# INVENTIONS IN EQUIPMENT SHAPED THE MILITARY POLICE SECURITY OPERATIONS

***Nenad TANESKI***[68]
***Metodija DOJCHINOVSKI***[69]
***Sasha SMILESKI***[70]

***Abstract:****Military police provide physical and technical security which describes control measures designed to deny unauthorized access to facilities, equipment, and resources and to protect staff and property from destruction or damage (such as espionage, theft, or terrorist attacks).*

*Physical and technical security involves the use of multiple layers of interdependent systems including CCTV surveillance, security guards, security barriers, locks, access control protocols, and many other techniques.*

*Since years technology made huge evolution, especially in digitalization, so the military police need sophisticated equipment necessary for physical and technical protection such as biometric enrollment (capture, process and store biographical or biometric data).*

***Key words:*** *security operations, physical, technical, equipment, biometric.*

## INTRODUCTION

The goal of deterrence methods is to convince potential attackers that a successful attack is unlikely due to strong defenses. The initial layer of security for a military facility, campus, building, office, or other physical space uses crime prevention through environmental design to deter threats. Some of the most common examples are also the most basic: warning signs or window stickers, fences, vehicle barriers, vehicle height-restrictors, restricted access points, security lighting and trenches.

Over the last some years, a new era of engineering science has been recognized whose products are likely to create a huge bazaar in the immediate future. It has been known as "biometrics". The innovators of this fresh domain mean to construct strategies which would permit credentials of a person on the foundation of his/her "biological" features: vocal sound, diminuendos of movements, features of expression and other portions of the body, optic nerve or sword lily pattern. Nature has completed human presences with unlike appearances which may alter from one person to another. This property is made up use of by Biometric technology to definitely identify each person.

### Physical barriers

Physical barriers such as fences, walls, and vehicle barriers act as the outermost layer of security. They serve to prevent, or at least delay, attacks, and also act as a psychological deterrent by defining the perimeter of the facility and making intrusions seem more difficult. Tall fencing, topped with barbed wire, razor wire or metal spikes are often emplaced on the perimeter of a property, generally with some type of signage that warns people not to attempt entry. However, in some facilities imposing perimeter walls/fencing will not be possible (e.g. an urban

[68]*PhD, Military academy „General Mihailo Apostolski“ - Skopje*
[69]*PhD, Military academy „General Mihailo Apostolski“ - Skopje*
[70]*MSc, Military academy „General Mihailo Apostolski“ - Skopje,*

office building that is directly adjacent to public sidewalks) or it may be aesthetically unacceptable (e.g. surrounding a shopping center with tall fences topped with razor wire); in this case, the outer security perimeter will be defined as the walls/windows/doors of the structure itself.[71]

**Combination barriers**

Barriers are typically designed to defeat defined threats. This is part of building codes as well as fire codes. Apart from external threats, there are internal threats of fire, smoke migration as well as sabotage. The National Building Code of Canada, as an example, indicates the need to defeat external explosions with the building envelope, where they are possible, such as where large electrical transformers are located close to a building. High-voltage transformer fire barriers can be examples of walls designed to simultaneously defeat fire, ballistics and fragmentation as a result of transformer ruptures, as well as incoming small weapons fire. Similarly, buildings may have internal barriers to defeat weapons as well as fire and heat. An example would be a counter at a police station or embassy, where the public may access a room but talk through security glass to employees in behind. If such a barrier aligns with a fire compartment as part of building code compliance, then multiple threats must be defeated simultaneously, which must be considered in the design.

Plastic deformation as a result of impact can knock loose, tear or squish passive fire protection (PFP) materials, particularly once the PFP materials are stressed. Some PFP materials can at times be very resilient, impact resistant and ductile at ambient. Once stressed by fire, that can change as free water dissipates at 100°C, and hydrates can be spent near 300°C, all of which is reached within minutes of a fire. Construction level binders, unlike certain refractories, can also degrade with heat, thus changing the physical properties of many PFP materials across different temperature ranges. None of that is normally a problem. In fact it is part of PFP designs for different reasons. But when combining PFP with ballistics or fragmentation, it is prudent to consider all relevant stresses in designing barriers that must (or may be presumed or advertised to) simultaneously defeat fire, followed by hose stream and impacts that come during a fire event.

**Natural surveillance**

Another major form of deterrence that can be incorporated into the design of facilities is natural surveillance, whereby architects seek to build spaces that are more open and visible to security personnel and authorized users, so that intruders/attackers are unable to perform unauthorized activity without being seen. An example would be decreasing the amount of dense, tall vegetation in the landscaping so that attackers cannot conceal themselves within it, or placing critical resources in areas where intruders would have to cross over a wide, open space to reach them (making it likely that someone would notice them).

**Security lighting**

Security lighting is another effective form of deterrence. Intruders are less likely to enter well-lit areas for fear of being seen. Doors, gates, and other entrances, in particular, should be well lit to allow close observation of people entering and exiting. When lighting the grounds of a facility, widely distributed low-intensity lighting is generally superior to small patches of high-

[71]Talbot, Julian & Jakeman, Miles, Security Risk Management Body of Knowledge, John Wiley & Sons, New Jersey, 2011, pp. 72–73.

intensity lighting, because the latter can have a tendency to create blind spots for security personnel and CCTV cameras. It is important to place lighting in a manner that makes it difficult to tamper with (e.g. suspending lights from tall poles), and to ensure that there is a backup power supply so that security lights will not go out if the electricity is cut off.[72] he introduction of low-voltage LED-based lighting products has enabled new security capabilities, such as instant-on or strobing, while substantially reducing electrical consumption.[73]

**Alarm systems and sensors**

Alarm systems can be installed to alert security personnel when unauthorized access is attempted. Alarm systems work in tandem with physical barriers, mechanical systems, and security guards, serving to trigger a response when these other forms of security have been breached. They consist of sensors including perimeter sensors, motion sensors, contact sensors, and glass break detectors.[74]

However, alarms are only useful if there is a prompt response when they are triggered. In the reconnaissance phase prior to an actual attack, some intruders will test the response time of security personnel to a deliberately tripped alarm system. By measuring the length of time it takes for a security team to arrive (if they arrive at all), the attacker can determine if an attack could succeed before authorities arrive to neutralize the threat. Loud audible alarms can also act as a psychological deterrent, by notifying intruders that their presence has been detected.[75] In some jurisdictions, law enforcement will not respond to alarms from intrusion detection systems unless the activation has been verified by an eyewitness or video.[76] Policies like this one have been created to combat the 94–99 percent rate of false alarm activation in the United States.[77]

**Access control**

Access control methods are used to monitor and control traffic through specific access points and areas of the secure facility. This is done using a variety of systems including CCTV surveillance, identification cards, security guards, biometric readers, and electronic/mechanical control systems such as locks, doors, turnstiles and gates.[78]

**Mechanical access control systems**

Mechanical access control systems include turnstiles, gates, doors, and locks. Key control of the locks becomes a problem with large user populations and any user turnover. Keys quickly become unmanageable, often forcing the adoption of electronic access control.

---

[72]Kovacich, Gerald L. & Halibozek, Edward P., The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program, Butterworth-Heinemann, Oxford, 2003, pp. 192–193.

[73] "Use of LED Lighting for Security Purposes, ". https://www.silvaconsultants.com/new-security-tips-1/use-of-led-lighting-for-security-purposes

[74]Field Manual 3-19.30: Physical Security, Headquarters, United States Department of Army, 2001, Chapter 6.

[75]Fennelly, Lawrence J., Effective Physical Security, Butterworth-Heinemann, Waltham, MA, 2012, pp. 345–346.

[76]Erwin A. Blackstone, Andrew J. Buck, Simon Hakim, "Evaluation of alternative policies to combat false emergency calls", Center for Competitive Government, Temple University, Philadelphia, 2004, p. 238.

[77]Erwin A. Blackstone, Andrew J. Buck, Simon Hakim, "Evaluation of alternative policies to combat false emergency calls", Center for Competitive Government, Temple University, Philadelphia, 2004, p. 233.

[78]Tyska, Louis A. & Fennelly, Lawrence J., Physical Security: 150 Things You Should Know, Butterworth-Heinemann, Waltham, MA, 2000, p. 3.

**Electronic access control systems**

Electronic access control manages large user populations, controlling for user life cycles times, dates, and individual access points. For example, a user's access rights could allow access from 0700h to 1900h Monday through Friday and expire in 90 days. These access control systems are often interfaced with turnstiles for entry control in buildings to prevent unauthorized access. The use of turnstiles also reduces the need for additional security personnel to monitor each individual entering the building allowing faster throughput.

An additional sub-layer of mechanical/electronic access control protection is reached by integrating a key management system to manage the possession and usage of mechanical keys to locks or property within a building or campus.[79]

**Identification systems and access policies**

Another form of access control (procedural) includes the use of policies, processes and procedures to manage the ingress into the restricted area. An example of this is the deployment of security personnel conducting checks for authorized entry at predetermined points of entry. This form of access control is usually supplemented by the earlier forms of access control (i.e. mechanical and electronic access control), or simple devices such as physical passes.[80]

**Biometrics enrollment**

The term biometrics denotes to the developing field of technology dedicated to the credentials of personalities using biological characters or behaviors. In preparation, this means taking an image of a unique feature of an individual such as a fingerprint, hand, eye or face, and comparing it with a template captured previously. For hardship of explanation this has been over-simplified, but in crux this is how biometric technology works. The statistical use of the characteristic differences in unique elements of living creatures is known as biometrics.

Biometric recognition offers a promising approach for security applications, with some advantages over the classical methods, which depend on something you have (key, card, etc.), or something you know (password, PIN, etc.). Authentication methods by means of biometrics are a particular portion of security systems, with a good number of advantages over classical methods. However, there are also drawbacks. Depending on the application, one of the previous methods, or a combination of them, will be the most appropriate.

[79]Field Manual 3-19.30, Physical Security. Headquarters, United States Department of Army, 2001, Chapter 7.
[80]Pearson, Robert, Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions, Butterworth-Heinemann, Waltham, MA, 2011, Chapter 1.

| Authentication method | Advantages | Drawbacks |
|---|---|---|
| Handheld tokens (card, ID, passport, etc.) | ▪ A new one can be issued.<br>▪ It is quite standard, although moving to a different country, facility, etc. | ▪ It can be stolen.<br>▪ A fake one can be issued.<br>▪ It can be shared.<br>▪ One person can be registered with different identities. |
| Knowledge based (password, PIN, etc.) | ▪ It is a simple and economical method.<br>▪ If there are problems, it can be replaced by a new one quite easily. | ▪ It can be guessed or cracked.<br>▪ Good passwords are difficult to remember.<br>▪ It can be shared.<br>▪ One person can be registered with different identities. |
| Biometrics | ▪ It cannot be lost, forgotten, guessed, stolen, shared, etc.<br>▪ It is quite easy to check if one person has several identities.<br>▪ It can provide a greater degree of security than the other ones. | ▪ In some cases a fake one can be issued.<br>▪ It is neither replaceable nor secret.<br>▪ If a person's biometric data is stolen, it is not possible to replace it. |

***Table 1. Advantages and drawbacks of the three main authentication method approaches***

**Design issues of biometric systems**

A significant question in scheming a practical system is to determine in what way a separated is recognized and are intended by keeping two characteristics in mind, they are:

Physical characteristics

- Fingerprint,

Handprint

- Face
- Scent,
- Thermal image
- Iris Pattern

Personal traits

- Voice pattern
- Handwriting
- Acoustic Signature

**Verification VS Identification**

There are two diverse ways to tenacity a person's identity: confirmation and proof of identity. Confirmation (Am I whom I claim I am?) involves confirming are rejecting a person's demanded identity. In proof of identity, one has to found a person's identity (Who am I?). Individually one of these strategies has its own difficulties and could maybe be resolved best by a certain biometric scheme.

**Security and privacy**

A nice property of biometric security systems is that security level is almost equal for all users in a system. This is not true for other security technologies. For instance, in an access

control based on password, a hacker just needs to break only one password among those of all employees to gain access. In this case, a weak password compromises the overall security of every system that user has access to. Thus, the entire system's security is only as good as the weakest password.[81] This is especially important because good passwords are nonsense

combinations of characters and letters, which are difficult to remember (for instance, "Jh2pz6R+"). Unfortunately, some users still use passwords such as "password", "Homer Simpson" or their own name.

Although biometrics offers a good set of advantages, it has not been massively adopted yet.[82] One of its main drawbacks is that biometric data is not secret and cannot be replaced after being compromised by a third party. For those applications with a human supervisor (such as border entrance control), this can be a minor problem, because the operator can check if the presented biometric trait is original or fake. However, for remote applications such as internet, some kind of liveliness detection and anti-replay attack mechanisms should be provided. This is an emerging research topic. As a general rule, concerning security matters, a constant update is necessary in order to keep on being protected. A suitable system for the present time can become obsolete if it is not periodically

improved. For this reason, nobody can claim that has a perfect security system, and even less that it will last forever.

***Conclusion***

In this paper, we present the traditional physical and technical security equipment used by military police units in operations to secure command posts, vital facilities. Physical and technical security are inevitable methods for securing facilities due to the nature of the physical distance with the use of means or barriers and the use of other equipment for entry and movement restricts access. These methods achieve control of entry and movement, but without sufficient coverage and monitoring by CCTV these methods are not sufficient.

With the introduction of biometric security technology, greater control of entry and movement is introduced, and on the other hand, due to the unique methods of recognition, the danger of endangering the guarded facility is reduced. Most importantly, through biometric data, military police officials have access to a large number of personal data of persons allowed to enter the guarded facility, but also when an unauthorized person attempts to attempt to breach security can be detected through one of the methods as face recognition, fingerprints, voice, etc. if the person has a valid ID card and has it in the data system.

The advances in accurateness and serviceability and reducing cost have made the biometric technology a secure, reasonable and cost-effective way of identifying individuals. Biometric strictures such as fingerprint perusing, retinal scanning, iris scanning, signature verification, hand geometry, voice verification and others are all well recognized with their own specific characteristics. The limiting factors of speed and band width are now a thing of the past and their practical performance might in many incidences be better than predictable.

[81]S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric recognition: security and privacy concerns" IEEE Security and Privacy, 2003, pp. 33-42.

[82]M. Faundez-Zanuy, "Biometric recognition: why not massively adopted yet?", IEEE Aerospace and Electronic Systems Magazine, August 2005.

**References**


1. Talbot, Julian & Jakeman, Miles, Security Risk Management Body of Knowledge, John Wiley & Sons, New Jersey, 2011.
2. Kovacich, Gerald L. & Halibozek, Edward P., The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program, Butterworth-Heinemann, Oxford, 2003.
3. "Use of LED Lighting for Security Purposes, ". https://www.silvaconsultants.com/new-security-tips-1/use-of-led-lighting-for-security-purposes
4. Field Manual 3-19.30: Physical Security, Headquarters, United States Department of Army, 2001.
5. Fennelly, Lawrence J., Effective Physical Security, Butterworth-Heinemann, Waltham MA, 2012.
6. Erwin A. Blackstone, Andrew J. Buck, Simon Hakim, "Evaluation of alternative policies to combat false emergency calls", Center for Competitive Government, Temple University, Philadelphia, 2004.
7. Tyska, Louis A. & Fennelly, Lawrence J., Physical Security: 150 Things You Should Know, Butterworth-Heinemann, Waltham, MA, 2000.
8. Pearson, Robert, Electronic Security Systems: A Manager's Guide to Evaluating and Selecting System Solutions, Butterworth-Heinemann, Waltham, MA, 2011, Chapter 1.
9. S. Prabhakar, S. Pankanti, A. K. Jain, ”Biometric recognition: security and privacy concerns” IEEE Security and Privacy, 2003
10. M. Faundez-Zanuy, “Biometric recognition: why not massively adopted yet?”, IEEE Aerospace and Electronic Systems Magazine, August 2005.