SMA1202

SECURITY: THEORY AND PRACTICE

หลักการและทฤษฎีความมั่นคงปลอดภัย

CHAPTER 2
FOUNDATIONS AND THEORIES OF SECURITY

ผศ.ดร.หทัยพันธน์ สุนทรพิพิธ

Asst.Prof.Hathaipan Soonthornpipit, Ph.D.

บทที่ 2
พื้นฐานและทฤษฎีความมั่นคงปลอดภัย
(Foundations and Theories of Security)

1. บทนำ (Introduction)

ความโกลาหล ความเป็นระเบียบ และตรรกะของการรักษาความมั่นคงปลอดภัย (Chaos, Order, and the Logic of Security)

ในภาพยนตร์แอคชั่นระทึกขวัญระดับตำนานอย่าง *The Dark Knight* (2008) เมืองก๊อตแธม (Gotham City) กลายเป็นสนามทดลองความเชื่อของตัวละคร “โจ๊กเกอร์” (The Joker) ผู้ซึ่งนิยามตนเองว่าเป็น “ตัวแทนแห่งความโกลาหล” (Agent of Chaos) สิ่งที่ทำให้โจ๊กเกอร์น่าสะพรึงกลัวไม่ใช่เพียงพฤติกรรมที่คาดเดาไม่ได้ แต่คือความเข้าใจอย่างลึกซึ้งใน “ระบบ” และความสามารถในการฉวยโอกาสจากจุดอ่อนของสถาบัน องค์กร กิจวัตรของมนุษย์ และตรรกะของการรักษาความมั่นคงปลอดภัยที่เปราะบาง ฉากเปิดเรื่องที่เป็นการปล้นธนาคารที่ควบคุมโดยมาเฟียไม่ได้เริ่มต้นด้วยการใช้กำลังป่าเถื่อน แต่เป็นผลงานชิ้นเอกของการคำนวณที่แม่นยำ โจ๊กเกอร์วางแผนให้เพื่อนร่วมทีมแต่ละคนสังหารกันเองตามลำดับเพื่อลดส่วนแบ่ง และใช้รถโรงเรียนสีเหลืองที่ดูธรรมดาทั่วไปแฝงตัวเข้าไปในขบวนรถที่เหมือนกันเพื่อหลบหนีอย่างแนบเนียน

เมื่อโจ๊กเกอร์กล่าวกับอัยการเมืองก๊อตแธม ฮาร์วีย์ เดนท์ ว่า “ไม่มีใครตื่นตระหนกตราบเท่าที่ทุกอย่างเป็นไปตามแผน แม้ว่าแผนนั้นจะน่าสยดสยองเพียงใดก็ตาม” (“Nobody panics when things go ‘according to plan.’ Even if the plan is horrifying,” *The Dark Knight*, 2008) เขากำลังวิเคราะห์จิตวิทยาความมั่นคงที่สำคัญอย่างยิ่ง นั่นคือมนุษย์มักยอมรับความเสี่ยงตราบเท่าที่รู้สึกว่า “ระบบยังถูกจัดการอยู่” แม้ว่าการจัดการนั้นจะเป็นเพียงภาพลวงตาก็ตาม บทเรียนจากภาพยนตร์เรื่องนี้สะท้อนสัจธรรมในโลกการทำงานจริงว่า ภัยคุกคามมักไม่ได้เกิดขึ้นโดยบังเอิญ แต่เกิดจากการฉวยโอกาสผ่าน “กิจวัตรประจำวัน” (Routines) การเฝ้าระวังที่ขาดประสิทธิภาพ (Weak Guardianship) และความบกพร่องในระบบธรรมาภิบาล (Flawed Governance)

ในโลกความเป็นจริง เหตุการณ์การเจาะข้อมูลครั้งใหญ่ของบริษัท Target ในปี 2013 เป็นตัวอย่างที่ชัดเจน โดยผู้ร้ายไม่ได้เจาะระบบผ่านกำแพงไฟที่ซับซ้อน แต่ใช้จุดอ่อนในสิทธิการเข้าถึงของบริษัทรับเหมาภายนอก (Third-party vendor) ซึ่งเป็นจุดบอดเชิงระบบที่ถูกมองข้าม สำหรับประเทศไทย สถานการณ์ความปลอดภัยไซเบอร์ในปี 2024-2025 ยิ่งตอกย้ำความสำคัญของเรื่องนี้ เมื่อสถิติระบุว่ามีการโจมตีเกิดขึ้นเฉลี่ย 3,180 ครั้งต่อสัปดาห์ ซึ่งสูงกว่าค่าเฉลี่ยทั่วโลกถึงร้อยละ 70 วิกฤตนี้ไม่ได้เกิดจาก

ปัญหาเชิงเทคนิคเพียงอย่างเดียว แต่เกิดจากความล้มเหลวในการตระหนักถึงความเสี่ยง การขาดนโยบายที่บูรณาการ และการทำงานที่เป็นเอกเทศของหน่วยงานรักษาความมั่นคง

ภาพที่ 2.1

ฉากการสอบสวนระหว่าง Batman และ The Joker จากภาพยนตร์ *The Dark Knight*

ที่มา: Warner Bros. Pictures (2008)

บทเรียนที่สำคัญที่สุดสำหรับนักศึกษาและผู้บริหารด้านการรักษาความมั่นคงปลอดภัยคือ “การรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพนั้นไม่ใช่เรื่องบังเอิญ แต่มัน

คือเรื่องของทฤษฎี" (Effective security is not accidental—it is theoretical) หากปราศจากรากฐานทางทฤษฎีที่มั่นคง มาตรการรักษาความมั่นคงปลอดภัยจะกลายเป็นเพียงการตอบสนองต่อปัญหาเฉพาะหน้าอย่างกระจัดกระจายและไร้ทิศทาง บทนี้จึงมุ่งเน้นการปูพื้นฐานทางความคิดเพื่อให้เข้าใจว่าเหตุใดภัยคุกคามจึงเกิดขึ้น เราจะออกแบบระบบป้องกันอย่างไรให้มีประสิทธิภาพ และเราจะสร้างความยืดหยุ่นให้แก่องค์กรในโลกที่เต็มไปด้วยความไม่แน่นอนได้อย่างไร

2. ความสำคัญของทฤษฎีต่อการจัดการรักษาความมั่นคงปลอดภัย (Why Theory Matters in Security Management)

บ่อยครั้งที่ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยมักพึ่งพา "ประสบการณ์" และ "สัญชาตญาณ" เป็นหลักในการตัดสินใจ แม้ว่าความรู้ในทางปฏิบัติจะเป็นสิ่งที่มีความสำคัญอย่างมาก แต่ทฤษฎีคือสิ่งที่ให้ "โครงสร้าง" (Structure) และ "ความสามารถในการทำนาย" (Predictability) แก่ระบบรักษาความมั่นคงปลอดภัย ทฤษฎีช่วยให้เราก้าวข้ามการมองเห็นเพียง "สิ่งที่เกิดขึ้น" ไปสู่การเข้าใจว่า "ทำไมมันจึงเกิดขึ้น" โดยทั่วไปทฤษฎีด้านความมั่นคงปลอดภัยจะช่วยตอบคำถามพื้นฐาน 3 ประการ:

1. เหตุใดเหตุการณ์ด้านความมั่นคงปลอดภัยหรืออาชญากรรมจึงเกิดขึ้นในบริบทนั้น ๆ?

2. ภายใต้เงื่อนไขหรือปัจจัยแวดล้อมใดที่ความเสี่ยงจะมีโอกาสกลายเป็นเหตุการณ์จริงมากที่สุด?

3. องค์กรสามารถแทรกแซงหรือปรับเปลี่ยนปัจจัยใดเพื่อป้องกันเหตุการณ์ได้อย่างมีประสิทธิภาพและคุ้มค่าที่สุด?

หากปราศจากทฤษฎี การลงทุนในระบบรักษาความปลอดภัยอาจกลายเป็นเพียง "ละครแห่งการรักษาความปลอดภัย" (Security Theater) ซึ่งหมายถึงมาตรการที่สร้างภาพลักษณ์ให้ดูปลอดภัยแต่ไม่ได้ลดความเสี่ยงจริงอย่างมีนัยสำคัญ ตัวอย่างเช่น การตรวจกระเป๋าที่ทางเข้าห้างสรรพสินค้าที่พนักงานเพียงแค่ใช้ไม้แตะหรือมองผ่าน ๆ โดยไม่ได้มีการตรวจสอบอย่างเป็นระบบ มาตรการนี้อาจช่วยลดความกังวลของลูกค้าได้ในระยะสั้น แต่ผู้ร้ายที่มีการเตรียมตัวมาอย่างดีย่อมมองเห็นจุดอ่อนนี้ได้โดยง่าย

ในบริบทของประเทศไทยที่องค์กรต้องเผชิญกับข้อจำกัดที่หลากหลาย ด้านงบประมาณและกฎระเบียบที่เข้มงวด เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ การใช้ทฤษฎีเป็นฐานในการตัดสินใจจะช่วยสร้าง "ความชอบธรรม" (Legitimacy) และ "ความเป็นวิชาชีพ" (Professionalism) การเสนอของบประมาณโดยอ้างอิงทฤษฎีการป้องกันอาชญากรรมด้วย

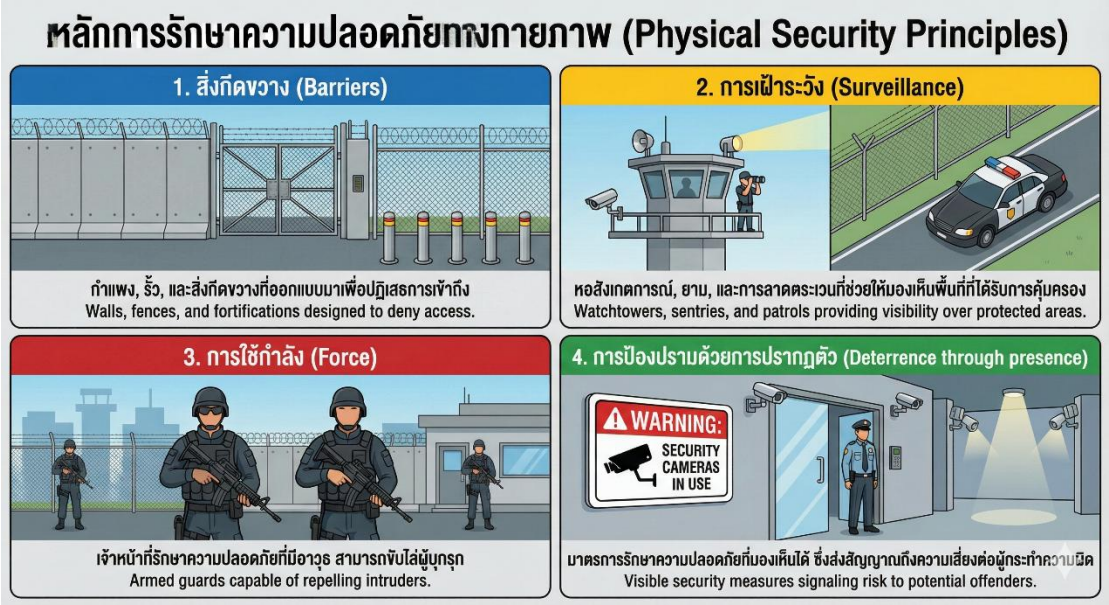
การออกแบบสภาพแวดล้อม (CPTED) จะมีน้ำหนักมากกว่าการอ้างเพียงความต้องการส่วนตัวของหัวหน้างาน

3. ทฤษฎีความมั่นคงแบบดั้งเดิม (Classical Security Theories)

รากฐานดั้งเดิมของทฤษฎีความมั่นคงเติบโตมาจากระบบความสัมพันธ์ระหว่างประเทศแบบเวสต์ฟาเลีย (Westphalian System) ซึ่งให้ความสำคัญกับ “รัฐ” (State) ในฐานะตัวละครหลักเพียงหนึ่งเดียว ความมั่นคงปลอดภัยในยุคนี้ถูกนิยามผ่านมุมมองของสัจนิยม (Realism) ซึ่งมีสมมติฐานหลักว่าโลกอยู่ในสภาวะอนาธิปไตย (Anarchy) คือไม่มีอำนาจเหนือรัฐใด ๆ ที่จะมาคอยดูแลความเรียบร้อยได้ ทำให้แต่ละรัฐต้องพึ่งพาตนเอง (Self-help) เพื่อความอยู่รอด

3.1 แนวคิดสัจนิยมเชิงโครงสร้างและความขัดแย้งเชิงอำนาจ (Security as Protection)

เคนเน็ธ วอลซ์ (Kenneth Waltz) ผู้นำแนวคิดสัจนิยมเชิงโครงสร้าง (Neorealism) อธิบายว่าโครงสร้างของระบบระหว่างประเทศบังคับให้รัฐต้องสะสมกำลังทหารและอำนาจเพื่อป้องกันตนเอง สิ่งนี้ก่อให้เกิด “ภาวะกลืนไม่เข้าคายไม่ออกด้านความมั่นคงปลอดภัย” (Security Dilemma) ซึ่งหมายถึงสถานการณ์ที่รัฐหนึ่งเสริมสร้างกำลังทหารเพื่อความปลอดภัยของตนเอง แต่อีกรัฐหนึ่งกลับมองว่าเป็นการคุกคาม จึงต้องเสริมสร้างกำลังทหารตาม เกิดเป็นวงจรการสะสมอาวุธที่ไม่มีสิ้นสุด (Waltz, 1979)



ภาพที่ 2.2

หลักการรักษาความปลอดภัยทางกายภาพ

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

ในขณะที่ จอห์น เมียร์ไชเมอร์ (John Mearsheimer) ผู้นำแนวคิดสัจนิยมเชิงรุก (Offensive Realism) มองว่ารัฐที่สมเหตุสมผลจะพยายามขยายอำนาจให้ได้มากที่สุดเท่าที่จะเป็นไปได้ โดยเป้าหมายสูงสุดคือการเป็นมหาอำนาจระดับภูมิภาค (Hegemon) เพื่อรับประกันความอยู่รอดของตนเอง ความมั่นคงปลอดภัยในมุมมองนี้จึงเป็นเรื่องของ “การทหาร” และ “อาณาเขต” เป็นหลัก ซึ่งสะท้อนผ่านการจัดตั้งกองทัพที่เข้มแข็ง การสร้างพันธมิตรทางทหาร และการป้องกันพรมแดน (Mearsheimer, 2001)

3.2 ความมั่นคงในฐานะความเป็นระเบียบเรียบร้อย (Order and Stability)

อีกแง่มุมหนึ่งของความมั่นคงคลาสสิกคือการมองว่าความมั่นคงคือ “ความเป็นระเบียบ” (Order) โทมัส ฮอบส์ (Thomas Hobbes) ได้อธิบายในหนังสือ Leviathan ว่าหากปราศจากอำนาจส่วนกลางหรือ “องค์อธิปัตย์” มนุษย์จะตกอยู่ในสภาวะสงครามของทุกคนต่อทุกคน (War of all against all) ความมั่นคงปลอดภัยจึงเกิดขึ้นเมื่อบุคคลยอมสละเสรีภาพบางส่วนให้แก่รัฐเพื่อแลกกับการได้รับความคุ้มครอง (Hobbes,1998)

สำหรับสังคมไทย แนวคิดนี้สอดคล้องกับคุณค่าเรื่อง “ความสงบสุข” (รักสันติ) และการรักษาความสามัคคีในชาติ เหตุการณ์ความวุ่นวายทางการเมืองในกรุงเทพมหานครช่วงปี 2553 และ 2557 เป็นบทเรียนสำคัญที่แสดงให้เห็นว่า เมื่อความเป็นระเบียบพื้นฐานของสังคมถูกกระทบ ความรู้สึกไม่มั่นคงจะแผ่ขยายไปทุกภาคส่วน ไม่ว่าจะเป็นภาคการท่องเที่ยวที่จำนวนนักท่องเที่ยวลดลงอย่างรวดเร็ว หรือภาคเศรษฐกิจที่ต้องหยุดชะงักลงเนื่องจากการปิดเส้นทางจราจร

4. แนวคิดความมั่นคงร่วมสมัย (Contemporary Security Concepts)

ตั้งแต่ทศวรรษที่ 1980 เป็นต้นมา ขอบเขตของความมั่นคงได้ขยายตัวออกไปอย่างมหาศาล (Broadening) และลงลึกไปถึงระดับปัจเจกมากขึ้น (Deepening) เนื่องจากภัยคุกคามไม่ได้มีเพียงแค่การสู้รบในสมรภูมิ แต่รวมถึงภัยคุกคามที่ไร้รูปแบบและข้ามพรมแดน

4.1ความมั่นคงของมนุษย์ (Human Security)

แนวคิดความมั่นคงของมนุษย์ได้รับการเสนออย่างเป็นทางการโดยโครงการพัฒนาแห่งสหประชาชาติ (UNDP) ในปี 1994 ซึ่งถือเป็นการเปลี่ยนผ่านครั้งสำคัญ จากการมอง “ความมั่นคงของรัฐ” มาเป็น “ความมั่นคงของคน” ความมั่นคงของมนุษย์ประอบด้วย 7 มิติที่เกื้อกูลกัน:

1. **ความมั่นคงทางเศรษฐกิจ (Economic Security):** การมีรายได้ที่เพียงพอและมั่นคงต่อการดำรงชีวิต

2. **ความมั่นคงทางอาหาร (Food Security):** การเข้าถึงอาหารที่มีคุณค่าทางโภชนาการและปลอดภัย

3. **ความมั่นคงทางสุขภาพ (Health Security):** การป้องกันจากโรคภัยไข้เจ็บและการเข้าถึงระบบสาธารณสุข (ตัวอย่างเช่น วิกฤต COVID-19 ในไทยที่แสดงให้เห็นความเปราะบางของมิตินี้)

4. **ความมั่นคงทางสิ่งแวดล้อม (Environmental Security):** การปกป้องจากมลพิษ ภัยธรรมชาติ และความเสื่อมโทรมของทรัพยากร

5. **ความมั่นคงส่วนบุคคล (Personal Security):** การปลอดภัยจากความรุนแรงทุกรูปแบบ ไม่ว่าจะเป็นจากรัฐหรืออาชญากรรม

6. **ความมั่นคงของชุมชน (Community Security):** การรักษาเอกลักษณ์ทางวัฒนธรรมและความสงบสุขของกลุ่มชาติพันธุ์

7. **ความมั่นคงทางการเมือง (Political Security):** การเคารพสิทธิมนุษยชนและการปราศจากการกดขี่โดยรัฐ

ในสังคมไทยปัจจุบัน ความไม่มั่นคงของมนุษย์มักสะท้อนผ่านปัญหาหนี้สินครัวเรือน (ความไม่มั่นคงทางเศรษฐกิจ) และมลพิษจากฝุ่น PM 2.5 (ความไม่มั่นคงทางสุขภาพและสิ่งแวดล้อม) ซึ่งปัญหาเหล่านี้รัฐไม่สามารถแก้ไขได้ด้วยกองทัพ แต่ต้องอาศัยการบริหารจัดการเชิงนโยบายที่ซับซ้อน

ภาพที่ 2.3

การเปรียบเทียบแนวคิดความมั่นคงแบบดั้งเดิมและความมั่นคงร่วมสมัย

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

4.2 สำนักโคเปนเฮเกนและทฤษฎีการทำให้เป็นประเด็นความมั่นคง (Securitization Theory)

สองนักคิด แบร์รี บูซาน (Barry Buzan) และ โอเล วีเวอร์ (Ole Wæver) แห่งสำนักโคเปนเฮเกน ได้นำเสนอว่าความมั่นคงปลอดภัยไม่ได้เป็นเพียงสถานะที่มีอยู่จริงตามธรรมชาติ (Objective) แต่เป็นสิ่งที่ถูกสร้างขึ้นผ่านกระบวนการสื่อสาร (Securitization) ประเด็นหนึ่งจะกลายเป็น “ประเด็นความมั่นคง” ก็ต่อเมื่อมี “ผู้ประกาศ” (Securitizing Actor) ที่มีอำนาจ สื่อสารไปยัง “ผู้ฟัง” (Audience) ว่าสิ่งนั้นคือภัยคุกคามที่ส่งผลต่อความอยู่รอด (Existential Threat) และจำเป็นต้องใช้มาตรการพิเศษ (Extraordinary Measures) ในการจัดการ (Buzan, Wæver, & de Wilde, 1998)

ตัวอย่างเช่น การที่ประเทศไทยยกระดับปัญหา “แก๊งคอลเซ็นเตอร์” หรือ “ยาเสพติด” ให้เป็นวาระแห่งชาติ ทำให้รัฐสามารถใช้งบประมาณและอำนาจการตรวจค้นหรือระงับบัญชีธนาคารได้รวดเร็วกว่าปกติ อย่างไรก็ตาม ทฤษฎีนี้เตือนให้เราพึงระวังว่า การทำให้ทุกอย่างกลายเป็นเรื่องความมั่นคง (Over-securitization) อาจนำไปสู่การละเมิดสิทธิเสรีภาพและการหลีกเลี่ยงกระบวนการตรวจสอบตามปกติได้

5. สังคมแห่งความเสี่ยงและความไม่แน่นอน (Risk Society and Uncertainty)

นักสังคมวิทยาชาวเยอรมัน อูลริค เบ็ค (Ulrich Beck) ได้เสนอทฤษฎี “สังคมแห่งความเสี่ยง” (Risk Society) ซึ่งเป็นเครื่องมือสำคัญในการทำความเข้าใจภัยคุกคามในศตวรรษที่ 21 ได้อย่างดี เบ็คโต้แย้งว่าสังคมในปัจจุบันกำลังก้าวพ้นจากการเป็น “สังคมอุตสาหกรรม” ที่มุ่งเน้นการกระจายความมั่งคั่ง (Wealth) ไปสู่การเป็นสังคมที่มุ่งเน้นการจัดการ “ผลกระทบข้างเคียง” หรือความเสี่ยง (Risks) ที่เกิดจากการพัฒนาเทคโนโลยีและเศรษฐกิจของเราเอง (Beck, 1992)

5.1 ความเสี่ยงที่มนุษย์สร้างขึ้น (Manufactured Uncertainty)

เบ็คจำแนกความเสี่ยงออกเป็นสองประเภท: ภัยธรรมชาติ (Natural hazards) เช่น น้ำท่วมหรือพายุที่เกิดขึ้นตามวัฏจักร และความเสี่ยงที่มนุษย์สร้างขึ้น (Manufactured risks) ความเสี่ยงประเภทหลังนี้เกิดจากการตัดสินใจของมนุษย์เอง เช่น อุบัติเหตุนิวเคลียร์ การเปลี่ยนแปลงสภาพภูมิอากาศ และวิกฤตการณ์ทางการเงิน คุณลักษณะของความเสี่ยงในโลกสมัยใหม่คือ:

1. คำนวณไม่ได้ (Incalculable): เราไม่สามารถใช้สถิติในอดีตมาทำนายโอกาสเกิดหรือความเสียหายของภัยคุกคามใหม่ ๆ ได้แม่นยำ เช่น ภัยไซเบอร์ในรูปแบบใหม่

2. **ไร้พรมแดน** (Transboundary): ความเสี่ยงสามารถแพร่กระจายไปทั่วโลกโดยไม่สนพรมแดนของประเทศ เช่น โรคระบาด หรือมลพิษข้ามพรมแดน

3. **แก้ไขไม่ได้** (Irreversible): เมื่อเกิดขึ้นแล้ว ความเสียหายนั้นยากเกินกว่าจะกู้คืนสู่สภาพเดิมได้ เช่น การสูญพันธุ์ของสิ่งมีชีวิต หรือการปนเปื้อนของกัมมันตภาพรังสี

5.2 ความรับผิดชอบที่ถูกจัดระบบให้หายไป (Organized Irresponsibility)

ในระบบที่ซับซ้อนและเชื่อมโยงกันอย่างมาก เมื่อเกิดเหตุการณ์ร้ายแรงขึ้น มักจะหาผู้รับผิดชอบที่ชัดเจนไม่ได้ เนื่องจากความล้มเหลวเกิดจากปฏิสัมพันธ์ของหน่วยงานและเทคโนโลยีจำนวนมาก กลายเป็นสภาวะที่ผู้ผลิตปฏิเสธความรับผิดชอบโดยตรงและสังคมก็ไม่รู้จะจัดการอย่างไร นำไปสู่ความไม่มั่นคงในชีวิต โดยเบ็คเรียกสภาวะนี้ว่า “ความไม่รับผิดชอบเชิงระบบ” ในกรณีของประเทศไทย เหตุการณ์สารเคมีระเบิดที่คลองเตยในปี 2534 หรือมหาอุทกภัยปี 2554 เป็นตัวอย่างของความเสี่ยงในสังคมสมัยใหม่ที่แสดงให้เห็นถึงความสับสนในการบริหารจัดการข้อมูลและความรับผิดชอบระหว่างหน่วยงานรัฐที่ซ้ำซ้อนกัน

ด้วยเหตุนี้ การจัดการความมั่นคงปลอดภัยสมัยใหม่จึงต้องเปลี่ยนจากการตั้งเป้าหมาย “กำจัดความเสี่ยงให้หมดไป” (Risk Elimination) ซึ่งเป็นไปไม่ได้ มาเป็นการ “สร้างความยืดหยุ่น” (Resilience) และการเฝ้าระวังอย่างต่อเนื่องแทน

ภาพที่ 2.4

สังคมความเสี่ยง (Risk Society): ลักษณะความเสี่ยงร่วมสมัยในบริบทโลกาภิวัตน์

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

6. ทฤษฎีโอกาสในการก่ออาชญากรรม (Crime Opportunity Theories)

ทฤษฎีกลุ่มนี้ถือเป็นรากฐานสำคัญของการบริหารจัดการความปลอดภัยทางกายภาพและการออกแบบพื้นที่ โดยเชื่อว่าการปรับเปลี่ยน “โอกาส” ในสภาพแวดล้อมมีประสิทธิภาพมากกว่าการพยายามเปลี่ยนนิสัยหรือแรงจูงใจของอาชญากร

6.1 ทฤษฎีหน้าต่างแตก (Broken Windows Theory)

เจมส์ คิว. วิลสัน และ จอร์จ เคลลิง ได้เสนอทฤษฎีนี้ในปี 1982 โดยใช้สัญลักษณ์ของ “กระจกหน้าต่างที่แตก” เพื่ออธิบายว่าสัญญาณของความไม่เป็นระเบียบ (Disorder) และการละเลย (Neglect) ในพื้นที่ใดพื้นที่หนึ่ง จะส่งสัญญาณไปยังชุมชนและอาชญากรว่า “ที่นี่ไม่มีคนดูแล” และจะนำไปสู่การกระทำผิดที่รุนแรงขึ้นเรื่อย ๆ (Wilson & Kelling, 1982) ซึ่งตรรกะนี้มาจากผลการทดลองทางสังคมวิทยาของ ฟิลิป ซิมบาร์โด (Philip Zimbardo) ในปี 1969 เขาจอดรถที่ไม่มีป้ายทะเบียนและเปิดฝากระโปรงทิ้งไว้ในสองพื้นที่: ย่านบรองซ์ (ย่านเสื่อมโทรมในนิวยอร์ก) และย่านพาโล อัลโต (ย่านร่ำรวยในแคลิฟอร์เนีย) ผลปรากฏว่า ในบรองซ์ รถถูกขโมยอะไหล่และทำลายภายในเวลาไม่กี่นาที แต่ในพาโล อัลโต รถจอดนิ่งอยู่เป็นสัปดาห์โดยไม่มีใครแตะต้อง จนกระทั่งซิมบาร์โดตัดสินใจใช้ค้อนทุบรถเสียเอง เมื่อเห็นร่องรอยความเสียหาย ประชาชนที่ดู “สุภาพ” ในย่านนั้นก็เริ่มเข้าร่วมการโจรกรรมทรัพย์สินในรถทันที

นัยสำคัญต่อความมั่นคงปลอดภัย: การปล่อยให้พื้นที่สกปรก มีไฟขาด หรือมีร่องรอยการงัดแงะแล้วไม่รีบแก้ไข คือการเปิดประตูเรียกอาชญากรรม การดูแลความสะอาดและความเป็นระเบียบ (Maintenance) จึงเป็นกลยุทธ์การรักษาความมั่นคงปลอดภัยที่มีต้นทุนต่ำแต่ได้ผลสูง

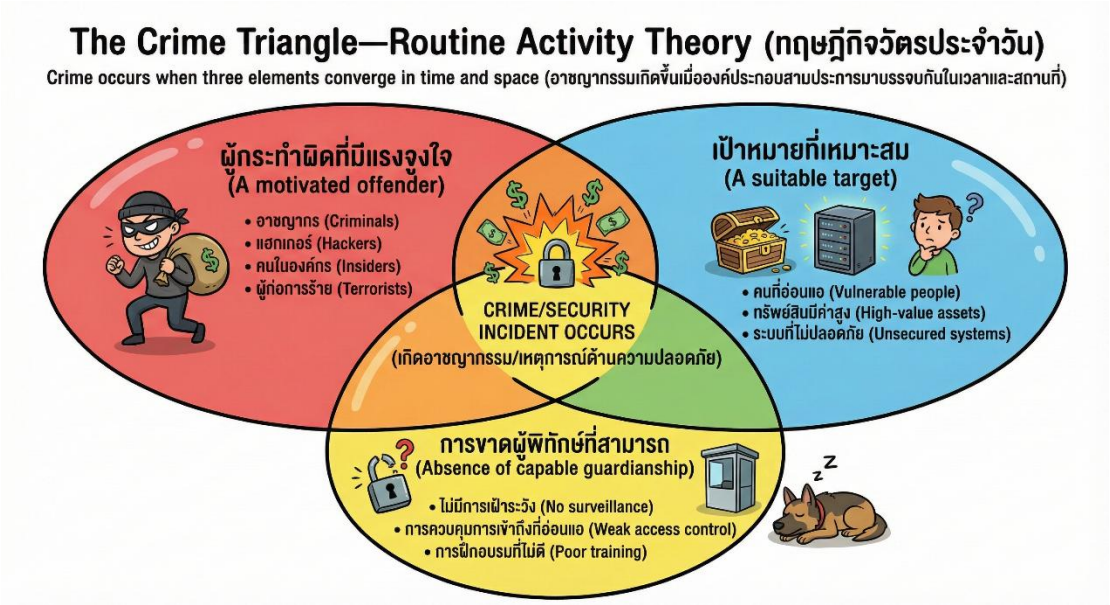
6.2 ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory - RAT)

ลอว์เรนซ์ โคเฮน และ มาร์คัส เฟลสัน (1979) เสนอว่าอาชญากรรมไม่ได้เกิดจากความยากจนเพียงอย่างเดียว แต่เกิดจากโครงสร้างของ “กิจกรรมประจำวัน” ในสังคม โดยอาชญากรรมจะเกิดขึ้นเมื่อองค์ประกอบ 3 ประการบรรจบกันในเวลาและสถานที่เดียวกัน

1. **ผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender):** บุคคลที่มีความตั้งใจและมีความสามารถในการก่อเหตุ

2. **เป้าหมายที่เหมาะสม (Suitable Target):** สิ่งของที่มีค่า ขนย้ายง่าย หรือบุคคลที่ขาดการระวังตัว (เช่น นักเรียนที่ทิ้งโน้ตบุ๊กไว้ในห้องสมุดช่วงสอบ)

3. **การขาดผู้พิทักษ์ที่สามารถ (Absence of Capable Guardian):** การไม่มีตำรวจ ยาม หรือแม้แต่เพื่อนบ้านที่คอยสอดส่อง (Cohen & Felson, 1979)



ภาพที่ 2.5

สามเหลี่ยมอาชญากรรมตามทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory)

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

ในประเทศไทย RAT ช่วยอธิบายว่าเหตุใดการล้วงกระเป๋าจึงเกิดขึ้นมากในรถไฟฟ้าช่วงเร่งด่วน เพราะมีความหนาแน่นของ “เป้าหมาย” และ “ผู้พิทักษ์” (เจ้าหน้าที่) ไม่สามารถมองเห็นเหตุการณ์ได้ทั่วถึงเนื่องจากฝูงชน หรือทำไมการโจรกรรมรถจักรยานยนต์มักเกิดขึ้นในจุดที่มืดและเปลี่ยวหลังเที่ยงคืน ซึ่งเป็นช่วงที่ผู้พิทักษ์ตามธรรมชาติ (คนเดินถนน) หายไป

6.3 ทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory)

ทฤษฎีนี้เชื่อว่าอาชญากรทำ “การคำนวณทางความสุข” (Hedonistic Calculus) คือชั่งน้ำหนักระหว่างผลประโยชน์ที่จะได้รับกับความเสี่ยงที่จะถูกจับและบทลงโทษ นักบริหารความมั่นคงปลอดภัยจึงต้องสร้างมาตรการที่ทำให้ผู้ร้ายรู้สึกว่า “ไม่คุ้มเสี่ยง” หรือต้องใช้ “ความพยายาม” (Effort) มากเกินไป

อย่างไรก็ตาม เราต้องเข้าใจแนวคิด “เหตุผลที่ถูกจำกัด” (Bounded Rationality) ว่าผู้ร้ายมักไม่ได้ตัดสินใจภายใต้ข้อมูลที่สมบูรณ์ แต่อาจตัดสินใจภายใต้ความกดดันหรือข้อมูลที่ผิดพลาด งานวิจัยของ ไรท์ และ เดคเกอร์ (Wright & Decker, 1994) ในการสัมภาษณ์โจรย่องเบาพบว่า พวกเขาเลือกบ้านโดยดูจากสัญญาณง่าย ๆ เช่น ไฟที่ปิดสนิทหรือกองจดหมายหน้าบ้าน มากกว่าการวางแผนที่ซับซ้อน

ภาพที่ 2.6

การประยุกต์ใช้ทฤษฎีกิจวัตรประจำวันสำหรับผู้จัดการด้านความมั่นคงปลอดภัย

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

6.4 ทฤษฎีพื้นที่ป้องกันได้ (Defensible Space Theory)

ออสการ์ นิวแมน (Oscar Newman, 1972) ได้เสนอแนวคิดนี้หลังจากการสังเกตความล้มเหลวของโครงการที่อยู่อาศัย พรูอิตต์-ไอโก (Pruitt-Igoe) ในเมืองเซนต์หลุยส์ ซึ่งเป็นอาคารสูงที่ไม่มีการแบ่งโซนพื้นที่ชัดเจน ทำให้ผู้อยู่อาศัยไม่รู้สึกเป็นเจ้าของพื้นที่ส่วนกลางและไม่ช่วยดูแลความปลอดภัย ทั้งนี้ นิวแมนเสนอหลักการ 4 ข้อ

1. **ความเป็นเจ้าของอาณาเขต (Territoriality):** การใช้รั้ว ป้าย หรือการออกแบบเพื่อแสดงว่าพื้นที่นี้มี “เจ้าของ”

2. **การเฝ้าสังเกตตามธรรมชาติ (Natural Surveillance):** การวางตำแหน่งหน้าต่างและทางเข้าให้คนภายในมองเห็นภายนอกได้ง่าย

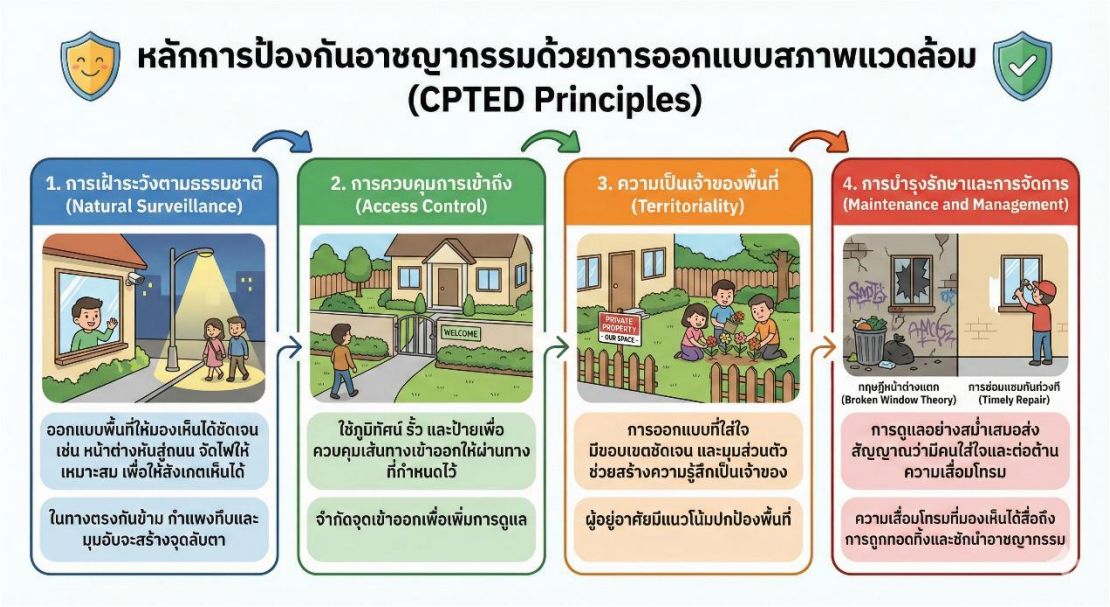
3. **ภาพลักษณ์ (Image):** การออกแบบที่ไม่ให้ดูเหมือน “แหล่งเสื่อมโทรม” ซึ่งจะดึงดูดอาชญากร

4. **บริบทแวดล้อม (Milieu):** การตั้งอยู่ใกล้กับพื้นที่ที่ปลอดภัยและมีกิจกรรมสม่ำเสมอ

6.5 การป้องกันอาชญากรรมด้วยการออกแบบสภาพแวดล้อม (CPTED)

CPTED คือการนำทฤษฎีพื้นที่ป้องกันได้มาประยุกต์ใช้ในระดับสากล โดยเน้นการออกแบบสภาพแวดล้อมที่ลดโอกาสการเกิดอาชญากรรมและลดความกลัวภัย ในกรุงเทพมหานคร ได้มีการนำหลักแนวคิด CPTED มาใช้อย่างเห็นได้ชัดในการออกแบบ

สวนสาธารณะสมัยใหม่ เช่น “อุทยาน 100 ปี จุฬาลงกรณ์มหาวิทยาลัย” ที่มีการกระจายห้องเรียนและพื้นที่กิจกรรมไว้รอบสวนเพื่อสร้าง “ความเคลื่อนไหว” (Activity Support) และการใช้รั้วที่โปร่งเพื่อให้เกิดการมองเห็นจากภายนอกสวน (Natural Surveillance) ซึ่งช่วยลดความเสี่ยงจากการถูกจี้ปล้นในจุดอับ



ภาพที่ 2.7

หลักการป้องกันอาชญากรรมด้วยการออกแบบสภาพแวดล้อม

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

6.6 การป้องกันอาชญากรรมตามสถานการณ์ (Situational Crime Prevention - SCP)

แนวคิดนี้พัฒนาโดยโรนัลด์ คลาร์ก (Ronald Clarke) โดยมุ่งเน้นที่การลดโอกาสในการก่ออาชญากรรม แทนที่จะพยายามเปลี่ยนแรงจูงใจของผู้กระทำผิด ทั้งนี้ SCP ตระหนักว่าการพยายามฟื้นฟูผู้กระทำผิดหรือแก้ไขสาเหตุรากฐาน (เช่น ความยากจน การว่างงาน ความผิดปกติในครอบครัว) เป็นเรื่องที่ทำได้ยาก ล่าช้า และไม่แน่นอน ดังนั้น SCP จึงมุ่งเป้าไปที่ปัจจัยสถานการณ์เฉพาะหน้าที่เอื้อให้เกิดอาชญากรรม ซึ่งเป็นแนวทางที่ปฏิบัติได้จริงและมุ่งผลลัพธ์ (Clarke, 1997)

SCP ได้รับอิทธิพลทางทฤษฎีจาก “ทฤษฎีการเลือกอย่างมีเหตุผล” ซึ่งตั้งสมมติฐานว่าผู้กระทำผิดตัดสินใจโดยการวิเคราะห์ต้นทุนและผลประโยชน์ แม้ว่าความมีเหตุผลนั้นอาจไม่สมบูรณ์ก็ตาม (Eck & Clarke, 2019) ผู้กระทำผิดจะพิจารณาถึงความพยายามที่ต้องใช้ ความเสี่ยงที่เกี่ยวข้อง ผลตอบแทนที่คาดว่าจะได้ สิ่งยั่วยุที่เผชิญ และข้ออ้างที่มี ก่อนที่

จะลงมือก่ออาชญากรรม การแทรกแซงของ SCP จึงมุ่งจัดการปัจจัยในการตัดสินใจเหล่านี้ เพื่อทำให้การก่ออาชญากรรมดูไม่น่าสนใจหรือได้ประโยชน์น้อยลง

ทั้งนี้ โรนัลด์ คลาร์ก ได้รวบรวมเทคนิคที่ใช้ในการลดโอกาสการเกิดอาชญากรรมออกมาเป็น 25 เทคนิค ภายใต้ 5 กลยุทธ์หลักตามภาพที่ 2.8

ภาพที่ 2.8

กลยุทธ์การป้องกันอาชญากรรมตามสถานการณ์: 5 กลยุทธ์หลัก 25 เทคนิค

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

การประยุกต์ใช้ SCP ในไทยที่เห็นได้ชัดคือ ระบบรถไฟฟ้า BTS/MRT ที่ใช้ประตูกั้นชานชาลา (Increase Effort/Risk) และการใช้กล้องวงจรปิดจำนวนมากร่วมกับระบบ AI เพื่อตรวจจับพฤติกรรมผิดปกติ (Increase Risk) เป็นต้น

7. กลยุทธ์การรักษาความมั่นคง: การป้องปราม การป้องกัน และความยืดหยุ่น

ในการจัดการความมั่นคงเชิงกลยุทธ์ เราสามารถแบ่งแนวทางการปฏิบัติออกเป็น 3 มิติสำคัญที่ต้องบูรณาการเข้าด้วยกันเพื่อให้เกิดความมั่นคงปลอดภัยที่ครอบคลุม

7.1 การป้องปราม (Deterrence): การสกัดกั้นผ่านความกังวล

ทฤษฎีการป้องปราม (Deterrence Theory) มีรากฐานมาจากแนวคิดของ เซซาเร เบคคาเรีย (1764) และ เจเรมี เบนแธม (1789) โดยมีสมมติฐานว่ามนุษย์คือ “สัตว์

เศรษฐกิจ” (Homo Economicus) ที่จะหลีกเลี่ยงการทำผิดหากทราบว่าบทลงโทษนั้นไม่คุ้มค่า องค์ประกอบของการป้องปรามที่มีประสิทธิภาพประกอบด้วย 3 ส่วน:

1. **ความแน่นอน (Certainty):** ผู้กระทำผิดต้องเชื่อมั่นว่า “ทำผิดแล้วต้องโดนจับได้แน่ ๆ” มีการศึกษามากมายยืนยันว่าความแน่นอนมีผลต่อการป้องปรามมากกว่าความรุนแรงของโทษ

2. **ความรุนแรง (Severity):** บทลงโทษต้องหนักพอที่จะกลบผลประโยชน์ที่จะได้รับจากการทำผิด

3. **ความรวดเร็ว (Celerity/Speed):** การลงโทษต้องเกิดขึ้นอย่างรวดเร็วเพื่อให้เกิดการเชื่อมโยงทางจิตวิทยาระหว่างการกระทำและความผิด (Vellani, 2020)

อย่างไรก็ตาม การป้องปรามมีขีดจำกัด ไม่สามารถใช้ได้ผลกับผู้ที่กระทำผิดด้วยอารมณ์ชั่ววูบ ผู้ที่มีอาการทางจิต หรือผู้ที่กระทำผิดด้วยอุดมการณ์ความเชื่อที่ไม่สนใจความตาย (เช่น โจ๊กเกอร์ ในภาพยนตร์เปิดเรื่อง)

ภาพที่ 2.9

ข้อจำกัดของการป้องปราม: สถานการณ์ที่มาตรการป้องปรามให้ผลจำกัด

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

7.2 การป้องกัน (Prevention): การตัดโอกาสก่อนเกิดเหตุ

การป้องกันเน้นที่การสร้างระบบนิเวศที่ปลอดภัยผ่านการใช้เทคโนโลยีและกระบวนการ (Procedures) เช่น การติดตั้ง Firewall การใช้การตรวจสอบสิทธิ์แบบสองขั้นตอน (MFA) และการฝึกอบรมพนักงาน (Awareness Training) การป้องกันพยายาม

ตอบโจทย์ “การบริหารความเสี่ยงล่วงหน้า” (Proactive Risk Management) เพื่อลดความสูญเสียก่อนที่จะเกิดขึ้นจริง

7.3 ทฤษฎีความยืดหยุ่นกับความมั่นคง (Resilience Theory): ความสามารถในการยืนหยัดและฟื้นตัว

ในยุคที่ภัยคุกคามมีความซับซ้อนและหลากหลายเกินกว่าจะป้องกันได้ร้อยเปอร์เซ็นต์ แนวคิดด้านความมั่นคงได้เปลี่ยนผ่านจาก “การป้องกันไม่ให้เกิด” มาสู่ “ความยืดหยุ่น” (Resilience) ซึ่งยอมรับความจริงที่ว่า “เหตุการณ์ร้ายแรงอาจเกิดขึ้นได้” เป้าหมายจึงไม่ใช่การป้องกันทุกภัยคุกคาม แต่เป็นขีดความสามารถในการดูดซับแรงกระแทก ปรับตัว และฟื้นคืนสู่การทำงานได้อย่างรวดเร็ว (Vellani, 2020)

ทฤษฎีความยืดหยุ่นมีต้นกำเนิดจากนิเวศวิทยาระบบและวิศวกรรมศาสตร์ ซึ่งอธิบายความสามารถของระบบในการรองรับการรบกวนโดยยังคงรักษาโครงสร้างและหน้าที่พื้นฐานไว้ได้ เมื่อนำมาประยุกต์ใช้ในการศึกษาด้านความมั่นคงปลอดภัย แนวคิดนี้ถูกแปลงมาเป็นความสามารถของระบบทางการเมือง สังคม เศรษฐกิจ หรือเทคโนโลยี ในการต้านทาน ปรับตัว และฟื้นคืนจากภัยคุกคามต่าง ๆ เช่น การก่อการร้าย ภัยพิบัติธรรมชาติ การโจมตีทางไซเบอร์ โรคระบาด หรือสงครามรูปแบบผสม (Chen & Liu, 2021)

ความมั่นคงแบบดั้งเดิมมุ่งเน้นที่การป้องกันภัยคุกคาม การปกป้องชายแดน สินทรัพย์ หรือประชากรโดยอาศัยมาตรการป้องปรามและการป้องกันเป็นหลัก ด้วยทัศนคติ “ป้องกันไม่ให้เกิดเหตุ” ในทางตรงกันข้าม ทฤษฎีความยืดหยุ่นเปลี่ยนจุดเน้นไปที่การจัดการกับความวุ่นวายที่หลีกเลี่ยงไม่ได้ โดยยอมรับว่าไม่สามารถป้องกันภัยคุกคามได้ทั้งหมด และให้ความสำคัญกับการเตรียมพร้อม การมีระบบสำรอง การปรับตัว และการฟื้นคืนสภาพการทำงานที่สำคัญได้อย่างรวดเร็ว แนวคิดนี้มองว่าความมั่นคงไม่ใช่ภาวะตายตัวที่ “ไม่มีภัยคุกคาม” แต่เป็นขีดความสามารถของรัฐ สังคม องค์กร หรือระบบในการทำงานต่อไปได้ภายใต้แรงกดดัน

กระบวนการสร้างความยืดหยุ่นประกอบด้วย:

1. การเตรียมพร้อม (Prepare): การซ้อมแผนเผชิญเหตุ (Emergency Drills) การสำรองทรัพยากรที่จำเป็น และการวางแผนรับมือเหตุการณ์ล่วงหน้า องค์กรที่มีแผนกู้คืนล่วงหน้า ระบบสำรอง และบุคลากรที่ผ่านการฝึกซ้อมมาแล้ว จะมีความพร้อมรับมือกับวิกฤตได้ดีกว่าองค์กรที่ต้องแก้ปัญหาเฉพาะหน้า

2. การดูดซับแรงกระแทก (Absorb): ความสามารถในการทำงานต่อได้แม้ระบบหลักจะล่ม (Business Continuity) การรักษาการทำงานที่สำคัญไว้ได้แม้เกิดการหยุดชะงัก ตัวอย่างเช่น โรงพยาบาลที่ถูกโจมตีทางไซเบอร์ยังคงให้การดูแลผู้ป่วยวิกฤตได้ด้วยการ

เปลี่ยนไปใช้ระบบปฏิบัติการด้วยมือ หรือบริษัทโลจิสติกส์ที่เปลี่ยนเส้นทางการขนส่งเพื่อเลี่ยงพื้นที่น้ำท่วมและรักษาคำสัญญาการจัดส่ง

3. การฟื้นฟู (Recover): การกลับสู่สถานะปกติอย่างรวดเร็วหลังเหตุการณ์สงบ การคืนสู่การดำเนินงานปกติได้อย่างมีประสิทธิภาพ องค์กรที่มีระบบสำรองและแผนการฟื้นตัวที่ชัดเจนจะสามารถลดระยะเวลาหยุดชะงักและความสูญเสียได้อย่างมีนัยสำคัญ

4. การเรียนรู้และปรับตัว (Adapt): การนำความผิดพลาดและบทเรียนที่ได้รับมาปรับปรุงระบบให้ดีขึ้น การทบทวนหลังเกิดเหตุช่วยระบุจุดอ่อน นำไปสู่การปรับปรุง และสร้างองค์ความรู้ให้กับองค์กรเพื่อเสริมความแข็งแกร่งให้ระบบในอนาคต (Fagan et al., 2010)

ภาพที่ 2.10

วงจรความยืดหยุ่นขององค์กร (Organizational Resilience Cycle)

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

ประเทศไทยเผชิญกับภัยคุกคามที่หลากหลาย ทั้งน้ำท่วมซ้ำซาก โรคระบาดระดับโลก (COVID-19, ไข้หวัดนก) และความไม่แน่นอนทางการเมืองเป็นระยะ ซึ่งมหาอุทกภัยปี 2554 ได้แสดงให้เห็นถึงความสำคัญของความยืดหยุ่นอย่างชัดเจน โดยองค์กรที่ไม่มีศูนย์สำรองข้อมูล (DR Site: Disaster Recovery Site) นอกพื้นที่น้ำท่วมได้รับความเสียหายมหาศาล ขณะที่องค์กรที่เตรียมพร้อมระบบคลาวด์และศูนย์ทำงานสำรองสามารถดำเนินกิจการต่อได้แม้สำนักงานใหญ่จะจมน้ำ อย่างไรก็ตาม ทุกองค์กรไม่สามารถป้องกันภัยธรรมชาติหรือโรคระบาดได้ทั้งหมด แต่สามารถสร้างขีดความสามารถในการดูดซับแรงกระแทก รักษาการดำเนินงานที่สำคัญ และฟื้นตัวได้อย่างมีประสิทธิภาพ ยุทธศาสตร์ความ

มั่นคงในปัจจุบันจึงได้ผนวกเอาความยืดหยุ่นเป็นหลักชี้นำมากขึ้น นำไปสู่นโยบายที่ลงทุนในโครงสร้างพื้นฐานที่หลากหลาย สร้างความสามารถที่กระจายตัว พัฒนาการจัดการภาวะฉุกเฉินที่แข็งแกร่ง ส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชน และจัดการหลายระดับอย่างบูรณาการ เพื่อสร้างขีดความสามารถให้รัฐ สังคม และองค์กรสามารถ “ต้านทาน ปรับตัว และเติบโต” ภายใต้ภัยคุกคามที่ซับซ้อนและไม่หยุดนิ่ง แทนที่จะมุ่งหวังการป้องกันที่เป็นไปไม่ได้ในโลกแห่งความไม่แน่นอน

ภาพที่ 2.11

ความยืดหยุ่นในระดับองค์กร (Organizational Resilience)

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

7.4 ความยืดหยุ่น: การปรับมุมมองต่อความล้มเหลว (Resilience Reframes Failure)

กรอบแนวคิดความยืดหยุ่นไม่ได้มองความล้มเหลวเป็นเพียงความไร้ความสามารถ แต่ถือเป็นโอกาสในการเรียนรู้และพัฒนาระบบให้แข็งแกร่งยิ่งขึ้น องค์กรที่มีความน่าเชื่อถือสูง (High-Reliability Organizations) เช่น โรงไฟฟ้านิวเคลียร์ เรือบรรทุกเครื่องบิน และศูนย์ควบคุมจราจรทางอากาศ ซึ่งต้องทำงานภายใต้เงื่อนไขที่ความผิดพลาดเพียงเล็กน้อยอาจนำไปสู่หายนะ กลับสามารถรักษาบันทึกความปลอดภัยที่โดดเด่นได้ด้วยการนำหลักการสำคัญห้าประการมาปฏิบัติ (Giang, 2025)

1. การหมกมุ่นกับความล้มเหลว (Preoccupation with Failure) คือการให้ความสำคัญกับเหตุการณ์ที่เกือบเกิดปัญหา (Near-misses) อย่างจริงจัง ดำเนินการสอบสวนอย่างละเอียดถี่ถ้วน และเรียนรู้จากเหตุการณ์เหล่านั้นก่อนที่จะลุกลามกลายเป็นภัยพิบัติจริง องค์กรเหล่านี้ไม่ปล่อยให้ “เกือบเกิด” ผ่านไปโดยไม่ได้บทเรียน

2. ความไม่ไว้วางใจต่อคำอธิบายง่าย ๆ (Reluctance to Simplify) หมายถึง การหลีกเลี่ยงการสรุปเหตุผลแบบตื้นเขิน ยอมรับในความซับซ้อนของระบบ และตระหนักว่าความล้มเหลวส่วนใหญ่มักเกิดจากปฏิกิริยาซับซ้อนระหว่างหลายปัจจัยที่เกี่ยวพันกัน ไม่ใช่สาเหตุเดียวที่ชัดเจน

3. ความตื่นตัวต่อการปฏิบัติงานจริง (Sensitivity to Operations) คือการรักษาการตระหนักรู้ต่อสภาพการณ์ในเวลาจริง (Real-time Situational Awareness) ให้อำนาจบุคลากรระดับปฏิบัติการในการรายงานปัญหา และตอบสนองต่อสัญญาณอ่อนๆ ก่อนที่สถานการณ์จะลุกลามเป็นวิกฤต

4. ความมุ่งมั่นสู่ความยืดหยุ่น (Commitment to Resilience) หมายถึงการสร้างขีดความสามารถในการรองรับความไม่คาดคิด ประยุกต์วิธีแก้ปัญหาเฉพาะหน้าอย่างสร้างสรรค์ และฟื้นตัวกลับมาจากการหยุดชะงักได้อย่างรวดเร็ว

5. การเชื่อฟังผู้มีความเชี่ยวชาญ (Deference to Expertise) คือการโอนอำนาจการตัดสินใจในช่วงวิกฤตไปยังบุคคลที่มีความรู้และความเชี่ยวชาญที่เกี่ยวข้องที่สุดกับสถานการณ์นั้นๆ โดยไม่ยึดติดกับลำดับชั้นองค์กร (LaPorte & Consolini, 1991; Weick & Sutcliffe, 2007)

องค์กรในประเทศไทยในที่มีความเสี่ยงสูง เช่น การบิน พลังงาน และการดูแลสุขภาพ สามารถนำหลักการขององค์กรที่มีความน่าเชื่อถือสูงนี้มาประยุกต์ใช้ เพื่อสร้างความยืดหยุ่นและรักษาความสมบูรณ์ของการดำเนินงานไว้ได้ แม้จะอยู่ในสภาพแวดล้อมที่เต็มไปด้วยความเสี่ยงที่ซับซ้อนและไม่อาจคาดการณ์ได้ทั้งหมด

8. ความมั่นคงในฐานะธรรมาภิบาลและความสามารถขององค์กร

ความมั่นคงในโลกสมัยใหม่ไม่ได้เป็นเพียงหน้าที่ของพนักงานรักษาความปลอดภัยที่หน้าประตูอีกต่อไป แต่มันคือส่วนหนึ่งของ “ธรรมาภิบาลองค์กร” (Security as Governance) และเป็นความสามารถเชิงยุทธศาสตร์ที่ส่งเสริมการบรรลุเป้าหมายขององค์กร

8.1 ระบบสังคมเทคนิค (Socio-Technical Systems)

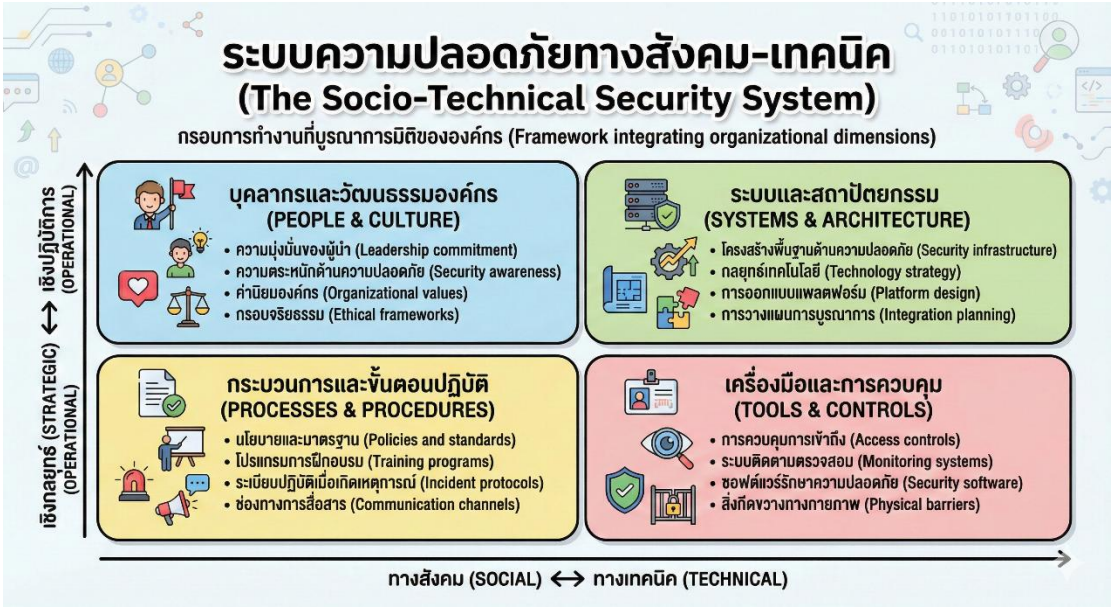
การรักษาความมั่นคงปลอดภัยจะล้มเหลวทันทีหากมองแต่เพียงแค่เทคโนโลยี ทฤษฎีสังคมเทคนิค (Socio-Technical) ระบุว่าความมั่นคงปลอดภัยเกิดจากปฏิสัมพันธ์ของ 4 ปัจจัยหลัก

1. **คน (People):** พฤติกรรม ทัศนคติ และวัฒนธรรมการระวังภัย
2. **เทคโนโลยี (Technology):** อุปกรณ์ กล้อง ซอฟต์แวร์ และโครงสร้างพื้นฐาน

3. กระบวนการ (Procedures): นโยบาย แผนปฏิบัติการ และมาตรฐานการทำงาน

4. **ธรรมาภิบาล (Governance):** ความรับผิดชอบของผู้บริหารและการกำกับดูแลอย่างเป็นธรรม

ตัวอย่างวิกฤตความมั่นคงปลอดภัยไซเบอร์ของไทยในปี 2024 ที่มีสถิติการโจมตีสูงถึง 196,078 ครั้งในไตรมาสเดียว สะท้อนว่าสาเหตุไม่ได้มาจากระบบคอมพิวเตอร์ที่ล้าสมัยเพียงอย่างเดียว แต่อยู่ที่พฤติกรรมของผู้ใช้ (เช่น การไม่ตั้งรหัสผ่านที่ซับซ้อน) และกระบวนการบริหารจัดการ (เช่น การไม่อัปเดตระบบปฏิบัติการอย่างสม่ำเสมอ ซึ่งมีอัตราความล้มเหลวสูงถึงร้อยละ 10) (Ani et al., 2023)



ภาพที่ 2.12

ระบบความปลอดภัยทางสังคม–เทคนิค (The Socio-Technical Security System)

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

มุมมองเชิงสังคมเทคนิค (The Socio-Technical Perspective) มองว่าความมั่นคงปลอดภัยเกิดขึ้นจากปฏิสัมพันธ์ระหว่างระบบย่อยสองส่วนที่ต้องทำงานประสานกัน ได้แก่ ระบบย่อยทางเทคนิค (ซึ่งรวมถึงฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย และโครงสร้างพื้นฐานทางกายภาพ) และระบบย่อยทางสังคม (ซึ่งรวมถึงบุคคล วัฒนธรรม บรรทัดฐาน และโครงสร้างองค์กร) (Mujinga et al., 2019) ทั้งนี้ ความล้มเหลวด้านความมั่นคงปลอดภัยมักเกิดจากความไม่สอดคล้องกันระหว่างองค์ประกอบทั้งสองส่วน เช่น ระบบควบคุมการเข้าถึงที่ซับซ้อนจะไร้ประโยชน์หากพนักงานแชร์รหัสผ่านหรือประตูหนีไฟเปิดไว้เพื่อความสะดวก ในทางกลับกัน พนักงานที่ผ่านการฝึกอบรมดีแล้วก็ไม่สามารถชดเชยเทคโนโลยีที่

ขาดความปลอดภัยโดยพื้นฐานได้ ความมั่นคงที่มีประสิทธิภาพจึงจำเป็นต้องปรับปรุงระบบย่อยทั้งสองส่วนให้เหมาะสมไปพร้อม ๆ กัน โดยเทคโนโลยีควรสนับสนุนมากกว่าขัดขวางการทำงานของมนุษย์ อีกทั้งขั้นตอนกระบวนการควรอำนวยความสะดวกมากกว่าละเลยข้อจำกัดของมนุษย์ และการฝึกอบรมควรส่งเสริมและเสริมสร้างมากกว่าสมมติว่ามนุษย์จะปฏิบัติตามได้อย่างสมบูรณ์แบบนั่นเอง (Ani et al., 2023)

ภาพที่ 2.13

ตัวอย่างความล้มเหลวด้านความมั่นคงเชิงสังคม–เทคนิค

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

8.2 จริยธรรมและความชอบธรรมในการรักษาความมั่นคงปลอดภัย

ในการใช้ทฤษฎีความมั่นคง ผู้บริหารต้องคำนึงถึงประเด็นจริยธรรมเสมอ ดังนี้

1. **ความเป็นส่วนตัว (Privacy):** มาตรการรักษาความปลอดภัย เช่น การเก็บข้อมูลชีวมาตร (Biometrics) ต้องไม่ละเมิดสิทธิส่วนบุคคลตามกฎหมาย PDPA ของไทย

2. **ความได้สัดส่วน (Proportionality):** มาตรการรักษาความปลอดภัยต้องมีความสมดุลกับความเสี่ยงที่แท้จริง ไม่รุนแรงจนเกินไปจนกระทบต่อสิทธิเสรีภาพ

3. **ความรับผิดชอบ (Accountability):** ผู้ปฏิบัติงานด้านความมั่นคงต้องสามารถถูกตรวจสอบและรับผิดชอบต่อการกระทำของตนได้

ในสังคมไทยที่ให้ความสำคัญกับเรื่อง “ความเกรงใจ” และ “ความสัมพันธ์ส่วนตัว” การบังคับใช้กฎระเบียบความมั่นคงต้องอาศัยทักษะการสื่อสารและความเป็นธรรม

(Legitimacy) เพื่อให้พนักงานยอมรับและปฏิบัติตามโดยไม่รู้สึกว่าถูกละเมิดหรือถูกควบคุมจนเกินไป

ภาพที่ 2.14

จริยธรรมด้านความเป็นส่วนตัวในการจัดการความมั่นคงปลอดภัย

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

ทั้งนี้ กรอบทฤษฎีเตือนให้ผู้ปฏิบัติงานตระหนักว่าความมั่นคงปลอดภัยที่ชอบธรรมจำเป็นต้องสร้างสมดุลระหว่างการปกป้องกับสิทธิเสรีภาพ การให้ความสำคัญกับความมั่นคงปลอดภัยมากเกินไป (Over-securitization) จะทำลายความไว้วางใจ ขณะที่การให้ความสำคัญน้อยเกินไป (Under-securitization) จะเปิดช่องให้เกิดอันตราย การค้นหาจุดสมดุลนี้จึงเป็นทั้งความท้าทายทางเทคนิคและจริยธรรม (Kazanskaia, 2025)

9. การบูรณาการทฤษฎีเข้าสู่ยุทธศาสตร์ความมั่นคง

จากการศึกษามาทั้งหมด เราพบว่าไม่มีทฤษฎีใดทฤษฎีหนึ่งที่สามารถอธิบายความท้าทายด้านความมั่นคงได้ครบทุกมิติ การจัดการความมั่นคงที่มีประสิทธิภาพจึงต้องบูรณาการมุมมองทางทฤษฎีหลากหลายเข้าด้วยกัน:

ภาพที่ 2.15
การบูรณาการทฤษฎีเข้าสู่ยุทธศาสตร์ความมั่นคง
ที่มา: ผู้เขียนสร้างขึ้นโดยใช้ Google Gemini (พ.ศ. 2569)

สำหรับตัวอย่างยุทธศาสตร์ความมั่นคงปลอดภัยแบบบูรณาการ หากเราพิจารณามหาวิทยาลัยในประเทศไทยแห่งหนึ่งที่ต้องการเสริมความมั่นคงในพื้นที่มหาวิทยาลัย เราสามารถดำเนินการได้ ดังนี้:

1. **การประยุกต์ใช้ RAT:** การโจรกรรมในมหาวิทยาลัยมักเกิดขึ้นในห้องสมุดช่วงสอบ (เป้าหมายที่เหมาะสม: คอมพิวเตอร์แล็ปท็อปและกระเป๋าที่ไม่มีคนดูแล; การขาดผู้ปกป้อง: นักศึกษามุ่งความสนใจไปที่การอ่านหนังสือ; ผู้กระทำผิดที่มีแรงจูงใจ: โจรฉวยโอกาส) การแทรกแซง: เพิ่มการดูแลผ่านนักศึกษาอาสา ปรับปรุงการมองเห็นด้วยไฟสว่างและจัดเตรียมตู้ล็อกเกอร์ที่ปลอดภัย (ลดความเหมาะสมของเป้าหมาย)

2. **การประยุกต์ใช้ SCP:** ติดตั้งกล้อง CCTV ในพื้นที่ทั่วไป (เพิ่มความเสี่ยงในการตรวจจับ) กำหนดให้ใช้บัตรนักศึกษาเพื่อเข้าอาคาร (เพิ่มความพยายามที่ต้องใช้) ทำเครื่องหมายทรัพย์สินของมหาวิทยาลัยด้วยแท็กที่ระบุตัวตนได้ (ลดผลตอบแทน) และติดประกาศเตือนเรื่องการป้องกันการโจรกรรม (ขจัดข้ออ้าง)

3. การประยุกต์ใช้ทฤษฎีป้องปราม: เผยแพร่การดำเนินคดีกับผู้ที่ถูกจับกุม (เพิ่มการรับรู้ถึงความแน่นอนและความรุนแรงของโทษ) ตอบสนองอย่างรวดเร็วต่อการรายงานเหตุ (เพิ่มความรวดเร็ว) และรักษาการปรากฏตัวของเจ้าหน้าที่ความปลอดภัยให้เห็นชัด (ส่งสัญญาณความเสี่ยงในการตรวจจับ)

4. การประยุกต์ใช้ทฤษฎีความยืดหยุ่น: พัฒนาโปรโตคอลการตอบสนองต่อเหตุการณ์ฉุกเฉิน ฝึกอบรมบุคลากรด้านการจัดการวิกฤต รักษาระบบการสื่อสารสำรอง และฝึกซ้อมตามแผนเป็นประจำ

5. การบูรณาการเชิงสังคมเทคนิค: ผนวกเทคโนโลยีควบคุมการเข้าถึงกับการฝึกอบรมบุคลากร ผสานระบบการเฝ้าระวังกับโปรโตคอลความปลอดภัย และส่งเสริมวัฒนธรรมในมหาวิทยาลัยให้นักศึกษาช่วยดูแลกันและกัน

6. การคำนึงถึงจริยธรรม: ตรวจสอบให้แน่ใจว่า CCTV เคารพความเป็นส่วนตัว (ไม่ติดกล้องในห้องน้ำหรือพื้นที่ส่วนตัว) ใช้ข้อมูลเพื่อวัตถุประสงค์ด้านความปลอดภัยเท่านั้น (ไม่ใช้เพื่อการเฝ้าระวังทางวินัย) และสื่อสารเกี่ยวกับมาตรการความมั่นคงอย่างโปร่งใส (เพื่อสร้างความไว้วางใจ)

แนวทางแบบบูรณาการความมั่นคงปลอดภัยนี้เปลี่ยนการจัดการความมั่นคงจากการควบคุมแบบแยกส่วนให้กลายเป็นยุทธศาสตร์ที่สอดคล้องกัน สอดรับกับเป้าหมายขององค์กร (สภาพแวดล้อมการเรียนรู้ที่ปลอดภัย) และความคาดหวังของสังคม (การเคารพสิทธิของนักศึกษา)

10. บทสรุป (Conclusion)

บทนี้แสดงให้เห็นว่าการจัดการความมั่นคงปลอดภัยเป็นแนวปฏิบัติที่มีพื้นฐานมาจากทฤษฎี ไม่ใช่เพียงการแก้ปัญหาเฉพาะหน้า ทั้งนี้ ทฤษฎีกิจวัตรประจำวันสอนว่าอาชญากรรมเกิดจากโอกาสที่ผู้กระทำผิดที่มีแรงจูงใจ เป้าหมายที่เหมาะสม และการขาดผู้ปกป้องบรรจบกัน การป้องกันอาชญากรรมตามสถานการณ์ให้เทคนิค 25 วิธีที่จัดเป็น 5 กลยุทธ์หลักเพื่อลดโอกาสในการเกิดอาชญากรรมอย่างเป็นระบบ การป้องกันอาชญากรรมผ่านการออกแบบสภาพแวดล้อมบูรณาการความมั่นคงปลอดภัยเข้าไว้ในการวางผังทางสถาปัตยกรรม ทฤษฎีการป้องปรามอธิบายว่ามาตรการความมั่นคงส่งสัญญาณเพื่อยับยั้งผู้กระทำผิดที่มีเหตุผล ทฤษฎีความยืดหยุ่นเน้นการดูดซับแรงกระแทก รักษาหน้าที่หลักและฟื้นตัวอย่างมีประสิทธิภาพ ทฤษฎีระบบสังคมเทคนิคยอมรับว่าความมั่นคงเกิดจากปฏิสัมพันธ์ระหว่างบุคคล เทคโนโลยี และกระบวนการ ขณะที่กรอบจริยธรรมรับประกันความสมดุลระหว่างการปกป้องกับสิทธิเสรีภาพ

อย่างไรก็ตาม ภาพยนตร์ *The Dark Knight* แสดงให้เห็นหลักการทางทฤษฎีในการปฏิบัติอย่างชัดเจน โจ๊กเกอร์ประสบความสำเร็จในการสร้างความโกลาหลไม่ใช่ด้วยพลัง

ที่เหนือกว่า แต่ด้วยความเข้าใจระบบและการใช้ประโยชน์จากทฤษฎีต่าง ๆ เขาใช้ทฤษฎีกิจวัตรประจำวันโดยการระบุและโจมตีจุดที่ผู้กระทำผิด เป้าหมายที่เหมาะสม และการขาดผู้ปกป้องบรรจบกัน เช่น การโจมตีขบวนรถของฮาร์วีย์ เดนท์ เขาจัดการปัจจัยเฉพาะสถานการณ์ตามหลักการป้องกันอาชญากรรมโดยลดความพยายามที่ต้องใช้ (โจมตีเป้าหมายที่อ่อนแอ) เพิ่มผลตอบแทน (สร้างความโกลาหลในวงกว้าง) และสร้างสิ่งยั่วยุ (ใช้ความกลัวและความสับสนวุ่นวาย) เขาบ่อนทำลายการป้องปรามโดยโจมตีในรูปแบบที่ไม่สามารถคาดเดาได้และไม่แสวงหาผลประโยชน์ที่เข้าใจได้ตามปกติ ทำให้การคำนวณต้นทุน-ผลประโยชน์แบบดั้งเดิมไร้ประโยชน์ และเขาทดสอบความยืดหยุ่นของระบบโดยบังคับให้สถาบันต่าง ๆ ต้องปรับตัวอย่างรวดเร็วหรือล้มเหลว ในทางตรงกันข้าม ความสามารถของแบทแมนมาจากความเข้าใจทฤษฎีที่ลึกซึ้ง เขาวิเคราะห์รูปแบบของโจ๊กเกอร์ ออกแบบการแทรกแซงเชิงป้องกันโดยปิดช่องโหว่ ส่งสัญญาณการป้องปรามผ่านการแสดงตนอย่างมองเห็นได้ และสร้างขีดความสามารถในการตอบสนองที่ยืดหยุ่นเพื่อรับมือกับภัยคุกคามที่ไม่คาดคิด การต่อสู้ระหว่างทั้งสองจึงไม่ใช่แค่การต่อสู้ทางกายภาพ แต่เป็นการประลองกันทางยุทธศาสตร์ระหว่างผู้ที่เข้าใจและนำหลักการทางทฤษฎีมาใช้

สำหรับองค์กรในประเทศไทยที่เผชิญภัยคุกคามทางไซเบอร์ อาชญากรรม ภัยธรรมชาติ และความวุ่นวายทางสังคม รากฐานทางทฤษฎีให้ความชัดเจนท่ามกลางความซับซ้อน ทฤษฎีเปลี่ยนความมั่นคงจากการแก้ปัญหาเฉพาะหน้าเป็นการบริหารความเสี่ยงเชิงยุทธศาสตร์ ช่วยให้องค์กรคาดการณ์ภัยคุกคาม ออกแบบการแทรกแซงอย่างเป็นระบบ จัดสรรทรัพยากรอย่างมีประสิทธิภาพ และแสดงเหตุผลของการลงทุนต่อผู้มีส่วนได้ส่วนเสีย กรอบจริยธรรมรับประกันความสมดุลระหว่างการปกป้องกับสิทธิเสรีภาพ ซึ่งสำคัญในสังคมไทยที่ให้คุณค่ากับความสามัคคีและความไว้วางใจ บทต่อไปจะศึกษาวิธีการประเมินภัยคุกคาม ช่องโหว่ และความเสี่ยง ซึ่งเป็นการแปลงทฤษฎีให้เป็นเครื่องมือวิเคราะห์เพื่อสนับสนุนการตัดสินใจด้านความมั่นคงบนพื้นฐานของหลักฐาน

11. คำถามทบทวน (Review Questions)

1. อธิบายเหตุผลว่าทำไม “ทฤษฎี” จึงมีความสำคัญต่อการจัดการความมั่นคงปลอดภัยมากกว่าการพึ่งพาเพียงประสบการณ์หรือสัญชาตญาณ พร้อมยกตัวอย่างสถานการณ์ที่การขาดกรอบทฤษฎีอาจนำไปสู่ “Security Theater”?

2. เปรียบเทียบแนวคิดความมั่นคงแบบดั้งเดิม (Classical Security) กับแนวคิดความมั่นคงร่วมสมัย (Contemporary Security) โดยอธิบายความแตกต่างในแง่ของ “ผู้ถูกคุ้มครอง” (Referent Object) และลักษณะของภัยคุกคาม?

3. ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) อธิบายการเกิดอาชญากรรมผ่านองค์ประกอบใดบ้าง และผู้จัดการความมั่นคงปลอดภัยสามารถแทรกแซงองค์ประกอบเหล่านี้ได้อย่างไรในบริบทขององค์กรหรือสังคมไทย?

4. อธิบายแนวคิด “สังคมแห่งความเสี่ยง” (Risk Society) ของอูลริค เบ็ค และวิเคราะห์ว่าความเสี่ยงแบบ “มนุษย์สร้างขึ้น” (Manufactured Risks) ส่งผลต่อแนวคิดการจัดการความมั่นคงปลอดภัยสมัยใหม่อย่างไร?

5. อภิปรายความแตกต่างระหว่างการจัดการความมั่นคงที่เน้น “การป้องกันและการป้องปราม” กับแนวคิด “ความยืดหยุ่น” (Resilience) พร้อมอธิบายว่าทำไมความยืดหยุ่นจึงกลายเป็นหัวใจสำคัญของยุทธศาสตร์ความมั่นคงในโลกปัจจุบัน?

12. เอกสารอ้างอิง (References)

Ani, U. D., Watson, J. D. M., Cook, A., & Nurse, J. R. C. (2023). Socio-technical security modelling: Addressing critical infrastructure security. *IET Cyber-Physical Systems: Theory & Applications, 8*(4). https://arxiv.org/pdf/2305.05108.pdf

Beck, U. (1992). *Risk society: Towards a new modernity* (M. Ritter, Trans.). SAGE Publications. (Original work published 1986)

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Chen, R., Xie, Y., & Liu, Y. (2021). Defining, conceptualizing, and measuring organizational resilience: A multiple case study. *Sustainability, 13*(5), 2517. https://doi.org/10.3390/su13052517

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608. https://doi.org/10.2307/2094589

Clarke, R. V. (Ed.). (1997). *Situational crime prevention: Successful case studies* (2nd ed.). Criminal Justice Press.

Eck, J. E., & Clarke, R. V. (2019). Situational crime prevention: Theory, practice and evidence. In M. D. Krohn, N. Hendrix, G. P. Hall, & A. J. Lizotte (Eds.), *Handbook on crime and deviance* (2nd ed., pp. 355–376). Springer International Publishing. https://doi.org/10.1007/978-3-030-20779-3_18

Fagan, J., Geller, A., Davies, G., & West, V. (2010). Street stops and broken windows revisited: The demography and logic of proactive policing in a safe and changing city. In S. K. Rice & M. D. White (Eds.), *Race, ethnicity, and policing: New and essential readings* (pp. 309–348). New York University Press.

Giang, L. H. (2025). Crisis management and organizational resilience: A framework for long-term recovery and growth. In T. Hoang (Ed.), *Proceedings of the International Conference on Contemporary Studies in Social Sciences (ICSSSS 2025)* (Advances in Social Science, Education and Humanities Research, Vol. 958, pp. 45–54). Atlantis Press. https://doi.org/10.2991/978-2-38476-470-9_5

Hobbes, T. (1998). *Leviathan* (J. C. A. Gaskin, Ed.). Oxford University Press. (Original work published 1651)

Kazanskaia, A. N. (2025). Cybersecurity ethics: Balancing security, privacy, and responsibility. *NEYA Global Journal of Non-Profit Studies*. https://doi.org/10.64357/neya-gjnps-tech-cyber-04

LaPorte, T. R., & Consolini, P. M. (1991). Working in practice but not in theory: Theoretical challenges of "high-reliability organizations." *Journal of Public Administration Research and Theory, 1*(1), 19–48.

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W. W. Norton & Company.

Mujinga, M., Eloff, M. M., & Kroeze, J. H. (2019). A socio-technical approach to information security. *Journal of Information Security, 10*, 39–54.

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

Vellani, K. (2020). *Strategic security management: A risk assessment guide for decision makers* (2nd ed.). CRC Press.

Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty* (2nd ed.). Jossey-Bass.

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

Wright, R. T., & Decker, S. H. (1994). *Burglars on the job: Streetlife and residential break-ins*. Northeastern University Press.