those threats with the highest commitment will stop at nothing in pursuit of the goal, while those with lower overall commitment will not share such drive and ambition.

There are three attributes in the commitment family: Intensity, Stealth, and Time.

3.1.1.1 Intensity

The threat attribute of Intensity describes the diligence, or persevering determination, of a threat in the pursuit of its goal. This attribute also includes the passion felt by the threat for its goal. Intensity is a measure of how far a threat is willing to go and what a threat is willing to risk to accomplish its goal. Threats with higher intensity are, therefore, considered more dangerous because of their driving ambition in pursuit of a goal.

There are three levels of Intensity:

- **High (H):** The threat is highly determined to pursue its goal and is willing to accept any and all consequences resulting from that pursuit. Acceptable consequences may include imprisonment or the death of organization members or innocent bystanders. The threat may be described as fanatical.
- **Medium (M):** The threat is moderately determined to pursue its goal and is willing to accept some negative consequences resulting from that pursuit. Acceptable consequences may include imprisonment, but usually not the death of group members or innocent bystanders.

- **Low (L):** The threat is determined to pursue its goal, but is not willing to accept negative consequences, such as imprisonment or death, from the pursuit of its goal.

3.1.1.2 Stealth

The threat attribute of Stealth describes the ability of the threat to maintain a necessary level of secrecy throughout the pursuit of its goal. The maintenance of secrecy may require the ability to obscure any or all details about the threat organization, including its goal, its structure, or its internal operations. A higher level of stealth allows a threat to hide its intended activities, as well as its internal structure, from the outside world. This hinders intelligence gathering and pre-emptive measures to counter, or prevent, attacks by the threat.

There are three levels of Stealth:

- **High (H):** The threat is highly capable of maintaining a necessary level of secrecy in pursuit of its goal.
- **Medium (M):** The threat is moderately capable of maintaining a necessary level of secrecy in pursuit of its goal, but is not able to completely obscure details about the threat organization or its internal operations.
- **Low (L):** The threat is not capable of maintaining a necessary level of secrecy in pursuit of its goal and is not able to obscure details about the threat organization or its internal operations.

3.1.1.3 Time

The threat attribute of Time quantifies the period of time that a threat is capable of dedicating to planning, developing, and deploying methods to reach an objective. In the case of a cyber or kinetic attack, it includes any time necessary for all steps of implementation up to actual execution. The more time a threat is willing and able to commit to preparing an attack, the more potential the threat has for devastating impacts.

There are four levels of Time:

- **Years to Decades:** The threat is capable of dedicating many, many years to planning, developing, and deploying methods to reach an objective.
- **Months to Years:** The threat is capable of dedicating several years to planning, developing, and deploying methods to reach an objective.
- **Weeks to Months:** The threat is capable of dedicating several months to planning, developing, and deploying methods to reach an objective.
- **Days to Weeks:** The threat is capable of dedicating several days up to a few weeks to planning, developing, and deploying methods to reach an objective.

3.1.2 Resource Attribute Family

Resource attributes are the characteristics of a threat that quantify the people, knowledge, and access available to a threat for pursuing its goal. Characteristics of resource are indicative of a threat's capability because greater resources may allow a threat to accomplish an objective or goal more easily and with greater overall adaptability.

There are three attributes in the resource family: Personnel, Knowledge, and Access.

3.1.2.1 Technical Personnel

The threat attribute of Technical Personnel quantifies the number of group members that a threat is capable of dedicating to the building and deployment of the technical capability in pursuit of its goal. Technical Personnel includes only group members with specific types of knowledge or skills, such as kinetic or cyber, and those directly involved with the actual fabrication of the group's weapons. A threat with a higher level of Technical Personnel has greater potential for innovative design and development, allowing for the possibility of new methods of reaching a goal that may not have been available in the past. In addition, a higher level of technical personnel also expedites the design and development of a threat's plans for attack.

There are four levels of Technical Personnel:

- **Hundreds:** The threat is capable of dedicating one to many hundreds of individuals to provide the technical capability of building and deploying weapons. These individuals have full communication between them for all design, development, and fabrication work.
- **Tens of Tens:** The threat is capable of dedicating multiple small groups of individuals to provide the technical capability of building and deploying weapons. These groups have only limited communication between groups, but there is full communication within the groups themselves.
- **Tens:** The threat is capable of dedicating a small, independent group of individuals to provide the technical capability of building and deploying weapons. There is full communication between the members of the group.
- **Ones:** The threat is capable of dedicating one to several individuals to provide the technical capability of building and deploying weapons. There is full communication between the individuals.

The designation given to each level of Technical Personnel (e.g., Ones or Hundreds) is intended as a relative measure only and does not necessarily limit or enumerate the actual physical count of active members in a threat organization. For example, a malevolent organization with a thousand members may have only fifty technical personnel capable of building and deploying weapons. Depending on the structure of the organization, the threat would have a Technical Personnel capability of only Tens or Tens of Tens.

3.1.2.2 Knowledge

The threat attribute of Knowledge defines the threat's level of theoretical and practical proficiency and the threat's capability of employing that proficiency in pursuit of its goal. Knowledge also includes the ability of a threat to share information, acquire training in a necessary discipline, and maintain a research and development program. However, this attribute does not include any proficiency found or purchased outside the threat organization. This attribute includes knowledge pertaining to both an offensive and defensive capability within the category. The greater the knowledge of a threat as a whole, the more capability a threat has to pursue its goal with fewer resources and in less time. Also, a threat's knowledge provides a means to differentiate between threats that are cyber-, kinetic-, or hybrid-based.

There are two basic categories of Knowledge:

- **Cyber Knowledge:** The theoretical and practical proficiency relating to computers, information networks, or automated systems.
- **Kinetic Knowledge:** The theoretical and practical proficiency relating to physical systems, the motion of physical bodies, and the forces associated with that movement.

Inside each category, there are three levels of Knowledge:

- **High (H):** The threat is capable of using expert proficiency—both theoretical and practical—in pursuit of its goal. The threat is able to participate in information sharing and is capable of maintaining a training program, as well as a research and development program.
- **Medium (M):** The threat is capable of using intermediate proficiency in pursuit of its goal. Intermediate proficiency can be described as being highly practical knowledge supported by a low or moderate amount of theoretical knowledge. The threat is able to participate in limited information sharing and is capable of providing and acquiring training, as opposed to education; however, the threat is not capable of maintaining a research and development program of its own.
- **Low (L):** The threat is capable of using novice proficiency in pursuit of its goal. Novice proficiency consists of a low to moderate amount of practical knowledge and little to no theoretical knowledge. The threat does not have the capability to share information, provide training, or maintain a research and development program.

3.1.2.3 Access

The threat attribute of Access defines a threat's ability to place a group member within a restricted system—whether through cyber or kinetic means—in pursuit of the threat's goal. A restricted system is considered to be any system, whether cyber or physical, where access is granted based on privileges or credentials. The characteristic of Access details a threat's ability to infiltrate a restricted system, whether through a privileged group member, the blackmail and coercion of an innocent bystander, or the corruption of an under-protected network or computer system. Infiltration by a threat can lead to a wide variety of effects: the need for fewer resources to achieve an objective, the implementation of a long-term scheme of product-tampering, or an increased level of intimate knowledge of a target.

There are three levels of Access:

- **High (H):** The threat is able to plan and place a group member with direct or unlimited access within a restricted system.
- **Medium (M):** The threat is able to plan and place a group member with indirect or limited access within a restricted system.
- **Low (L):** The threat is not able to plan and place a group member within a restricted system.

3.2 Generic Threat Profiles

Using the attributes of threat defined above, generic threat profiles were generated. While it is impossible to consistently capture each distinct type of threat, the generic threat matrix (Table 3.1) enables government entities and intelligence organizations to categorize threat into a common vocabulary. Government organizations, such as SNL and DOE/OE, can use these profiles to identify potential attack paths and initial mitigation strategies. Critical infrastructure entities, such as utility owners and operators, can then use those mitigation strategies to implement actual mitigation plans, specific to their system architectures, to protect infrastructure assets.

Table 3.1 Generic Threat Matrix

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Threat Level 1 will always be the most capable of achieving an objective or goal, while Threat Level 8 is the least capable. There are at least three different attribute levels between each subsequent threat profile in the matrix; for lower-level threats (levels 6 through 8), there are four different attribute levels. In general, each threat level from Level 8 to Level 1 represents a more dangerous threat than the previous level. Although a Level 8 threat may be able to attain the same objective as a Level 1 threat, it will be through an unprotected vulnerability of an asset, the fortuitous timing of an attack, or simple luck, rather than a capability characteristic possessed by the threat organization.

It is possible, indeed likely, that at least one specific threat—out of the full spectrum of threat—will not fit exactly into a specific Threat Level. In this case, the threat should be categorized into the level which has the most similar threat profile. This is the very reason that the generic threat matrix has been designed with levels-of-magnitude difference between subsequent threat levels: to ensure that a threat is not equally similar to two adjacent levels.

3.2.1 Observations

There are several observations that can be made on review of the generic threat matrix. First, there are two boundary conditions necessary for establishing viable threat profiles:

- Threats with a Threat Level 1 profile will always have the highest capability within each attribute.
- Threats with the highest numbered level (Level 8 in this matrix) will always have the lowest capability within each attribute.

Second, a threat's level of Technical Personnel can aid in understanding a threat's other attributes:

- Threats with more Technical Personnel will necessarily have greater Intensity, Knowledge, and Access. This is based on the assumption that more personnel create more viable opportunities.
- Threats with a Technical Personnel level of Ones will not have high Knowledge, because these threats have little capacity for information sharing or research and development programs.
- Threats with Technical Personnel level of Ones will not have high Intensity, because these threats are not likely to be self-sacrificing.

The level of Knowledge possessed by a threat organization also follows an observable pattern:

- Threats with high Cyber Knowledge will not have low Kinetic Knowledge—and vice-versa—because of the application of expert proficiency in both theoretical and practical domains.

A final observation can be made regarding a threat organization's capability for Access:

- Threats with high Knowledge—Cyber or Kinetic—will have at least medium Access due to the assumption that it is easier to attain and harder to detect access achieved through expert proficiency.

3.2.2 Multipliers

There are some properties of threats that, while not distinctive characteristics, can affect one or more threat attributes; they can enhance a threat's capabilities, but do not affect the threat's profile level. Three of these multipliers are Funding, Assets, and Technology.

3.2.2.1 Funding

Funding, the monetary support available to a threat, has historically been used to define the capability of threat groups; however, because the value of currency fluctuates over time, it is a difficult factor to translate into actual capability. As a multiplier, Funding can be used to enhance certain threat attributes, such as Knowledge or Access. On the other hand, it can also reduce the level of a threat attribute such as Stealth—the purchase of greater knowledge or increased access may make an organization more detectable because it is using outside resources.

3.2.2.2 Assets

The multiplier of Assets is similar to that of Funding above. It can enhance a threat's ability to carry out its mission, but can be a difficult factor to translate into actual capability. It is defined as a threat's ability to have, build, or acquire the equipment, tools, and material necessary for the pursuit of its goal.

3.2.2.3 Technology

The type of technology that a threat is capable of utilizing or targeting in pursuit of its goal can be a limiting factor on certain threat attributes, such as Time and Knowledge. The fast-paced, dynamic nature of some technology and its development requires up-to-date knowledge and quick implementation or application.

3.3 Validation of the Generic Threat Matrix

During this work, two methods were employed to validate the applicability of the generic threat matrix. The first was an attack tree analysis to verify the mutual independence of the discrete threat attributes. In addition to establishing variable independence, a series of case studies was performed to verify that a broad range of threat can be binned into the generic threat matrix.

3.3.1 Attack Tree Analysis

The generic threat matrix developed by this project is already being used in attack tree analysis by another research team at Sandia National Laboratories. That team is identifying attack paths against cargo shipments and requires a method for connecting threats to attack paths based on capability profiles; this is achieved using attack tree analysis.

Basic attack tree analysis relies on three classes of information:

1. the events an adversary must undertake to achieve a goal,
2. the parameters associated with these events, and
3. the capabilities of the adversary.

Successful attack tree analysis requires well-defined parameters and capabilities. These should be relatively complete and orthogonal. Incomplete or overlapping parameters and capabilities hinder analysis of the attack tree. Further, when parameters and capabilities vary too much across assessments, comparison becomes increasingly difficult.

Through the attack tree analysis, the attributes and threat profiles developed by this project were found to be both complete and orthogonal; the set of capabilities was found to span the entire "capability space" and each capability was non-overlapping or mutually independent of the others. By providing this set of off-the-shelf parameters and capabilities, the generic threat matrix allows the attack tree analyst to save time and achieve accurate, consistent analysis.

3.3.2 Case Studies

A series of short case studies was performed to validate the applicability of threat level profiles to previously occurring events and the discovered or conjectured capabilities of the adversary involved. The following three examples demonstrate this process.

3.3.2.1 High-level Threat

On April 27, 2007, in the face of disapproval by ethnic Russians, the Estonian government relocated a Soviet war memorial from the center of Tallinn, the Estonian capital city, to a military cemetery. This move sparked rioting, looting and a least a two-month attack on Estonian cyber resources.[27] As reported by several news resources,[28,29] the country of Estonia was subjected to massive distributed denial-of-service (DDoS) attacks targeted at websites of government ministries, political parties, newspapers, banks, and communication companies. Many of the attacks came from ordinary computers, partially thanks to anonymously posted instructions, on Russian-language internet sites, on how to launch DDoS attacks. Estonia was forced to prohibit access to its websites from abroad, an action that caused a potentially huge impact on the country's economy.[27]

BBC News reported that the Estonian foreign ministry published a list of IP addresses from which the DDoS attacks originated; the list included addresses in the Russian government and presidential administration.[30,31] However, as stated by a Kremlin spokesman, "[I]t does not mean that foreign governments are behind these attacks. Moreover, as you probably know, IP address can be fake."[30] This type of sustained cyber-attack against a state's critical infrastructure may be the first known incident of such an assault; if the Estonian government were ever able to attribute the attacks to Russia, it would be the first known case of one state targeting another through cyber-warfare.[32]

These types of attacks, particularly if they were the result of state-on-state cyber-warfare, could be perpetrated by a high-level threat. As seen in Figure 3.2, a high-level threat may match to a Level 1, 2, or 3 profile, which consists of high and medium capabilities. Based on the sustained nature of the attacks, and the type of event that triggered them, the threat is assumed to have a high-level of Intensity, even though the attack did not result in loss of life. The fact that the attacks were cyber-based and effective against a wide-variety of high-security targets, leads to the assumption that the threat has a high-level of Stealth, and at least medium levels of Knowledge and Access. The types of attacks pursued (e.g., website-defacing by groups or individuals and DDoS attacks employing botnets) and the level of information sharing involved suggests that the threat has a Technical Personnel contingent of at least Tens of Tens.

---

[27] "Estonia and Russia: A cyber-riot." (2007). *The Economist*. http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598 Accessed July 19, 2007.
[28] "Russia accused of unleashing cyberwar to disable Estonia." (2007). *The Guardian*. http://www.guardian.co.uk/russia/article/0,,2081438,00.html. Accessed July 27, 2007.
[29] "Cyber assaults on Estonia typify a new battle tactic." (2007). *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122_pf.html. Accessed July 27, 2007.
[30] "The cyber raiders hitting Estonia." (2007). *BBC News*. http://news.bbc.co.uk/2/hi/europe/6665195.stm. Accessed July 27, 2007.
[31] "Estonia hit by 'Moscow cyber war.'" (2007). *BBC News*. http://news.bbc.co.uk/2/hi/europe/6665145.stm. Accessed July 27, 2007.
[32] "Russia accused of unleashing cyberwar to disable Estonia." (2007). *The Guardian*. http://www.guardian.co.uk/russia/article/0,,2081438,00.html. Accessed July 27, 2007.

It is important to remember that the Estonian government was never able to attribute these attacks to another state. This analysis of the responsibility party as a high-level threat is based solely on information gathered from news sources under the assumption that the attacks were the result of a single organization. If, instead, the attacks came from multiple, separate threats with the same objective or goal, the analysis would need to be reformulated for each individual threat.

Table 3.2 High-level Threat Profiles

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
					KNOWLEDGE		
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	CYBER	KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M

3.3.2.2 Mid-level Threat

In December of 2002, Joseph Konopka, also known as "Dr. Chaos", pleaded guilty to six federal felonies including conspiracy, arson, creating counterfeit software, and interfering with computers.[33] After Konopka's arrest in January 2001, the number of power failures caused by vandalism in the affected region dropped from 28 to zero, and the number of minor arsons dropped from more than 200 to a handful. Konopka recruited followers through a chat room called "Teens For Satan" and the group, often known as "The Realm of Chaos" is believed responsible for setting numerous grass fires, vandalizing power substations, damaging communication equipment, and igniting chemicals under gas pipes; damages have been estimated at $2.5 million to $3 million.[34]

The type of attacks perpetrated by Konopka could be the result of a mid-level threat. As seen in Figure 3.3, a mid-level threat has mostly medium capabilities. Although Konopka called himself an anarchist, he claimed that he pursued attacks against utility and communication infrastructure simply because he felt "a sense of intellectual superiority."[33] This type of determination or purpose results in a medium level of Intensity. These types of attacks require at least a medium level of Knowledge of both cyber and physical systems and a low to medium level of Access to restricted systems. In addition, the attacks can be conducted with a fairly small contingent of Technical Personnel with limited planning and development Time. While Konopka himself may be classified as a Level 6 threat, these types of attacks may be pursued by any mid-level threat.

Table 3.3 Mid-level Threat Profiles

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE		ACCESS
					CYBER	KINETIC	
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L

[33] Barton, G. (2002). "'Dr. Chaos' says crime spree was result of 'intellectual superiority.'" *The Milwaukee Journal Sentinel*. http://findarticles.com/p/articles/mi_qn4196/is_20021221/ai_10826333. Accessed July 19, 2007.

[34] Jones, M., & Held, T. (2002). "Lost months of 'Dr. Chaos' interest police: Cyanide suspect disappeared in June." *The Milwaukee Journal Sentinel*. http://www.jsonline.com/story/index.aspx?id=26946. Accessed July 19, 2007.

3.3.2.3 Low-level Threat

There have been several incidents of sabotage and vandalism against electric facilities over the last few years:

- On March 21, 2004, vandals in Prineville, Oregon, disabled a Bonneville Power Administration interstate transmission line.[35] Extensive damage from gunfire put two towers carrying a direct-current transmission line out of service for eight hours. The repairs to the line cost approximately $10,000.
- In May of 2006, a high-voltage electrical facility owned by Western Area Power Administration in Henderson, Nevada, was the target of vandals who cut the fence surrounding the facility and stole aluminum and copper cable from the site.[36] Incidents like these can contribute to higher operation and maintenance costs.
- On October 20, 2006, Appalachian Power announced a reward for information involving vandalism to or theft from the company's electrical facilities. The company reported that each year near Halloween, vandals in rural southern West Virginia cut trees so that they fall on top of power lines. In the two weeks prior to this announcement, vandalism caused the loss of power in four separate counties, affecting thousands of customers.[37]

As seen in Figure 3.4, this type of seemingly-random vandalism, or sabotage, is often caused by a low-level threat due to the relatively low capabilities demonstrated by the responsible party.

Table 3.4 Low-level Threat Profiles

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE		ACCESS
					CYBER	KINETIC	
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

[35] "Reward offered for spring vacation power line vandals." (2004). Bonneville Power Administration. http://www.bpa.gov/corporate/kc/media/NewsRelease.cfm?ReleaseNo=453. Accessed May 30, 2007.
[36] "Help Western combat vandalism at Henderson electric facility." (2006). Western Area Power Administration. http://www.wapa.gov/newsroom/NewsRelease/2006/060106_HendesonVandalism.htm. Accessed July 27, 2007.
[37] "Appalachian Power offers reward for information on vandals, thieves." (2006). Appalachian Power. http://www.appalachianpower.com/news/releases/viewrelease.asp?releaseID=322. Accessed July 27, 2007.

This page intentionally left blank

4 Conclusions

The key piece of knowledge necessary for building defenses capable of withstanding or surviving cyber and kinetic attacks is an understanding of the capabilities posed by threats to both cyber and physical systems, such as SCADA systems used to control the physical processes of critical infrastructure assets. However, current methodologies for analyzing high-level threat do not provide government entities, such as the Department of Energy and intelligence organizations, with an effective means for sharing unclassified actionable threat information with critical infrastructure entities, such as utility owners and operators. There is need for a common vocabulary that can be used by both government and industry to communicate about threat capability while still protecting the classified information source.

With the number of threats continuing to increase, it is no longer feasible to enumerate the capabilities of all known threats and then build defenses based on those threats that are considered, at the time, to be most relevant. To reduce the complexity of the threat space while protecting classified sources, an abstraction must be created to allow all threats to be grouped into a small number of distinctly different levels, based on measurable capabilities. The generic threat matrix proposed in this report abstracts the continuous threat space into eight discrete levels; each level has a specific profile based on quantifiable attributes of Intensity, Stealth, Time, Technical Personnel, Cyber and Kinetic Knowledge, and Access. The magnitude of difference between each level in the generic threat matrix ensures that every unique threat can be catalogued into one specific threat level that defines the threat's ability to pursue a class of attacks.

As part of an overall threat analysis framework, the generic threat matrix allows government and critical infrastructure entities to identify potential attack paths based on a specific threat capability profile, develop mitigation strategies for those attacks, and implement defenses to thwart both the attack and the threat. Through this sharing of actionable threat information, not only will utility owners and operators become more aware of potential vulnerabilities in their related infrastructure, but the overall critical infrastructure of the United States will become more secure and reliable.

This page intentionally left blank

5 Recommendations

The historical approach to dealing with threat by identifying each unique threat and learning its particular capabilities, then identifying protection mechanisms to be implemented, does not work well as the number of these threats increases. The generic threat matrix, as part of an overall threat analysis framework, provides a new method for objective quantification of threat capabilities. This method allows for the transfer of threat capability information to the unclassified domain where it can then be used by analysts to identify potential attack paths that could be supported by the asserted capability and proper mitigation steps to thwart attacks.

This report provides the U.S. Government, including the Department of Energy (DOE), with a means to communicate to critical infrastructure providers and utility owners, in a non-classified manner, the dangers they face from potential threats and possible mitigation strategies of those dangers. The generic threat matrix allows for intelligence organizations and other government entities to communicate threat information easily, and without classification issues, by removing the details of a threat, while still capturing its level of commitment and capability. In this way, government entities, such as DOE, and critical infrastructure entities, such as utility owners, are able to communicate with fewer barriers and, in the end, are able to provide a more secure and reliable infrastructure than exists today.

This work is designed to be understood by both government and critical infrastructure entities to allow both to communicate with a common vocabulary and the same basic understanding of possible threats. The generic threat matrix, as part of an overall threat analysis framework, should be used by

- government entities to communicate with industry regarding the nature of threats while still protecting classified information sources;
- threat analysts to identify potential attack paths based on threat capability and to suggest mitigation strategies relevant to those attacks; and
- critical infrastructure entities to identify and prioritize expenditures for mitigation solutions.

In order to ensure the continued validity of the generic threat matrix, work should continue to be funded to provide greater detail in the capability portions of the matrix and their connection with mitigation design and implementation. This further detail will enable the integration of the generic threat matrix into future attack path research. In addition, the adoption and integration of the overall threat analysis framework will allow critical infrastructure and government entities to be proactive in ensuring the security and reliability of infrastructure assets.

This page intentionally left blank

Appendix A: Bibliography

Ackerman, G., et al. (2007). *Assessing terrorist motivations for attacking critical infrastructure*, UCRL-TR-227068. Lawrence Livermore National Laboratory.

Anatomy of a terrorist attack: An in-depth investigation into the 1998 bombings of the U.S. embassies in Kenya and Tanzania. (2005). The Matthew B. Ridgway Center for International Security Studies at the University of Pittsburgh.

"Appalachian Power offers reward for information on vandals, thieves." (2006). *Appalachian Power*. http://www.appalachianpower.com/news/releases/viewrelease.asp?releaseID=322. Accessed July 27, 2007.

Backus, G. A., & Glass, R. J. (2005). *An agent-based model component to a framework for the analysis of terrorist-group dynamics*, SAND2006-0860P. Sandia National Laboratories.

Baker, A. B., et al. (2002). *A scalable systems approach for critical infrastructure security*, SAND2002-0877. Sandia National Laboratories.

Barton, G. (2002). "'Dr. Chaos' says crime spree was result of 'intellectual superiority.'" *The Milwaukee Journal Sentinel*. http://findarticles.com/p/articles/mi_qn4196/is_20021221/ai_10826333. Accessed July 19, 2007.

Baybutt, P. (2002). "Assessing risks from threats to process plants: Threat and vulnerability analysis." *Process Safety Progress*, 21:4, 269-275.

Bush, G. W. (2003). *Homeland Security Presidential Directive (HSPD-7): Critical infrastructure identification, prioritization, and protection*.

The Clinton Administration's policy on critical infrastructure protection: Presidential Decision Directive 63 (NSC-63). (1998).

Cragin, K., & Daly, S. A. (2004). *The dynamic terrorist threat: An assessment of group motivations and capabilities in a changing world*. RAND, Project AIR FORCE.

Criminal Intelligence Service Canada (2006). *2006 Annual Report on Organized Crime in Canada*. Her Majesty the Queen in Right of Canada.

"Cyber assaults on Estonia typify a new battle tactic." (2007). *The Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802112_pf.html. Accessed July 27, 2007.

Cyber operations and cyber terrorism, DCSINT Handbook No. 1.02. (2005). U.S. Army Training and Doctrine Command.

"The cyber raiders hitting Estonia." (2007). *BBC News*. http://news.bbc.co.uk/2/hi/europe/6665195.stm. Accessed July 27, 2007.

Depoy, J., et al. (2006). *Critical infrastructure systems of systems assessment methodology*, SAND2006-6399. Sandia National Laboratories.

Duggan, D. P., & Michalski, J. T. (2007). *Threat analysis framework report*, SAND2007-XXXX. Sandia National Laboratories.

Duggan, D. P. (2006). *Generic attack approaches for Industrial Control Systems*, SAND2006-0650. Sandia National Laboratories.

Duggan, D. P. (2005). *Generic threat profiles*, SAND2005-5411. Sandia National Laboratories.

Durling, Jr., R. L., Price, D. E., & Spero, K. K. (2005). "Vulnerability and risk assessment using the Homeland-Defense Operational Planning System (HOPS)", UCRL-CONF-209028. *Proc. of International Symposium on Systems and Human Science*.

Eisenhauer, J., et al. (2006). *Roadmap to secure control systems in the energy sector*. Energetics Incorporated.

"Estonia and Russia: A cyber-riot." (2007). *The Economist*. http://www.economist.com/world/Europe/displaystory.cfm?story_id=9163598. Accessed July 19, 2007.

"Estonia hit by 'Moscow cyber war.'" (2007). *BBC News*. http://news.bbc.co.uk/2/hi/europe/6665145.stm. Accessed July 27, 2007.

Examining the cyber capabilities of Islamic terrorist groups. (2003). [Presentation.] Institute for Security Technology Studies at Dartmouth College.

Guzie, G. L. (2000). *Vulnerability risk assessment*, ARL-TR-1045. Survivability/Lethality Analysis Directorate, Information & Electronic Protection Division, Army Research Laboratory.

Hayden, N. K, & Craft, R. L. (2003). *The Knowledge Network (KnowNet): Deepening the nation's understanding of terrorist behavior*, SAND2004-0476P. Sandia National Laboratories Advanced Concepts Group.

"Help Western combat vandalism at Henderson electric facility." (2006). Western Area Power Administration. http://www.wapa.gov/newsroom/NewsRelease/2006/060106_HendesonVandalism.htm. Accessed July 27, 2007.

Jones, M., & Held, T. (2002). "Lost months of 'Dr. Chaos' interest police: Cyanide suspect disappeared in June." *The Milwaukee Journal Sentinel*. http://www.jsonline.com/story/index.aspx?id=26946. Accessed July 19, 2007.

Lambakis, S., Kiras, J., & Kolet, K. (2002). *Understanding "asymmetric" threats to the United States*. National Institute for Public Policy.

Lemley, J. R., Fthenakis, V. M., & Moskowitz, P. D. (2003). "Security risk analysis for chemical process facilities." *Process Safety Progress*, 22:3, 153-162.

Luiijf, E. A. M. (2005). "Energy sector threats and vulnerabilities." *Proc. of 3rd EAPC/PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning*.

Matalucci, R. V., & O'Connor, S. (2000). "Infrastructure and Architectural Surety[SM]." *Materials Research Society: When Materials Matter—Analyzing, Predicting and Preventing Disasters. 630*, GG1.3.1-9.

Merkle, P. B. (2006). *Extended defense systems: I. Adversary-defender modeling grammar for vulnerability analysis and threat assessment*, SAND2006-1484. Sandia National Laboratories.

A military guide to terrorism in the twenty-first century, TRADOC DCSINT Handbook No. 1. Version 3.0. (2005). U.S. Army Training and Doctrine Command.

MIPT Terrorism Knowledge Base (TKB). (2007). http://www.tkb.org .

National Strategy for Homeland Security. (2002). Office of Homeland Security.

NetBreaker analytical tools identify terrorist groups, members, capabilities. (2007). Argonne National Laboratory.

Olson, D. T. (2005). *The path to terrorist violence: A threat assessment model for radical groups at risk of escalation to acts of terrorism.* Naval Postgraduate School.

Plum, M. M., Gertman, D. I., & Beitel, G. A. (2004). *Novel threat-risk index using probabilistic risk assessment and human reliability analysis*, INEEL/EXT-03-01117. Idaho National Engineering and Environmental Laboratory.

Post, J. M., Ruby, K. G., & Shaw, E. D. (2002). "The radical group in context: 1. An integrated framework for the analysis of group risk for terrorism." *Studies in Conflict & Terrorism*, 25:2, 73-100.

Post, J. M., Ruby, K. G., & Shaw, E. D. (2002). "The radical group in context: 2. Identification of critical elements in the analysis of risk for terrorism by radical group type." *Studies in Conflict & Terrorism*, 25:2, 101-126.

Purvis, J. W. (1999). *Sabotage at nuclear power plants*, SAND99-1850C. Sandia National Laboratories.

"Reward offered for spring vacation power line vandals." (2004). Bonneville Power Administration. http://www.bpa.gov/corporate/kc/media/NewsRelease.cfm?ReleaseNo=453. Accessed May 30, 2007.

Rollins, J., & Wilson, C. (2007). *Terrorist capabilities for cyberattack: Overview and policy issues*, CRS Report for Congress, RL33123. Congressional Research Service, The Library of Congress.

"Russia accused of unleashing cyber war to disable Estonia." (2007). *The Guardian*. http://www.guardian.co.uk/russia/article/0,,2081438,00.html. Accessed July 27, 2007.

Stamp, J., Young, W., & DePoy, J. (2003). *Common vulnerabilities in critical infrastructure control systems*, SAND2003-1772C. Sandia National Laboratories.

Terror operations: Case studies in terrorism, DCSINT Handbook No. 1.01. (2005) U.S. Army Training and Doctrine Command.

Wilson, C. (2005). [Presentation.] *Emerging terrorist capabilities for cyber conflict against the U.S. Homeland*. Congressional Research Service, The Library of Congress.

This page intentionally left blank

Appendix B: Acronyms

COTS	commercial off-the-shelf
DOE	Department of Energy
DOE/OE	Department of Energy Office of Electricity
DDoS	distributed denial-of-service
HOPS	Homeland-Defense Operational Planning System
INL or INEEL	Idaho National Laboratory, previously known as Idaho National Engineering and Environmental Laboratory
LLNL	Lawrence Livermore National Laboratory
MIPT	Memorial Institute for the Prevention of Terrorism
QTRIM	Quantitative Threat-Risk Index Model
SCADA	supervisory control and data acquisition
SNL	Sandia National Laboratories

This page intentionally left blank

Appendix C: Glossary

access	The attribute of a threat that defines the threat's ability to place a group member within a restricted system—whether through cyber or kinetic means—in pursuit of the threat's goal.
actionable information	Information that allows a decision to be made or an action to be taken.
assets	The threat's ability to have, build, or acquire the equipment, tools, and material necessary for the pursuit of its goal.
attack path	The sequence of steps and accesses necessary to complete an assault on a target.
attribute	A discrete characteristic or distinguishing property, of a threat.
commitment	The attributes of a threat that qualify the threat's willingness to pursue its goal.
critical infrastructure	Those systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[38]
funding	The monetary support available to a threat for the pursuit of its goal.
goal	The threat's overall intent or the end-result the threat is trying to achieve.
intensity	The attribute of a threat that describes the diligence, or persevering determination, of a threat in the pursuit of its goal.
knowledge	The attribute of a threat that defines the threat's level of theoretical and practical proficiency and the threat's capability of employing that proficiency in pursuit of its goal; knowledge includes the ability of a threat to share information, acquire training in a necessary discipline, and maintain a research and development program.
knowledge, cyber	The theoretical and practical proficiency relating to computers or automated systems.
knowledge, kinetic	The theoretical and practical proficiency relating to physical systems or the motion of physical bodies and the forces associated with that movement.
mitigation strategy	A set of design criteria for a system that is intended to enable the system to overcome or survive a particular type of event.

[38] *National Strategy for Homeland Security*. (2002). Office of Homeland Security.

multipliers	The properties of a threat that, while not distinctive characteristics, can affect one or more threat attributes; they can enhance a threat's capabilities, but do not affect the threat's profile level.
objective	A task, such as a specific attack, that a threat must accomplish to progress toward the goal.
resources	The attributes of a threat that quantify the people, knowledge, and access available to a threat for pursuing its goal.
stealth	The attribute of a threat that describes the ability of a threat to maintain a necessary level of throughout the pursuit of its goal.
technical personnel	The attribute of a threat that quantifies the number of group members that a threat is capable of dedicating to the building and deployment of the technical capability in pursuit of its goal.
threat	A malevolent actor, whether an organization or an individual, with a specific political, social, or personal goal and some level of capability and intention to oppose an established government, a private organization, or an accepted social norm.
threat, abnormal	A natural disaster, such as hurricane-force winds or earthquakes, resulting in the failure of structural steel frames.[40]
threat, malevolent	A manmade event or condition; for example, a bombing of a federal facility or the use of chemical and biological agents in terrorist attacks.[40]
threat, normal	An event or condition that affects the reliability of the day-to-day operations; for example, the mean time between failures or inefficient repair and replacement (maintenance) schedules to offset the effects of aging.[39]
time	The attribute of a threat that quantifies the period of time that a threat is capable of dedicating to planning, developing, and deploying methods to reach an objective.

[39] Matalucci, R. V., & O'Connor, S. (2000). Infrastructure and Architectural Surety[SM]. *Materials Research Society: When Materials Matter—Analyzing, Predicting and Preventing Disasters. 630,* GG1.3.1-9.

Appendix D: For More Information

NSTB (National SCADA Testbed) Project	Jennifer DePoy, manager, Critical Infrastructure Systems, Sandia National Laboratories, jdepoy@sandia.gov.
ieRoadmap	http://www.energetics.com/csroadmap/index.aspx Interactive Energy Roadmap to Secure Control Systems Energetics Incorporated