INTRODUCTION

Over the past century, New York City's skyline has become an enduring image of America's vitality and strength. Although each building faces a low probability of being attacked, in the post-September 11, 2001 era, building owners should consider security during their planning and design processes. Yet security must be balanced against aesthetic appeal, functionality, cost, and sustainability, among other concerns. Because each building is distinct, the New York City Police Department (NYPD) cannot offer a single blueprint for protective security design. Therefore, *Engineering Security* presents a general approach to assessing risk and designing security into new building construction and major renovations.

Buildings in dense urban environments are vulnerable to several different forms of terrorist attack. To date, threats from explosive devices have been most common; in the future, threats from chemical, biological, and radiological weapons may grow with the proliferation of those technologies. Given these threats, protective security design provides a comprehensive approach to improving security in buildings that present elevated risk levels. Protective security design aims to identify a series of key actions and design criteria to reduce physical damage to structural and non-structural components of buildings and related infrastructure.[1] Information about a building's protective security design features can, however, prove dangerous in the hands of potential terrorists, so safeguarding sensitive security documents is essential.

Every building faces a unique set of security concerns, based on variations in the threat, vulnerability, and potential impact associated with a terrorist attack. *Engineering Security* sets out a risk-tiering system designed to categorize

buildings based on these variables. A set of protective security design recommendations correlates to each risk tier, providing guidance to building owners and design professionals; these recommendations include attack prevention and mitigation measures.

Because of the great uncertainties in any assessment of terrorism risk, *Engineering Security* applies a "minimax" strategy to protective security design. Developed to identify solutions in the face of uncertainty, the minimax theorem minimizes the maximum expected loss associated with a given risk.[2] Accordingly, the protective security design measures set out in this document seek to minimize the maximum potential casualties, damage, and economic loss caused by a terrorist attack.

The advent of computer modeling has made the need for protective security design more acute than ever before. In the pre-computer era, architects and engineers were forced to overbuild structures to ensure stability. New technologies have allowed the building community to optimize structures – to create soaring towers and expansive curtain walls just strong enough to support predictable loads. The advances of computing power have thus created an almost paradoxical tradeoff: the more efficiently built the structure, the more vulnerable it is to catastrophic failure when subjected to abnormal loading.

Evolution of Protective Security Guidelines

The recommendations presented in subsequent chapters can best be understood in light of an evolving series of federal and local government guidelines concerning protective security design. For nearly three decades, building security has been the subject of debate in various federal agencies, including the Department of State, the Department of Defense, the Department of Justice, and, most recently, the Department of Homeland Security.

Initially, federal guidelines focused on protecting U.S. interests abroad, primarily embassies and government buildings. The scope of these guidelines expanded to include the security of buildings on U.S. soil after the bombing of the Alfred P. Murrah Federal Building in Oklahoma City in 1995 and the attacks of September 11, 2001.

The first federal protective security guidelines were set out in the *Inman Report* of 1985, issued by the Secretary of State's Advisory Panel on Overseas Security.[3] Written in response to the 1983 vehicle-borne explosives attacks against a U.S. Marine Corps Barracks and the U.S. Embassy in Beirut, the report details the need for increased security at diplomatic facilities overseas, ultimately tying the level of security that buildings require to the level of threat that buildings and their occupants face. Although the *Inman Report* applies a risk-tiering method only to diplomatic facilities, the Department of State has since employed such a method in its *Security Guidelines for American Enterprises Abroad*, concerning the vulnerability of American private-sector interests overseas.[4]

Another risk-tiering method has been used in the context of protecting domestic buildings. Two months after the 1995 attack on the Alfred P. Murrah Federal Building in Oklahoma City, the Department of Justice issued *Vulnerability Assessment of Federal Facilities*, listing over 50 minimum protective security standards proposed for existing federal facilities and defining five risk tiers, each with corresponding security standards.[5] In 2001, the Interagency Security Council first published its own set of guidelines in *Security Design Criteria*, a periodically updated series.[6] While the starting point for *Security Design Criteria* was the Department of Justice's *Vulnerability Assessment of Federal Facilities* guidelines, the Interagency Security Council's guidelines ultimately employ different criteria for rating risk and assigning protection levels.[7]

Federal Emergency Management Agency Guidelines

Following the attacks of September 11, 2001, the Federal Emergency Management Agency (FEMA) published a series of documents addressing the various risks, including the terrorism risk, to buildings and related infrastructure nationwide. FEMA's *Risk Management Series* provides design guidance to enhance security and mitigate the potential impact of terrorist attacks. These best practices inform and complement the recommendations presented in subsequent chapters.

The core security documents in the *Risk Management Series* include: FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*; FEMA 430, *Site and Urban Design for Security: Guidance Against Potential*

Terrorist Attacks; and FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*. FEMA 426 details security measures designed to reduce the physical damage caused by terrorist attacks.[8] FEMA 430 emphasizes architectural and engineering design considerations.[9] Finally, FEMA 452 sets out a process for determining threats to critical assets within buildings and assessing vulnerabilities to those threats.[10] The *Risk Management Series* includes specific case studies on integrating security with site design and should be referenced when selecting solutions to security needs at building sites. The recommendations set out in the FEMA studies are not legally compulsory.

National Institute of Standards and Technology Recommendations

In response to the destruction of the World Trade Center in 2001, the National Institute of Standards and Technology (NIST), a federal agency within the Department of Commerce, conducted a three-year building and fire safety investigation to study the factors contributing to the post-impact collapse of the World Trade Center Towers (WTC1 and WTC2) and Building 7 (WTC7). The final report on WTC1 and WTC2, published in September 2005, describes the aircraft impacts, subsequent fires, and eventual collapse of the towers, including an evaluation of the evacuation and emergency response procedures as well as the practices employed in the design, operation, and maintenance of the buildings.[11] The final report on WTC7, published in August 2008, finds that uncontrolled fires were the primary cause of the building's collapse: as heat from the fires caused steel floor beams and girders to expand, a catastrophic chain of events ensued, leading to the failure of a key structural column, which initiated the progressive collapse of the entire building.[12]

Both NIST reports conclude with a series of recommendations for improving building and fire safety. The report on WTC1 and WTC2 presents a total of 30 recommendations, ranging from enhancements to structural integrity and new methods for fire-resistant design, to improved evacuation and emergency response protocols.[13] The report on WTC7 offers an additional recommendation, suggesting that buildings be evaluated to ensure adequate fire performance of structural systems.[14] Additionally, both reports address existing codes, standards, and industry practices that warrant revision, while offering practical guidance to

engage the building and fire-safety communities in implementing the proposed changes.[15] Like the FEMA recommendations, the NIST recommendations are not legally compulsory.

The NIST recommendations serve as the foundation for 23 new provisions that were adopted by the International Code Council for incorporation in the 2009 editions of the International Building Code (IBC) and International Fire Code (IFC), including: enhanced structural resistance to building collapse; an additional exit stairway in tall buildings; a 50 percent increase in stairway width for new high-rise buildings; strengthened bonding, installation, and inspection criteria for fireproofing; more reliable automatic sprinkler systems; new fire service access elevators for emergency responders; more visible and prevalent exit path markings; and more effective coverage for emergency responder radio communications.[16] While jurisdictions may modify these provisions prior to adoption, the standards advocated by the International Code Council are widely considered minimum safety standards that most jurisdictions strive to meet.[17]

Many of the recommendations presented in *Engineering Security* are predicated on the NIST recommendations: several have incorporated the NIST recommendations in whole or in part. Subsequent chapters expand on the integration of the NIST findings into *Engineering Security*.

Municipal Codes and Standards

While the federal government has promulgated comprehensive protective security design criteria to meet emerging terrorist threats to federal buildings, municipal governments have yet to codify these standards in the same way.[18]

Local building and fire codes are typically shaped by the demands of the marketplace, as real estate developers and design professionals seek to balance security concerns with economic considerations. Traditionally, such codes have required structural designs that can withstand normal loads as well as those associated with environmental conditions such as wind, snow, fire, and earthquakes.[19] Although few, if any, municipal codes fully account for the risks associated with terrorist bombings, in recent years, such codes have increasingly

adapted to meet post-September 11, 2001, realities. New York City is pioneering this effort with its Building Code and Fire Code modeled on the IBC and IFC, respectively.[20]

Effective July 1, 2008, the New York City Building Code streamlines and modernizes the City's 1968 Code. The Building Code mandates certain protective security measures of universal applicability and suggests several design methods to improve structural performance and prevent progressive collapse.[21] The New York City Building Code goes further than most building codes to account for extreme loads associated with vehicular impact and accidental gas explosions.[22] Effective July 1, 2008, the New York City Fire Code also sets enhanced fire protection standards as well as operational and maintenance requirements for fire alarm systems, emergency communication systems, and means of egress.[23]

Unlike the recommendations developed by the federal government, the New York City Building Code and Fire Code – and municipal codes more generally – carry the force of law: failure to comply with them carries legal consequences.

Purpose and Process

Engineering Security presents a forward-looking approach to protective security design that will undoubtedly evolve as new countermeasures are developed to address emerging threats. Accordingly, the recommendations set forth in subsequent chapters are intended to be fluid and adaptable to a changing environment.

Recognizing that every building faces unique security concerns, *Engineering Security* presents not a one-size-fits-all prescriptive approach, but a method for tailoring protective security measures to meet particular needs. Buildings in New York City require varying levels of security: the vast majority warrant no special precautions, while a mere handful necessitate heightened security. The recommendations set forth in this document apply primarily to the latter group. While these recommendations provide specific direction, they should not be viewed as onerous requirements; these recommendations are instructive, not obligatory. *Engineering Security* sets out best practices for the building community, not legal requirements.

Box 1: Security Consultation with NYPD

Prior to initiating contact with the NYPD, building owners should conduct a risk assessment of their buildings to determine the appropriate risk tier (as outlined in Chapter Two). Owners of High Tier buildings and certain Medium Tier buildings are encouraged to contact the NYPD's Counterterrorism Bureau early in the design process. In appropriate circumstances, a member of the Counterterrorism Bureau will contact the owner to arrange a meeting. At the meeting, owners should be prepared to discuss their assessment of the building's risk, as well as protective security design features, including those that would require the consent of other City agencies.

Ultimately, achieving effective protective security design requires a public-private partnership between security experts and the building and design community. Box 1 outlines the NYPD's consultative process for facilitating such a partnership: a collaborative effort that should be thought of as a negotiation resulting in a series of action-oriented protective security design recommendations.

While the process described in Box 1 is particular to New York City, many of the recommendations outlined in subsequent chapters are widely applicable and may be applied to densely populated urban environments more generally.

Limitations

The NYPD authored *Engineering Security* with new building construction projects in mind. Nevertheless, many of the document's protective security design recommendations may be suitable for retrofitting existing structures. Certain existing buildings will require critical upgrades based on unique structural vulnerabilities; for example, exposed columns on some buildings may require retrofit upgrades such as localized hardening. Other existing buildings should incorporate sensible security upgrades, as appropriate, during the course of general renovations.[24]

Additionally, to the extent that zoning resolutions, as applied to specific buildings, may conflict with certain recommendations presented in *Engineering*

Security, building owners must work within the confines of local regulations. Building owners should consult with relevant professionals about the possibility of applying for waivers, variances, or exemptions to permit appropriate protective security design measures.

Organization and Content

Engineering Security was written for the use of building owners and design professionals as they select and implement appropriate protective security design measures. With this audience in mind, the document's recommendations – presented as suggestions rather than mandates – are organized thematically by chapter.

Chapter One provides background on the threat to buildings from explosive devices, including a discussion of different types of explosive devices and an overview of blast effects. Chapter Two presents a risk-tiering system that categorizes buildings into three risk tiers: Low, Medium, and High, based on assessed threat, vulnerability, and impact levels. The recommendations presented in subsequent chapters address the specific security challenges facing Medium and High Tier buildings.

Chapters Three through Seven present the NYPD's protective security design recommendations. Chapter Three focuses on perimeter security, emphasizing the importance of performing a vehicle threat vector analysis and evaluating the benefits of installing hard and soft perimeters. Chapter Four addresses building design features, including site layout and orientation choices that may affect the impact of an explosives attack as well as measures designed to mitigate the hazards associated with debris in large explosions and prevent collapse. Chapter Five discusses access control, screening, and monitoring techniques that may prove useful in preventing and deterring potential terrorist attacks. Chapter Six surveys emergency preparedness solutions, including fire-resistance, emergency egress, and communication system standards. While the recommendations presented in Chapters Two through Six focus mainly on threats from explosive devices, the recommendations presented in Chapter Seven pertain to unconventional terrorist threats involving chemical, biological, and radiological weapons; the recommendations focus on heating, ventilation, and air

conditioning (HVAC) systems and detection technology.

Taken together, these chapters describe the NYPD's approach to protective security design, beginning with a risk assessment and determination of a risk tier, and leading to risk-appropriate protective security design recommendations.