SMA1202

SECURITY: THEORY AND PRACTICE

หลักการและทฤษฎีความมั่นคงปลอดภัย

CHAPTER 5
PHYSICAL SECURITY AND ASSET PROTECTION

ผศ.ดร.หทัยพันธน์ สุนทรพิพิธ
Asst.Prof.Hathaipan Soonthornpipit, Ph.D.

บทที่ 5
ความมั่นคงปลอดภัยทางกายภาพและการปกป้องทรัพย์สิน
Physical Security and Asset Protection

1. บทนำ (Introduction)

1.1 ปฐมบทแห่งการจารกรรม: การปล้นที่ไม่ใช้กำลัง แต่ใช้สมอง

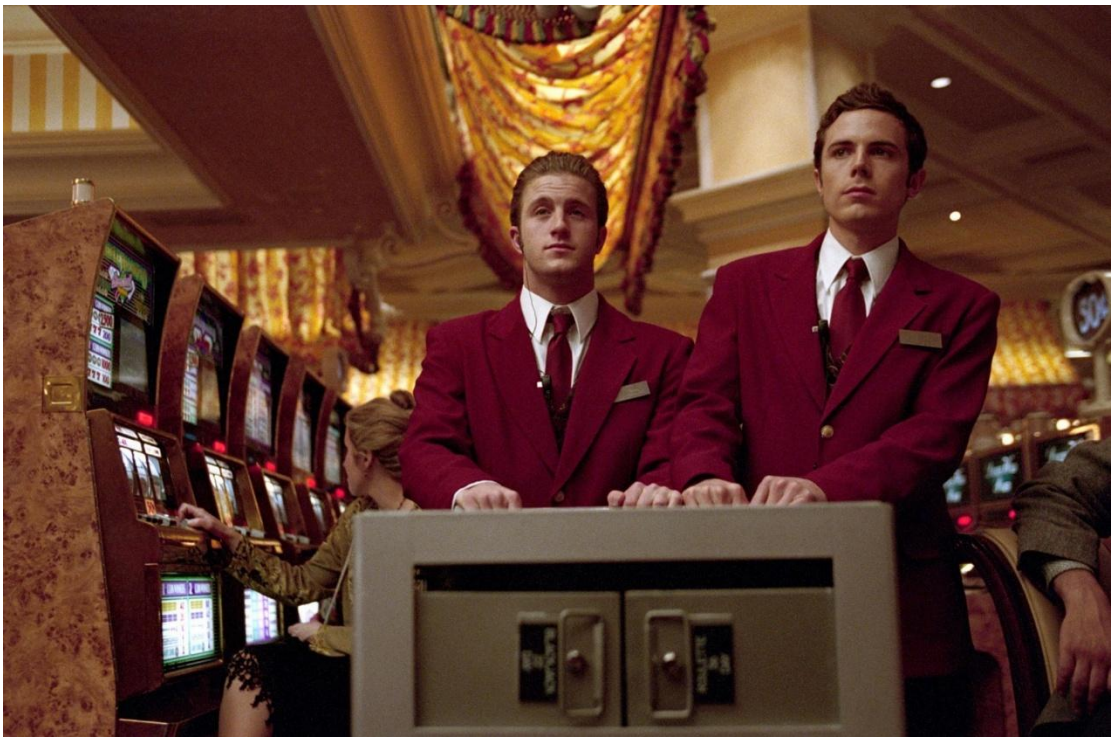
ในภาพยนตร์ *Ocean's Eleven* (2001) แดนนี่ โอเชียน (Danny Ocean) และทีมงานของเขาดำเนินการจารกรรมที่ได้รับการยกย่องว่าเป็นหนึ่งในปฏิบัติการที่ซับซ้อนที่สุดในประวัติศาสตร์ภาพยนตร์ ด้วยการขโมยเงินมูลค่า 160 ล้านดอลลาร์สหรัฐจากห้องนิรภัยใต้คาสิโนสามแห่งในลาสเวกัส ซึ่งเป็นทรัพย์สินของเทอร์รี เบเนดิกต์ (Terry Benedict) นักธุรกิจผู้ทรงอิทธิพล สิ่งที่ทำให้การจารกรรมครั้งนี้โดดเด่นไม่ได้อยู่ที่การใช้กำลังหรืออาวุธ หากแต่อยู่ที่การใช้ประโยชน์จาก ช่องโหว่ทางสถาปัตยกรรมและเชิงปฏิบัติการอย่างเป็นระบบ

ทีมของโอเชียนไม่ได้เอาชนะระบบรักษาความปลอดภัยด้วยการเผชิญหน้าโดยตรง แต่เลือกศึกษา "ตัวอาคาร" อย่างละเอียด ก่อนที่จะก้าวเข้าไปในคาสิโนแม้แต่ก้าวเดียว พวกเขาใช้เวลาหลายสัปดาห์ในการ "อ่านอาคาร" เสมือนเป็นตำราที่เขียนด้วยภาษาของช่องโหว่ ทีมงานศึกษาผังอาคารอย่างละเอียดจนเข้าใจทุกเส้นทาง เฝ้าสังเกตกิจวัตรของเจ้าหน้าที่รักษาความปลอดภัยจนทราบรูปแบบเวรยามและช่วงเวลาเปลี่ยนเวร ติดตามการสัญจรของพนักงานและแขกเพื่อระบุจุดที่สายตาการเฝ้าระวังอ่อนแอ สำรวจจุดบอดของกล้องวงจรปิดนับร้อยตัว และที่สำคัญที่สุดคือการทำความเข้าใจระบบสนับสนุนที่เชื่อมโยงกันเป็นเครือข่าย ตั้งแต่ระบบไฟฟ้า ระบบกล้อง ระบบคอมพิวเตอร์ ไปจนถึงระบบการสื่อสารภายใน ทั้งหมดนี้ทำให้ทีมของโอเชียนไม่ได้มองอาคารเป็นเพียงโครงสร้างทางกายภาพ หากแต่มองเป็น "ระบบ" ที่มีตรรกะ มีรูปแบบ และมีจุดอ่อนซ่อนอยู่

สิ่งที่พวกเขาค้นพบคือ ระบบรักษาความปลอดภัยของเบลลาจิโอ (Bellagio) แม้จะใช้เทคโนโลยีล้ำสมัยและมีมูลค่าสูง แต่กลับเปราะบางในสามมิติสำคัญ ได้แก่ ความคาดเดาได้ของขั้นตอนและตารางเวร การทำงานแบบแยกส่วนของแต่ละระบบ และการบูรณาการที่ไม่สมบูรณ์ระหว่างระบบทางกายภาพกับระบบดิจิทัล ช่องโหว่เหล่านี้เปิดโอกาสให้ทีมงานแทรกซึมในฐานะพนักงานซ่อมบำรุง ควบคุมระบบกล้องวงจรปิด และแทนที่ภาพสดด้วยวิดีโอที่บันทึกไว้ล่วงหน้าโดยไม่ถูกตรวจจับ การจารกรรมครั้งนี้จึงไม่ได้สำเร็จเพราะ

เจ้าหน้าที่ขาดความสามารถหรือเทคโนโลยีด้อยประสิทธิภาพ หากแต่สำเร็จเพราะตัวอาคารและระบบที่รองรับมัน “เปิดเผยความลับ” ผ่านการออกแบบที่คาดเดาได้ การแยกส่วนของระบบ และกระบวนการทำงานที่ตายตัวจนผู้บุกรุกสามารถอ่านและใช้ประโยชน์ได้อย่างเป็นระบบ

พวกเขาปลอมตัวเป็นพนักงานซ่อมบำรุงเพื่อเข้าถึงระบบกล้องวงจรปิด และเชื่อมต่อสัญญาณเพื่อแทนที่ภาพสดด้วยวิดีโอที่บันทึกไว้ล่วงหน้า ทีมงานยังใช้ประโยชน์จากตารางเวรที่คาดเดาได้ เลี่ยงระบบควบคุมการเข้าออกด้วยบัตรประจำตัวที่ถูกทำซ้ำ ควบคุมระบบแสงสว่างและไฟฟ้า รวมถึงใช้เทคนิคการชักจูงทางสังคม (social engineering) เพื่อสร้างความไว้วางใจให้กับบุคลากรในพื้นที่ แผนการทั้งหมดเริ่มต้นด้วยการลักลอบนำสมาชิกคนหนึ่งเข้าไปซ่อนในรถเข็นเพื่อเข้าสู่ห้องนิรภัยล่วงหน้า จากนั้นจึงก่อให้เกิดสถานการณ์ฉุกเฉินด้วยการข่มขู่ว่าจะทำลายเงินในตู้นิรภัย และจบลงด้วยการเดินออกจากพื้นที่ในคราบของหน่วยปฏิบัติการพิเศษ (SWAT) ที่เข้ามาตอบสนองต่อเหตุฉุกเฉินที่เบเนดิกต์โทรแจ้งด้วยตนเอง



ภาพที่ 5.1
ฉากภายในคาสิโนจากภาพยนตร์ *Ocean's Eleven* (2001)
ที่มา: Warner Bros. Pictures.

1.2 เมื่ออาคารพูดได้: ภาษาเงียบของสภาพแวดล้อม

แม้ *Ocean's Eleven* จะเป็นเพียงภาพยนตร์สมมติ แต่เรื่องราวดังกล่าวสะท้อนหลักการพื้นฐานที่สุดประการหนึ่งของการรักษาความปลอดภัยทางกายภาพอย่างชัดเจน นั่นคือ อาคารและสภาพแวดล้อมสื่อสารระดับความเสี่ยงอยู่ตลอดเวลา (Buildings Communicate Risk) โดยไม่ต้องอาศัยคำพูดหรือป้ายเตือนใด ๆ การจัดวางผังอาคาร แสงสว่าง เส้นทางเข้า–ออก สิ่งกีดขวาง และการแบ่งเขตพื้นที่ ล้วนส่งสัญญาณเงียบไปยังทั้งผู้ใช้งานที่ถูกกฎหมายและผู้ที่มีเจตนาร้ายว่า พื้นที่นั้นถูกควบคุมได้มากน้อยเพียงใด มีการเฝ้าระวังจริงหรือไม่ การบุกรุกจะถูกตรวจจับได้ง่ายหรือยาก และหากเกิดเหตุ ระบบจะตอบสนองได้รวดเร็วเพียงใด หลักการนี้สอดคล้องกับแนวคิดของการออกแบบสิ่งแวดล้อมเพื่อป้องกันอาชญากรรม (Crime Prevention Through Environmental Design: CPTED) ซึ่งมองว่าสภาพแวดล้อมทางกายภาพเป็น "ผู้สื่อสาร" ด้านความมั่นคงปลอดภัยที่ทรงพลังที่สุด

การรักษาความปลอดภัยทางกายภาพที่มีประสิทธิภาพจึงไม่ได้เริ่มต้นจากการติดตั้งกล้องวงจรปิดหรือการจัดกำลังเจ้าหน้าที่ หากแต่เริ่มต้นตั้งแต่ขั้นตอนของ การออกแบบสภาพแวดล้อม นั่นก็คือ การกำหนดรูปแบบของพื้นที่อย่างตั้งใจเพื่อป้องปราม หน่วงเหนี่ยว และตรวจจับภัยคุกคาม ขณะเดียวกันก็ยังเอื้อต่อการใช้งานที่ถูกต้องตามปกติ สภาพแวดล้อมทางกายภาพทำหน้าที่เป็นด่านแรกที่มองเห็นได้ชัดเจนที่สุดของระบบความมั่นคงปลอดภัย ไม่ว่าจะเป็นศูนย์การค้า นิคมอุตสาหกรรม มหาวิทยาลัย โรงพยาบาล โรงแรม สนามบิน หรือหน่วยงานภาครัฐ โดยพื้นที่เหล่านี้ไม่เพียงรองรับกิจกรรมทางเศรษฐกิจและสังคมจำนวนมหาศาล หากยังต้องรับมือกับภัยคุกคามที่หลากหลาย ตั้งแต่อาชญากรรมทั่วไป การบุกรุก ไปจนถึงเหตุฉุกเฉินและการก่อวินาศกรรม

1.3 จากคาสิโนสู่ความเป็นจริงในไทย: ภัยคุกคามที่เราเผชิญ

บริบทของประเทศไทยยิ่งตอกย้ำความสำคัญของการรักษาความปลอดภัยทางกายภาพในฐานะหัวใจของการปกป้องชีวิตและทรัพย์สิน ไม่ว่าระบบความมั่นคงปลอดภัยทางไซเบอร์จะเข้มแข็งเพียงใด หากผู้ไม่หวังดีสามารถเดินเข้าสู่พื้นที่สำคัญได้โดยง่าย ทุกมาตรการย่อมไร้ความหมาย เช่นเดียวกัน นโยบายและคู่มือที่รัดกุมก็ไม่อาจชดเชยการออกแบบอาคารที่เปิดช่องโหว่ให้เกิดการแทรกซึมได้ กรณีศึกษาจาก *Ocean's Eleven* จึงมิใช่เพียงเรื่องราวในจอภาพยนตร์ หากเป็นภาพสะท้อนว่า เมื่อผู้โจมตีเข้าใจโครงสร้าง การเชื่อมโยงของระบบ และพฤติกรรมของผู้คน พื้นที่ที่ดูปลอดภัยที่สุดก็สามารถถูกเจาะได้

เป้าหมายของบทนี้คือการทำให้ "พื้นที่" กลายเป็นพันธมิตรในการป้องกันภัย ผ่านแนวคิดการออกแบบสภาพแวดล้อมเชิงกลยุทธ์ การสร้างชั้นของการป้องกัน (defense in

depth) การแบ่งเขตพื้นที่ตามระดับความเสี่ยง และการบูรณาการเทคโนโลยีสมัยใหม่เข้ากับกระบวนการทำงานและบุคลากร เราจะเห็นว่า ความมั่นคงปลอดภัยที่แท้จริงไม่เกิดจากระบบใดระบบหนึ่ง หากเกิดจากการออกแบบที่ทำให้การป้องกันฝังตัวอยู่ในสภาพแวดล้อมอย่างเป็นธรรมชาติ จนภัยคุกคามถูกป้องปรามตั้งแต่ยังไม่เริ่มต้น จากบทเรียนในห้องนิรภัยกลางลาสเวกัส สู่การสร้างพื้นที่ที่ปลอดภัยและยั่งยืนในโลกแห่งความเป็นจริง

2. นิยามและความสำคัญของการรักษาความมั่นคงปลอดภัยทางกายภาพและการปกป้องทรัพย์สิน

การรักษาความปลอดภัยทางกายภาพ (Physical Security) คือมาตรการที่ออกแบบมาเพื่อปกป้องบุคคล อาคารสถานที่ และทรัพย์สินที่จับต้องได้จากภัยคุกคาม เช่น การเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม การทำลายทรัพย์สิน การก่อวินาศกรรม และความรุนแรงในรูปแบบต่าง ๆ แตกต่างจากความปลอดภัยทางไซเบอร์ที่ดำเนินการในพื้นที่ดิจิทัล ความปลอดภัยทางกายภาพดำเนินการใน “พื้นที่เชิงกายภาพที่จับต้องได้” และมีปฏิสัมพันธ์โดยตรงกับพฤติกรรมมนุษย์ สภาพแวดล้อม และสถาปัตยกรรม (Senna, Iglesias, & Matsunaga, 2025)

หัวใจสำคัญของการรักษาความปลอดภัยไม่ได้จำกัดเพียงการติดตั้งอุปกรณ์เสริมความแข็งแกร่ง (Hardware) แต่ครอบคลุมถึงองค์ประกอบสำคัญสี่ประการที่ต้องสอดประสานกัน ได้แก่:

1. **การออกแบบสภาพแวดล้อม (Environmental Design):** การจัดวางผังอาคาร แสงสว่าง และเส้นทางเพื่อลดโอกาสการเกิดอาชญากรรม

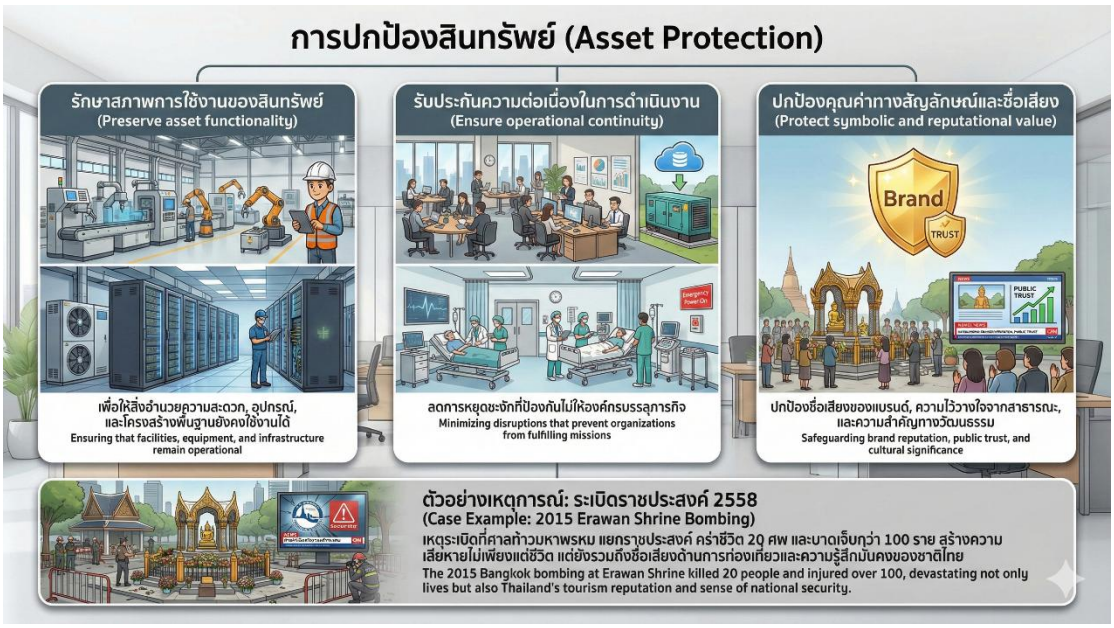
2. **นโยบายและขั้นตอนปฏิบัติ (Policies and Procedures):** การกำหนดสิทธิการเข้าถึง การจัดการผู้มาติดต่อ และแผนเผชิญเหตุ

3. **พฤติกรรมและบุคลากร (Human Presence and Behavior):** การใช้เจ้าหน้าที่รักษาความปลอดภัย และการสร้างจิตสำนึกความปลอดภัยให้กับผู้อยู่อาศัยหรือพนักงาน

4. **การบูรณาการเทคโนโลยี (Technology Integration):** การเชื่อมต่อกล้องวงจรปิด ระบบควบคุมการเข้าออก และระบบตรวจจับการบุกรุกเข้าด้วยกัน

ในบริบทของประเทศไทย การปกป้องทรัพย์สิน (Asset Protection) มีความหมายลึกซึ้งกว่าเพียงแค่การป้องกันตัวเงิน ทั้งนี้ ทรัพย์สินหลายอย่างมีคุณค่าทางสัญลักษณ์และสังคม เช่น วัดสำคัญ โรงพยาบาลรัฐ หรือระบบขนส่งมวลชน ยกตัวอย่างเช่น เหตุการณ์

ระเบิดที่แยกราชประสงค์ในปี พ.ศ. 2558 ไม่เพียงแต่สร้างความเสียหายต่อชีวิตและศาลท้าวมหาพรหมเท่านั้น แต่ยังทำลายความเชื่อมั่นด้านการท่องเที่ยวและชื่อเสียงของประเทศอย่างมหาศาล การปกป้องทรัพย์สินจึงเป็นกระบวนการบริหารจัดการเพื่อรักษาหน้าที่การทำงานขององค์กร (Functionality) สร้างความต่อเนื่องในการดำเนินธุรกิจ (Operational Continuity) และรักษาชื่อเสียงและความไว้วางใจจากสาธารณชน



ภาพที่ 5.2
การปกป้องสินทรัพย์ขององค์กร
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

3. กลยุทธ์พื้นฐาน 4 D: หัวใจของการออกแบบความปลอดภัยทางกายภาพ

เพื่อให้เข้าใจถึงแนวทางการออกแบบระบบรักษาความปลอดภัยทางกายภาพที่มีประสิทธิภาพ นักศึกษาควรทำความเข้าใจหลักการ 4D ซึ่งเป็นกรอบแนวคิดที่ใช้ในการวิเคราะห์และจัดลำดับความสำคัญของมาตรการป้องกัน

1. การหน่วงเหนี่ยว (Deterrence)

การหน่วงเหนี่ยวมีวัตถุประสงค์เพื่อ **ทำให้ผู้ไม่ประสงค์ดีตัดสินใจไม่ลงมือก่อเหตุ** ตั้งแต่ระยะเริ่มต้น โดยมุ่งเน้นการสร้าง *การรับรู้ถึงความเสี่ยง ความยากลำบาก และโอกาสถูกตรวจพบ* มาตรการหน่วงเหนี่ยวที่มีประสิทธิภาพมักเป็นมาตรการที่ “มองเห็นได้ชัดเจน” (Visible Security) เช่น การมีเจ้าหน้าที่รักษาความปลอดภัย การจัดแสงสว่าง

อย่างเหมาะสม การติดตั้งรั้ว ป้ายเตือน และจุดควบคุมการเข้า–ออก (Senna, Iglesias, & Matsunaga, 2025)

แนวคิดด้านอาชญาวิทยาสิ่งแวดล้อมและ CPTED ชี้ให้เห็นว่า **สภาพแวดล้อมที่ได้รับการดูแลอย่างดี** (Maintenance) เป็นสัญญาณสำคัญที่บ่งบอกว่าพื้นที่นั้นอยู่ภายใต้การจัดการและการเฝ้าระวัง ซึ่งสามารถลดแรงจูงใจในการก่ออาชญากรรมได้ดีกว่าพื้นที่ที่ถูกปล่อยปละละเลยหรือทรุดโทรม ทั้งนี้ การหน่วงเหนี่ยวจึงทำงานผ่าน *กลไกทางจิตวิทยาและการรับรู้* มากกว่าการใช้กำลังโดยตรง (Lee, Lee, Nam, Moudon, & Mendoza, 2023)

2. การตรวจจับ (Detection)

เมื่อมาตรการหน่วงเหนี่ยวไม่สามารถยับยั้งภัยคุกคามได้ ระบบตรวจจับจะทำหน้าที่ **ระบุความผิดปกติหรือกิจกรรมที่ไม่ได้รับอนุญาตให้ได้เร็วที่สุด** เพื่อเปิดโอกาสให้เกิดการตอบโต้ที่ทันท่วงที เทคโนโลยีด้านการตรวจจับในปัจจุบันครอบคลุมทั้งกล้องวงจรปิด (CCTV) เซนเซอร์ตรวจจับความเคลื่อนไหว ระบบแจ้งเตือน สัญญาณเตือนภัย และระบบวิเคราะห์วิดีโอด้วยปัญญาประดิษฐ์ (Video Analytics)

ประเด็นสำคัญที่ต้องเน้นย้ำคือ **การตรวจจับต้องมีทั้งความรวดเร็วและความน่าเชื่อถือ** ไม่ใช่เพียงความแม่นยำทางเทคนิคเท่านั้น ระบบที่ตรวจจับได้ช้า หรือไม่มีผู้รับสัญญาณเพื่อนำไปสู่การตอบโต้ ย่อมไม่สามารถสร้างความมั่นคงปลอดภัยที่แท้จริงได้ ดังที่มักกล่าวกันว่า *"การตรวจจับที่ไม่มีการตอบโต้ คือความปลอดภัยจอมปลอม"* (Detection without response creates false security)

3. การประวิงเวลา (Delay)

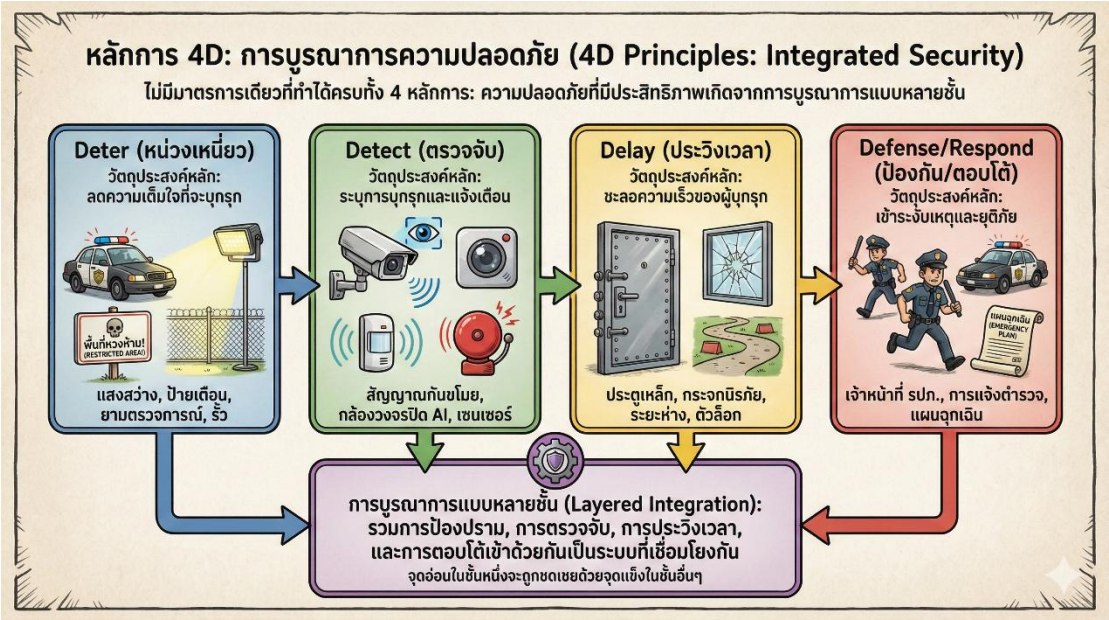
การประวิงเวลาเป็นองค์ประกอบที่ทำหน้าที่ **ชะลอความก้าวหน้าของผู้บุกรุก** เพื่อซื้อเวลาให้กับระบบการตอบโต้ มาตรการในขั้นนี้มักเป็นสิ่งกีดขวางทางกายภาพหรือเชิงโครงสร้าง เช่น รั้วหลายชั้น ประตูเสริมความแข็งแรง ประตูนรภัย กระจกนิรภัย ระบบควบคุมการเข้า–ออก และการแบ่งพื้นที่ภายในออกเป็นโซน (Layered Access Control)

ในการออกแบบระบบรักษาความปลอดภัยระดับสูง แนวคิดเรื่อง **ระยะห่างเพื่อความปลอดภัย (Stand-off Distance)** ถือเป็นกลยุทธ์การประวิงเวลาที่มีประสิทธิภาพอย่างยิ่ง เพราะช่วยเพิ่มเวลาที่ผู้บุกรุกต้องใช้ก่อนจะเข้าถึงทรัพย์สินหรือพื้นที่สำคัญ หลักคิดสำคัญของขั้นตอนนี้คือ *"เวลาเท่ากับความปลอดภัย"* เนื่องจากการประวิงเวลาทำหน้าที่เชื่อมโยงระหว่างการตรวจจับกับการตอบโต้โดยตรง

4. การตอบโต้หรือการป้องกัน (Response/Defend)

ขั้นตอนสุดท้ายของกรอบ 4D คือการดำเนินการเพื่อ **ยุติ ควบคุม หรือจำกัดผลกระทบของภัยคุกคาม** หลังจากที่ระบบตรวจจับได้แจ้งเตือนแล้ว การตอบโต้สามารถอยู่ในรูปแบบของการเข้าระงับเหตุโดยเจ้าหน้าที่รักษาความปลอดภัย การประสานงานกับเจ้าหน้าที่ตำรวจหรือหน่วยงานฉุกเฉิน ตลอดจนการใช้ระบบอัตโนมัติ เช่น การล็อกดาวน์อาคารหรือการปิดกั้นพื้นที่เสี่ยง

ประสิทธิภาพของการตอบโต้ขึ้นอยู่กับ **การวางแผนล่วงหน้า ขั้นตอนปฏิบัติงานที่ชัดเจน การสื่อสารที่มีประสิทธิภาพ และการฝึกซ้อมอย่างสม่ำเสมอ** หากไม่มีความสามารถในการตอบโต้ แม้ระบบตรวจจับจะทันสมัยเพียงใด ก็ไม่อาจถือว่าเป็นระบบความมั่นคงปลอดภัยที่สมบูรณ์ได้



ภาพที่ 5.3
หลักการ 4D ของการบูรณาการความปลอดภัย
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

4. การรักษาความปลอดภัยแนวเขต: ปราการด่านแรกและการสร้างระยะห่าง (Perimeter Security: The First Line of Defense)

การรักษาความปลอดภัยแนวเขต (Perimeter Security) คือการกำหนดขอบเขตระหว่างพื้นที่ที่องค์กรควบคุมและพื้นที่สาธารณะที่ไม่สามารถควบคุมได้ วัตถุประสงค์ไม่ใช่เพียงเพื่อกั้นคนออกไป แต่คือการแสดงความเป็นเจ้าของพื้นที่ (Territoriality) และการคัดกรองผู้ที่เข้า-ออกอย่างเป็นระบบ

4.1 สิ่งกีดขวางทางกายภาพและเชิงสัญลักษณ์ (Physical and Symbolic Barriers)

สิ่งกีดขวาง (Barriers) สามารถแบ่งได้เป็นสองประเภทใหญ่ ๆ คือ “สิ่งกีดขวางทางกายภาพ” เช่น รั้ว กำแพง และประตูกั้น ซึ่งทำหน้าที่หน่วงเหนี่ยวและประวิงเวลาอย่างแท้จริง และ “สิ่งกีดขวางเชิงสัญลักษณ์” เช่น การปูพื้นผิวที่แตกต่างกัน การใช้แนวพุ่มไม้หรือป้ายแจ้งเขตพื้นที่ส่วนบุคคล ในห้างสรรพสินค้าของไทย เช่น สยามพารากอน หรือเซ็นทรัลเวิลด์ มักใช้การผสมผสานระหว่างกำแพงเตี้ยที่ดูสวยงาม (ซึ่งทำหน้าที่เป็นแบริเออร์กันรถยนต์พุ่งชนไปในตัว) และการใช้เจ้าหน้าที่รักษาความปลอดภัยคอยตรวจกระเป๋าที่จุดทางเข้า (Senna, Iglesias, & Matsunaga, 2025)

4.2 ระยะห่างจากจุดเสี่ยง (Stand-off Distance) และการป้องกันการพุ่งชน

ระยะห่าง (Stand-off Distance) คือพื้นที่ว่างระหว่างจุดที่ภัยคุกคามภายนอก (เช่น รถยนต์ที่บรรทุกระเบิดหรือผู้บุกรุก) กับตัวอาคารหรือทรัพย์สินที่ต้องการปกป้อง ยิ่งระยะห่างมากเท่าใด ผลกระทบจากแรงระเบิดหรือความสามารถในการบุกรุกก็จะลดน้อยลงเท่านั้น ในสถานที่ที่มีความเสี่ยงสูง เช่น สถานทูต หรือดาต้าเซ็นเตอร์ในไทย มีการติดตั้ง “เสาโบลาลาร์ด” (Bollards) และเครื่องกั้นยานพาหนะที่ผ่านการทดสอบแรงกระแทกตามมาตรฐาน ASTM F2656 เพื่อป้องกันเหตุการณ์รถยนต์พุ่งชน (Vehicle Ramming) (Senna, Iglesias, & Matsunaga, 2025)

ภาพที่ 5.4

หลักการ 4D ของการบูรณาการความปลอดภัย

ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) ซึ่งกล่าวถึงในบทที่ 2 ชี้ให้เห็นว่า การรับรู้ถึงการมีผู้ดูแลเฝ้าระวัง (perceived guardianship) สามารถมีอิทธิพลต่อการยับยั้งอาชญากรรมได้ไม่ยิ่งหย่อนไปกว่าการมีสิ่งกีดขวางทางกายภาพจริง งานวิจัยจำนวนมากยืนยันว่า พื้นที่ที่ได้รับการดูแลรักษาอย่างดี มีการกำหนดขอบเขตที่ชัดเจน และแสดงสัญญาณของการจัดการอย่างเป็นระบบ โดยเฉพาะในกรณีที่ไม่มีโครงสร้างป้องกันที่แข็งแรง จะสามารถลดโอกาสในการก่ออาชญากรรมได้อย่างมีนัยสำคัญ โดยส่งสารไปยังผู้ที่อาจกระทำผิดว่า “พื้นที่นี้มีผู้ดูแลและอยู่ภายใต้การเฝ้าระวัง” (Cohen & Felson, 1979)

5. ระบบควบคุมการเข้า-ออก: จากกุญแจดั้งเดิมสู่ไบโอเมตริกซ์ (Access Control Systems: From Traditional Locks and Keys to Biometric)

ระบบควบคุมการเข้า-ออก (Access Control Systems) มีหน้าที่ตัดสินใจว่า “ใคร” สามารถผ่านประตูได้บ้าง และในเงื่อนไข “อย่างไร” ในบทเรียนนี้ เราจะพิจารณาวิวัฒนาการของเทคโนโลยีที่ถูกนำมาใช้ในประเทศไทยเพื่อให้เห็นภาพรวมของการจัดการความปลอดภัย

5.1 ประเภทของเทคโนโลยีควบคุมการเข้า-ออก

การเลือกเทคโนโลยีต้องพิจารณาถึงสมดุลระหว่าง “ความปลอดภัย ความสะดวก และต้นทุน” ตัวอย่างเช่น

1. ระบบกลไก (Mechanical Systems): ได้แก่ กุญแจและแม่กุญแจแบบดั้งเดิม ข้อดีคือราคาถูกและไม่ต้องใช้ไฟฟ้า แต่ข้อเสียคือสำเนากุญแจได้ง่าย และไม่มีบันทึกข้อมูลว่าใครเป็นคนเปิดประตู

2. บัตรสมาร์ทการ์ดและ RFID: นิยมมากในคอนโดมิเนียมและอาคารสำนักงานในกรุงเทพมหานคร สามารถบันทึกเวลาการเข้า-ออกได้ แต่มีความเสี่ยงจากการถูกขโมยบัตรหรือการที่ผู้อื่นนำบัตรมาสแกนแทนกัน

3. เทคโนโลยีชีวภาพ (Biometrics): เช่น การสแกนลายนิ้วมือ และการจดจำใบหน้า (Facial Recognition) ในช่วงหลังการระบาดของ COVID-19 ประเทศไทยมีการนำระบบจดจำใบหน้ามาใช้ในหน่วยงานรัฐและอาคารสำนักงานอย่างแพร่หลายเพื่อลดการสัมผัส โดยระบบนี้สามารถระบุตัวตนบุคคลได้อย่างแม่นยำและยากต่อการปลอมแปลง (El Bouhissi & Yurko, 2025)

4. การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA): สำหรับพื้นที่ความมั่นคงสูง เช่น ห้องเซิร์ฟเวอร์ หรือคลังเก็บเงิน ระบบจะกำหนดให้ต้องใช้

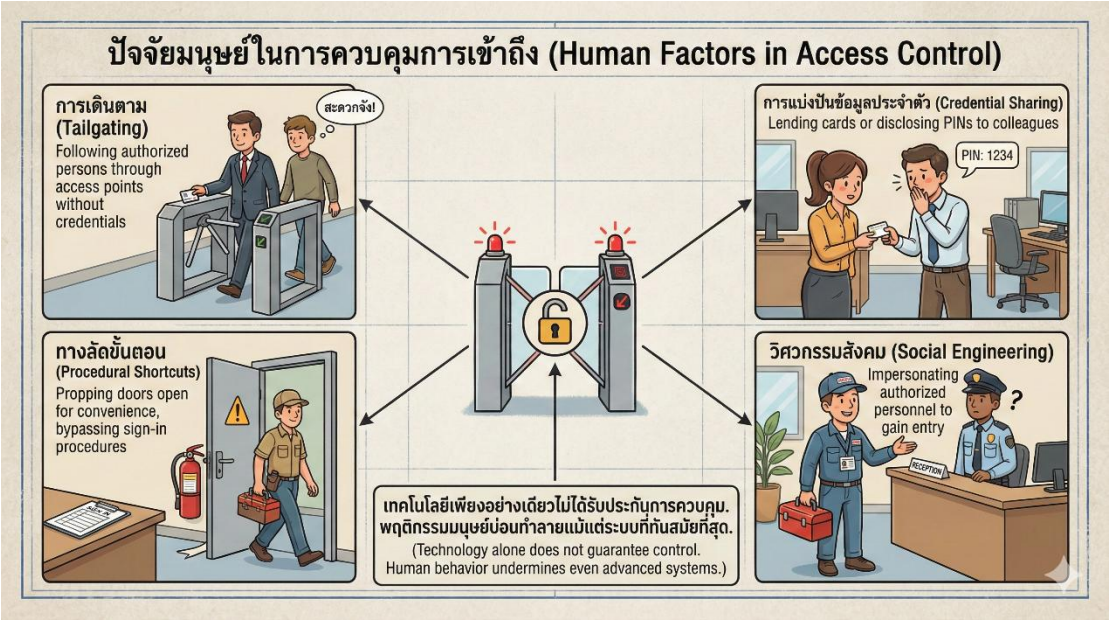
มากกว่าหนึ่งปัจจัย เช่น “บัตร + รหัส PIN” หรือ “บัตร + การสแกนม่านตา” เพื่อเพิ่มความมั่นใจสูงสุด (Senna, Iglesias, & Matsunaga, 2025)

5.2 กรณีศึกษาการใช้ Access Control

ระบบรถไฟฟ้า BTS และ MRT ของไทยใช้บัตร RFID และ QR Codes เป็นหัวใจสำคัญในการจัดการคนจำนวนมหาศาล ข้อมูลจากระบบไม่เพียงแต่ใช้เพื่อความปลอดภัย แต่ยังนำมาใช้วิเคราะห์เพื่อปรับปรุงการเดินรถ ขณะที่ท่าอากาศยานสุวรรณภูมิได้ยกระดับความมั่นคงด้วยการนำระบบไบโอเมตริกซ์มาใช้ตรวจสอบผู้โดยสารขาออกเพื่อลดข้อผิดพลาดจากการตรวจสอบของมนุษย์

ภาพที่ 5.5
แอปพลิเคชันการควบคุมการเข้าถึง
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

ด้วยเหตุนี้ การฝึกอบรม วัฒนธรรมองค์กร และการบังคับใช้นโยบายอย่างจริงจัง จึงเป็นองค์ประกอบที่ มีความสำคัญอย่างยิ่งต่อประสิทธิผลของระบบควบคุมการเข้าออก งานวิชาการด้านการควบคุมการเข้าถึงชี้ให้เห็นว่า ประสิทธิภาพของระบบไบโอเมตริกไม่ได้วัดจากความแม่นยำของเทคโนโลยีเพียงอย่างเดียว หากแต่ขึ้นอยู่กับการปฏิบัติตามกฎของผู้ใช้งาน และระดับความมุ่งมั่นขององค์กรในการยึดถือและบังคับใช้ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ (Mofidi, Hounsinou, & Bloom, 2024)



ภาพที่ 5.6
แอปพลิเคชันการควบคุมการเข้าถึง
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

6. ระบบเฝ้าระวังและการตรวจจับ: “ดวงตา” ของเมืองและเทคโนโลยี AI (Surveillance as Guardianship)

กล้องวงจรปิด (CCTV) ไม่ใช่เรื่องใหม่ในสังคมไทย แต่การพัฒนาสู่ “ระบบเฝ้าระวังอัจฉริยะ” (Smart Surveillance) กำลังเปลี่ยนโฉมหน้าการรักษาความปลอดภัยอย่างสิ้นเชิง

6.1 โครงข่ายกล้องวงจรปิดในกรุงเทพมหานคร

กรุงเทพมหานครมีกล้องวงจรปิดมากกว่า 62,000 ตัวกระจายอยู่ใน 50 เขต อย่างไรก็ตาม ความท้าทายที่สำคัญคือ “การเฝ้าติดตามแบบเรียลไทม์” (Real-time Monitoring) งานวิจัยพบว่าประสิทธิภาพของระบบ CCTV มักถูกบั่นทอนจากการขาดแคลนเจ้าหน้าที่เฝ้าหน้าจอ และจุดบอดของกล้องที่เกิดจากการวางผังเมืองที่หนาแน่น ดังนั้น เทรนด์ในปี 2568 จึงมุ่งเน้นไปที่การใช้ AI CCTV ที่สามารถตรวจจับพฤติกรรมผิดปกติได้โดยอัตโนมัติ เช่น การจอดรถในที่ห้ามจอด การปีนข้ามรั้ว หรือการรวมตัวกันของคนจำนวนมากในยามวิกาล (Anderson & McAtamney, 2011)

6.2 บทบาทของแสงสว่าง (Lighting)

งานวิจัยด้าน Crime Prevention Through Environmental Design (CPTED) ชี้ให้เห็นอย่างสม่ำเสมอว่า แสงสว่างที่ไม่เพียงพอมีความสัมพันธ์อย่างใกล้ชิดกับความกลัว

อาชญากรรม แม้ในพื้นที่ที่อัตราการเกิดอาชญากรรมจริงอยู่ในระดับปานกลางก็ตาม (Cozens, Babb, & Stefani, 2023) ทั้งนี้ แสงสว่างที่เหมาะสมไม่เพียงช่วยเพิ่มประสิทธิภาพของระบบเฝ้าระวัง เช่น กล้องวงจรปิด แต่ยังส่งผลโดยตรงต่อการรับรู้ความเสี่ยงของผู้ที่อาจก่อเหตุ โดยทำให้การหลบซ่อนและการเคลื่อนไหวโดยไม่ถูกสังเกตเป็นไปได้ยากยิ่งขึ้น การออกแบบแสงสว่างเพื่อการรักษาความปลอดภัยจึงควรให้ความสำคัญกับ “ความสม่ำเสมอ” ของแสง เพื่อหลีกเลี่ยงการเกิดเงามืดซึ่งอาจกลายเป็นพื้นที่เอื้อประโยชน์ต่อผู้กระทำผิด (Trimek, 2016)

6.3 ระบบตรวจจับการบุกรุก (Intrusion Detection Systems)

มาตรฐาน ISO/IEC 27002:2022 หมวดควบคุม 7.1 ว่าด้วยขอบเขตความปลอดภัยทางกายภาพ เน้นย้ำว่า องค์กรควรติดตั้งระบบตรวจจับการบุกรุกที่เหมาะสมตามมาตรฐานระดับชาติ ภูมิภาค หรือสากล และต้องมีการทดสอบอย่างสม่ำเสมอเพื่อครอบคลุมประตูและช่องเปิดภายนอกทั้งหมด อย่างไรก็ตาม การตรวจจับเพียงอย่างเดียวไม่เพียงพอ หากขาดการตอบสนองที่มีประสิทธิภาพ

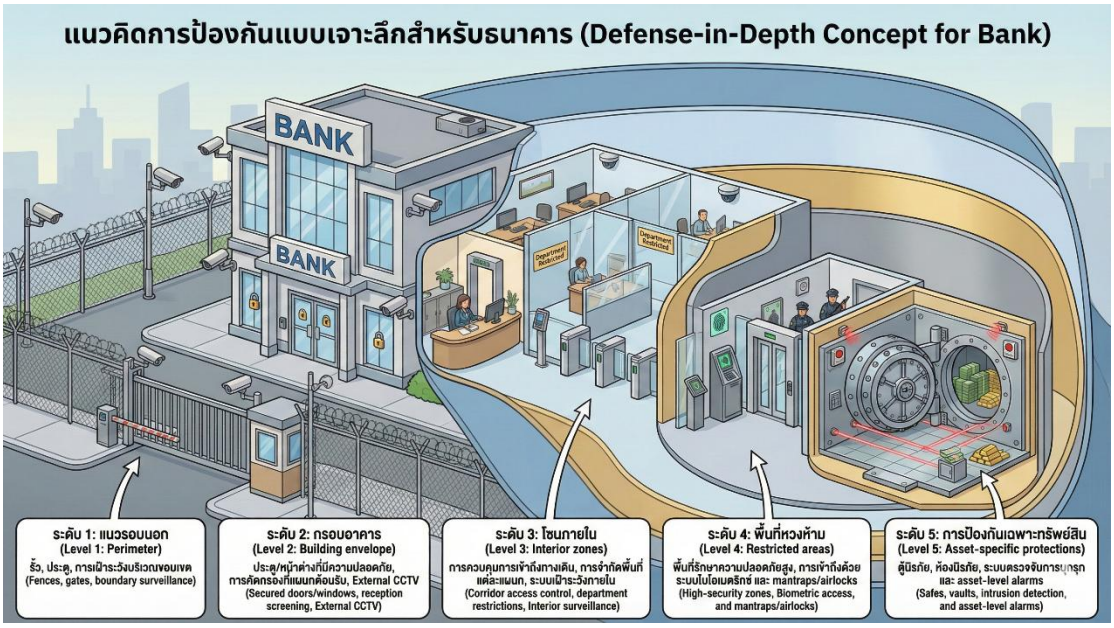
ภาพที่ 5.7
ระบบเฝ้าระวังและการตรวจจับ
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

ทั้งนี้ ระบบตรวจจับที่ไม่เชื่อมโยงกับขั้นตอนการปฏิบัติและบุคลากรที่ผ่านการฝึกอบรมย่อมก่อให้เกิด “ความมั่นคงปลอดภัยลวงตา” (false sense of security) ในทางปฏิบัติ ระบบตรวจจับการบุกรุกที่แนวเขตพื้นที่ (Perimeter Intrusion Detection

Systems: PIDS) เช่น เซนเซอร์ตรวจจับแรงสั่นสะเทือนบนรั้ว หรือระบบคานอินฟราเรด จะส่งสัญญาณเตือนไปยังศูนย์ควบคุมเพื่อให้เจ้าหน้าที่สามารถตอบสนองและระงับเหตุได้อย่างทันท่วงทีผ่านกระบวนการที่กำหนดไว้อย่างชัดเจน (Jos, Dupski, & Amilkar, 2024)

7. การวางผังสถานที่และการป้องกันแบบหลายชั้น (Layered Defense)

หลักการ “การป้องกันเชิงลึก” (Defense-in-Depth) ตั้งอยู่บนแนวคิดพื้นฐานว่าองค์กรไม่ควรพึ่งพามาตรการป้องกันเพียงจุดเดียว หากแต่ควรสร้างชั้นของการป้องกันที่ซ้อนทับกันอย่างเป็นระบบ แนวคิดนี้มีรากฐานจากยุทธศาสตร์ทางทหารในอดีต ซึ่งออกแบบป้อมปราการให้มีหลายชั้น เช่น คูน้ำ กำแพงชั้นนอก กำแพงชั้นใน และป้อมกลางเมือง เพื่อทำให้ผู้โจมตีต้องเผชิญอุปสรรคต่อเนื่องจนสูญเสียเวลา ทรัพยากร และความได้เปรียบ (Mofidi, Hounsinou, & Bloom, 2024)



ภาพที่ 5.8
การป้องกันเชิงลึก (Defense-in-Depth)
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

ปัจจุบัน หลักการดังกล่าวถูกประยุกต์ใช้ทั้งในด้านความมั่นคงปลอดภัยไซเบอร์และทางกายภาพ โดยยึดแก่นสำคัญเดียวกันคือ “ความซ้ำซ้อนและความหลากหลาย” ของมาตรการในแต่ละชั้น เพื่อให้เมื่อมาตรการหนึ่งล้มเหลว ชั้นถัดไปยังคงทำหน้าที่ป้องกัน

หน่วงเหนี่ยว และตรวจจับภัยคุกคามได้อย่างต่อเนื่อง โดยมีทรัพย์สินที่สำคัญที่สุดอยู่ศูนย์กลางของระบบป้องกันหลายชั้นนั้น ดังนี้

1. **ชั้นที่ 1 แนวเขตภายนอก (Perimeter):** รั้ว แสงสว่าง และป้ายเตือน

2. **ชั้นที่ 2 เปลือกอาคาร (Building Envelope):** ประตู หน้าต่าง จุดคัดกรองพนักงาน

3. **ชั้นที่ 3 โซนภายในอาคาร (Interior Zones):** การคัดกรองผู้มาติดต่อ การจำกัดสิทธิเข้าถึงแต่ละชั้น

4. **ชั้นที่ 4 พื้นที่ควบคุมพิเศษ (Restricted Areas):** พื้นที่ความมั่นคงสูงที่ต้องใช้รหัสผ่านหรือไบโอเมตริกซ์

5. **ชั้นที่ 5 การปกป้องทรัพย์สินหลัก (Asset Protection):** ตู้นิรภัย ห้องนิรภัย หรือระบบล็อกอุปกรณ์

ภาพที่ 5.9
การป้องกันแบบแบ่งชั้น (Layered Defense)
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

การออกแบบระบบป้องกันที่มีประสิทธิภาพต้องกำหนดให้แต่ละชั้นของการป้องกันมีระดับความแข็งแกร่งและบทบาทที่แตกต่างกันอย่างชัดเจน หากผู้บุกรุกสามารถผ่านด่านแรกเข้ามาได้ ระบบในชั้นถัดไปควรสามารถตรวจจับความผิดปกติได้ทันที และในชั้นลึกลงไปควรทำหน้าที่หน่วงเหนี่ยวหรือประวิงเวลาเพื่อเปิดโอกาสให้เจ้าหน้าที่ตอบสนองอย่าง

ทันท่วงที ตัวอย่างเช่น ค่ายทหารหรือศูนย์ข้อมูล (Data Center) มาตรฐานสากลของบริษัทเทคโนโลยีชั้นนำในประเทศไทย มักใช้ระบบ “Mantraps” หรือห้องเปลี่ยนผ่านที่อนุญาตให้เข้าได้ครั้งละหนึ่งคน เพื่อป้องกันการเดินตามหลัง (tailgating) เข้าสู่พื้นที่วิกฤตโดยไม่ได้รับอนุญาต ในทางตรงกันข้าม สถานที่ที่วางผังอย่างขาดการวางแผนมักก่อให้เกิดคอขวดและจุดบอดที่คาดเดาได้ เปิดโอกาสให้ผู้ไม่หวังดีใช้ประโยชน์ได้ ดังที่ปรากฏทั้งในกรณีศึกษาภาพยนตร์และเหตุการณ์จริงจำนวนมาก พื้นที่ที่ออกแบบอย่างรอบคอบจึงต้องทำให้การเคลื่อนไหวที่ไม่ได้รับอนุญาตเป็นเรื่องยาก มองเห็นได้ชัด และใช้เวลานาน ขณะเดียวกันยังต้องสนับสนุนการดำเนินกิจกรรมที่ถูกต้องตามปกติได้อย่างราบรื่น (Mofidi, Hounsinou, & Bloom, 2024)

8. การป้องกันอาชญากรรมผ่านการออกแบบทางสถาปัตยกรรม (CPTED: Crime Prevention Through Environmental Design)

Crime Prevention Through Environmental Design (CPTED) ตั้งอยู่บนแนวคิดพื้นฐานว่า การออกแบบสภาพแวดล้อมมีอิทธิพลต่อพฤติกรรมของมนุษย์ แนวคิดนี้ได้รับการบัญญัติคำโดย C. Ray Jeffery ในปี ค.ศ. 1971 ขณะที่ Oscar Newman พัฒนาแนวคิดที่สอดคล้องกันในชื่อ “Defensible Space” ซึ่งมุ่งเน้นการออกแบบพื้นที่ให้เอื้อต่อการควบคุม ดูแล และป้องกันอาชญากรรมอย่างเป็นธรรมชาติ (Newman, 1972) โดยสาระสำคัญของ CPTED คือความเชื่อว่า “การปรับเปลี่ยนสิ่งแวดล้อมทางกายภาพสามารถลดโอกาสในการเกิดอาชญากรรมได้” ผ่านการจัดวางพื้นที่ การกำหนดขอบเขต และการเสริมสร้างการรับรู้ถึงการมีผู้ดูแล ปัจจุบันแนวคิดนี้ได้รับความนิยมอย่างกว้างขวางในหมู่นักสถาปนิก นักผังเมือง และผู้พัฒนาโครงการต่าง ๆ โดยเฉพาะในการออกแบบโครงการที่อยู่อาศัย ศูนย์การค้า และพื้นที่สาธารณะให้มีความปลอดภัยตั้งแต่ระดับโครงสร้างพื้นฐาน (Lee, Park, & Jung, 2016)

8.1 หลักการ 5 ประการของ CPTED

1. การเฝ้าระวังตามธรรมชาติ (Natural Surveillance)

การเฝ้าระวังตามธรรมชาติเป็นหลักการสำคัญของ CPTED ที่มุ่งทำให้ พื้นที่สามารถถูกมองเห็นได้โดยง่าย จากผู้อยู่อาศัย พนักงาน หรือผู้สัญจรผ่านไปมา โดยไม่ต้องพึ่งพาเทคโนโลยีเพียงอย่างเดียว แนวคิดนี้ตั้งอยู่บนสมมติฐานว่า การเพิ่ม “สายตาในพื้นที่” จะช่วยยับยั้งการกระทำผิด เพราะผู้ก่อเหตุรับรู้ว่ามีโอกาสถูกสังเกตเห็นสูง กลยุทธ์การออกแบบที่สำคัญ ได้แก่ การรักษาแนวสายตาให้ชัดเจนโดยหลีกเลี่ยงรั้วทึบหรือพืชพรรณหนาทึบที่บดบังทัศนวิสัย การออกแบบหน้าต่างให้หันสู่ถนนหรือพื้นที่สาธารณะ การจัดผัง

พื้นที่แบบเปิดเพื่อลดมุมอับและซอกหลืบที่ซ่อนตัวได้ รวมถึงการจัดแสงสว่างอย่างเหมาะสมในทางเดิน ลานจอดรถ และจุดเข้า–ออก งานวิจัยเกี่ยวกับ CPTED ยังพบว่า การเฝ้าระวังตามธรรมชาติเป็นตัวแปรที่มีอิทธิพลต่อ “ความกลัวอาชญากรรม” มากกว่าการแสดงอาณาเขต (territoriality) และพื้นที่ที่ขาดการมองเห็นที่เพียงพอมักสัมพันธ์กับระดับความหวาดกลัวที่สูงขึ้น ดังนั้น การออกแบบให้ผู้คนสามารถมองเห็นและถูกมองเห็นได้จึงไม่เพียงลดโอกาสการกระทำผิด แต่ยังเสริมสร้างความรู้สึกปลอดภัยในระดับจิตวิทยาอีกด้วย (Lee, Lee, Nam, Moudon, & Mendoza, 2023)

2. การควบคุมการเข้า–ออกตามธรรมชาติ (Natural Access Control)

การควบคุมการเข้า–ออกตามธรรมชาติ เป็นแนวคิดในกรอบ CPTED ที่ใช้ การออกแบบทางกายภาพเพื่อกำหนดทิศทางการเคลื่อนไหวของผู้คน และนำทางให้การเข้า–ออกเกิดขึ้นผ่านจุดที่สามารถเฝ้าระวังและควบคุมได้อย่างมีประสิทธิภาพ โดยไม่สร้างความรู้สึกว่าถูกบังคับ กลยุทธ์สำคัญ ได้แก่ การกำหนดจุดเข้า–ออกหลักเพียงไม่กี่จุดเพื่อลดความซับซ้อนในการตรวจสอบ การใช้ภูมิทัศน์ เช่น แนวพุ่มไม้ กระถางต้นไม้ หรือการเปลี่ยนระดับพื้นผิว เพื่อชี้นำทิศทางการสัญจร การจัดทางเดินที่ชัดเจนเพื่อลดการลัดเลาะผ่านพื้นที่ส่วนตัว และการจัดพื้นที่ต้อนรับ (reception area) เพื่อคัดกรองและทักทายผู้มาติดต่ออย่างเป็นระบบ ตัวอย่างเช่น ศูนย์การค้าขนาดใหญ่ที่กำหนดจุดทางเข้าเพียงบางจุดและจัดระบบคัดกรองความปลอดภัย ทำให้ผู้มาใช้บริการทั้งหมดต้องผ่านพื้นที่ที่อยู่ภายใต้การสังเกตการณ์ การออกแบบลักษณะนี้ช่วยเพิ่มระดับการควบคุม ขณะเดียวกันยังคงบรรยากาศที่เป็นมิตรและเอื้อต่อการใช้งานตามปกติ (Lee, Park, & Jung, 2016)

3. การเสริมสร้างอาณาเขต (Territorial Reinforcement)

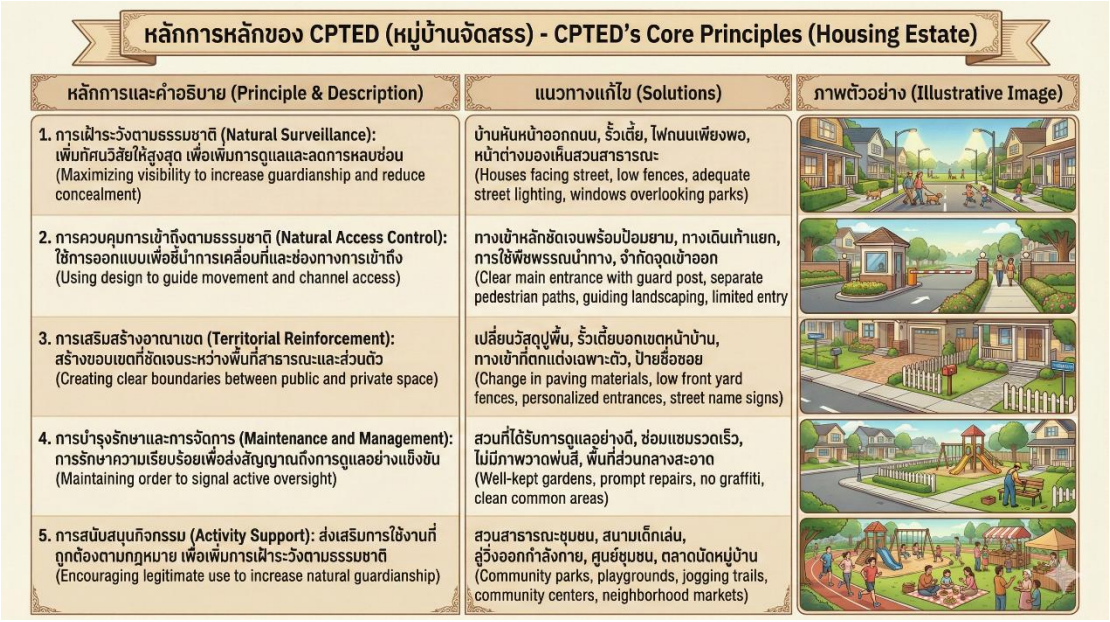
การเสริมสร้างอาณาเขต เป็นหลักการสำคัญของ CPTED ที่มุ่งสร้าง ขอบเขตที่ชัดเจนระหว่างพื้นที่สาธารณะ กึ่งสาธารณะ และพื้นที่ส่วนตัว เพื่อแสดงความเป็นเจ้าของและความรับผิดชอบต่อพื้นที่นั้น องค์ประกอบทางการออกแบบที่ใช้บ่อย ได้แก่ รั้วและประตูเพื่อกำหนดขอบเขตทรัพย์สิน ป้ายแสดงสถานะพื้นที่ เช่น “Private Property” หรือ “Authorized Personnel Only” การจัดภูมิทัศน์ด้วยแนวพุ่มไม้ แปลงดอกไม้ หรือการเปลี่ยนวัสดุปูพื้นเพื่อสื่อถึงการเปลี่ยนผ่านของเขตพื้นที่ รวมถึงสิ่งกีดขวางเชิงสัญลักษณ์ เช่น กำแพงเตี้ย ม้านั่ง หรือกระถางต้นไม้ ซึ่งช่วยแบ่งโซนโดยไม่บดบังทัศนวิสัย (Lee, Park, & Jung, 2016)

แนวคิด “Defensible Space” ของ Oscar Newman (1972) ชี้ว่า เมื่อผู้อยู่อาศัยรับรู้ว่าพื้นที่เป็น “อาณาเขตของตน” พวกเขาจะมีแนวโน้มเฝ้าระวัง ดูแลรักษา และตั้งคำถามกับบุคคลแปลกหน้าเพิ่มขึ้น งานวิจัยในโครงการที่อยู่อาศัยซึ่งนำแนวคิดนี้ไปใช้พบว่า

การสร้างเขตชุมชนย่อยผ่านการปิดถนนบางส่วนและการกำหนดเครื่องหมายแสดงอาณาเขตอย่างชัดเจน สามารถลดอาชญากรรมได้โดยเสริมสร้างความรู้สึกเป็นเจ้าของและความรับผิดชอบร่วมกันของผู้อยู่อาศัย ดังนั้น การทำให้พื้นที่ “ดูเหมือนมีเจ้าของและมีผู้ดูแล” คือกลไกเชิงจิตวิทยาที่ทรงพลังในการยับยั้งพฤติกรรมเบี่ยงเบนโดยไม่ต้องพึ่งพามาตรการแข็งเพียงอย่างเดียว (Lee, Park, & Jung, 2016)

4. การดูแลรักษาและภาพลักษณ์ (Maintenance and Image)

ทฤษฎี “หน้าต่างแตก” (Broken Windows Theory) ของ Wilson และ Kelling (1982) เสนอว่า ความไม่เป็นระเบียบที่มองเห็นได้ เช่น กราฟฟิตี ขยะ หรืออุปกรณ์ที่ชำรุด ส่งสัญญาณถึงการละเลยและอาจเชื้อเชิญให้เกิดพฤติกรรมเบี่ยงเบนหรืออาชญากรรมเพิ่มเติม ในทางกลับกัน พื้นที่ที่ได้รับการดูแลรักษาอย่างดีจะสื่อสารถึงการจัดการที่มีประสิทธิภาพและการเฝ้าระวังอย่างต่อเนื่อง ซึ่งช่วยยับยั้งผู้ที่อาจก่อเหตุ หลักการ CPTED จึงให้ความสำคัญกับการซ่อมแซมความเสียหายอย่างทันท่วงที การทำความสะอาดสม่ำเสมอ การตัดแต่งภูมิทัศน์ และการรักษาความเป็นระเบียบโดยรวม เพื่อส่งสารว่า “พื้นที่นี้มีผู้ดูแล” การดูแลรักษาไม่ได้เป็นเพียงเรื่องความสวยงาม หากเป็นกลไกเชิงสัญญะที่ลดโอกาสการก่ออาชญากรรมผ่านการเสริมสร้างความรู้สึกถึงการควบคุมและความรับผิดชอบต่อพื้นที่อย่างต่อเนื่อง (Cozens, Babb, & Stefani, 2023)



ภาพที่ 5.10

ตัวอย่างหลักการป้องกันอาชญากรรมผ่านการออกแบบทางสถาปัตยกรรม (CPTED)

ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

5. CPTED กับบริบทวัฒนธรรมไทย (Cultural Adaptation of CPTED)

แนวคิด CPTED จำเป็นต้องปรับให้สอดคล้องกับบริบททางวัฒนธรรมและสังคมของแต่ละประเทศ ในประเทศไทย พื้นที่สาธารณะและพื้นที่ชุมชนมีคุณค่าทางสังคมสูง การออกแบบที่เน้นการปิดล้อมหรือเสริมกำแพงอย่างเข้มข้นเกินไปอาจลดความรู้สึกเป็นชุมชนและก่อให้เกิดความไม่มั่นคงเชิงรับรู้โดยไม่ตั้งใจ ชุมชนที่อยู่อาศัยแบบ “หมู่บ้านจัดสรร” ได้นำหลัก CPTED มาประยุกต์ใช้ผ่านผังโครงการแบบมีประตูทางเข้า–ออกจำกัด จุดรักษาความปลอดภัย พื้นที่ส่วนกลางร่วมกัน และการกำหนดขอบเขตที่มองเห็นได้ชัดเจนซึ่งยังคงรักษาบรรยากาศที่เป็นมิตร ขณะที่วัดและสวนสาธารณะในไทยใช้การเสริมสร้างอาณาเขตผ่านป้ายบอกเขต การจัดภูมิทัศน์ และการดูแลรักษาอย่างสม่ำเสมอ โดยยังเปิดกว้างสำหรับการทำกิจกรรมทางศาสนาและนันทนาการ งานวิจัยในบริบททางวัฒนธรรมพบว่าการเฝ้าระวังและการควบคุมการเข้า–ออกมีความสัมพันธ์อย่างมีนัยสำคัญกับระดับความรู้สึกปลอดภัยของผู้ใช้พื้นที่ และการออกแบบที่เปิดโล่งอย่างเหมาะสมมีประสิทธิผลสูงในพื้นที่สาธารณะ ทั้งนี้ หลักการ “การสนับสนุนกิจกรรม” (Activity Support) ยังมีบทบาทสำคัญ โดยการจัดให้มีกิจกรรมเชิงบวกในพื้นที่สาธารณะอย่างต่อเนื่องจะเพิ่มจำนวน “สายตาในพื้นที่” และสร้างแรงกดดันทางสังคมที่ทำให้ผู้ไม่หวังดีรู้สึกไม่สะดวกในการก่อเหตุ (Cozens, Babb, & Stefani, 2023)

9. การปกป้องโครงสร้างพื้นฐานสำคัญ (Protecting Critical Infrastructure and Facilities)

9.1 โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) คืออะไร?

โครงสร้างพื้นฐานสำคัญ หมายถึง สถานที่ ระบบ หรือสิ่งอำนวยความสะดวกที่หากเกิดการหยุดชะงัก ความเสียหาย หรือการถูกทำลาย จะส่งผลกระทบอย่างรุนแรงต่อความปลอดภัยสาธารณะ เสถียรภาพทางเศรษฐกิจ ความมั่นคงของรัฐ และคุณภาพชีวิตของประชาชน โครงสร้างพื้นฐานเหล่านี้มีบทบาทเป็นกลไกหลักที่ทำให้สังคมสามารถดำเนินกิจกรรมประจำวันได้อย่างต่อเนื่องและปลอดภัย

ในมิติของ ความปลอดภัยสาธารณะ โครงสร้างพื้นฐานสำคัญครอบคลุมระบบไฟฟ้า ระบบประปา โรงพยาบาล และบริการฉุกเฉิน ซึ่งเป็นสิ่งจำเป็นต่อการดำรงชีวิตของประชาชน ในด้าน เสถียรภาพทางเศรษฐกิจ รวมถึงศูนย์กลางคมนาคม ท่าอากาศยาน ท่าเรือ ระบบการเงิน และโครงข่ายโทรคมนาคมที่รองรับกิจกรรมทางธุรกิจและการค้าระหว่างประเทศ ขณะที่ในมิติของ ความมั่นคงแห่งชาติ ครอบคลุมสถานที่ราชการ ฐานทัพ ศูนย์ข้อมูล (data centers) และจุดผ่านแดน ตัวอย่างของโครงสร้างพื้นฐานสำคัญ ได้แก่

โรงไฟฟ้า สนามบิน ท่าเรือ เขื่อน สะพาน ศูนย์ข้อมูล และเครือข่ายโทรคมนาคม ซึ่งล้วนเป็นทรัพย์สินเชิงยุทธศาสตร์ที่ต้องได้รับการปกป้องอย่างเป็นระบบและรัดกุม

9.2 ความยืดหยุ่นและการฟื้นตัว (Resilience)

ในบริบทของประเทศไทย ความท้าทายด้านโครงสร้างพื้นฐานวิกฤตมีลักษณะเฉพาะที่เชื่อมโยงกับความเสี่ยงจากภัยธรรมชาติ โดยเฉพาะ “อุทกภัย” เหตุการณ์น้ำท่วมใหญ่ปี 2554 ซึ่งสร้างความเสียหายทางเศรษฐกิจกว่า 45,000 ล้านดอลลาร์สหรัฐ และส่งผลกระทบต่อห่วงโซ่อุปทานระดับโลก (Marks, 2016) เป็นบทเรียนสำคัญที่ตอกย้ำแนวคิดเรื่อง “ความยืดหยุ่นและการฟื้นตัว” (resilience) องค์กรจำนวนมากจึงต้องออกแบบอาคารและโครงสร้างพื้นฐานให้รองรับภัยพิบัติทางธรรมชาติควบคู่กับภัยคุกคามด้านความมั่นคง เช่น การสร้างกำแพงกั้นน้ำรอบนิคมอุตสาหกรรม การยกระดับห้องเซิร์ฟเวอร์และระบบไฟฟ้าสำรองให้อยู่เหนือระดับน้ำท่วม รวมถึงการพัฒนาโครงข่ายคมนาคมที่มีความทนทานต่อสภาพอากาศรุนแรง ตลอดจนการนำแนวทางธรรมชาติเป็นฐาน (Nature-based Solutions) เช่น พื้นที่ชุ่มน้ำ หลังคาเขียว และพื้นผิวซึมน้ำ มาเสริมความสามารถในการรับมือกับน้ำหลาก (Laeni, van den Brink, & Arts, 2019)

ภาพที่ 5.11
ประเด็นปัญหาการป้องกันโครงสร้างพื้นฐานของไทย
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

ขณะเดียวกัน หน่วยงานรัฐและสถานพยาบาลขนาดใหญ่ในประเทศไทยต้องเผชิญความท้าทายด้านความปลอดภัยที่ซับซ้อน โรงพยาบาลชั้นนำหลายแห่งนำมาตรฐานสากล

เช่น JCI และ HA มาใช้ในการจัดการสิ่งแวดล้อมทางกายภาพ โดยให้ความสำคัญกับการควบคุมการเข้าถึงพื้นที่อ่อนไหว เช่น ห้องเก็บก๊าซทางการแพทย์ ห้องปฏิบัติการชีวภาพ และระบบไฟฟ้าสำรอง (UPS) ซึ่งต้องได้รับการปกป้องอย่างเข้มงวด ในระดับโครงข่ายพลังงาน หน่วยงานอย่างการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (EGAT) จำเป็นต้องใช้แนวคิดการป้องกันหลายชั้น (defense-in-depth) เพื่อคุ้มครองโรงไฟฟ้าและโครงข่ายส่งไฟฟ้าจากภัยคุกคามทั้งทางกายภาพและไซเบอร์ ท่ามกลางบริบทเมืองที่มีความหนาแน่นสูง เช่น กรุงเทพมหานคร ซึ่งการหยุดชะงักของระบบหนึ่งสามารถกระจายผลกระทบอย่างรวดเร็ว ความท้าทายสำคัญจึงอยู่ที่การสร้างสมดุลระหว่างการคุ้มครองที่เข้มแข็งกับความคาดหวังด้านการเข้าถึงและความเปิดกว้างของสังคมไทย

10. บทบาทบุคลากร ความเป็นมืออาชีพ และกรอบกฎหมายในบริบทไทย

การมี “มนุษย์” อยู่ในระบบรักษาความปลอดภัยยังคงเป็นองค์ประกอบที่เทคโนโลยีไม่อาจทดแทนได้อย่างสมบูรณ์ เจ้าหน้าที่รักษาความปลอดภัยทำหน้าที่ทั้งเป็นเครื่องยับยั้งเชิงสัญลักษณ์ผ่านการปรากฏตัวที่มองเห็นได้ เป็นผู้สังเกตการณ์ที่ตรวจจับความผิดปกติ เป็นผู้ตอบสนองเบื้องต้นเมื่อเกิดเหตุฉุกเฉิน และในหลายกรณียังทำหน้าที่ด้านบริการลูกค้า เช่น การให้ข้อมูล การจัดการความขัดแย้ง และการบังคับใช้นโยบายขององค์กร อย่างไรก็ตาม ประสิทธิผลของบทบาทเหล่านี้ขึ้นอยู่กับคุณภาพการฝึกอบรม ขอบเขตอำนาจหน้าที่ที่ชัดเจน และการบูรณาการเข้ากับระบบเทคโนโลยีและกระบวนการปฏิบัติงาน หากขาดการกำกับดูแลที่เหมาะสม บุคลากรที่ไม่ได้รับการฝึกฝนหรือขาดมาตรฐานอาจกลายเป็นความเสี่ยงมากกว่าจะเป็นทรัพยากรด้านความมั่นคงปลอดภัย

ความเป็นมืออาชีพและจริยธรรมจึงเป็นรากฐานสำคัญของงานรักษาความปลอดภัย พฤติกรรมที่ไม่เหมาะสม เช่น การใช้กำลังเกินสมควร ความหยาบคาย การเลือกปฏิบัติ หรือการทุจริต ไม่เพียงกระทบภาพลักษณ์องค์กร แต่ยังบ่อนทำลายความชอบธรรม (legitimacy) และความร่วมมือจากประชาชน แนวคิดการจัดการความมั่นคงปลอดภัยสมัยใหม่จึงเน้นการพัฒนาทักษะด้านการสื่อสาร การระงับข้อพิพาทโดยสันติ การเคารพสิทธิขั้นพื้นฐาน หลักความได้สัดส่วน (proportionality) และความรับผิดรับชอบตรวจสอบได้ (accountability) ควบคู่กับการฝึกอบรมต่อเนื่องเพื่อให้บุคลากรสามารถใช้เทคโนโลยีใหม่และปฏิบัติตามขั้นตอนฉุกเฉินได้อย่างถูกต้อง

ในประเทศไทย ธุรกิจรักษาความปลอดภัยอยู่ภายใต้กรอบกฎหมายที่ชัดเจน โดยพระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. 2558 กำหนดให้พนักงานรักษาความปลอดภัยต้องผ่านการฝึกอบรมและได้รับใบอนุญาตก่อนปฏิบัติหน้าที่ เพื่อยกระดับ

มาตรฐานวิชาชีพและสร้างความเชื่อมั่นต่อสาธารณะ นอกจากนี้ การใช้เทคโนโลยี เช่น กล้องวงจรปิดและระบบไบโอเมตริกซ์ ต้องสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) ซึ่งกำหนดให้ผู้ควบคุมข้อมูลต้องแจ้งวัตถุประสงค์การเก็บข้อมูล มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล และห้ามนำข้อมูลไปใช้หรือเผยแพร่โดยไม่ได้รับอนุญาต มิฉะนั้นอาจมีทั้งโทษทางแพ่ง อาญา และทางปกครอง (Trimek, 2016)

แนวโน้มปัจจุบันของบริษัทรักษาความปลอดภัยในไทยคือการใช้โมเดลผสมผสานระหว่างกำลังคนกับเทคโนโลยี เช่น การให้เจ้าหน้าที่ปฏิบัติงานควบคู่กับระบบ CCTV ระบบแจ้งเตือนอัตโนมัติ และการประสานงานกับตำรวจหรือหน่วยงานรัฐแบบเรียลไทม์ ความท้าทายจึงไม่ได้อยู่เพียงการมีบุคลากรเพียงพอ แต่คือการสร้าง “บุคลากรอาชีพ” ที่เข้าใจทั้งมิติทางเทคนิค กฎหมาย และจริยธรรม เพื่อให้การรักษาความปลอดภัยทางกายภาพในบริบทไทยมีความสมดุลระหว่างประสิทธิภาพ ความชอบธรรม และการเคารพสิทธิของประชาชน (Anderson & McAtamney, 2011)

ภาพที่ 5.12
การบูรณาการความมั่นคงปลอดภัยทางกายภาพกับการบริหารความเสี่ยง
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

11. บทสรุป (Conclusion)

บทนี้แสดงให้เห็นอย่างชัดเจนว่า การรักษาความปลอดภัยทางกายภาพและการปกป้องทรัพย์สินไม่ใช่เพียงการติดตั้งอุปกรณ์ราคาแพงหรือเพิ่มจำนวนเจ้าหน้าที่ หากแต่เป็น “ศาสตร์และศิลป์แห่งการออกแบบพื้นที่” ให้ทำหน้าที่ปกป้องผู้คนและทรัพย์สินอย่าง

แนบเนียนและมีประสิทธิภาพ ภาพยนตร์ *Ocean's Eleven* เตือนเราว่า ระบบที่ดูแข็งแกร่งที่สุดอาจพ่ายแพ้ได้ หากการออกแบบมีความคาดเดาได้ แยกส่วน และขาดการบูรณาการ ในทางกลับกัน หากองค์กรเข้าใจหลัก 4D ได้แก่ การยับยั้ง (Deterrence) การหน่วงเหนี่ยว/ประวิงเวลา (Delay) การตรวจจับ (Detection) และการตอบสนองหรือป้องกัน (Response/Defense) พร้อมบูรณาการเทคโนโลยี เช่น AI เข้ากับการออกแบบเชิงพื้นที่อย่างเป็นระบบ พื้นที่เองจะกลายเป็น "ผู้พิทักษ์" ที่ทำงานอยู่ตลอดเวลาโดยไม่ต้องแสดงตัวอย่างโจ่งแจ้ง

หัวใจของความมั่นคงปลอดภัยที่ยั่งยืนอยู่ที่การสร้าง "ชั้นของการป้องกัน" (Defense-in-Depth) กระจายมาตรการไปยังแนวเขตรอบนอก เปลือกอาคาร พื้นที่ภายใน และโซนจำกัดสิทธิ์ เพื่อให้ความล้มเหลวของชั้นหนึ่งไม่ทำให้ทั้งระบบพังทลาย หลัก CPTED ย้ำเตือนว่า การออกแบบสิ่งแวดล้อมมีอิทธิพลต่อพฤติกรรมมนุษย์ การเฝ้าระวังตามธรรมชาติ การควบคุมการเข้า–ออก การเสริมสร้างอาณาเขต การดูแลรักษา และการสนับสนุนกิจกรรม ล้วนช่วยลดโอกาสการก่อเหตุโดยไม่บั่นทอนการใช้งานตามปกติ ขณะเดียวกัน เทคโนโลยีควบคุมการเข้าออก ตั้งแต่กุญแจกลไกไปจนถึงไบโอเมตริกซ์และการพิสูจน์ตัวตนหลายปัจจัย ต่างมีข้อแลกเปลี่ยนด้านความสะดวก ต้นทุน และระดับความปลอดภัย ซึ่งต้องเลือกใช้ให้เหมาะกับบริบทขององค์กร

ในบริบทประเทศไทย การออกแบบความมั่นคงปลอดภัยต้องคำนึงถึงปัจจัยเฉพาะ เช่น ความหนาแน่นของกรุงเทพมหานคร การขยายตัวของกล้องวงจรปิดในเมืองใหญ่ การยกระดับมาตรการรักษาความปลอดภัยหลังเหตุการณ์ความไม่สงบในอดีต ตลอดจนความเปราะบางจากอุทกภัยที่กระทบโครงสร้างพื้นฐานวิกฤต บทเรียนจากน้ำท่วมปี 2554 สะท้อนว่า "ความยืดหยุ่นและการฟื้นตัว" เป็นส่วนหนึ่งของการออกแบบทางกายภาพ ไม่ใช่เรื่องเสริมท้าย นอกจากนี้ วัฒนธรรมไทยที่ให้คุณค่ากับความเปิดกว้างและการต้อนรับ ยังทำให้การรักษาความปลอดภัยต้องหาจุดสมดุลระหว่างการปกป้องกับการเข้าถึง เพราะการเสริมกำแพงมากเกินไปอาจบั่นทอนความไว้วางใจและความเป็นชุมชน

ท้ายที่สุด เทคโนโลยีเพียงอย่างเดียวไม่อาจสร้างความปลอดภัยได้ หากปราศจากบุคลากรที่ได้รับการฝึกอบรม วัฒนธรรมองค์กรที่ให้ความสำคัญกับความรับผิดชอบ และการบูรณาการระบบอย่างชาญฉลาด บทเรียนจาก *Ocean's Eleven* ไม่ได้สอนให้เราหวาดกลัวช่องโหว่ แต่สอนให้เรา "มองเห็น" ความเสี่ยงก่อนที่ผู้อื่นจะมองเห็นมัน และออกแบบสภาพแวดล้อมให้ตอบสนองต่อความเสี่ยงนั้นอย่างรอบด้าน สำหรับองค์กรไทยที่ดำเนินงานท่ามกลางบริบททางสังคมและสิ่งแวดล้อมที่ซับซ้อน การรักษาความปลอดภัยที่ดี

จึงต้องสร้างพื้นที่ที่ปลอดภัยและเป็นมิตรในเวลาเดียวกัน กล่าวคือ ควบคุมได้แต่ไม่อึดอัด เปิดกว้างแต่ไม่เปราะบาง

"The best security doesn't announce itself—it embeds itself in the environment so naturally that threats are deterred before they even begin."

12. คำถามทบทวน (Review Questions)

1. จากกรณีศึกษาในภาพยนตร์ *Ocean's Eleven* บทเรียนสำคัญที่เกี่ยวข้องกับ "ความคาดเดาได้ (Predictability)" และ "การบูรณาการระบบ (Integration)" มีความหมายอย่างไรต่อการออกแบบระบบรักษาความปลอดภัยทางกายภาพในองค์กรจริง?

2. อธิบายหลักการ 4D (Deterrence, Detection, Delay, Response/Defense) และวิเคราะห์ว่าหากขาดองค์ประกอบใดองค์ประกอบหนึ่ง ระบบรักษาความปลอดภัยจะเกิดจุดอ่อนในลักษณะใด?

3. เปรียบเทียบแนวคิด Defense-in-Depth กับหลักการ CPTED ในแง่ของบทบาท "การออกแบบพื้นที่" ต่อการลดความเสี่ยง และยกตัวอย่างการประยุกต์ใช้ในบริบทประเทศไทย?

4. เทคโนโลยีควบคุมการเข้า–ออก (Access Control) เช่น บัตร RFID, Biometrics และ Multi-Factor Authentication มีข้อดีและข้อจำกัดแตกต่างกันอย่างไร และองค์กรควรพิจารณาปัจจัยใดก่อนเลือกใช้งาน?

5. ในบริบทประเทศไทย เหตุการณ์น้ำท่วมปี 2554 และความหนาแน่นของกรุงเทพมหานครสะท้อนความสำคัญของแนวคิด "Resilience" และ "Critical Infrastructure Protection" อย่างไรต่อการออกแบบความมั่นคงปลอดภัยทางกายภาพ?

13. เอกสารอ้างอิง (References)

Anderson, J., & McAtamney, A. (2011). Considering local context when evaluating a closed circuit television system in public spaces. *Trends & Issues in Crime and Criminal Justice, 430*, 1–9. Australian Institute of Criminology.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Cozens, P., Babb, C., & Stefani, D. (2023). Exploring and developing crime prevention through environmental design (CPTED) audits: An iterative process. *Crime Prevention and Community Safety, 25*, 1–19. https://doi.org/10.1057/s41300-022-00170-0

El Bouhissi, H., & Yurko, P. (2025). Analysis of biometric access control systems. *Computer Systems and Information Technologies, 2*, 87–96. https://doi.org/10.31891/csit-2025-2-10

Jos, D. A. M., Dupski, D. S., & Amilkar, K. (2024). Framework for Security Risk Assessment (FSRA) and Fuzzy Risk Inference System (FRIS) based on standard ISO/IEC 27002:2022. *Revista de Informática Teórica e Aplicada, 31*(2), 43–55. https://doi.org/10.22456/2175-2745.136309

Laeni, N., van den Brink, M., & Arts, J. (2019). Is Bangkok becoming more resilient to flooding? A framing analysis of Bangkok's flood resilience policy combining insights from both insiders and outsiders. *Cities, 90*, 157–167. https://doi.org/10.1016/j.cities.2019.02.002

Lee, J. S., Park, S., & Jung, S. (2016). Effect of crime prevention through environmental design (CPTED) measures on active living and fear of crime. *Sustainability, 8*(9), 872. https://doi.org/10.3390/su8090872

Lee, S., Lee, C., Nam, J. W., Moudon, A. V., & Mendoza, J. (2023). Street environments and crime around low-income and minority schools: Adopting an environmental audit tool to assess crime prevention through environmental design (CPTED). *Landscape and Urban Planning, 232*, 104676. https://doi.org/10.1016/j.landurbplan.2022.104676

Marks, D. (2016). *"It is built against nature": Floodwalls built after the 2011 floods in Central Thailand* (Research report). Thailand Development Research Institute.

Mofidi, F., Hounsinou, S. G., & Bloom, G. (2024, January). *L-IDS: A multi-layered approach to ransomware detection in IoT*. In *2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE. https://doi.org/10.1109/CCWC60891.2024.10427870

Newman, O. (1972). *Defensible space: Crime prevention through urban design*. Macmillan.

Senna, I., Iglesias, F., & Matsunaga, L. H. (2025). Measuring the effects of Crime Prevention Through Environmental Design (CPTED) on fear of crime in public spaces. *Crime Prevention and Community Safety, 27*, 1–17. https://doi.org/10.1057/s41300-025-00223-0

Trimek, J. (2016). Bangkokians' confidence in Bangkok Metropolitan Administration (BMA)'s CCTV. *Rangsit Journal of Social Sciences and Humanities, 3*(2), 13–26.

Wilson, J. Q., & Kelling, G. L. (1982, March). Broken windows: The police and neighborhood safety. *The Atlantic Monthly, 249*(3), 29–38.