รายงานการเข้าร่วมประชุมเชิงปฏิบัติการด้านอาชญากรรมและความมั่นคงปลอดภัยทางไซเบอร์ สำหรับประเทศสมาชิก BIMSTEC ภายใต้คณะทำงานย่อยด้านการป้องกันปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายในกรอบ BIMSTEC (SG-AML/CFT) เมื่อวันที่ ๑๓-๑๕ มีนาคม ๒๕๖๑ ณ กรุงธากา สาธารณรัฐประชาชนบังกลาเทศ จัดโดย หน่วยข่าวกรองทางการเงินบังกลาเทศ (BFIU) ธนาคารแห่งบังกลาเทศ และกลุ่มธนาคารโลก (WBG)

นางสาวพีรยา ป้อมสุข
นักวิชาการคอมพิวเตอร์ชำนาญการ
ส่วนตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์
ศูนย์เทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. ส่งเสริมความร่วมมือระหว่างประเทศสมาชิก BIMSTEC (บังคลาเทศ อินเดีย พม่า ศรีลังกา ไทย ภูฏาน และเนปาล) ตามอนุสัญญาระหว่างประเทศ
๒. เพิ่มขีดความสามารถในการประสานงานระหว่างหน่วยงานในประเทศ และการประสานงานในการป้องกันอาชญากรรมในโลกไซเบอร์ การพัฒนามาตรการด้านความปลอดภัยในระบบอินเทอร์เน็ตที่มีประสิทธิภาพ และเส้นทางการร่วมมืออย่างไม่เป็นทางการกับคู่ค้าในประเทศและต่างประเทศ
๓. หาแนวทางในการปรับปรุงความร่วมมือระหว่างประเทศอย่างเป็นทางการและไม่เป็นทางการ

ผู้เข้าร่วมประชุม (เอกสารแนบ ๑)

วาระการประชุม (เอกสารแนบ ๒)

เอกสารนำเสนอตามวาระการประชุม (เอกสารแนบ ๓)

ข้อมูลการประชุมโดยสังเขป :

๑. Introduction to WB Combatting Cybercrime Project

(Mr. Seunghwan Park – World Bank)

- World Bank ได้ให้การสนับสนุนเงินทุนหลายล้านดอลลาร์แก่โครงการต่างๆ เช่น โครงสร้างพื้นฐานด้าน ICT / โทรคมนาคม การขนส่ง เมือง พลังงาน สุขภาพ การศึกษา การคุ้มครองทางสังคม การเงินและตลาด เพื่อให้มั่นใจว่าโครงสร้างพื้นฐาน ระบบที่สำคัญ และข้อมูลของรัฐบาล ธุรกิจ และผู้ใช้ที่ไหลผ่านระบบเหล่านั้นจะได้รับความคุ้มครอง
- World Bank มีโครงการต่อต้านอาชญากรรมทาง Cyber เพื่อเป็นเครื่องมือและเสริมสร้างขีดความสามารถสำหรับประเทศเศรษฐกิจเกิดใหม่ โดยสาธารณรัฐเกาหลีผ่านความร่วมมือของธนาคารโลกเกาหลีใต้ เป็นผู้ดูแลโครงการ โดยมีหลายหน่วยงานร่วมสนับสนุน แบ่งระยะเวลาการดำเนินโครงการเป็น ๒ ระยะ (ระยะที่ ๑ : กรกฎาคม ๒๕๕๗ – มิถุนายน ๒๕๖๐ / ระยะที่ ๒ : กุมภาพันธ์ ๒๕๖๑ – มิถุนายน ๒๕๖๓)

- ปัจจุบันได้ดำเนินการโครงการในระยะที่ ๑ แล้วเสร็จ มีผลสำเร็จตามโครงการ ดังนี้
    - Toolkit คือ หนังสือ Combatting Cybercrime : Tools and Capacity Building for Emerging Economies (เอกสารแนบ ๔) สามารถ download ได้ที่ http://www.combattingcybercrime.org เป็นหนังสือซึ่งรวบรวมแนวทางปฏิบัติที่น่าสนใจในการต่อสู้กับอาชญากรรมในโลกไซเบอร์ระหว่างประเทศ
    - Assessment Tool คือ โปรแกรมที่ถูกพัฒนาขึ้นเพื่อเป็นเครื่องมือสำหรับประเมินที่ช่วยให้ประเทศต่างๆ สามารถประเมินขีดความสามารถในปัจจุบันของตนในการต่อสู้กับอาชญากรรมในโลกไซเบอร์ และระบุถึงลำดับความสำคัญในการสร้างขีดความสามารถ
    - Virtual Library คือ ห้องสมุดเสมือน ที่จัดเตรียมโดยองค์กรที่เข้าร่วมโครงการ และอื่นๆ เป็นแพลตฟอร์มบนเว็บและแบบโต้ตอบของเนื้อหาขององค์กรพันธมิตรและผู้เข้าร่วม รายอื่นๆ ในการต่อสู้กับอาชญากรรมโดยการแชร์ข้อมูลประสบการณ์และความชำนาญ

International Cooperation in Combatting Cybercrime

(Mr. Keong Min Yoon – World Bank)

- Ransomware ที่รู้จักกันในชื่อ "WannaCry" เป็น cryptoworm ransomware มีเป้าหมาย คือ คอมพิวเตอร์ที่ใช้ Microsoft ซึ่งมีประมาณ ๘๐% ของคอมพิวเตอร์ทั่วโลก มีการเข้ารหัสลับข้อมูลและเรียกร้องการชำระเงินด้วย bitcoin และถึงแม้ว่า Microsoft จะหยุดการโจมตีได้ภายในสองสามวัน แต่ก็ได้สร้างความเสียหายแก่หน่วยงานระดับชาติ และองค์กรระดับโลก ตลอดจนโรงพยาบาลกว่า ๑๕๐ ประเทศ มีการประเมินว่าการสูญเสียทั้งหมดประมาณ ๔ พันล้านเหรียญ

- ความร่วมมือระหว่างประเทศด้านอาชญากรรมทางไซเบอร์ จะเกี่ยวข้องกับ เขตอำนาจศาล กฎหมายสำคัญ ขั้นตอนทางกฎหมาย และความคุ้มครอง

- เขตอำนาจศาล มีไว้เพื่ออธิบายประเด็นทางกฎหมายต่างๆ ตามหลักการของกฎหมายระหว่างประเทศ แบ่งออกเป็นสามส่วน การดำเนินการใดๆ ของรัฐต้องใช้หนึ่งในสามส่วน คือ อำนาจตามกฎหมายที่กำหนดไว้ หมายถึง ความสามารถของรัฐในการกำหนดและใช้กฎหมายในเรื่องต่างๆ อำนาจในการพิจารณาพิพากษา หมายถึงความสามารถของศาลรัฐในการตัดสินคดี และการบังคับใช้ หมายถึงความสามารถของรัฐที่จะทำให้เกิดผลต่อกฎหมาย รวมถึงความสามารถของเจ้าหน้าที่บังคับใช้กฎหมายเพื่อตรวจสอบ ซึ่งกรณีอาชญากรรมทางไซเบอร์โดยส่วนมากจะเกี่ยวข้องกับทั้งสามส่วนดังกล่าว

- ในสาระสำคัญเขตอำนาจศาลระหว่างประเทศจะเป็นตัวกำหนดว่ารัฐแต่ละรัฐจะทำอะไรในหรือนอกเขตแดนของตน โดยหลักการของเขตอำนาจต่างๆ ได้รับการพัฒนาขึ้นในกฎหมายระหว่างประเทศเพื่อให้รัฐสามารถบรรเทาความขัดแย้งที่อาจเกิดขึ้นจากการอ้างสิทธิ์ในเขตอำนาจศาลเดียวกัน ซึ่งในสถานการณ์ส่วนใหญ่ความขัดแย้งในเขตอำนาจศาลสามารถแก้ไขได้เป็นการเฉพาะกิจ และสามารถต่อรองได้ เช่นถ้าชาวเกาหลีกระทำการฆาตกรรมในประเทศสหรัฐอเมริกา แม้ว่าเกาหลีจะมีเขต

อำนาจศาลของประเทศตนเอง แต่ทั้งสองประเทศที่เกี่ยวข้องสามารถตกลงยินยอมให้สหรัฐอเมริกาดำเนินการทางคดีได้ เนื่องจากมีการก่ออาชญากรรมโดยมีหลักฐานปรากฏอยู่ ณ ประเทศดังกล่าว

- นักพัฒนาซอฟต์แวร์ของรัสเซีย พัฒนามัลแวร์โทรจัน SpyEye ที่สร้างความเสียหายมากกว่า ๑.๔ ล้าน เครื่องมุ่งเน้นที่ข้อมูลส่วนบุคคลและข้อมูลการเงินจากเหยื่อ หลอกให้ผู้ใช้ดาวน์โหลดแอปพลิเคชันมาติดตั้ง โดยภายในมีคำสั่งไม่พึ่งประสงค์ที่จะแอบดักอุปกรณ์ของเหยื่อ ทำให้อาชญากรไซเบอร์สามารถควบคุมอุปกรณ์ของเหยื่อได้จากระยะไกลที่เรียกว่า C๒

- อุปสรรคเกิดจากการที่ไม่มีข้อตกลงในการส่งผู้ร้ายข้ามแดนอย่างเป็นทางการระหว่างรัสเซียกับสหรัฐอเมริกา ทำให้ต้องติดตามจำเลยโดยกลุ่มของหน่วยงานบังคับใช้กฎหมายเป็นเวลาหลายปี สหราชอาณาจักร สหรัฐอเมริกาไทย ดัตช์ โดมินิกัน บัลแกเรีย และออสเตรเลีย พร้อมหน่วยงานภาคเอกชนหลายแห่ง (Trend Micro, Dell Secureworks, Trusteer, Underworld.no) ซึ่งได้รับการสนับสนุนจาก INTERPOL เพื่อจับกุมจำเลยในสาธารณรัฐโดมินิกันในที่สุด และนี่คือตัวอย่างของความร่วมมือทั้งภาครัฐและเอกชนระดับนานาชาติที่ดีเยี่ยม

- "Love Bug" แสดงให้เห็นถึงขอบเขตของความคิดแบบดั้งเดิมของเขตอำนาจศาลของอาชญากรรมในโลกไซเบอร์ : การเปิดอีเมลที่มีชื่อว่า "ILOVEYOU" ทำให้เกิดความเสียหายและผลกระทบที่เป็นอันตรายในบางประเทศกว่า ๒๐ ประเทศ กระจายไปทั่วโลก ประมาณ ๕๐ ล้านคน แต่เนื่องจากอาชญากรอยู่ในเขตอำนาจศาลที่พฤติกรรมไม่สามารถดำเนินการทางคดีได้โดยรัฐ และเป็นที่น่าสงสัยว่าอยู่ในฟิลิปปินส์ มีการฟ้องร้องและส่งผู้ร้ายข้ามแดนแต่ล้มเหลว

- กฎหมายที่สำคัญ จะเกี่ยวข้องกับการประสานกันของกฎหมายระดับประเทศ ความผิดตามกฎหมายของแต่ละประเทศ และสนธิสัญญา

- ขั้นตอนทางกฎหมาย จะเกี่ยวข้องกับอำนาจการสืบสวนระหว่างประเทศ การได้รับหลักฐาน และการป้องกัน

- ความร่วมมืออย่างเป็นทางการ ได้แก่ สนธิสัญญาระหว่างประเทศและภูมิภาค สนธิสัญญาพหุภาคีที่เฉพาะเจาะจงเกี่ยวกับไซเบอร์ MLA และการส่งผู้ร้ายข้ามแดน

- UNCTOC (United Nations Convention against Transnational Organized Crime) เป็นเครื่องมือที่ใช้มากที่สุดสำหรับความร่วมมือในคดีอาญา แม้ว่าเครื่องมือนี้จะเป็นประโยชน์สำหรับความร่วมมือระหว่างประเทศแต่ก็ไม่ได้ออกแบบมาโดยคำนึงถึงอาชญากรรมในโลกไซเบอร์ กับที่กล่าวว่าไม่สามารถตอบสนองคำขอเร่งด่วนเพื่อรักษาข้อมูล นอกจากนี้ยังมีประสิทธิภาพในการต่อต้านอาชญากรรมที่ก่ออาชญากรรมตามที่กำหนดโดยกลุ่มอาชญากรรมที่จัดเป็นกลุ่มที่มีโครงสร้างตั้งแต่สามคนขึ้นไป อย่างไรก็ตามความเกี่ยวข้องกับอาชญากรรมในโลกไซเบอร์มีความไม่แน่นอนเนื่องจากอาชญากรไซเบอร์จำนวนมากมีแนวโน้มที่จะมีโครงสร้างที่ไม่แน่นอนมากขึ้น

- สำหรับรัฐ เครื่องมือด้านพหุภาคีที่มีผลผูกพันเกี่ยวกับอาชญากรรมในโลกไซเบอร์รวมทั้งเครื่องมือต่อต้านอาชญากรรมทั่วไปอื่นๆ ที่มีบทบัญญัติด้านความร่วมมือระหว่างประเทศที่สามารถนำมาใช้เพื่อต่อต้านอาชญากรรมทางอาญา ได้ให้กรอบกฎเกณฑ์พื้นฐานสำหรับการกำหนดอาชญากรรมในโลกไซเบอร์ ใน ๕ สนธิสัญญาพหุภาคีที่สำคัญอยู่ (The Budapest Convention, The CIS Agreement, The SCO Agreement, The Arab Convention, The AU Convention) อย่างไรก็ตามแม้จะมีประเทศมากกว่า ๘๐ ประเทศ อยู่ในสนธิสัญญาเหล่านี้อย่างใดอย่างหนึ่งหรือมากกว่า แต่ความคุ้มครองที่มีอยู่อย่างจำกัดของสนธิสัญญาพหุภาคีที่มีอยู่ยังคงนำไปสู่การประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญาครั้งที่ ๑๒ ในปี ๒๕๕๓ จึงมีการจัดทำอนุสัญญาเพื่อต่อสู้กับอาชญากรรมในโลกไซเบอร์ แต่ในขณะที่สนธิสัญญาเป็นไปในเชิงบวก แต่เนื่องจากเครื่องมือที่แตกต่างกันอาจต้องมีข้อผูกพันที่แตกต่างกันเกี่ยวกับความร่วมมือ

- การประชุมในบูดาเปสต์เป็นเครื่องมือระดับโลกอย่างแท้จริงเพียงอย่างเดียวในเรื่องอาชญากรรมไซเบอร์ เนื่องจากเปิดให้แก่ประเทศสมาชิกที่ไม่ใช่สมาชิก COE โดยได้กำหนดกฎเกณฑ์ที่ครอบคลุมเกี่ยวกับด้านต่างๆ ของอาชญากรรมในโลกไซเบอร์ รวมทั้งประเด็นด้านเนื้อหา ประเด็นกระบวนการยุติธรรม และความร่วมมือระหว่างประเทศ กำหนดคำจำกัดความของความผิดให้สมดุลกับการป้องกันและขั้นตอนในการปฏิบัติ ทั้งนี้คู่สัญญาจะต้องปฏิบัติตามกระบวนการ และสิทธิมนุษยชนอย่างเหมาะสมในขณะที่ต่อสู้กับอาชญากรรมในโลกไซเบอร์

- แม้ว่าเครื่องมือด้านพหุภาคีที่มีผลผูกพันถือเป็นพื้นฐานที่สำคัญสำหรับความร่วมมือระหว่างประเทศ แม้ MLAT ที่ไม่มีผลบังคับจะมีแนวทางที่เป็นประโยชน์สำหรับมาตรฐานระดับสากลหรือระดับภูมิภาคสำหรับการจัดการกับอาชญากรรมในโลกไซเบอร์ แต่ก็ยังคงเป็นหนึ่งในเครื่องมือที่ครอบคลุมมากที่สุดสำหรับการสร้างกรอบกฎหมายที่สามารถทำงานร่วมกันได้ในระดับนานาชาติ และเพื่อเอาชนะปัญหาด้านเขตอำนาจศาล ยังคงมีเพียงสองประเทศที่มีผลผูกพันระหว่างประเทศ คือ อนุสัญญาบูดาเปสต์และอนุสัญญาสถานสันนิบาตอาหรับ โดยเฉพาะอย่างยิ่งต้องมีการส่งผู้ร้ายข้ามแดน

- การอำนวยความสะดวกในขั้นตอนการบริหาร MLA เป็นเรื่องที่ต้องใช้เวลามากและซับซ้อน เป็นปัญหาโดยเฉพาะอย่างยิ่งเมื่อพิจารณาถึงลักษณะของอาชญากรรมในโลกไซเบอร์

- MLAT มุ่งเน้นไปที่การแลกเปลี่ยนข้อมูลสนธิสัญญาส่งผู้ร้ายข้ามแดน ให้ความสำคัญกับการให้อำนาจส่วนบุคคลแก่รัฐที่ร้องขอเนื่องจากเป็นเรื่องเกี่ยวกับเขตอำนาจศาล การส่งผู้ร้ายข้ามแดนถือเป็นหนึ่งในประเด็นที่ยากที่สุดในความร่วมมือระหว่างประเทศ การขอให้ส่งผู้ร้ายข้ามแดนต้องสมดุลกับความจำเป็นที่รัฐจะต้องปกป้องพลเมืองของตนโดยไม่จำเป็นต้องให้ความเคารพและสนับสนุนการสอบสวนต่อเนื่องในต่างประเทศ

- ความร่วมมือทางการ ได้แก่ สนธิสัญญาบูดาเปสต์และสันนิบาตอาหรับแห่งรัฐ ตำรวจ - ตำรวจ ("P๒P") หน่วยงานระหว่างหน่วยงานหรือเครือข่ายระหว่างประเทศ (เช่น INTERPOL) และต้องมีการสื่อสารก่อนที่จะขอความร่วมมืออย่างเป็นทางการ

- ศูนย์ข้อมูลและการประสานงานด้านข้อมูล
  - INTERPOL’s Global Complex for Innovation
  - Europol’s European Cybercrime Center
  - EU’s Judicial Cooperation Unit
  - US National Cyber-forensics & Training Alliance
  - Commonwealth Cybercrime Initiatives
  - OAS Initiatives

- ทั่วโลกมีเครือข่ายความร่วมมือเกี่ยวกับอาชญากรรมทางอาญาอยู่เป็นจำนวนมาก นอกเหนือจากเครือข่ายของรัฐภาคีของสภาคองเกรสแห่งทวีปยุโรป อาชญากรรมไซเบอร์ ๒๔ ประเทศ ตลอด ๒๔ ชั่วโมง

- มีการสร้างเครือข่าย ๒๔/๗ เพื่อตอบสนองความต้องการอย่างทันท่วงที เป็นสิ่งที่มีความสำคัญมากขึ้น เนื่องจากข้อมูลการจราจรและข้อมูลเนื้อหามีจำนวนมากที่จำเป็นในการระบุและค้นหาผู้กระทำความผิดสามารถถูกลบออกภายในระยะเวลาสั้นๆ เครือข่ายตลอด ๒๔ ชั่วโมง มีข้อดีในการใช้ประโยชน์จากจุดเริ่มต้นที่พร้อมสำหรับการร้องขอความร่วมมือ

- เพื่อปรับปรุงประสิทธิภาพของคำขอความช่วยเหลือซึ่งกันและกัน หลายประเทศได้สร้างสัญญาซึ่งพร้อมใช้งานเสมอ เครือข่ายของจุดติดต่อเหล่านี้มีความสำคัญมากขึ้น

- อนุสัญญาบูดาเปสต์ข้อ ๓๕ - เครือข่าย ๒๔/๗
  ๑. ภาคีแต่ละฝ่ายจะกำหนดจุดติดต่อซึ่งมีอยู่ตลอด ๒๔ ชั่วโมง ๗ วัน ต่อสัปดาห์ เพื่อให้แน่ใจว่าการให้ความช่วยเหลือในทันที สำหรับวัตถุประสงค์ของการสืบสวนหรือการดำเนินคดี เกี่ยวกับความผิดทางอาญาที่เกี่ยวกับระบบคอมพิวเตอร์และข้อมูล หรือเพื่อรวบรวมพยานหลักฐานในรูปแบบอิเล็กทรอนิกส์ของความผิดทางอาญา ความช่วยเหลือดังกล่าวจะรวมถึงการอำนวยความสะดวกหรือถ้าได้รับอนุญาตจากกฎหมายภายในประเทศและแนวปฏิบัติโดยตรงในการดำเนินมาตรการต่อไปนี้ :
     ก. การจัดหาคำแนะนำด้านเทคนิค
     ข. การเก็บรักษาข้อมูลตามข้อ ๒๙ และข้อ ๓๐
     ค. การจัดเก็บหลักฐาน การจัดหาข้อมูลทางกฎหมาย และการระบุตำแหน่งของผู้ต้องสงสัย
  ๒. a - จุดติดต่อจะต้องมีความสามารถในการสื่อสารกับจุดการติดต่อของอีกฝ่ายอย่างรวดเร็ว
     b – หากจุดที่ผู้ติดต่อกำหนดโดยภาคี ไม่ได้เป็นส่วนหนึ่งของอำนาจ หรืออำนาจของภาคีนั้นรับผิดชอบในการช่วยเหลือซึ่งกันและกันระหว่างประเทศ หรือการส่งผู้ร้ายข้ามแดน ผู้ติดต่อต้องมั่นใจว่าสามารถประสานงานกับหน่วยงานหรือเจ้าหน้าที่ได้อย่างรวดเร็ว

๓. ภาคีแต่ละฝ่ายจะต้องมั่นใจว่าบุคลากรได้รับการฝึกอบรม พร้อมปฏิบัติงานเพื่ออำนวยความสะดวกในการทำงานของเครือข่าย

- การป้องกัน เป็นการช่วยป้องกันการบุกรุก รักษาความสมดุลของมาตรการการสืบสวน จำกัดการใช้งานเฉพาะในสถานการณ์ที่จำเป็น โดยมีการกำหนดเวลาและวิธีการใช้อำนาจในการสืบสวน ระบุเจ้าหน้าที่ผู้มีอำนาจ และระบุระยะเวลาที่อนุญาตให้ใช้มาตรการ

- แนวคิดเรื่องกระบวนการยุติธรรม และการเคารพในหลักนิติธรรมเป็นที่ยอมรับว่าเป็นพื้นฐานของระบบกฎหมาย

- โดยทั่วไปขั้นตอนที่ถูกต้องในกระบวนการยุติธรรม หมายถึง สิทธิของจำเลยที่จะเผชิญหน้ากับโจทก์ สิทธิในการให้คำปรึกษา และสิทธิในการพิจารณาคดีอย่างรวดเร็ว เน้นประเด็นปัญหาเกี่ยวกับอาชญากรรมทางอาญาที่เฉพาะเจาะจงและบ่อยขึ้น : (๑) ความไม่สมดุลของการได้รับหลักฐาน และ (ข) การค้นหาและการยึด

- รอสส์วิลเลี่ยม Ulbricht หรือที่รู้จักว่า "Dread Pirate Roberts" ถูกตัดสินประหารชีวิตในคุก โดยเกี่ยวข้องกับการดำเนินการและเป็นเจ้าของเว็บไซต์ Silk Road ในช่วงปี ๒๐๑๑ และ ๒๐๑๓ เว็บไซต์อนุญาตให้ผู้ใช้ซื้อและขายสินค้าและบริการที่ไม่ชอบด้วยกฎหมายโดยไม่ระบุชื่อ Ulbricht เรียกร้องความเชื่อมั่นของเขาโดยบอกว่า "ศาลใช้ดุลพินิจและปฏิเสธสิทธิประการที่ห้าและหกของเขาในการดำเนินการตามสิทธิที่จะเสนอการป้องกันและการพิจารณาคดีที่เป็นธรรมโดย (a) ป้องกันการใช้หลักฐานจากหลักฐานที่เกี่ยวข้อง การทุจริต Carl Force ของหน่วยงานพิเศษของ DEA (b) ปฏิเสธที่จะสั่งให้รัฐบาลได้ค้นพบหลักฐานเพิ่มเติม และวัสดุ 'Brady' เกี่ยวกับการทุจริต และ (c) ปฏิเสธการเคลื่อนไหวของ Ulbricht สำหรับการทดลองใหม่บนพื้นฐานของการเปิดเผยข้อมูลเพิ่มเติมเกี่ยวกับการบังคับคดีและการบังคับใช้กฎหมายการทุจริตอื่นๆ ที่เกี่ยวข้องกับการสืบสวน Silk Road "

- แม้จะมีความซับซ้อนในการตรวจสอบและฟ้องร้องอาชญากรไซเบอร์จากทั่วโลก แต่ก็ยังสามารถทำให้เกิดความไม่สมดุลระหว่างอำนาจระหว่างหน่วยงานสืบสวนสอบสวนและจำเลยได้

- การต่อรองอำนาจ : นักวิจัยมีอำนาจในการต่อรองมากขึ้นโดยเฉพาะอย่างยิ่งในการค้นหาและรักษาหลักฐาน เมื่อมีการสอบสวนถึงขั้นการฟ้องร้องแล้วมีแนวโน้มที่จะเป็นพยานหลักฐานเพิ่มเติม ในความโปรดปรานของรัฐมากกว่าหลักฐานที่ออกนอกลู่นอกทางในความโปรดปรานของจำเลย แต่ระบบความยุติธรรมซึ่งเป็นที่ยอมรับในหลักนิติธรรมก็ต้องเป็นธรรมและเป็นกลาง

- ในสหรัฐอเมริกามีกฎหมายหลายข้อ จำกัด อำนาจการสอบสวน : (๑) Wiretap Act, (๒) Pen Register and Trap and Trace Statute, (๓) Electronic Communications Privacy Act, and (๔) Fourth Amendment of US Constitution กฎหมายเหล่านี้ร่วมกันปกป้องการสื่อสารความเป็นส่วนตัวและความชอบธรรมของแต่ละบุคคล

- ในสหราชอาณาจักรเมื่อเร็วๆ นี้ได้ขยายขีดความสามารถในการเฝ้าระวังของหน่วยงานบังคับใช้กฎหมายของตนโดยอาศัยขั้นตอนที่เรียกว่า "double-lock" เพื่อจำกัดการล่วงละเมิดทางราชการที่อาจเกิดขึ้น เช่น
    - ผู้ให้บริการการสื่อสารต้องรักษาข้อมูลลูกค้าไว้เป็นเวลาหนึ่งปี
    - ลบการเข้ารหัสที่รบกวนการทำงานของใบสำคัญแสดงสิทธิ
    - ให้เจ้าหน้าที่สามารถสกัดกั้น และจัดเก็บข้อมูลรูปแบบต่างๆ ได้ โดยใช้เทคนิคต่างๆ รวมถึงการแฮ็ก และการสำรวจอุปกรณ์อิเล็กทรอนิกส์ของบุคคล
    - การรวบรวมข้อมูลจำนวนมาก ต้องได้รับอนุญาตเพื่อวัตถุประสงค์ในการรับข้อมูลข่าวสารที่เกี่ยวข้องกับบุคคลที่อยู่นอกขอบเขตอาณาเขตของสหราชอาณาจักรตราบเท่าที่มีการออกใบสำคัญแสดงสิทธิ
    - การกำกับดูแลการกระทำ
    - ต้องมีหมายจับที่ได้รับการอนุมัติจากรัฐมนตรีทั้งสอง และคณะกรรมการพิจารณาคดีพิเศษที่เรียกว่าคณะกรรมาธิการอำนาจสืบสวนสอบสวน
    - อย่างไรก็ตามในกรณีเร่งด่วนใบสำคัญแสดงสิทธิสามารถออกได้โดยไม่ต้องมีส่วนเกี่ยวข้องกับค่าคอมมิชชั่นเท่าที่จะอยู่ภายใต้การทบทวนโดยคณะกรรมการภายในสามวันทำการ

- กฎหมายเกาหลีรับรองสิทธิของจำเลยในการเข้าร่วมค้นหาและยึดอุปกรณ์จัดเก็บข้อมูล เช่น คอมพิวเตอร์ โดยศาลสูงสุดของเกาหลีได้ตีความบทบัญญัติอย่างเคร่งครัด

- ทุกแง่มุมของการตรวจสอบและการฟ้องร้อง มาตรฐานสิทธิมนุษยชนต้องได้รับการคุ้มครองตามความเป็นส่วนตัวภายใต้กฎหมายระหว่างประเทศและระดับชาติ

- การสืบสวนอาชญากรรมในหลายรูปแบบจะท้าทายสิทธิในความเป็นส่วนตัว โดยเฉพาะอย่างยิ่งในกรณีที่บุคคลไม่ทราบว่ากำลังถูกรวบรวมข้อมูลของตน ภายใต้กฎหมายระหว่างประเทศสิทธิส่วนบุคคลจะไม่สมบูรณ์และอาจมีข้อจำกัด

- โดยทั่วไปแล้ว "ความปลอดภัย" สามารถเข้าใจได้ว่าเป็นชุดของมาตรการด้านเทคโนโลยีที่เป็นสื่อกลางในการเข้าถึงข้อมูลส่วนบุคคลที่จัดเก็บหรือส่งผ่านระบบ หรือเครือข่าย ICT ในขณะที่ "ความเป็นส่วนตัว" เป็นกรอบการกำหนดกฎเกณฑ์สำหรับการจัดสรรผู้ที่สามารถเข้าถึงข้อมูลดังกล่าวรวมทั้งสิทธิ แก้ไขอะไรก็ได้

- เครื่องมือทางกฎหมายรับประกันการปกป้องข้อมูลและความเป็นส่วนตัว ได้แก่ ICCPR, ECHR และ ACHR มีข้อห้ามในการแทรกแซงโดยชอบกับความเป็นส่วนตัว ครอบครัวบ้าน และการติดต่อกัน ICCPR, Art. ๑๗; ECHR, Art. ๘; ACHR, Art. ๑๑

- แนวทางในการรักษาความปลอดภัยของระบบสารสนเทศและเครือข่าย
    - หลักการข้อจำกัดในการเก็บข้อมูล - Collection Limitation Principle
    - หลักการเกี่ยวกับคุณภาพข้อมูล - Data Quality Principle
    - วัตถุประสงค์หลักเกณฑ์ - Purpose Specification Principle
    - ใช้หลักการข้อจำกัด - Use Limitation Principle
    - หลักการป้องกันความปลอดภัย - Security Safeguards Principle
    - หลักการเปิดกว้าง - Openness Principle
    - หลักการการมีส่วนร่วมของแต่ละบุคคล - Individual Participation Principle
    - หลักการความรับผิดชอบ - Accountability Principle

- การพัฒนาทางไซเบอร์และ ICT อย่างรวดเร็ว ช่วยให้อินเทอร์เน็ตเป็นตัวขับเคลื่อนที่มีประสิทธิภาพยิ่งขึ้นในการเปลี่ยนแปลงทางเศรษฐกิจ สังคม และการเมือง แม้กระทั่งอินเทอร์เน็ตที่เจริญเติบโตในการแลกเปลี่ยนข้อมูลเปิด ที่ถูกเรียกว่า "market of ideas" นวัตกรรมและแรงจูงใจในการคิดค้นสิ่งใหม่ๆ ขึ้นอยู่กับความสมดุลที่เหมาะสมระหว่างการเข้าถึงข้อมูลและการให้รางวัลนักประดิษฐ์ด้วยการปกป้องสิทธิในทรัพย์สินทางปัญญา

- ผลการศึกษาล่าสุดของยูเนสโกเกี่ยวกับการรักษาเสรีภาพในการแสดงออกทางออนไลน์เพื่อสนับสนุนความสมดุลระหว่างความมั่นคงและการแสดงออก จากการศึกษาดังกล่าวรัฐบาลควรใช้วิธีการเชิงปฏิบัติที่ช่วยลดข้อจำกัดทางออนไลน์ที่ช่วยแก้ไขปัญหาที่เกิดขึ้นจากค่านิยมทางสังคมที่ถูกกฎหมาย วิธีการดังกล่าวช่วยให้มั่นใจได้ถึงอนาคตอันสดใสของอินเทอร์เน็ต โดยคงบทบาทของตนไว้ เป็นสถานที่สำหรับการแลกเปลี่ยนความคิดเห็นที่ทำให้แพลตฟอร์มดังกล่าวมีลักษณะเฉพาะและมีประสิทธิภาพสำหรับความก้าวหน้าทางเศรษฐกิจสังคมและการเมือง นอกจากนี้ ความสำคัญของเสรีภาพในการแสดงออกทางอินเทอร์เน็ตในฐานะกลไกสิทธิมนุษยชนได้รับความสนใจทั้งในระดับประเทศและระดับภูมิภาค บ่อยครั้งที่เสรีภาพในการแสดงออกจะถูกห้ามถ้าคำพูดอยู่ในรูปของ (๑) คำพูดแสดงความเกลียดชัง (๒) การยั่วยุให้กับการก่อการร้าย (๓) สื่อลามกอนาจารของเด็ก เป็นต้น

- การเปลี่ยนวิธีที่เราใช้ในอาชญากรรมในโลกไซเบอร์เป็นการสร้างวิธีใหม่ในการกำหนดความสำเร็จในฐานะที่เป็นประชาคมระหว่างประเทศ งานของเราไม่เพียงแต่ช่วยปรับปรุงการเปิดเผยข้อมูลอาชญากรรมในโลกไซเบอร์ แต่ยังเกี่ยวกับการทำความเข้าใจและการหาสาเหตุ

- ในปัจจุบันทั่วโลกมองเห็นความไม่สมดุลอย่างมากต่อความสามารถทางด้านเทคนิค กฎหมาย และสถาบัน แม้ว่าจะมีแนวทางปฏิบัติที่ดีที่สุดอยู่แล้ว แต่เราจำเป็นต้องทำงานร่วมกันโดยใช้แนวทางทั่วโลกในการต่อสู้กับอาชญากรรมในโลกไซเบอร์ ซึ่งเราต้องยอมรับว่าบุคคลและสถานการณ์ที่แตกต่างกันมีความเสี่ยงที่จะเกิดความเสี่ยงและภัยคุกคามต่างๆ จึงต้องมีการวางแผนอย่างรอบคอบ ดังนั้น การประชุมเชิงปฏิบัติการนี้ เป็นภาพความก้าวหน้าในการลดอาชญากรรม และการเติบโต

ทางเศรษฐกิจเพียงอย่างเดียวไม่เพียงพอ เนื่องจากอาชญากรรมในโลกไซเบอร์ยังคงพัฒนาอยู่ สิ่งที่กล่าวมาทั้งหมดเป็นเพียงข้อเสนอเบื้องต้น ซึ่งยังคงต้องหาวิธีที่จะทำให้คู่สัญญามีความหมายด้วย

The Budapest Convention on Cybercrime: Benefits for BIMSTEC members based on the experience of Sri Lanka

(Mr. Jayantha Fermando – Council of Europe)

- ภาค ICT ของศรีลังกา นำรายได้เข้าประเทศมากที่สุดเป็นอันดับ ๕ ของศรีลังกา เปิดเสรีภาคโทรคมนาคมเริ่มต้นในเอเชียใต้โดยมีผู้ประกอบการมือถือ ๕ ราย ผู้ให้บริการอินเทอร์เน็ต ๑๖ ราย และเกตเวย์ ๕ แห่ง มีการเจาะผ่านมือถือเกินกว่า ๑๑๐.๔% ในปี ๒๐๑๕ มีการเติบโตของภาคธุรกิจ / BMPO / KPO ซึ่งมีการจ้างงานด้านบัญชี การจ้างตามกฎหมาย โดยมีการเติบโตของแรงงานไอทีในอัตรา ๓๐% ต่อปี ทั้งนี้ ศรีลังกาเป็นประเทศที่เป็นอันดับหนึ่งในเอเชียใต้ในดัชนีความพร้อมในการเข้าถึงเครือข่าย (Networked Readiness Index - NRI) และดัชนีความพร้อมของรัฐบาลอิเล็กทรอนิกส์ของสหประชาชาติ (๒๐๑๔) และมี RTGS ยุคใหม่, ระบบการหักบัญชีระหว่างธนาคารและระบบการชำระเงินผ่านโทรศัพท์มือถือ

- World Bank เป็นผู้สนับสนุนให้เกิด eSri Lanka (Smart Island – Smart People) ในโครงการ ICT๔D โดยนำ ICT เข้าสู่ทุกหมู่บ้าน ประชาชนทุกคน ทุกธุรกิจ และเปลี่ยนวิธีคิดและการทำงานของรัฐบาล ซึ่งเป็นการดำเนินการโดยหน่วยงาน ICT ของศรีลังกา (ICTA) และมีการแก้ไขเพิ่มเติมกฎหมายเทคโนโลยีสารสนเทศและการสื่อสารฉบับที่ ๒๗ ปี ๒๕๔๖ (แก้ไขเพิ่มเติมโดยพระราชบัญญัติฉบับที่ ๓๓ ปี ๒๕๕๑) มีการปฏิรูปกฎหมายและนโยบาย รวมถึงการปฏิรูประบบความปลอดภัยทาง Cyber และอาชญากรรมออนไลน์

- วาระการรักษาความปลอดภัย Cyber แห่งชาติ มีการรวมเข้ากับกรอบอาชญากรรมไซเบอร์ มีวัตถุประสงค์เพื่อสร้างความเชื่อมั่นและความมั่นใจในธุรกรรมทางอิเล็กทรอนิกส์ผ่านมาตรการทางกฎหมายและนโยบาย ได้แก่ พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ ฉบับที่ ๑๙ ปี ๒๕๔๙ ซึ่งมีเทคโนโลยีสำหรับลายเซ็นอิเล็กทรอนิกส์และเทคโนโลยีการตรวจสอบ และมาตรการด้านเทคนิคและนโยบาย มีการใช้ DNSSEC ในระดับ ccTLD เป็นครั้งแรกในเอเชียใต้ ซึ่งเป็นกรอบนโยบายของรัฐบาลอิเลคทรอนิคส์ที่เป็นนโยบายระดับสูง

- มาตรการรักษาความปลอดภัยไซเบอร์มาตรการเกี่ยวกับระบบ - National CERT โดย ICTA จัดตั้ง Sri Lanka CERT ในปี พ. ศ. ๒๕๔๙ ในรูปแบบการทำงานร่วมกับรัฐบาล มีหน้าที่จัดการกับภัยคุกคาม นิติวิทยาศาสตร์ และพัฒนานโยบายด้าน IS และเป็นสมาชิกเต็มรูปแบบของ APCERT และ FIRST มีการดำเนินการร่วมกับ CERT-CC ในการเจาะระบบ APCERT เมื่อปี ๒๐๑๑, ๒๐๑๓ และ ๒๐๑๕ และมีโครงการความปลอดภัยไซเบอร์สำหรับเด็ก และสัปดาห์ความปลอดภัยไซเบอร์ ซึ่งดำเนินการเป็นระยะเวลา ๖ ปี

- กลยุทธ์อาชญากรรมทางไซเบอร์และกรอบความยุติธรรมทางอาญา : ประเทศศรีลังกามีกฎหมาย COMPUTER CRIME ACT ฉบับที่ ๒๔ ปี พ.ศ. ๒๕๕๐ กฎหมาย PAYMENT DEVICES FRAUDS ACT ฉบับที่ ๓๐ และศรีลังกาได้ออกคำแนะนำจาก FATF (Financial Action Task Force) ในกฎหมายการป้องกันการฟอกเงินฉบับที่ ๕ ของปี พ.ศ. ๒๕๔๙ กฎหมายว่าด้วยการรายงานธุรกรรมทางการเงินฉบับที่ ๖ ปี พ.ศ. ๒๕๔๙ และมาตรการอื่นๆ เกี่ยวกับอาชญากรรมทางนิติวิทยาศาสตร์ดิจิทัลสำหรับหน่วยงานตำรวจ โดยมีการพัฒนามาตรฐานกระบวนการปฏิบัติงาน

- เงื่อนไขการป้องกันและความร่วมมือระหว่างประเทศ : พระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ – ครอบคลุมประเด็นที่นอกเหนือจากความผิดที่สำคัญ เงื่อนไข และการป้องกันภายใต้อนุสัญญาบูดาเปสต์ มีมาตรการต่างๆ เช่น การค้นหาและการยึดคอมพิวเตอร์ การสกัดกั้นการสื่อสารที่จะต้องได้รับการรับรองจากผู้พิพากษา คำร้องดูแลรักษา ใบสั่งผลิตเพื่อการผลิตในประเทศ การเก็บรักษา คำร้องขอให้ผู้ให้บริการต่างชาติให้ความช่วยเหลือด้านกฎหมายร่วมกัน เป็นต้น

- ศรีลังกาได้รับเชิญให้เข้าร่วมการประชุมบรอดแบนด์อาชญากรรมไซเบอร์ (๒๓ กุมภาพันธ์ ๒๐๑๕) เข้าร่วมการประชุมอาชญากรรมทางอาญา (๒๙ พ.ค. ๒๐๑๕) ซึ่งเป็นประเทศแรกในเอเชียใต้และประเทศที่ ๒ ในเอเชียหลังจากประเทศญี่ปุ่น โดยศรีลังกาก้าวหน้านำ ฟิลิปปินส์ เกาหลีใต้ มาเลเซีย และประเทศอื่นๆ และได้เข้าเป็นสมาชิกสภายุโรปเร็วที่สุด ตั้งแต่วันที่ ๑ กันยายน ๒๐๑๕

- หน่วยงานพหุภาคีสามารถช่วยเหลือประเทศต่างๆ ในการพัฒนานโยบายและยุทธศาสตร์ด้านนโยบายภายในอย่างครบถ้วนภายในโครงการ ICT๔D ช่วยในการสร้างรูปแบบสถาบัน (ตัวอย่าง CERT ของศรีลังกา) โดยการสนับสนุนอย่างต่อเนื่องและยั่งยืน

UNODC Facilitation of Effective and Efficient Implementation of MLA in Southest Asia
(Mr. Gunsu Yang – UNODC)

- UNODC (United Nations Office on Drugs and Crime) ในเอเชียตะวันออกเฉียงใต้และแปซิฟิก มีสำนักงานภูมิภาคเอเชียตะวันออกเฉียงใต้ในภูมิภาคเอเชีย ๖ แห่ง คือ กัมพูชา อินโดนีเซีย สาธารณรัฐประชาธิปไตยประชาชนลาว พม่า เวียดนาม ไทย และฟิจิ (สำนักงานโครงการ)

- UNODC มีโครงการในภูมิภาคเอเชียตะวันออกเฉียงใต้ เกี่ยวกับการรวมตัวในระดับภูมิภาค โดยสนับสนุนกรอบและเครือข่ายที่สอดคล้องกับความต้องการของประเทศ และปรับปรุงความสามารถของรัฐในการตอบสนองต่อกฎกติกาและความปลอดภัย รวมถึงอาชญากรรมในโลกไซเบอร์ การค้ามนุษย์ และการแสวงหาผลประโยชน์ทางเพศจากเด็ก

- โครงการภูมิภาคของ UNODC ปี ๒๐๑๔ – ๒๐๑๙ มีโครงสร้างของโครงการะดับภูมิภาคที่ส่งผลกระทบในการเพิ่มขีดความสามารถของเอเชียตะวันออกเฉียงใต้ในการป้องกันและตอบสนองต่อยาเสพติดและการคุกคามทางอาญา แบ่งออกเป็น อาชญากรรมที่จัดเป็นองค์กรข้ามชาติและการค้ามนุษย์ที่ผิดกฎหมาย การต่อต้านการทุจริต การป้องกันการก่อการร้าย ความยุติธรรมทางอาญา การลดความต้องการยา เอชไอวี และการพัฒนาทางเลือก

- UNODC ให้ความร่วมมือระหว่างประเทศในเรื่องคดีอาญา ได้แก่ การตรวจสอบหาทรัพย์สินที่ได้มาจากการกระทำความผิด การส่งผู้ร้ายข้ามแดน การโอนกรรมสิทธิคดีอาญา ความช่วยเหลือด้านกฎหมายร่วมกัน และ การโอนตัวบุคคลที่ถูกคุมขัง

- UNODC มีการให้ความร่วมมืออย่างไม่เป็นทางการ ผ่านทางผู้ปฏิบัติงาน หรือเจ้าหน้าที่กำกับดูแล โดยจำกัดการเข้าถึงข้อมูลและปัญหาในประเด็นที่มีหลักฐานชัดเจน

- UNODC มีการให้ความร่วมมืออย่างเป็นทางการด้านพื้นฐานทางกฎหมาย อนุสัญญา/ สนธิสัญญา พหุภาคี ได้แก่ อนุสัญญาสหประชาชาติอาเซียน MLAT สนธิสัญญาทวิภาคี กฎหมายในประเทศ และสัญญาการแลกเปลี่ยนผ่านทางช่องทางการทูต

- จากการวิเคราะห์ขั้นตอนทั่วไปของกระบวนการทางกฎหมายภายในประเทศต่างๆ ที่จะนำไปสู่การใช้กฎหมายระหว่างประเทศ จะเริ่มต้นจากตำรวจหรืออัยการสูงสุด กระทรวงยุติธรรมหรือสำนักงานอัยการสูงสุด และกระทรวงการต่างประเทศ

- รูปแบบของโครงสร้างหน่วยงานกลาง ต้องเป็นหน่วยงานที่รับผิดชอบด้านความร่วมมือระหว่างประเทศและความยุติธรรม อาจแตกต่างกันไปขึ้นอยู่กับสนธิสัญญาหรือกฎหมายภายในประเทศ การติดต่อหน่วยงานกลางอาจเป็นการติดต่อโดยตรง หรือผ่านทางช่องทางการทูต และต้องอาศัยประสิทธิผลและขีดความสามารถของเจ้าหน้าที่ระดับกลาง

- หน่วยงานกลางภายใต้สนธิสัญญาการให้ความช่วยเหลือด้านกฎหมายร่วมกันของอาเซียน มีดังนี้
    - บรูไน พม่า มาเลเซีย สิงคโปร์ และไทย : อัยการสูงสุด
    - กัมพูชา และสาธารณรัฐประชาธิปไตยประชาชนลาว : รัฐมนตรีว่าการกระทรวงยุติธรรม
    - อินโดนีเซีย : รัฐมนตรีว่าการกระทรวงกฎหมายและสิทธิมนุษยชน
    - ฟิลิปปินส์ : เลขานุการเพื่อความยุติธรรม
    - เวียดนาม : รัฐมนตรีว่าการกระทรวงความมั่นคงสาธารณะ

  จากรูปแบบของโครงสร้างของหน่วยงานกลางดังกล่าว แสดงให้เห็นถึงการขาดสนธิสัญญาตามกฎหมาย/พหุภาคี หรือกฎหมายภายในประเทศ มีอุปสรรคด้านภาษา/ขาดรูปแบบมาตรฐาน มีปัญหาเกี่ยวกับการรักษาความลับ การสื่อสารและการประสานงานภายในไม่เพียงพอ และขาดการติดต่อสื่อสารทางอ้อม

- UNODC มีการจัดประชุมระดับภูมิภาค โดยมีการฝึกอบรมการให้ความช่วยเหลือด้านกฎหมายร่วมกัน ซึ่งเป็นการประชุมระดับอาวุโสเกี่ยวกับการให้ความช่วยเหลือด้านกฎหมายร่วมกัน และการประชุมเชิงปฏิบัติการเกี่ยวกับหน่วยงานกลางในการให้ความช่วยเหลือด้านกฎหมายร่วมกัน

- UNODC มีการจัดฝึอบรมในระดับภูมิภาค เพื่อเสริมสร้างขีดความสามารถภายใต้การประเมินความต้องการโดยมุ่งเน้น ที่พม่า ลาว กัมพูชา เวียดนาม โดยมีการแปลคู่มือการใช้งานของ UNODC MLA, การศึกษาเกี่ยวกับหลักฐานดิจิทัล

- การเสริมสร้างเครือข่ายระดับภูมิภาค โดยเป็นการเสริมสร้างเครือข่ายระดับภูมิภาคเพื่อความร่วมมือระหว่างประเทศในเรื่องอาชญากรรม ที่ CCPCJ รับรอง

- ARIN-AP (Asset Recovery Agency Network - Asia Pacific) network เป็นเครือข่ายที่มุ่งเน้นการดำเนินการเกี่ยวกับการดำเนินการด้านอาชญากรรม เพื่อเพิ่มประสิทธิภาพของของรัฐในการสืบหาทรัพย์สินที่ใช้ในการกระทำความผิด

- ให้การวิเคราะห์ความร่วมมือทางอาญาในระดับภูมิภาค โดยการวิเคราะห์ช่องโหว่ทางกฎหมายและการปฏิบัติงาน และเสนอข้อเสนอแนะเพื่อปรับปรุงการให้ความช่วยเหลือด้านกฎหมายร่วมกัน การสืบค้นทรัพย์สินที่ใช้ในการกระทำความผิด และการดำเนินการส่งผู้ร้ายข้ามแดน

- การสนับสนุนการประชุมเจ้าหน้าที่อาวุโสอาเซียนเกี่ยวกับ ASEAN MLAT และการประชุมหน่วยงานกลางระหว่างประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้

- ข้อเสนอแนะเกี่ยวกับแนวทางปฏิบัติ
  - ทบทวนและปรับปรุงกฎหมาย MLA
  - ร่างและใช้สนธิสัญญา MLA ระดับภูมิภาค
  - จัดตั้งหน่วยงานกลางเพื่ออำนวยความสะดวกด้านความร่วมมือระหว่างประเทศ ในเรื่องอาชญากรรม ผ่านการช่วยเหลือด้านกฎหมายและการส่งผู้ร้ายข้ามแดน
  - หน่วยงานกลางควรได้รับการจัดสรรทรัพยากรอย่างเพียงพอ และมีบุคลากรที่เชี่ยวชาญเฉพาะด้านเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ
  - เจ้าหน้าที่ระดับกลางควรสามารถสื่อสารภาษาอังกฤษได้อย่างมีประสิทธิภาพ หรือสามารถเข้าถึงนักแปลได้
  - สื่อสารโดยตรงกับหน่วยงานกลางอื่นๆ
  - สร้างช่องทางการสื่อสารอย่างเป็นทางการและไม่เป็นทางการ
  - มีส่วนร่วมในช่องทางการให้ความช่วยเหลืออย่างไม่เป็นทางการก่อน ระหว่าง และหลังการส่งคำขอ MLA
  - ให้ข้อมูลที่ชัดเจนและสามารถเข้าถึงได้ง่ายเกี่ยวกับข้อกำหนด ขั้นตอนในประเทศ สำหรับ MLA ผ่านทางอินเทอร์เน็ต
  - มีการประสานงานระหว่างหน่วยงานต่างๆ ในระดับประเทศ
  - ลดความซับซ้อนของขั้นตอนสำหรับ MLA
  - เพิ่มการฝึกอบรมบุคลากรที่เกี่ยวข้องกับ MLA

E-Evidence and Digital Forensics

(Mr. Seunghwan Park – World Bank)

- หลักฐานทางอิเล็กทรอนิกส์มีความผันผวน หลากหลาย และมีหลายเขตอำนาจศาล นิติดิจิตอลกำลังกลายเป็นเรื่องจำเป็นมากขึ้น หลักฐานทางอิเล็กทรอนิกส์ต้องมีการพิจารณาขั้นตอน หลักฐาน และการพิจารณาคดี

- ต้องมีการพิจารณาขั้นตอนในการค้นหาและการจับกุม เนื่องจากฮาร์ดแวร์อิเล็กทรอนิกส์ และข้อมูลอิเล็กทรอนิกส์จะมีขั้นตอนและวิธีการปฏิบัติที่แตกต่างกัน จึงจำเป็นต้องมีการป้องกันการค้นหาโดยพลการ และการละเมิดสิทธิในความเป็นส่วนตัว โดยต้องมีแนวทางในการปฏิบัติเพื่อจัดการกับหลักฐานทางอิเล็กทรอนิกส์

- ตัวอย่างกรณีการพิจารณาคดีทางศุลกากรเกาหลี :
  - เจ้าหน้าที่บังคับใช้กฎหมายได้สืบสวนสำนักงานของ บริษัท A เมื่อมีข้อสงสัยเกี่ยวกับการหลีกเลี่ยงภาษีโดยลดต้นทุนต่อหน่วย จึงยึดเอกสารและข้อมูลอิเล็กทรอนิกส์
  - ในระหว่างการค้นหาและจับกุมในสำนักงานของ บริษัท A เครื่องคอมพิวเตอร์โน๊ตบุ๊ค เอกสาร และข้อมูลอิเล็กทรอนิกส์ เกี่ยวกับ บริษัท B ถูกยึดด้วย
  - บนพื้นฐานของข้อมูลที่ยึด บริษัท B ถูกเรียกเก็บเงินภายหลังจากที่ได้รับการยืนยันว่า บริษัท B ได้หลีกเลี่ยงอัตราภาษีศุลกากรเช่นเดียวกับ บริษัท A

  จึงต้องพิจารณาว่ามีการเก็บรวบรวมพยานหลักฐานตามขั้นตอนที่กำหนดหรือไม่ และมีการละเมิดสิทธิใดๆ หรือไม่ อย่างไร

- การพิจารณาด้านสิทธิมนุษยชน :
  - การสกัดกั้นแบบ Real Time : ส่วนใหญ่เป็นการล่วงล้ำ คล้ายกับการสกัดกั้นทางโทรศัพท์
  - ข้อมูลที่จัดเก็บในเครือข่าย : ความเป็นส่วนตัวลดลง เนื้อหาที่เฉพาะเจาะจง
  - การเก็บรักษาข้อมูล : ล่วงล้ำให้น้อยที่สุด

- การพิจารณาหลักฐาน : มีการเปลี่ยนการครอบครองพยานหลักฐานโดยพนักงานเจ้าหน้าที่ในทุกขั้นตอนการปฏิบัติงาน (Chain of Custody) จึงต้องมีการบันทึกการครอบครองพยานหลักฐานเพื่อให้มั่นใจว่าเป็นพยานหลักฐานจริง ยอมรับได้ มีความน่าเชื่อถือ และมีความสมบูรณ์

- ตัวอย่างขั้นตอนในการยึดคอมพิวเตอร์ในบ้าน :
  - ดูด้านหน้าและด้านหลังของเครื่องคอมพิวเตอร์ รวมทั้งสายไฟ และอุปกรณ์เชื่อมต่อตามที่พบ
  - ถ่ายภาพบริเวณโดยรอบก่อนที่จะย้ายหลักฐานใดๆ
  - หากเครื่องคอมพิวเตอร์ "ปิด" อย่า "เปิด"
  - หากเครื่องคอมพิวเตอร์ "เปิด" และแสดงภาพบนจอภาพให้ถ่ายภาพหน้าจอ
  - ถอดสายไฟและอุปกรณ์ทั้งหมดออก
  - เก็บรวบรวมให้เป็นระเบียบ (รวมทั้งเราเตอร์และโมเด็ม) ทำการขนส่ง และจัดเก็บ

- เก็บสื่อทั้งหมดไว้ห่างจากแม่เหล็ก เครื่องส่งสัญญาณวิทยุ และส่วนประกอบที่อาจเป็นอันตรายอื่น
- รวบรวมคู่มือ เอกสาร และบันทึกย่อ
- ทำเอกสารขั้นตอนทั้งหมดที่เกี่ยวข้องกับการยึดคอมพิวเตอร์และส่วนประกอบ

- เครือข่ายเซิร์ฟเวอร์ / เครือข่ายธุรกิจ :
  - ปรึกษาผู้เชี่ยวชาญด้านคอมพิวเตอร์เพื่อขอความช่วยเหลือ
  - ต้องคำนึงถึงความปลอดภัยในที่เกิดเหตุ และอย่าให้ใครสัมผัสยกเว้นบุคลากรที่ได้รับการฝึกอบรมเพื่อจัดการกับระบบเครือข่าย
  - การดึงปลั๊กอาจทำลายระบบอย่างรุนแรง ทำให้ขัดขวางธุรกิจที่ถูกกฎหมาย ซึ่งเป็นการสร้างความรับผิดชอบให้กับพนักงานเจ้าหน้าที่

- ข้อพิจารณาเขตอำนาจศาล :
  - ความร่วมมืออย่างเป็นทางการ : สนธิสัญญาตามความช่วยเหลือทางกฎหมาย มีระยะเวลาการตอบกลับใช้เวลานาน
  - ความร่วมมืออย่างไม่เป็นทางการ : การสื่อสารระหว่างหน่วยงานกับหน่วยงาน มีระยะเวลาการตอบสนองสั้นลง มีข้อจำกัดด้านอรรถประโยชน์และความสม่ำเสมอ
  - Cloud Storage : อาณาเขตหลากหลาย ค้นหาเขตอำนาจศาลของผู้ให้บริการ

- ข้อพิจารณาเขตอำนาจศาล: ความร่วมมืออย่างเป็นทางการ / ไม่เป็นทางการ :

ข้อพิจารณา	เป็นทางการ	ไม่เป็นทางการ
วัตถุประสงค์	ได้รับหลักฐานเพื่อใช้ในการพิจารณาคดีและริบทรัพย์สิน	ได้รับข้อมูลข่าวสารและข้อมูลเพื่อช่วยในการตรวจสอบ
ประเภทของความช่วยเหลือ	มาตรการการสอบสวนในลักษณะบังคับและรูปแบบอื่นๆ ด้านตุลาการ	มาตรการการสอบสวนที่ไม่บังคับ (เช่น การเปิดเผยข้อมูลการสืบสวนร่วม)
กระบวนการติดต่อ	โดยทั่วไปไม่ตรง	โดยตรง
ความต้องการ	อาจรวมถึงความผิดทางอาญาของประเทศที่เกี่ยวข้อง ความสัมพันธ์พิเศษ	โดยปกติจะเป็นเพียงการติดต่อหน่วยงานกับหน่วยงาน
ข้อดี	หลักฐานเป็นที่ยอมรับได้ในศาล ช่วยให้สามารถบังคับใช้กฎหมายได้	ได้รับข้อมูลอย่างรวดเร็ว
ข้อจำกัด	ใช้เวลานาน ทรัพยากรหลากหลาย	ข้อมูลไม่สามารถใช้เป็นหลักฐานได้เสมอ

- Korea National Digital Forensics Center (NDFC) : ส่วนดิจิทัลฟอเรนสิกส์ ประกอบด้วย
  - Computer Forensics Team
  - Mobile Forensics Team
  - Database Forensics Team
  - Anti-Anti Forensics Team

  มีระบบการจัดการพยานหลักฐานดิจิทัล และมีการฝึกอบรม

Cybersecurity-Bangladesh Perspective

(Mr. Debdulal Roy - General Manager, Information Systems Development Department, Bangladesh Bank)

- คำจำกัดความของไซเบอร์ (Cyber) คือสิ่งใดๆก็ตามที่เกี่ยวข้องกับอินเตอร์เน็ต และถูกใช้เป็นคำนำหน้าของคำศัพท์เพื่ออธิบายถึงสิ่งใหม่ๆที่เกิดขึ้นจากการแพร่กระจายของคอมพิวเตอร์

- การรักษาความปลอดภัยไซเบอร์ (Cyber Security) คือการรวบรวมเทคโนโลยี, กระบวนการ และการควบคุม มาหลอมรวมกันเพื่อปกป้องระบบคอมพิวเตอร์, ระบบเครือข่าย และข้อมูล ให้ปลอดภัยจากการโจมตีในโลกไซเบอร์ โดยการรักษาความปลอดภัยในโลกไซเบอร์ที่มีประสิทธิภาพจะช่วยลดความเสี่ยงจากการโดนโจมตี และปกป้องค์กรและบุคคลจากการใช้ประโยชน์จากผู้ไม่ได้รับสิทธิในการเข้าถึงระบบคอมพิวเตอร์, ระบบเครือข่าย และเทคโนโลยี เป็นต้น

- เสาหลักทั้ง ๕ ของการรักษาความปลอดภัยไซเบอร์ (Five Pillars of Cyber Security) ได้แก่
  - การแยกแยะ (Identify) : ความเสี่ยงทางไซเบอร์ทั้งจากภายในและภายนอก
  - การตรวจจับ (Detect) : การบุกรุกระบบ, การละเมิดข้อมูล และการเข้าถึงโดยไม่ได้รับอนุญาต
  - การป้องกัน (Protect) : ระบบของหน่วยงาน, สินทรัพย์ และข้อมูล
  - การตอบสนอง (Respond) : เหตุการณ์ความปลอดภัยในโลกไซเบอร์ที่อาจเกิดขึ้น
  - การกู้คืน (Recover) : การกู้คืนการดำเนินงาน และสามารถให้บริการได้ตามปกติเมื่อเกิดเหตุการณ์ด้านความปลอดภัยไซเบอร์

- ทำไมเราจึงต้องมีการรักษาความปลอดภัยไซเบอร์นั่นหลายปัจจัย ตัวอย่างเช่น ไวรัสคอมพิวเตอร์ที่เรียกว่า MyDoom ซึ่งนับเป็นไวรัสแพงที่สุดตลอดกาล สร้างความเสียหายทางการเงินประมาณ ๓๑ พันล้านเหรียญ, บัญชีผู้ใช้งาน Facebook ประมาณ ๖๐๐,๐๐๐ บัญชีถูกบุกรุกทุกวัน, จำนวนเงินกองทุนที่สูญหายในการโจมตีทางอินเทอร์เน็ตไม่สามารถกู้คืนเกือบ ๖๘% และในการตรวจพบการโจมตีหรือโจรกรรมทางไซเบอร์ ใช้เวลาโดยเฉลี่ยเกือบ ๑๗๐ วัน

- ตัวอย่างล่าสุดของเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยไซเบอร์ ได้แก่
  - จุดแลกเปลี่ยนของ Cryptocurrency ที่โตเกียว เปิดเผยว่าถูกแฮ็กเกอร์ขโมยเงินมูลค่ากว่า 58 พันล้านเยน (532 ล้านเหรียญสหรัฐ) ทำให้ลูกค้าเกิดความวิตกถึงสถานการ์ณในอนาคตของสินทรัพย์เสมือน [๒๗ ม.ค. ๒๐๑๘]
  - พนักงานไปรษณีย์ขโมยบัตรเครดิตนับสิบใบเพื่อมาซื้อรถซูเปอร์คาร์มาเซราตี [๒๔ ม.ค. ๒๐๑๘]
  - พนักงาน Greenbay ได้แฮ็กข้อมูลส่วนบุคคลจากไฟล์ของฝ่ายทรัพยากรบุคคลผ่านเครื่องเซิร์ฟเวอร์ที่ไม่ได้ทำการอุดช่องโหว่ ซึ่งแฮกเกอร์ได้นำข้อมูลนั้นไปทำการโจรกรรรมเงินจากบัญชีธนาคารของผู้เสียหายหลายคน [๒๓ ม.ค. ๒๐๑๘]
  - บริษัท National Stores แจ้งให้ลูกค้าทราบว่าตรวจพบมัลแวร์ซึ่งอาจเป็นไปได้ว่ามีบัญชีบัตรที่อาจถูกบุกรุกได้ [๒๓ ม.ค. ๒๐๑๘]
  - OnePlus ปิดการประมวลผลบัตรเครดิตหลังจากลูกค้าแจ้งว่าพบช่องโหว่ในแพลตฟอร์มการประมวลผลการชำระเงินเครดิตบนเว็บไซต์ ซึ่งอาจทำให้ถูกโจมตีได้ [๑๖ ม.ค. ๒๐๑๘]

- ร้านค้าออนไลน์ไม่สามารถระบุความรุนแรงของการละเมิดบัตรเนื่องจาก "ขาดการสำรองข้อมูล"
- Thefly.com แจ้งว่า ยังมีบัตรเครดิตอีก ๒๗,๐๐๐ ใบทที่เหลืออยู่ในฐานข้อมูลที่ใช้ร่วมกันนั้นยังไม่ได้มีการเข้ารหัสเพื่อความปลอดภัยไว้ [๐๒ ม.ค. ๒๐๑๘]
- Jason's Deli ประสบปัญหาการละเมิดช่องโหว่ของ POS ที่มีผลต่อลูกค้า ๒ ล้านราย
- ที่รัสเซีย แฮกเกอร์ขโมยเงินกว่า ๓๑ ล้านเหรียญสหรัฐจากบัญชีผู้สื่อข่าวที่ธนาคารกลางรัสเซียและจากบัญชีธนาคารพาณิชย์ (ธ.ค. ๒๐๑๖)
- ธนาคารเทสโก้: ลูกค้า ๒๐,๐๐๐ รายมีพบว่ามีการลบกองทุนเถื่อนออกจากบัญชีของพวกเขา (พ.ย. ๒๐๑๖)
- National Payment Corporation of India พบการโจมตีด้วยมัลแวร์ที่มาจากตู้เอทีเอ็มทำให้เกิดปัญหากับบัตรเดบิต ๓.๒ ล้านใบ ของธนาคารอินเดีย ๑๙ แห่ง (ตุลาคม ๒๐๑๖) เป็นต้น

- แนวโน้มเรื่องการรักษาความปลอดภัยไซเบอร์ (Cyber Security Predictions)
  - มีการใช้อุปกรณ์ในการแฮ๊คระบบหรือหาช่องโหว่โดยอัตโนมัติ ซึ่งสามารถหาช่องโหว่ได้อย่างรวดเร็ว
  - ปัญญาประดิษฐ์แบบสั่งงานด้วยเสียง เช่น SIRI หรือ Alexa จะช่วยเปิดประสบการณ์ใหม่ของผู้ใช้และจะมีแอพลิเคชั่นที่ออกมารองรับระบบดังกล่าวเป็นจำนวนมากในปี 2018 นี้
  - ประชากรคนรุ่นใหม่ (คนยุค Millennials) จะเป็นตัวแทนของการเปลี่ยนแปลงทางวัฒนธรรมที่อาจท้าทายนโยบายการรักษาความปลอดภัยในที่ทำงาน ซึ่งจะมีการแบ่งปันข้อมูลส่วนบุคคลและการใช้งานอุปกรณ์ดิจิตอลของตัวเองมากขึ้น ทำให้อาจเกิดการละเมิดข้อมูลโดยไม่ได้ตั้งใจเพิ่มขึ้น
  - ผู้ผลิต IoT จะต้องรับผิดชอบต่อความปลอดภัยการละเมิดมากยิ่งขึ้น
  - อุปกรณ์ IoT จะถูกใช้เป็นการโจมตีบริการแบบ DDoS มากกว่าเดิม

- นวัตกรรมในการรักษาความปลอดภัยไซเบอร์ (Innovations in Cyber Security) มีดังนี้
  - การตรวจจับการโจมตี ได้แก่ การใช้ Machine Learning หรือปัญญาประดิษฐ์ ที่มีศักยภาพในการตรวจจับมัลแวร์แบบ zero-day และภัยคุกคามแบบถาวรขั้นสูง (APT)
  - การใช้ข้อมูลขนาดใหญ่ในการตรวจสอบความสัมพันธ์กับข้อมูลเพื่อเข้าใจภัยคุกคามได้ทันท่วงทีและสามารถปกป้องเครือข่ายได้
  - การรักษาความปลอดภัยของเครือข่าย โดยใช้ Software Defined Wide Arew Network
  - การรักษาความปลอดภัยของลูกค้าเสมือนอุปกรณ์ (vCPE) คือการให้บริการเครือข่ายแก่องค์กรต่างๆโดยใช้ซอฟต์แวร์มากกว่าอุปกรณ์ฮาร์ดแวร์เฉพาะแบบเดิม
  - การเพิ่มการรักษาความปลอดภัยให้กับคอนเทนเนอร์ โดยคอนเทนเนอร์จะช่วยให้ผู้ใช้สามรถจัดเก็บ แจกจ่าย และจัดการแอ็พพลิเคชันของ LINUX ได้ภายในตัวคอนเทนเนอร์เอง
  - นวัตกรรมในการรักษาความปลอดภัยไซเบอร์ที่อยู่ระหว่างการศึกษา ได้แก่ เทคโนโลยีBlockchain, การรักษาความปลอดภัย Cloud, ปัญญาประดิษฐ์ และเทคโนโลยีการเรียนรู้พฤติกรรม เป็นต้น

- สถานการณ์ด้าน ICT ของบังคลาเทศ
  - บังคลาเทศ มีทั้งสิ้น ๕๘ กระทรวง ในเว็บเชื่อมโยงกลาง (Portal) มีการให้บริการ eServices มากกว่า ๔๕๐ ระบบ โดยครอบคลุม ๔๓,๐๐๐ หน่วยงานราชการ
  - มีจำนวนผู้ใช้อินเทอร์เน็ตที่ลงทะเบียนทั้งสิ้น ๘๐.๘๓ ล้านคน และมีจำนวนผู้ใช้มือถือที่ลงทะเบียนทั้งสิ้น ๑๔๗ ล้านคน
  - มีศูนย์ดิจิตอล มากกว่า ๕,๒๐๐ ศูนย์ ทั่วประเทศ
  - ดัชนี Global Cybersecurity Index (GCI) ปีล่าสุดของบังคลาเทศ ได้คะแนน ๐.๕๒๔ อยู่อันดับที่ ๕๓ ของโลก และอันดับที่ ๑๓ ของเอเชียแปซิฟิค
  - ในส่วนที่ยังคงต้องมีการพัฒนาเพิ่มเติม ได้แก่
    (๑) เกี่ยวกับมาตรการทางกฎหมาย ควรมีการจัดทำกฎหมายเฉพาะเรื่องอาชญากรรมทางอินเทอร์เน็ต และมีข้อบังคับและข้อกำหนดด้านการปฏิบัติตามข้อกำหนดเฉพาะโลกไซเบอร์
    (๒) เกี่ยวกับมาตรการทางเทคนิค จำนวนบุคลากรที่ทำงานใน CIRT ยังไม่เพียงพอ, จัดทำกรอบความปลอดภัยของการรักษาความปลอดภัยไซเบอร์ที่ได้รับการยอมรับเป็นมาตรฐานสากลและได้รับการรับรอง
    (๓) เกี่ยวกับมาตรการทางหน่วยงาน จัดทำกลยุทธ์ความมั่นคงแห่งชาติ, จัดทำแผนงานการกำกับดูแลกิจการแห่งชาติเพื่อการรักษาความปลอดภัยไซเบอร์, จัดตั้งหน่วยงานที่รับผิดชอบในการดำเนินการระดับชาติเพื่อจัดทำแผนกลยุทธ์การรักษาความปลอดภัยไซเบอร์ และมีการทดสอบ Benchmarking แห่งชาติเพื่อวัดพัฒนาการและประสิทธิภาพในการรับมือการรักษาความปลอดภัยไซเบอร์
    (๔) มีมาตรการในการคุ้มครองเด็กในโลกออนไลน์
    (๕) การเพิ่มขีดความสามารถ โดยมี โครงการ R & D เพื่อการพัฒนามาตรฐานกลาง, มีการพัฒนากำลังคนเพื่อรับมือกับเหตุการณ์ต่างๆในโลกไซเบอร์, การสำรวจเพื่อติดตามผู้เชี่ยวชาญที่ผ่านการรับรองและขอคำแนะนำ
    (๖) ความร่วมมือ ต้องมีความร่วมมือระหว่างรัฐ เช่น ITU, APCERT, OIC-CERT, ความร่วมมือระหว่างหน่วยงานในการแบ่งปันทรัพย์สินในการรักษาความปลอดภัยไซเบอร์, ความร่วมมือภาครัฐในการแบ่งปันทรัพย์สินการรักษาความปลอดภัยไซเบอร์ และความร่วมมือระหว่างประเทศ เช่น APCERT, JPCERT, KRCERT

UNODC Response to Cybercrime

(Mr. Gunsu Yang – UNODC)

- คณะกรรมการป้องกันอาชญากรรมและความยุติธรรมทางอาญาแห่งสหประชาชาติ มอบหมาย UNODC ในปี พ.ศ. ๒๕๕๓ จัดตั้งกลุ่มผู้เชี่ยวชาญระหว่างรัฐบาลเกี่ยวกับอาชญากรรมขึ้นในปี พ.ศ. ๒๕๕๔ ตีพิมพ์ร่างการศึกษาเกี่ยวกับอาชญากรรมในปี พ.ศ. ๒๕๕๖ และก่อตั้งโครงการระดับโลกในปี พ.ศ. ๒๕๕๖

- เริ่มโครงการทั่วโลกเกี่ยวกับอาชญากรรม ปี พ. ศ. ๒๕๕๖ โดยมุ่งเน้นการเสริมสร้างศักยภาพและความช่วยเหลือด้านเทคนิค ซึ่งได้รับทุนสนับสนุนจากผู้บริจาคทั้งหมด

- UNODC มีการให้ความช่วยเหลือด้านเทคนิค การเสริมสร้างขีดความสามารถ การป้องกัน การทูตความร่วมมือข้ามชาติ และการทำงานร่วมกัน

- UNODC ดำเนินการสร้างการตอบสนองข้ามรัฐบาล ในหลายๆ ด้าน เช่น
  - การทูต : การทำงานร่วมกับคณะทูตถาวรกับองค์การสหประชาชาติและกระทรวงต่างๆ
  - นโยบาย : กระทรวงยุติธรรม การสื่อสาร การต่างประเทศ ความมั่นคงแห่งชาติ การศึกษา
  - การบังคับใช้กฎหมาย : ตำรวจ ความมั่นคง ตำรวจท้องที่ การบังคับใช้กฎหมายระหว่างประเทศและการข่าวกรอง
  - การฟ้องร้อง / คำพิพากษา : อัยการรัฐและแห่งชาติ และผู้พิพากษา
  - การป้องกัน : กระทรวงศึกษาธิการ เอ็นจีโอ กลุ่มศรัทธา ภาคเอกชน และอื่น ๆ
  - การตอบสนองแบบจำลองแห่งชาติ

- โครงการในอเมริกากลาง เริ่มที่ประเทศเอลซัลวาดอร์ ปีพ. ศ. ๒๕๕๗ และกัวเตมาลาปี พ.ศ. ๒๕๕๙ ปัจจุบันเอลซัลวาดอร์มีหน่วยงานอาชญากรรมไซเบอร์แห่งชาติดำเนินการอยู่ภายในหน่วยงานตำรวจแห่งชาติ UNODC ได้ให้การฝึกอบรมและให้คำปรึกษาอย่างสม่ำเสมอ และมีการทำงานร่วมกับทวิภาคีและระหว่างประเทศ รวมถึงศูนย์นานาชาติ กรณีเด็กหายและถูกแสวงประโยชน์

- สิ่งที่น่าสนใจคือ การเสริมสร้างความร่วมมือในระดับนานาชาติและระดับชาติ ความสามารถในการไต่สวนของอัยการ และการพิจารณาพิพากษา หลักฐานดิจิทัล / darknet / hidden-services

Capacity assessment

(Mr. Keong Min Yoon – World Bank)

- Assessment Tool คือ โปรแกรมที่ถูกพัฒนาขึ้นเพื่อเป็นเครื่องมือสำหรับประเมิน ที่ช่วยให้ประเทศต่างๆ สามารถประเมินขีดความสามารถในปัจจุบันของตนในการต่อสู้กับอาชญากรรมในโลกไซเบอร์ และระบุถึงลำดับความสำคัญในการสร้างขีดความสามารถ ในที่นี้เป็นไฟล์ Excel (เอกสารแนบ ๕)

- วัตถุประสงค์ของเครื่องมือการประเมิน คือ เพื่อให้ผู้ใช้สามารถกำหนดช่องว่างในขีดความสามารถ และเพื่อเน้นความสำคัญในการกำกับทรัพยากร การสร้างสมรรถนะ การใช้เครื่องมือประเมินผลครั้งแรกจะเป็นข้อมูลพื้นฐาน การอัปเดตมีเป็นระยะเพื่อเป็นการติดตามความคืบหน้า คำถามแต่ละข้อมีเป้าหมายที่จะตอบด้วยคำตอบ "ใช่ / ไม่ใช่" หรือเป็นตัวเลือกเดียวในกลุ่มคำตอบ มีการประเมินแบ่งเป็น ๙ หัวข้อ ซึ่งเป็นไปตามการจัดระเบียบใน Toolkit การอ่านแบบฟอร์มจะอ่านจากซ้ายไปขวาในแต่ละหัวข้อ ระดับ ๑ กำหนดแต่ละเรื่อง ระดับ ๒ ตั้งค่าเฟรมทั่วไปสำหรับแต่ละคำถามซึ่งจะถามในระดับ ๓ หรือปรับแต่งเพิ่มเติมในระดับ ๔ มีการตอบคำถามเป็นส่วนสุดท้าย การใช้และผลของการประเมินนั้นเป็นประโยชน์สำหรับหน่วยงานผู้นำไปใช้ และไม่มีการติดตามการจัดอันดับหรือการรายงานผลการค้นหา

- หลังจากตอบคำถามแล้วเสร็จ คลิกที่ "submit" จะแสดงผลลัพธ์โดยรวมเป็นแผนภูมิ "แมงมุม" การประเมินแต่ละหัวข้อจะแสดงความคืบหน้าตามรัศมีในแผนภูมิผลลัพธ์โดยรวม ผลลัพธ์ที่มาถึงด้านนอกสุดแสดงความสามารถที่สูงกว่า ผลลัพธ์ที่ใกล้กับศูนย์แสดงถึงความสามารถที่ต่ำกว่า โดยผลลัพธ์โดยรวมจะแสดงเป็น ๙ รัศมี เมื่อคลิกที่รัศมีของหัวข้อเฉพาะในแผนภูมิแมงมุม ผลลัพท์ที่ละเอียดขึ้นของแต่ละหัวข้อจะปรากฏขึ้น

- หน่วยงานหรือประเทศต่างๆ สามารถนำเครื่องมือนี้ไปทดลองศึกษา และใช้งานได้

รูปภาพการประชุม :















