PHYSICAL SECURITY

Physical Hardening "Armoring" for Security

Physical Security, when a security practitioner hears that definition, usually two things happen:

1) That person will think about the more common denominators that come to mind such as access control, perimeter detection, fences, response forces/patrols, upgraded locks, lighting, barriers, firewalls, software, sensors, bars, etc., or that person will:

2) Consider a much broader scope of the definition and derive at one or more additional questions based on a need for further information. These questions will provide the additional information that will lead to a definitive direction or approach to ensure a proper integration of measures such as: Physical security for what? What type of threat? What level of threat? For people, property or both?

Physical security is any and all necessary requirements that once implemented are designed to prevent, deter, inhibit or mitigate threats that face the safety and security of persons and/or property.

With respect to safety and security, the two are distinguished by the following definitions:

> ***Safety*** **-** Provides for the reduction of the risk of occurrence of injury, loss or death from accidental or natural causes.
>
> ***Security*** **-** Provides for the reduction of the risk of occurrence of injury, loss or death from the deliberate or intentional actions of man.

Physical threats come in all shapes and sizes. But, they all will fall into three broad range categories with a compendium of elemental terms that are utilized to describe the specific ways of how the "attack" will occur. These three categories are: ***Forced Entry Threats, Ballistic Threats, and Explosive Blast Threats.***

Now some of you are thinking wait a minute, your going beyond the scope of standard physical security into high threat physical security situations! *Wrong.* All types of safety and security measures should be scrutinized and looked over several times to ensure that they fulfill the entire current and future status of the physical security requirements, laid out to cover both safety and security in their entirety. Neither safety nor security are requisites that once implemented are complete. Both safety and most of all security are continual and dynamic, always changing with technological advancements, and the advancement in the art of circumventing those technological wonders. Safety and security are and should be considered and handled as a continuous full time advancing and adapting implementation of measures.

Now each of the three threats, forced entry, ballistic and explosive blast cover a myriad of more specifically defined types of attack, such as sabotage, burglary, theft, car jackings, drive by shootings, kidnapping, armed robbery, network/data intrusions, murder, etc. For example, forced entry threats generally categorized, covers any and all attempts to circumvent electronic, structural, mechanical, biological or other "physical barriers" to either gain access into, out of, or to destroy, cripple or kill the property or persons within. This type of threat can also be aided by the use of other threat types such as

ballistic or explosive blast threats in an effort to structurally weaken or damage systems and components prior to or subsequent to the actual forced entry attack. Each of these threats have specification prerequisites that categorize and delineate the actual attacking variables, but, before we get into each, let us go back to the various definitions of physical security.

For the intended purpose of this chapter, physical security will go beyond the use of devices to detect, alert and deter perpetrators. We will focus on the least of all considered, but most predominately relied on feature within the whole compedium of measures at our disposal that we actually rely on when all else fails - the Physical "Hardening" or "Armoring" of the target. This is oftentimes thought of as the last measure of importance to be implemented or the choice most likely not utilized until the risk of the threat has escalated beyond the capabilities of all other extraneous implemented measures and coupled devices, whether state of the art in technology or not.

Remember, anything that is electrical, mechanical or biological can and will have problems and failures.

Therefore, as a prudent and technologically thoroughly educated security practitioner you will see that physical hardening or (Armoring) can eliminate or mitigate the need for much of the ancillary devices used today with the proper selection and integration of foundational hardening components, sub-systems and assemblies. Armoring does not necessarily mean the heavy cladding of steels and thick bullet resistant glazings. *Not at all!* Armoring covers threats from the incidental smash and grab forced entry threats to the effects sustained from such attacking elements as one would encounter during any war time scenario and everything in between. The "Physical Hardening" or strengthening of facilities, vehicles, vessels, aircraft to personal protection garments such a body armor is far more reaching and diversified than most security practitioners assume to know.

Physical hardening or armoring of a facility for example, if implemented and correctly installed, does work in favor for the security department and personnel in several ways. It not only reduces the costs associated with the various types of electronic devices utilized when properly interfaced to detect, alert and deter perpetrators, as the sophistication becomes dependent primarily upon the structural weaknesses of the ingress and egress areas, but the correctly armored (hardened) facility utilizes materials that preclude easily attained access through them.

One good example is a large Fortune 1000 firm that had multiple redundant intrusion access detection devices throughout their facility providing overlapped coverage surrounding the door and window areas. This was specified due to lack of appropriate physical "armoring" hardening doors and window assemblies. The doors were hollow core steel 16 gauge doors that had been breached three times in the past, one time subsequent to the bypassing of the digital dialer communication unit. These doors, three of them had been pried upon forcing the thin gauge hollow core doors to separate around the locking strike areas twice and separating the door from the hinges themselves once. Needless to say, had appropriate forced entry resistant doors been specified and installed this would have precluded the 3 entry breaches that occurred. The cost difference between the originally installed door units excluding the replacement costs for the door repairs and the $750,000.00 lost during the breach was $475.00. Now that was just through the door openings! There were also two attempts, one successful and the other abandoned through the window glazing units.

Secondly, it reduces the redundancy often required for electronic devices due to their limitations and restraints placed upon them such as inadequate wide coverage areas and zones, hardware/software incompatibilities, human error, equipment failure and environmental conditions. Third, the human impact and it's responses from such installations need be assessed with reference to not only the possible prevention due to the awareness of such devices but also the avoidance (lack of possible business) due to the facility being in a seemingly non-desirable location that necessitates such implementations.

For example, commercial and/ or retail businesses or banks which are frequently attacked, robbed or vandalized, are often closed or operate on specifically limited times regardless of their location or the volume of business they transact. Today, all prudent facility designers pay serious attention to the specific issues of security and safety - especially to those issues which are most apparent to the users of the facilities. This may not be an obstacle in all cases, but there are other issues with respect to every type of facility, vehicle, vessel or aircraft utilized with the organization that will ultimately require quantifying the bottom line costs vs. the bottom line savings to upper management. It does not matter whether it is commercial, industrial, government, residential, military or civilian, every situation does have its own inherent variables that can be worked with or manipulated to reduce existing costs, and/or new implementation costs with careful planning and foresight, as well as reducing the associated costs to other sections or divisions within the organization.

As has been seen, and as it will continue, one will always have to quantify the costs of security and compare that with its capabilities. I have seen billion dollar net figured multi-national firms decide against a security implementation on the onset, to turn around and have in implemented subsequent to an incident. This happened purely from those left in charge of the security procurement process, not being able to justify in dollars and operable sense, the assets of the security measure(s).

In order to start with a base from which to specify what types of armoring implementations you will utilize and how to integrate that hardening with other various types of devices to detect, alert and deter perpetrators, you need to have a fundamental understanding of the various types of threat terminology.

THREAT - *A perception of the capability, skill and motivation of an intruder based upon:*

1. The intruders accessibility to the target without substantial risk to the intruder.
2. The time of opportunity presented for the attack, combined with the allowable duration to complete the attack, and
3. The monetary funding available for appropriate attacking/defeating devices.

THREAT LEVEL 1

One or more unskilled individuals with little or no knowledge of security systems or physical protective measures, who attack with little or no advanced planning, usually on targets with little or no security measures. Motivation being monetary gain or vandalism.

THREAT LEVEL 2

One or more semi-skilled individuals with some knowledge of and ability to defeat or compromise low-level security systems and physical protective measures. Motivation being profit.

THREAT LEVEL 3

A group of skilled individuals with strong motivations and the capability, knowledge and funding for the devices necessary to defeat the implemented security measures. Motivated by profit, public attention, or interruption of production and/or services (sabotage).

THREAT LEVEL 4

A group of highly skilled individuals with extremely strong motivation, substantial knowledge and capabilities, and the funding for the state of the art technological support. Motivated by profit, public attention, terrorism or acts of war.

As you can see, the variables for any of the three types of threats - forced entry, ballistic and explosive blast have several levels based on:

- The severity of the attack.
- The physical capabilities of the person(s) involved in the attack.
- The motivational element outweighing the inherent risk of being caught or killed.
- The quantity of man power needed to complete the entire sequence(s) within the attack.
- The varied times necessary to complete the entire sequence(s) of the attack including the pre and post transportation and logistics.
- The types and advancements of implements coupled with the sophistication of and necessary education and training with the various materials, equipment, and compositions.
- The complexity of the attack which requires or utilizes liaison resources to procure information, access codes, specifications/blueprints or drawings, distraction/interference, or forced/paid cooperation from entities or sources.

Each threat category has specific prerequisite elements associated with the various levels of severity. Each level of severity resistance is based upon specific testing criteria established by select testing procedures and protocol. There are numerous testing agencies and laboratories that conduct tests accordingly. However, to refrain from encroaching upon confidential and/or proprietary government and military standards, I will provide common base-line definitions of the more commonly utilized and recognized certifiable civilian standards.

Please note: This text attempts to refrain from the more common misused or slang variations of words to describe specific items such as:

- *Weapon* - Weapon is a very broad based term. When in reference to ballistic threats it will not be used. Firearm is the appropriate term when describing handguns, shotguns and rifles used, if not specifically called out. When in reference to forced entry it will not be used. The word implement or the specific types of tools, equipment or devices will be used to describe what is used during the attack.

- *Clip* – When used in reference to firearms, is a device utilized to reload a magazine. A magazine is a container that holds a specific amount or quantity of ammunition for a firearm. A magazine can either be built into the firearm or is detachable. When in reference to ballistic threats the proper term magazine will be used.

- *Bullet* - is often a term used incorrectly to describe an individual round of ammunition. A bullet is a type of projectile fired from the firearm. The proper term for an individual round of ammunition loaded into a firearm is cartridge. When in reference to ballistic threats the proper term cartridge will be used.

- *Explode* - This term is often incorrectly used to describe what gun powder does inside the firearm. This is incorrect. All gun powder burns. They may burn at specific varying rates, but they do not explode. Therefore, when describing affects of powder with ballistic threats the proper term of burning rates will be used. When describing explosive blast threats the term detonate will be used instead of the word explode, as it once again is the more correct terminology to use.

FORCED ENTRY:

Testing Standards -

AMERICAN SOCIETY FOR TESTING AND MATERIALS - ASTM - F1233 (Physical Attack Method for Security Glazing Materials and Systems).

UNDERWRITERS LABORATORIES - UL972 (Burglar Resistant Glazing Material).

H. P. WHITE LABORATORIES - TP-500.00 Phase II (Forced Entry Testing of Resistance of Structural Systems).

Threat Specification prerequisites -

Forced Entry Threat specification prerequisites are based upon the following capabilities of those attacking and of the armor resisting the attack:

Type of Attack. The attack to gain egress or ingress falls into two needs. The first is the need to obtain an opening in the armoring material for ingress just large enough to reach through and obtain something on the inside and remove it, or to place something inside from the outside.

The second would be the need to make an ingress opening large enough for personal passage through the armoring material, without causing substantial injury from passing through the edges of the armoring material or having difficulty passing through it expediently.

Each of these cases can be reversed should the attacker be inside and wishing to gain egress out through the armoring material such as in a detention or prison type of compound setting.

Quantity of Personnel. The attack or need to breach the armor will require substantial manpower to achieve one or more of the above needs. Any hardening material or "armor" has compositional features designed to withstand specific if not always substantial amounts of abuse during an attack to perform its function. Therefore, it is not uncommon for a material to resist the attempts of numerous persons. One must remember, that an individual has only a limited amount of energy and enthusiasm, which can be expected to be expended through rigorous exertion for only a short period of time without wavering. This the reason that most attacks require either substantial amounts of man power to breach the armor or require additional threat types to bear upon the armor to facilitate quicker and easier penetration capabilities.

Attack Duration. The attack duration is based upon the amount of time required to keep the attacker(s) at bay for either a deterrent which is accomplished after frustration has mounted from the inability to penetrate or breach the armor, or for the necessary time for a selected type of response to the attack. This duration is generally chosen from five incremental time allotments. 1) Random attack types and duration's of 1-3 minutes. 2) Short continual duration's of 3-5 minutes. 3) Sustained continual attacking from duration's of 15 minutes in total time. 4) Sustained continual attacking from duration's of 30 minutes in total time. 5) Sustained continual attacking from duration's of 60 minutes in total time. Each of these time limits are based around any combination of the quantity of personnel, implement types, any incurred thermal stressing, chemical deterroriation, or assisted attack variables.

Implement Types. The types of "implements" or tools and equipment utilized during the attack to penetrate the armor are classified into four types.

The first is blunt impacting implements such as two handed sledge hammers, one handed hammers, clubs, bars, bricks, blocks, beams, large diameter pipes or just about any type of makeshift or selected object.

The second type of implement utilized during the attack to penetrate the armor is the sharp impacting implement such as a two handed pick, a single or two handed axe, pointed devices used with hammer type tools such as chisels, ripping bars, pipes or other objects ground to a pointed or sharp edge, small diameter pipes, etc.

The third type of implement type is one that is considered chemical deterioration. This is from a variety of chemicals that are usually highly caustic and corrosive, and are designed to weaken the armor to allow for quicker penetration and destruction of the armor in a shorter duration. The

primary point to make here is that these are very caustic and/or corrosive, as the time necessary to force a breach in the armor is short, therefore, the chemicals used are designed to deteriorate, fatigue, or in some way cause a failure in the compositional makeup of the armor or destruction of a specific amount of the armor thickness to allow for a breach to be finished with brute force.

One should remember that the individuals utilizing these types of chemicals will need to have the appropriate protective garments and other protective equipment such as gloves, foot wear, eye protection and self contained breathing apparatus (SCBA) or filtering apparatus. One positive point to make here is, that with the appropriate use of armor and detection devices to sniff for these gasses which are a by product of the chemicals deterioration process of the armor, this aids in reducing the risk of the armor being breached with success.

The fourth is thermal stressing. This is another type of weakening of the armor prior to conducting the full physical attack to force a breach. Thermal stressing can be aided with chemicals that are then ignited to attempt to burn through or weaken an area. Thermal stressing can also be from the use of torches to try to cut through the armor or by utilizing chemicals and/or chemical dispensing equipment that cause the armoring material to reach sub-zero temperatures and freeze it to the point of fatigue or failure. The common types being CO_2 or liquid nitrogen. These types of stress applied techniques are usually utilized in addition to the brute physical attack that is still required to force a breach in the armor. However, there are inherent risks involved with the use and transportation of any chemicals that are highly caustic, corrosive and which are considered temperature accelerants. Therefore the use of these, especially the use of liquid nitrogen, are not usually found being used in the level 1 or 2 type incidents.

Assisted Attack. This is utilizing other threat types to aid in the weakening or causing substantial failure to specific sections or points in the armor. This is utilizing either ballistic or explosive blast attacks to assist in the breaching process. This can be a combination of one or the other or all three. Therefore, it is incumbent that the armor be specified appropriately to circumvent attempts at breaching the armor as much as possible. By this, we mean to the expected threat type specification prerequisite levels, established for the protection of the target, as much as possible. This also means to the extent that the structural capabilities of the rest of the facility, vessel, aircraft or vehicle are not exceeded by the specification requirements of the armor. In each case, the object being armored has a structural component variable that has itself, a certain realistic useful structural capability that can be exceeded. Exceeding this limit is both a waste of armor, money, and serves to only provide a false sense of security and safety.

BALLISTIC:

Testing Standards -

AMERICAN SOCIETY FOR TESTING AND MATERIALS - ASTM - F1233 (Ballistic Test Method for Security Glazing Materials and Systems).

UNDERWRITERS LABORATORIES - UL752 (Bullet Resisting Equipment).

H. P. WHITE LABORATORIES - TP-500.00 Phase I (Ballistic Testing of Resistance of Structural Systems).

NATIONAL INSTITUTE OF JUSTICE - NIJ Standard 0108.01 (Ballistic Resistant Protective Materials)

Threat Specification prerequisites -

Ballistic Threat specification prerequisites are based upon the following capabilities of those types of firearms being utilized during the attack and of the armor resisting the attack:

Firearm Caliber. The caliber of the firearm is a very important component in the appropriate specification of the armor to be installed. The caliber dictates the minimum and maximum amounts of energy dispersion or damage that can be delivered into the armor medium (substrate). This is based upon the mass of the bullet or projectile being fired from the firearm coupled with its velocity.

Bullet Velocity. The velocity at which the bullet travels is of critical importance in that it is a deciding factor in equating the total possible minimum and maximum amounts of energy that can be delivered from a specific type of projectile or bullet into the target medium. The higher the velocity, the greater the amount of available energy there is for any given caliber and bullet or projectile mass.

Stand-Off Distance. This is an important factor that determines how much velocity has been lost subsequent to the bullet or projectile exiting the muzzle of the barrel and prior to the bullet or projectile impacting the target medium. The greater the distance the more the velocity will start to waver and be reduced by the time it reaches the armor. Stand-off distance also sets the stage for determining specific types of firearm deployment variables.

Concentration of Fire. This is a definition of the amount of ammunition that can be expected to be fired or expended from the firearm within a given amount of time. Commonly referred to as the cyclic capability of the firearm or “firepower”. How many times the firearm can be fired in one minute. This is based upon several factors. First, the manner in which the firearm is shot or deployed. Is it specifically aimed fire by the shooter, taking the time to aim it at the target or is it fired in a more pointed fashion. This is often common place when fully automatic capable firearms are utilized. Fully automatic firearms will continue to fire as long as the trigger is pressed until the ammunition capacity of the firearm is exhausted.

However, the term used to describe some handguns as automatic or autoloading handguns does not mean the same thing. In this definition it only refers to the re-chambering process of a new cartridge subsequent to the firing of another cartridge. This is considered a semi-auto capable firearm, which requires the trigger to be depressed each and every time the firearm is to be fired. The concentration of fire is specifically the amount of projectile or bullet concentration within a given amount of armor surface area. For example, a person has fired twenty rounds into an area of approximately 2' x 2' square feet is not as concentrated as if that shooter fired those twenty rounds into an area of 8" x 8" square inches. Tighter "groupings" or concentrations of fire oftentimes result in quicker fatigue or failure of the armor resulting in a quicker penetration of the armor.

Three variables effect the capability of the person shooting the firearm, with points of impacts resulting into tight concentrations in a small impact area upon the armor are: random firing without any specific aiming, rapid firing with or without any specific aiming or steady determined aimed firing. The other variable affecting the concentration of projectile impacts, is based upon the ammunition capacity that a specific firearm has at any given time. This is directly related to the capacity of its magazine or cylinder. The more cartridges a firearm can hold, the more rounds (bullets, projectiles) it can fire before they have all been expended, and therefore necessitating a reload.

Quantity/Types of Firearms. The various types of firearms, is a critical part of determining the available calibers and projectile configurations, weights, velocities, methods of deployment and rates of fire. The associated types are: *Handguns* - either revolvers or semi-automatic/autoloading; *Shotguns* - either semi-automatic, single shot or automatic; Sub-Machine Gun - firearms designed to fire typical handgun ammunition at higher velocities and higher cyclic rates, with substantial amounts or quantities of ammunition within their magazines; or the *High Power Rifle* - which can be of a single shot variant, semi-automatic or fully automatic.

Bullet/Projectile Type. This is a crucial piece of the puzzle in that it helps to establish what that bullet or projectile is designed to do once it impacts the surface of the targets armor. Some of the criteria specifying those parameters are the projectile or bullets core composition and/or jacket composition.

EXPLOSIVE BLAST:

Testing Standards -

AMERICAN SOCIETY FOR TESTING AND MATERIALS - ASTM - F1642 (Test Method for Glazing and Glazing Systems Subject to Airblast Loadings).

Threat Specification prerequisites -

Explosive Blast Threat specification prerequisites are based upon the following capabilities of those types of explosives and explosive devices being utilized during the attack and of the armor resisting the attack:

Explosive Types. There are two categories of explosives. High and low brisance explosives. These fall into three types of configurations such as solid, liquid or gas. This is very important information in the initial determining specifications of the armor and the structural capabilities of that which the armor is attached to. It also aids it determining the manner in which the explosives and/or devices will be deployed.

Charge Weight. This is a factor that establishes the densities of the explosive types and the subsequent encasement materials and design parameters of the devices complete with the firing trains. Another critical factor that can be derived from this information is the blast wave parameters of the detonated device and how the energy is to be dissipated upon the type of detonation burst which is determined by the manner of deployment.

Encasement Material. The factors associated with this are device weights, firing train selections, method of deployment parameters, detonation effects and destruction capabilities of the encasement material (fragmentation).

Destruction Type. This is split into two types categories that determine the type of destruction the device is designed to create. One is incendiary, by which destruction is primarily caused by creating substantial heat and rates of burning. The second is by shrapnel, and its varying types, compositions, shapes, and configurations of propagation. This can also be combined with the fragmentation variables of the encasement materials.

Attack Geometry. This is a variable dependent upon several factors such as stand-off distances, structural dimensions and shapes of the armored target and surrounding environmental considerations.

Avoidance Criteria. The avoidance criteria aids to establish deterrent and deployment difficulties for the explosive devices. This is based upon three primary parameters such as stand-off distances, deflection and absorption characteristics of explosive blast mitigation defenses.

One important note to make here: *The current explosive blast testing procedures and protocol take into consideration over blast pressures* ***only****! They do not take into consideration destruction, damage or injury from fragmentation or shrapnel.*

This is of critical importance in the appropriate selection of armor to defeat explosive blast attacks. There has been numerous improvised explosive devices detonated at various medical, and federal locations including the device at the Olympic games in Atlanta, Georgia that had objects included within them such as nails. These objects are designed for primary and secondary collateral damage and will cause failure in an otherwise non-failing armor designed to withstand the over blast pressures of such devices alone. This type of additional resistance factor sets forth a whole new set of parameters for the armor. Always consider the destruction type of the explosive device and include this in the selection of the appropriate armors. This is a relatively new area for most “experts” in the industry. Ask for a specification, if it does not include such prerequisites they more than likely do not know - and should be avoided!