เกร็ดความรู้ที่ 3

การบริหารจัดการวิกฤตด้านความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐาน

สถาบันความมั่นคงศึกษา

สถาบันความมั่นคงศึกษาได้จัดกิจกรรมการประชุมวิชาการการบริหารจัดการวิกฤตด้านความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐาน ประจำปี พ.ศ. 2566 ร่วมกับ บริษัท ปตท. สำนักงานใหญ่ สำนักข่าวกรองแห่งชาติ บริษัทการปิโตรเลียมแห่งประเทศไทย จำกัด มหาชน บริษัทการรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย จำกัด มหาชน กองบัญชาการตำรวจสอบสวนกลาง กองบัญชาการตำรวจสันติบาล และคณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ระหว่างวันที่ 12 – 13 กันยายน 2566 ณ ศูนย์เอนเนอร์ยี่ คอมเพล็กซ์ เพื่อเสริมสร้างการบูรณาการและการประสานงานร่วมกันระหว่างหน่วยงานด้านความมั่นคงและหน่วยงานโครงสร้างพื้นฐานสำคัญ เพื่อเป็นการพัฒนาเครือข่ายงานด้านความมั่นคง การแลกเปลี่ยนข้อมูลข่าวสารระหว่างกัน ตลอดจนการแลกเปลี่ยนแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐานสำคัญของประเทศให้เกิดความเข้มแข็ง

การประชุมเชิงวิชาการฯ แบ่งออกเป็นหัวข้อต่าง ๆ ดังนี้

1 การเสวนา **“นโยบายและแนวทางบูรณาการความร่วมมือด้านความมั่นคงปลอดภัยในการจัดการกับภาวะวิกฤตความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐานสำคัญ”** หน่วยงานที่เกี่ยวข้องได้มีการเตรียมความพร้อมในการรับมือกับภัยคุกคามที่อาจเกิดขึ้นต่อโครงสร้างพื้นฐานสำคัญ อาทิ ไฟฟ้า ประปา พลังงาน ซึ่งหากว่าโครงสร้างพื้นฐานสำคัญเหล่านี้ถูกโจมตี จะส่งผลกระทบอย่างรุนแรงต่อการดำเนินชีวิตของประชาชน แต่ในสถานการณ์ปัจจุบัน หน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญยังขาดความสามารถในการดูแลรักษาความปลอดภัยได้ด้วยตนเอง และบ่อยครั้งที่ความช่วยเหลือจากภาครัฐไม่สามารถดำเนินการได้อย่างทันท่วงที จึงเสนอให้มีการฝึกจำลองสถานการณ์ร่วมกับหน่วยงานที่เกี่ยวข้องทั้งหมดเพื่อให้มีความเข้าใจที่ตรงกันของทุกภาคส่วน

2 การประชุมเชิงปฏิบัติการ **“นโยบายและแนวทางบูรณาการความร่วมมือด้านความมั่นคงปลอดภัยในการจัดการกับภาวะวิกฤตความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐานสำคัญ”** โดยมีการสะท้อนให้เห็นถึงปัญหาต่าง ๆ ที่มีพื้นฐานมาจากการที่ประเทศไทยยังขาดคำจำกัดความและข้อกฎหมายที่ระบุถึงนิยามของโครงสร้างพื้นฐานสำคัญที่มีความชัดเจน ส่งผลให้เกิดความซ้ำซ้อนและความไม่ชัดเจนในการปฏิบัติงาน นอกจากนี้ยังได้มีการยกตัวอย่างปัญหาที่เกิดขึ้นภายในหน่วยงานโครงสร้างพื้นฐานสำคัญ อาทิ การขาดการเข้าถึงข้อมูลข่าวสารที่มีความทันท่วงที การขาดความสามารถในการตรวจสอบความรุนแรงของสถานการณ์ได้อย่างเหมาะสม รวมถึงการขาดความรู้ความเข้าใจขั้นพื้นฐานในการดำเนินการในฐานะเจ้าหน้าที่เผชิญเหตุ (First Responder)

3 **ยุทธศาสตร์ นโยบาย และแผนที่เกี่ยวข้องกับการต่อต้านการก่อการร้าย และกรณีศึกษา**

1) การประเมินสถานการณ์การก่อการร้ายและนโยบายในการวางมาตรการรับมือ มุ่งเน้นความร่วมมือกับหลายภาคส่วนและการขจัดแนวคิดหัวรุนแรงและสุดโต่งในสังคม โดยการบังคับใช้แผนปฏิบัติการด้านการต่อต้านการก่อการร้าย เพื่อให้มีการประสานความร่วมมือและระบบแจ้งเตือนภัยอย่างทันท่วงที การกำหนดและป้องกันรักษาโครงสร้างพื้นฐานของประเทศ รวมถึงการพัฒนาบุคลากรในหน่วยงานที่เกี่ยวข้องต่าง ๆ ให้พร้อมต่อการรับมือสถานการณ์เฉพาะหน้าได้อย่างมีประสิทธิภาพ

2) กรณีศึกษากฎหมายควบคุมอาวุธปืนของแคนาดา ซึ่งเป็นประเทศที่กฎหมายในประเด็นดังกล่าวมีความเข้มงวดสูงเมื่อเปรียบเทียบกับอัตราการเกิดเหตุที่ต่ำ ที่ระบุให้ปืนในครอบครองทุกกระบอกต้องจดทะเบียน และการขอใบอนุญาตพกพาอาวุธปืนต้องผ่านกระบวนการสอบประวัติและสภาวะทางจิตที่เข้มงวด จนถึงปัจจุบัน แคนาดายังคงดำเนินนโยบายเชิงรุกแบบประนีประนอมในการควบคุมอาวุธปืนอย่างต่อเนื่องจากการเปิดรับความเห็นสาธารณะ

3) นิยามการก่อการร้ายจากแต่ละภาคส่วนที่ไม่ตรงกันเป็นอุปสรรคในการบูรณาการการรับมือและต่อต้านการก่อการร้าย ประกอบกับการมุ่งป้องกันเพียงพื้นที่สำคัญ อาทิ หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญ จนส่งผลให้ขาดการป้องกันพื้นที่อ่อนไหวที่เสี่ยงต่อการถูกโจมตี (soft target) อาทิ ห้างสรรพสินค้า สถานกักเก็บเชื้อเพลิง ดังนั้น จึงควรให้มีความร่วมมือของทุกภาคส่วนในประเทศเพื่อแสวงหามาตรการรับมืออย่างรัดกุมและสอดคล้องกัน

4 **สถานการณ์อาชญากรรมทางไซเบอร์ และเทคนิค การจัดทำฐานข้อมูล นำมาสู่การทำความเชื่อมโยง I2 ใน Critical Infrastructure : CI เพื่อดูแลงานด้านความมั่นคงปลอดภัย** กล่าวคือ อาชญากรรมไซเบอร์ในประเทศไทยในรูปแบบการหลอกลวง โดยมุ่งให้เกิดความเสียหายต่อทรัพย์สินและข้อมูลส่วนบุคคล ดังนั้น การเสริมสร้างความรู้ความเข้าใจของประชาชนให้มีความรู้เท่าทันในประเด็นดังกล่าว จึงเป็นวิธีการป้องกันและแก้ไขปัญหาการเกิดอาชญากรรมทางไซเบอร์ขั้นพื้นฐานได้อย่างมีประสิทธิภาพมากที่สุด นอกจากนี้ การจัดทำฐานข้อมูลอาชญากรรมไซเบอร์ รวมถึงการประสานข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องจึงเป็นกระบวนการสำคัญในการรับมือและเฝ้าระวังอาชญากรรมทางไซเบอร์อีกวิธีหนึ่ง

5 **การบริหารจัดการภาวะวิกฤต หน่วยงานเจ้าของโครงสร้างพื้นฐานที่สำคัญ (CI) กรณีศึกษา การกราดยิง (Active Shooter) หรือการเจรจาต่อรองกับผู้ก่อเหตุที่มีปัญหาด้านสุขภาพจิต** ผลกระทบที่มีต่อเจ้าหน้าที่เผชิญเหตุ (First Responder) โดยส่วนมากมักจะเป็นผู้ที่ไม่มีความสามารถในการรับมือหรือจัดการกับเหตุเฉพาะหน้า ดังเช่นกรณีการกราดยิงโคราชที่เกิดขึ้นในพื้นที่ห้างสรรพสินค้า เจ้าหน้าที่เผชิญเหตุจึงเป็นฝ่ายรักษาความปลอดภัยที่ไม่สามารถรับมือกับผู้ก่อเหตุที่มีความคุ้นเคยกับอาวุธสงคราม จึงเป็นการถอดบทเรียนให้พิจารณาถึงการตรวจสุขภาพจิตของบุคคล โดยเฉพาะเจ้าหน้าที่ด้านความมั่นคงอย่างต่อเนื่องเพื่อประเมินและป้องกันความเสี่ยงในการก่อเหตุกราดยิงขึ้นด้วยการฟื้นฟูรักษาสุขภาพจิต นอกจากนี้ หากเหตุกราดยิงเกิดขึ้น การเจรจาต่อรองจะเป็นไปได้อย่างมีประสิทธิภาพที่สุด หากผู้เจรจาต่อรองได้รับทราบถึงสภาวะทางจิตเบื้องต้นของผู้ก่อเหตุเพื่อใช้ในการระงับยับยั้งหรือทำความเข้าใจในพฤติกรรมของผู้ก่อเหตุกราดยิงไปได้เช่นกัน

6 **เทคโนโลยีการบริหารจัดการยานไร้คนขับเพื่อความมั่นคงปลอดภัยสาธารณะ** ปัจจุบันได้มีการนำเทคโนโลยียานไร้คนขับมาใช้ในกิจการหลายประเภท ได้แก่ กิจการทางทหาร กิจการที่เกี่ยวข้องกับการหารายได้ และการใช้ในงานอดิเรก ทั้งนี้ ยานไร้คนขับสามารถจำแนกเป็น 2 ประเภท ดังนี้

1) Open Category เพื่อส่งเสริมการใช้โดรนสำหรับผู้สนใจในขั้นต้น ซึ่งไม่ต้องมีการขออนุญาตเมื่อทำการขึ้นบิน มีขนาดน้ำหนักเบา ห้ามบินเหนือกลุ่มคนจำนวนมากเพื่อลดความเสี่ยงจากภัยอันตรายของโดรนที่อาจตกปะทะ และต้องมีกลไกในการใช้ฮาร์ดแวร์และซอฟต์แวร์ในกรณีที่โดรนเกิดขัดข้อง เพื่อให้โดรนทำงานในโหมดปลอดภัยได้โดยอัตโนมัติ

2) Specific Operation Category โดยต้องขออนุญาตก่อนทำการขึ้นบินและต้องมีกระบวนการบินที่ผ่านการกำกับและควบคุมโดยหน่วยงานที่รับผิดชอบ รวมถึงต้องมีการกำหนดแผนการบิน การจองใช้ห้วงอวกาศ ระยะเวลาในการปฏิบัติการบิน และภารกิจที่ปฏิบัติในห้วงอากาศ ทั้งนี้ สำหรับข้อพิจารณาด้านการกำกับและดูแล สามารถแบ่งได้ ดังนี้

(1) การกำหนดให้มีการขึ้นทะเบียนโดรนของผู้ผลิต ผู้นำเข้า ผู้ครอบครอง และผู้ควบคุม

(2) การกำหนดกระบวนการที่เกี่ยวข้องกับใบอนุญาต โดยจะต้องมีการกำหนดขั้นตอนการออกใบอนุญาต การทบทวน การต่ออายุ การพักใช้ และการยกเลิกใบอนุญาต

(3) การบริหารจัดการ โดยจะต้องมีการกำหนดกระบวนการขออนุญาตนำโดรนขึ้นสู่ห้วงอากาศ การนำโดรนเข้าสู่ภารกิจการบิน และการรายงานผลภายหลังเสร็จสิ้นภารกิจการบิน

(4) การกำหนดหลักสูตร การเรียนการสอน และการฝึกภาคปฏิบัติ

(5) การควบคุมโดยหน่วยงานความมั่นคง ทั้งในส่วนของการรับแจ้งเหตุ การเฝ้าระวังและตรวจสอบ และการแทรกแซงและเข้ายึดการควบคุม

7 **เทคโนโลยีด้านความมั่นคงปลอดภัย** ปัจจุบันองค์กรต่าง ๆ ได้มีการนำระบบคลาวด์มาใช้ในการปฏิบัติงานที่หลากหลาย ส่งผลให้เกิดความเสี่ยงในการถูกโจมตีแบบทำลายล้าง ซึ่งในห้วงปี พ.ศ. 2565 พบว่า ร้อยละ 82 ของการละเมิดทางไซเบอร์เกี่ยวข้องกับข้อมูลในระบบคลาวด์ถึงร้อยละ 39 ดังนั้น หน่วยงานจึงควรพิจารณาดำเนินกลยุทธ์และแผนงานด้านความปลอดภัยทางไซเบอร์แบบ Zero Trust เพื่อช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ ได้แก่

1) การคาดการณ์ ป้องกัน และตอบสนองต่อภัยคุกคามสมัยใหม่ โดยการผสานรวมข่าวกรองทางระบบปัญญาประดิษฐ์ (AI) และระบบอัตโนมัติเพื่อจัดการความเสี่ยงและหยุดแรนซัมแวร์อย่างต่อเนื่อง

2) รวมศูนย์เพื่อความปลอดภัยของข้อมูลและแผนการปฏิบัติตามข้อกำหนด โดยรวมการป้องกันบนคลาวด์เพื่อเร่งการปฏิบัติตามข้อกำหนดและปกป้องชื่อเสียงของหน่วยงาน

3) ตรวจสอบผู้ใช้และจัดการอุปกรณ์ของเจ้าหน้าที่ โดยใช้การควบคุมตามความเสี่ยงและการเข้าถึงแบบสะดวก เพื่อปกป้องผู้ใช้ โปรแกรม และอุปกรณ์ในระบบคลาวด์และในหน่วยงาน