Crime Prevention Through Environmental Design (CPTED, Chapter 1)

September 2021

The Environment

- Using Design to Control Human Behaviour
- The design must recognize the intended use of the space
- Threats specific to the space are identified
- Mitigating actions (i.e. design) must suit the intended use of the space

Space

- Public – use by the resident and the public. Parking lot
- Semi-Public – use by the public without passing through security barriers. Lobby, waiting room, reception area.
- Semi-Private – use by residents and guests (with some restrictions). Usually behind some form of access control. Offices, meeting rooms.
- Private – use by residents, invited (accompanied) guests and service people only. Strict access control. Labs.

Transition boundaries between spaces should be clearly implied.

Target Hardening

- Denying access to the protected asset.
- May impede use.
- Hardening may involve natural and/or artificial elements
- Natural elements may have less impact on use.
- Elements are inter-related. I.e. lighting is only useful when some form of visual surveillance is present.

3 CPTED Strategies

Spatial Management arises from the overlap of three strategies

- Natural Access Control
- Natural Surveillance
- Territorial Reinforcement

These strategies overlap and may be mutually supportive.

3 CPTED Strategies

- Access Control
  - locks, lighting, alarms (mechanical), guards (organized), Spatial definition (natural).
  - Creates the perception of risk.
  - Access Control & Surveillance have traditionally overlooked environmental measures.
- Surveillance
  - Keeps intruders under observation.
  - May act as an access control by increasing the perception of risk.
  - Mechanical (Lighting, cameras), Organized (guards), Natural (windows).
  - Incorporating Natural elements has led to Territoriality.
- Territorial Definition
  - Creates a sense of community made up of those that belong and excludes those that don’t.
  - Use of natural elements promotes territorial reinforcement by engaging the members of the community and creates greater perception of risk by potential offenders.

Maintenance

Create a sense of tolerance of disorder and a lack of care and attention and decreases the sense of Territoriality.

Protects public health safety and wellness.

- Broken locks
- Rusted fences
- Burnt out lights
- Overgrown shrubbery and grasses
- Graffiti

Natural Surveillance Caveat

If people observe inappropriate behaviour and do nothing, then the Natural Surveillance strategy becomes useless.


Carrington St
Rosemead Ct
Memorial Dr
Robie St
High St
Leeds St
Leaman St
Novatea Dr
Normandy Dr
Basin
© 2020 Google


nscc
Institute of Technology Campus
5685


nscc
Institute of Technology Campus
5685


ONE WAY


ONE WAY


3729
NO PARKING
BEYOND THIS
POINT


40


FOR YOUR SAFETY


NO
PARKING


HALIFAX
TRANSIT
7
FOR DEPARTURE TIMES
CALL 902-480-8000
or halifax.ca/transit
Stop #:
7133


Building Nova Sco
economy and quality
through education and i
Our Mission


EXIT
A WING
EXIT
A WING
WASHROOM
AMBITION WINS EVERY TIME.
Women in Trades and Technology
nscc


WASHROOM
Please wait here to be called


A-Wing West 2nd Floor
To President's Offi
Grant Free College

The 3-D Approach – Three Dimensions of Human Space

1. All human space has a designated purpose

2. All human space has social, cultural, legal or physical definitions that prescribe the desired and acceptable behaviours. (i.e. you inherently know what you do here or how you should act)

3. All human space is designed to support and control the desired behaviours.

The 3-D Approach – Space may be evaluated by asking these questions.

- Designation
  - What is the purpose of the space
  - What was it originally intended to be used for
  - How well does the space support its intended AND current use. Are there conflicts
- Definition
  - How is the space defined
  - Is ownership clear
  - Where are the borders
  - Are there cultural or social definitions of use
  - How well are the rules for use defined (signs?)
  - Are there conflicts between the purpose and the definition
- Design
  - Does the design support the function
  - Does the design conflict with, impede, the expected activity
  - Does the design impede the use
  - Is there confusion in the design about how it is intended to control the expected behaviour

Use CPTED to Provide

Clear border definition

Cleary marked transition zones

Relocate gathering areas to take advantage of natural surveillance, access control and away from view or access of offenders.

Place safe activities in unsafe locations to increase natural surveillance.

Place unsafe activities where natural surveillance is present.

Redesign space to use natural barriers to reduce conflict

Reschedule the use of space to allow for effective use.

Redesign space to increase the perceived or real natural surveillance.

Overcome distance between spaces with better communication.

Use of Information in Planning and Design

Five Pieces of Information that you should gather

- Crime analysis – geographic and similarity of offense patterns
- Demographic – information on the population of the space
- Land Use – zones, uses, barriers and traffic flow
- Observational – observe the use of the space (users, behaviours, barriers)
- User Interviews – inquire as to their perceptions

Awareness

- Become aware of your community so that you can spot the unusual, the stranger.
- Observe behavior. Notice the different or unusual.

Scalability

CPTED Strategies are scalable to:

- Communities
- Facilities
- Rooms or points of concern

Prevention

Strategies to develop preventions requires an understanding of criminal behaviour when the criminal examines the environment of the target.

Time Scales to Achieve Success

While CPTED goals may take sometime to accomplish (i.e. a Sense of Community), CPTED strategies also include opportunities for immediate success through implementing measures that will bring immediate improvent (i.e. improving Access Control)

Collective Response

CPTED strategy seeks to involve response and monitoring of all members of the community by building and atmosphere of “Neighbourhood Watch”.

Interdisciplinary Approach

All Hands on Deck!

Previously isolated areas of expertise and skills are encouraged to work cooperatively to a common objective.

Removing “Silos” through increased coordination and involvement.

(i.e. Fire, Physical, Cyber)

The Right Tools and Training

Security personnel must be provided with the appropriate and consistent:

- Training
- Equipment
- Communication
- Integrated Command & Control

And, should be subject to coordinated guidelines, policies and standards.

Will prevent the internal development of undocumented, unintentional vulnerabilities. ***Note: This is common and difficult to overcome.***

Approaches to Physical Security (Chapter 4)

- Any system that can be conceived can be defeated.
- Components must be combined and integrated to work together.
- Is the cost of the security system greater than the value of the asset.

Know Your Asset!

This is Rule Number 1 in your security planning

What is it you are trying to protect?

What is it's value:

- ***Cost (tangible and intangible)***
- ***Maintenance***
- ***Management***
- ***Repair***
- ***Temporary Loss / Permanent Loss***

This information will drive (and support) your budgeting.

Levels of Security

Minimum – impedes unauthorized external activity (barriers, doors and windows with locks).

Low-Level – impedes and detects unauthorized external activities (add better locks, lighting and alarms (un-monitored).

Medium – Impedes, detects and assesses unauthorized external activity (Intrusion detection systems that signal staff, establish a broader perimeter with fences or dogs , un-armed security personnel with basic training).

High – Impedes, detects and assesses both internal and external unauthorized activity (state of the art equipment, CCTV, security lighting, trained trustworthy armed guards, increased access control such as bio-metrics, incident response plans, coordination with external resources, regular security assessments).

Maximum – Impede, detect, assess and neutralize any unauthorized external or internal activity (back-up power for redundant interconnected alarm systems, armed trained trustworthy active response personnel capable of neutralizing the expected threat).

Psychology of Maximum Security – create the appearance of impenetrability to deter less capable adversaries.

Criminals need **desire** and **opportunity**. A higher level of security posture will reduce desire.

Change components and methods when personnel leave.

List the Basic Requirements Do you want to:

- Impede
- Deter
- Delay
- Detect
- Deny
- Assess
- Respond
- Neutralize

Planning - For each requirement, choose the appropriate component (but ensure they work together)

- Impediments
- Alarm/Sensor Systems
- Lighting
- Video Systems
- Communication Systems (this requires thought)
- Security Force
- Response Force

Design Reference Threat : examples of realistic threats. Probability ~=> Priority

Threats

- Burglary
- Theft
- Assault
- Power Outage
- …….?

For each threat, characterize the **Threat**, the **likelihood of the Threat**, the **Threat Actor**(s) and the Threat Actor's **likelihood of Encounter**.

For each Threat, correlate to Threat Actor(s). Consider the most capable Threat Actor who is associated with the most likely Threat.

Layering Protection

- Physical Barriers.
- Isolation Zones in font of, behind and between barriers.
- Security doors and windows (installed or upgraded).
- Must be matched to the capability of the Design Reference Threat.
- Barriers can also function as Traps.
- Locks – avoid grand master keys
- Access Control – who, when, where, how? Remember – maybe they don’t have to get in to achieve their purpose.
- Security Force – Amount, training, Equipment.
- Alarm Systems – Tamper Monitoring, Detect, Assess, Respond, Neutralize.
- Lighting – Paired with other technology, avoid silhouetting your people.
- Communication – build in redundancy.

A Security Plan should contain…..

- A description of the facility.
- The Security organization.
- Discussion/Description of:
    - Physical Barriers.
    - Alarm Systems.
    - Access Controls.
    - Lighting.
    - Communications Systems
    - Surveillance Systems.
- A description of the Security Team (Org, Training, Equipment, Resources, Procedures etc).
- Third-party resources (i.e. agreements with police forces or policing agencies).
- Plan for annual assessment and upgrading.

Steps in Selling the Plan and Convincing Others

Define the problem.

What if this continues?

Alternatives.

Eliminate each alternative until only your plan is left.

Detail of your plan.

Taylor your presentation, and the features of your solution, to the audience…specifically to those members of the audience that must approve your plan.