การสืบสวนคดีอาชญากรรมทางไซเบอร์ (Cybercrime): บทเรียนจากสหภาพยุโรป (EU) สู่อาเซียน (ASEAN)

พลตำรวจโท ศักดา เตชะเกรียงไกร*
พันตำรวจโท ดร.นรินทร์ เพชรทอง**

ประวัติความเป็นมาศูนย์อาชญากรรมทางไซเบอร์ของยุโรป (European Cyber Crime Center / EC3)

เพื่อให้มีความพร้อมกับการรับมือของอาชญากรรมคอมพิวเตอร์นยุคดิจิทัล คณะกรรมการโทรคมนาคมของสหภาพยุโรปได้อนุมัติให้มีการจัดตั้งศูนย์อาชญากรรมทางไซเบอร์ของยุโรปขึ้นเมื่อ พ.ศ. 2556 โดยมีสำนักงานใหญ่อยู่ที่ตำรวจสากลภาคพื้นยุโรป (EUROPOL) ณ กรุงเฮก ประเทศเนเธอร์แลนด์ศูนย์ EC3 นี้จะเป็นจุดหลักสำคัญของสหภาพยุโรปในการรับมือกับอาชญากรรมทางไซเบอร์ทุกประเภท โดยจะทำให้การตอบสนองต่อเหตุการณ์และภัยคุกคามจากอาชญากรคอมพิวเตอร์เป็นไปอย่างรวดเร็ว โดยศูนย์นี้จะให้ความช่วยเหลือประเทศสมาชิกและสถาบันภายใต้สหภาพยุโรปในการสร้างความร่วมมือและความสามารถในการวิเคราะห์ในการสืบสวนสอบสวนต่อพันธมิตรนานาชาติ

ศูนย์ EC3 เป็นหน่วยงานภายในของตำรวจสากลภาคพื้นยุโรป (EUROPOL) ในการให้การสนับสนุนช่วยเหลือการสืบสวนสอบสวนคดีอาชญากรรมต่าง ๆ ภายใต้เขตอำนาจของตำรวจสากลภาคพื้นยุโรป โดยศูนย์ EC3 ได้เริ่มก่อตั้งตั้งแต่วันที่ 1 มกราคม 2556 ได้รวบรวมความเชี่ยวชาญด้านต่าง ๆ และข้อมูลข่าวสาร สนับสนุนการสืบสวนคดีอาชญากรรมเพื่อสนับสนุนงานในการแก้ปัญหาต่าง ๆ ของสหภาพยุโรป ซึ่งโดยปกติตำรวจสากลภาคพื้นยุโรปจะให้การสนับสนุนในการวิเคราะห์และสนับสนุนการปฏิบัติการต่อสหภาพยุโรปอยู่แล้ว ศูนย์ EC3 นี้จะเป็นเหมือนศูนย์กลางด้านข่าวสารอาชญากรรมทางไซเบอร์ (Cybercrime Hub) ให้กับสหภาพยุโรป, พัฒนาขีดความสามารถด้านดิจิทัลฟอเรนสิค (Digital Forensics) เพื่อสนับสนุนด้านการสืบสวนสอบสวนให้กับสหภาพยุโรปและสร้างบุคลากรให้มีความสามารถในการต่อกรกับอาชญากรรมไซเบอร์ ผ่านช่องทางการฝึกอบรม, การสร้างความตระหนักและการผลิตแนวทางการปฏิบัติที่ดีสุด (Best practice) ในการแก้ปัญหาของอาชญากรรมทางไซเบอร์ นอกจากนี้ทางศูนย์ EC3 จะสร้างนิคมของผู้เชี่ยวชาญโดยมีผู้เกี่ยวข้องมาจากทุกภาคส่วนในสังคมในการรับมือและป้องกันอาชญากรรมทางไซเบอร์รวมไปถึงคดีเกี่ยวกับการประทุษร้ายทางเพศต่อเด็กทางออนไลน์ (Online Child Sexual Abuse)

อาชญากรรมทางไซเบอร์นี้นับว่าเป็นปัญหาสำคัญมากขึ้นทุกวันอันเนื่องมาจากการทำกิจกรรมต่าง ๆ ได้ถูกย้ายจากออฟไลน์มาทำผ่านทางออนไลน์หรืออินเทอร์เน็ต ดังนั้นภัยคุกคามจากอาชญากรรมทางไซเบอร์ได้มีเพิ่มสูงขึ้น โดยมีกลุ่มผู้เสียหายเป้าหมายเป็นประชาชนโดยทั่วไปที่ใช้บริการออนไลน์ องค์กรทางธุรกิจ และรัฐบาลประเทศต่าง ๆ โดยสหภาพยุโรปก็ถือว่าเป็นเป็นเป้าหมายหลักของอาชญากรทางไซเบอร์

---

*ผู้บัญชาการโรงเรียนนายร้อยตำรวจ
**อาจารย์ (สบ2) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

มีผลการรายงานความเสียหายทางเศรษฐกิจทั่วโลกจากอาชญากรรมทางไซเบอร์ ซึ่งมีมูลค่าสูงถึงเกือบสามร้อยล้านยูโรในแต่ละปี ซึ่งอาชญากรรมทางไซเบอร์นี้ได้สร้างผลตอบแทนมากกว่ามูลค่าทางการค้าของยาเสพติดผิดกฎหมาย อาทิเช่นกัญชา, โคเคน และเฮโรอีน รวมกัน

ในการสืบสวนสอบสวนคดีฉ้อโกงทางออนไลน์, การประทุษร้ายต่อเด็กทางออนไลน์ และคดีอาญากรรมอื่น ๆ ทางออนไลน์โดยปกติจะต้องมีการเกี่ยวข้องกับเหยื่ออาชญากรรมนับร้อยนับพันและผู้ต้องสงสัยเกิดขึ้นพร้อม ๆ กันในหลากหลายที่ทั่วโลก การปฏิบัติการและรับมือกับคดีอาชญากรรมทางไซเบอร์เหล่านี้ไม่สามารถประสบความสำเร็จได้ด้วยอาศัยตำรวจจากประเทศใดประเทศหนึ่งเพียงลำพัง โดยเป็นที่รู้กันว่าไม่มีอาชญากรรมใดที่จะไร้พรมแดน (Borderless) ได้เท่ากับอาชญากรรมทางไซเบอร์ จึงจำเป็นอย่างยิ่งที่เจ้าหน้าที่บังคับใช้กฎหมายจะได้ปรับใช้ความร่วมมือและการประสานงานกันโดยไม่ยึดติดกับพรมแดน ซึ่งจะต้องทำงานร่วมกันในแนวทางนี้ไม่ว่าจะเป็นภาคเอกชนหรือภาครัฐบาล โดยตำรวจสากลภาคพื้นยุโรปถือว่าเป็นองค์กรที่มีความเด่นทางด้านผู้เชี่ยวชาญในด้านการบังคับใช้กฎหมาย ในการสนับสนุนการปฏิบัติการต่าง ๆ การประสานงาน และผู้เชี่ยวชาญทางอาชญากรรมทางไซเบอร์ ศูนย์ EC3 นี้จะได้จัดให้มีการตอบเสนอต่อความร่วมมือต่อประเทศต่าง ๆ ดังนี้

- ประเทศสมาชิกสหภาพยุโรป
- ประเทศที่ไม่ได้เป็นสมาชิกสหภาพยุโรป
- องค์กรระหว่างประเทศ
- ผู้ให้บริการอินเทอร์เน็ตต่าง ๆ
- บริษัทที่เกี่ยวข้องกับความปลอดภัยทางอินเทอร์เน็ตและธุรกิจภาคการเงิน
- ผู้เชี่ยวชาญทางฝ่ายวิชาการ
- องค์กรภาคสังคม
- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERTs) ทั้งในระดับโลกและระดับสหภาพยุโรป

ดังเช่นคำกล่าวให้สัมภาษณ์ของคุณร็อบ เวนไรท์ (Rob Wainwright) ผู้อำนวยการของตำรวจสากลภาคพื้นยุโรป ได้กล่าวไว้ว่า

“การจัดตั้งศูนย์ EC3 จะเป็นประวัติศาสตร์การพัฒนาของสหภาพยุโรปในการต่อกรกับอาชญากรรมทางไซเบอร์ ผมดีใจที่คณะกรรมการของสหภาพยุโรปได้เสนอให้มีการจัดตั้งหน่วยนี้ขึ้นภายใต้สังกัดของตำรวจสากลภาคพื้นยุโรป องค์กรอาชญากรรม, กลุ่มก่อการร้าย และอาชญากรในคดีอื่น ๆ ได้ฉวยโอกาสอย่างรวดเร็วในการใช้ช่องทางและโอกาสจากการพัฒนาการอย่างรวดเร็วของเทคโนโลยี และขณะนี้ก็ถือว่าเป็นโอกาสที่เหมาะสมแล้วของฝ่ายเจ้าหน้าที่ที่จะต้องก้าวไปให้ไวกว่าอาชญากรเหล่านี้อีกหนึ่งก้าว ศูนย์ EC3 นี้จะได้นำเสนอรัฐบาลต่าง ๆ ภาคธุรกิจ และประชาชนทั่วทั้งภาคพื้นยุโรปด้วยเครื่องมือที่จะใช้ในการรับมือกับอาชญากรรมทางไซเบอร์ ซึ่งศูนย์ EC3 นี้จะทำให้สหภาพยุโรป สมาร์ท, รวดเร็ว และเข้มแข็งในการต่อสู้กับอาชญากรรมทางไซเบอร์”

ย้อนมองดูเรา

จากคู่มือประชาคมอาเซียน ปี 2558 กับสำนักงานตำรวจแห่งชาติ[1] ซึ่งอาเซียนประกาศเจตจำนงที่จะมีเป้าหมายร่วมกันในการเข้าสู่การเป็นประชาคมอาเซียน ในวันที่ 31 ธันวาคม 2558 ซึ่งประกอบไปด้วยสามประชาคมหลักดังนี้ ประชาคมการเมืองและความมั่นคงอาเซียน, ประชาคมเศรษฐกิจอาเซียน, และประชาคมสังคมและวัฒนธรรมอาเซียน ในส่วนของกฎบัตรอาเซียน (ASEAN Charter) ที่เกี่ยวข้องกับการรับมือกับอาชญากรรมทางไซเบอร์ นั้นน่าจะเข้าตามความมุ่งประสงค์ของอาเซียนข้อที่ 8 ในคู่มือประชาคมอาเซียนปี 2558 ในหน้าที่ 23 ที่ระบุว่า “เพื่อตอบสนองอย่างมีประสิทธิภาพ ตามหลักความมั่นคงที่ครอบคลุมในทุกมิติต่อสิ่งท้าทายทุกรูปแบบ อาชญากรรมข้ามชาติและสิ่งท้าทายของพรมแดนอื่น ๆ” เพราะถือว่าอาชญากรรมทางไซเบอร์เป็นการกระทำความผิดที่ไร้พรมแดน มีผู้เกี่ยวข้องไม่ว่าจะเป็นเหยื่อหรือผู้เสียหาย, ผู้กระทำความผิด และฝ่ายผู้บังคับใช้กฎหมายมาจากหลายประเทศ แม้ว่ากฎบัตรอาเซียนยังไม่ได้มีการระบุโดยตรงเกี่ยวกับแนวทางในการรับมืออาชญากรรมทางไซเบอร์ แต่ในส่วนของประเทศไทยโดยสำนักงานตำรวจแห่งชาติที่เป็นหน่วยงานที่รับผิดชอบหลักเกี่ยวกับการสืบสวนสอบสวนคดีด้านอาชญากรรมทางไซเบอร์ของประเทศก็ได้ยึดแนวทางยุทธศาสตร์ประเทศ ยุทธศาสตร์ที่ 4 การสร้างความสมดุลและการปรับระบบบริหารจัดการภาครัฐ ในด้านการสร้างความร่วมมือด้านการป้องกันปราบปรามอาชญากรรมประกอบแนวทางการพัฒนากลไกความร่วมมือกับหน่วยงานตำรวจในอาเซียนและหน่วยงานความมั่นคงอื่น ๆ (คู่มือประชาคมอาเซียน ปี 2558, หน้า 27) ซึ่งในส่วนของยุทธศาสตร์การเข้าสู่ประชาคมอาเซียนของสำนักงานตำรวจแห่งชาติในยุทธศาสตร์ที่ 3 การสร้างความร่วมมือด้านการป้องกันและปราบปรามอาชญากรรม ทั้งในและนอกอาเซียน ในภารกิจที่ 7 การพัฒนากลไกการประสานงานระหว่างหน่วยงานตำรวจของประเทศสมาชิก ซึ่งปัจจุบันทางสำนักงานตำรวจแห่งชาติเองได้มีการเพิ่มประจำการของผู้ช่วยทูตฝ่ายตำรวจประจำการอยู่ใน 4 ประเทศเพื่อนบ้าน ดังนี้ ลาว กัมพูชา พม่าและจีน และในส่วนของกองบัญชาการตำรวจสันติบาลสำหรับประเทศมาเลเซีย ซึ่งผู้ช่วยทูตฝ่ายตำรวจนี้จะเป็นการช่วยส่งเสริมในด้านสนับสนุนการสืบสวนสอบสวนและการประสานขอความร่วมมือเกี่ยวกับการสกัดกั้นในด้านอาชญากรรมโดยทั่วไป โดยเน้นทางด้านอาชญากรรมเกี่ยวกับการค้ายาเสพติด (Drug Smuggling) เป็นหลัก ไม่ได้เน้นเฉพาะในด้านอาชญากรรมทางไซเบอร์และยังไม่ครอบคลุมประเทศทั้งหมดของประเทศสมาชิกอาเซียนที่เหลือไม่ว่าจะเป็นบรูไน ดารุสซาลาม, อินโดนีเซีย, มาเลเซีย[2], ฟิลิปปินส์, สิงคโปร์, และเวียดนาม

สรุปโดยรวมแล้วองค์กรตำรวจอาเซียน[3] (ASEANAPOL) ยังไม่มีหน่วยงานเฉพาะที่รับผิดชอบและรับมือกับอาชญากรรมทางไซเบอร์เหมือนกับการจัดตั้งศูนย์ EC3 ของตำรวจสากลภาคพื้นยุโรป (EUROPOL) เพื่อการประสานงานด้านการรับมือกับอาชญากรรมทางไซเบอร์ ซึ่งประเทศในกลุ่มอาเซียนถือว่าเป็นเป้าหมายในการโจมตีของกลุ่มแฮกเกอร์ต่าง ๆ ทั่วโลก ไม่ว่าจะเป็นทางด้าน

[1] ประชาคมอาเซียนกับสำนักงานตำรวจแห่งชาติ (2558)

[2] ประเทศที่ตั้งของสำนักงานองค์กรตำรวจอาเซียน (ASEANAPOL)

[3] โครงสร้างองค์กรตำรวจอาเซียน (2558) http://www.aseanapol.org/about-aseanapol/governance

การเป็นจุดเริ่มต้น (Origin), การเป็นจุดเชื่อมต่อ (Transit)[4] หรือจุดหมายปลายทาง (Destination)[5] ของอาชญากรทางไซเบอร์ ซึ่งผู้เขียนเห็นว่าหากประเทศในกลุ่มอาเซียนจะมีหน่วยงานรับผิดชอบโดยตรงเกี่ยวกับการต่อต้านอาชญากรรมทางไซเบอร์ในโอกาสที่อาเซียนกำลังจะมีการเกิดขึ้นอย่างเป็นทางการของประชาคมเศรษฐกิจอาเซียนหรืออีซี (AEC) ภายในสิ้นปี 2558 นี้ โดยในการนี้ควรจะต้องมีการริเริ่มหรือเสนอแนวความคิดมาจากประเทศใดประเทศหนึ่งหรือร่วมกัน ซึ่งอาจจะเป็นจากรัฐบาลไทยเองในที่ประชุมสุดยอดอาเซียน (ASEAN Summit) ในการประชุมในครั้งที่ 27 (ครั้งถัดไป) ดังเช่นผลการประชุมสุดยอดอาเซียนเมื่อเร็ว ๆ ที่จัดขึ้นที่กรุงกัวลาลัมเปอร์และลังกาวี ประเทศมาเลเซีย ทางรัฐบาลไทยโดยนายกรัฐมนตรีก็ได้เสนอในที่ประชุมให้มีความร่วมมือในการบริหารจัดการที่เกี่ยวกับปัญหาชายแดน ในการป้องกันและปราบปรามปัญหาด้านอาชญากรรมข้ามชาติ (Transnational Crime) การโยกย้ายถิ่นฐาน (Migration) รวมไปถึงด้านปัญหาการค้ายาเสพติด (Drug Smuggling)[6] ที่จะได้ริเริ่มให้มีการตั้งหน่วยงานที่รับมือกับอาชญากรรมทางไซเบอร์ โดยเฉพาะให้เป็นหน่วยงานหนึ่งภายใต้องค์กรตำรวจอาเซียน (ASEANAPOL) ก็จะทำให้การประสานความร่วมมือและการรับมือกับอาชญากรรมทางไซเบอร์นี้เป็นไปอย่างเป็นระบบ และมีประสิทธิภาพโดยได้รับความร่วมมือกันในส่วนของผู้บังคับใช้กฎหมายของทั้งสิบประเทศสมาชิกอาเซียนให้ได้ประสิทธิภาพดังเช่นที่ได้มีตัวอย่างให้เห็นมาแล้ว ในส่วนของศูนย์ EC3 ของสหภาพยุโรป โดยทางสำนักงานตำรวจแห่งชาติเองมีหน่วยงานที่เกี่ยวกับกับการรับมือกับอาชญากรรมทางไซเบอร์ไม่ว่าจะเป็น กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.), กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยีของกองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.), สำนักงานพิสูจน์หลักฐาน (สพฐ.) ที่มีหน้าที่เกี่ยวกับการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ หรือแม้แต่คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ (รร.นรต.) ผู้ให้ความรู้ด้านการศึกษาอบรมเกี่ยวกับอาชญากรรมคอมพิวเตอร์แก่ นักเรียนนายร้อยตำรวจและนักเรียนนายร้อยอบรม ผู้ที่จะสำเร็จการศึกษาไปเป็นข้าราชการตำรวจสัญญาบัตรในอนาคตอันใกล้และจะเป็นกำลังหลักสำคัญของสำนักงานตำรวจแห่งชาติในการขับเคลื่อนองค์กรในการต่อสู้กับอาชญากรรมทางไซเบอร์ต่อไป

นอกจากนี้ในการจะรับมือกับอาชญากรรมทางไซเบอร์จะไม่สามารถเกิดขึ้นได้อย่างมีประสิทธิภาพ หากขาดความร่วมมือของหน่วยงานดังต่อไปนี้ ไม่ว่าจะเป็น กระทรวงยุติธรรมที่มีหน่วยงานในสังกัดเช่น กรมสอบสวนคดีพิเศษ (DSI), สำนักงานป้องกันและปราบปรามการฟอกเงิน (ป.ป.ง.),

[4] ดีเอสไอโดยการประสานความร่วมมือกับ FBI ได้ทำการจับกุมแฮกเกอร์ชาวรัสเซีย (FaridEssebar) ซึ่งได้แฮกเว็บไซต์ของธนาคารในรัสเซียทำให้เกิดมูลค่าความเสียหายกว่าแสนล้านบาทไทย, http://www.nationmultimedia.com/national/Thai-agencies-nab-Russian-hacker-30229545.html

[5] เมื่อเดือนกรกฎาคม 2558 นี้เอง กลุ่มแฮกเกอร์โจมตี 82 เว็บในไทยโดยการเปิดเผยของกระทรวงไอซีที ซึ่งในการโจมตีนี้เป็นส่วนหนึ่งของการโจมตีของกลุ่มแฮกเกอร์นี้ของเว็บไซต์กว่า 500 เว็บทั่วโลก ซึ่งเว็บไซต์ที่ถูกโจมตีนี้ประกอบไปด้วยสถาบันการศึกษาและภาคธุรกิจของไทยไม่ว่าจะเป็นเว็บห้างสรรพสินค้าและเว็บธุรกิจด้านบันเทิง โดยตั้งแต่ต้นปีของปี 58 นี้มีการคุกคามด้านความมั่นคงปลอดภัยทางไอทีเกิดขึ้นแล้วกว่า 3,456 ครั้ง,http://www.bangkokpost.com/news/general/612444/hacker-gang-attacks-82-thai-websites

[6] ผลการประชุมที่เกี่ยวข้องในการประชุมอาเซียนครั้งที่ 26, กระทรวงการต่างประเทศ (2558), www.mfa.go.th/asean/th/news/2352/56441-การประชุมสุดยอดอาเซียน-ครั้งที่-26-และการประชุมที่.html

กระทรวงกลาโหม, กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงานอัยการสูงสุด หรือแม้แต่กรมสรรพากร ซึ่งการบูรณาการจากหน่วยงานต่าง ๆ ที่เกี่ยวข้องนี้ จะทำให้การประสานข้อมูลของสำนักงานตำรวจแห่งชาติกับหน่วยงานเหล่านี้ทำให้ได้ข้อมูลข่าวกรองด้านอาชญากรรมทางไซเบอร์ที่มีประสิทธิภาพ เพื่อให้การประสานงานในส่วนของผู้บังคับใช้กฎหมายในประเทศอาเซียนเกิดขึ้นได้อย่างเป็นระบบและมีประสิทธิภาพ อาจจะทำให้เกิดการร่วมปฏิบัติการ (ASEAN Operations) ในระดับประเทศสมาชิกอาเซียนในการต่อต้านอาชญากรรมทางไซเบอร์ร่วมกันดังเช่นที่มีการเกิดการปฏิบัติการในกลุ่มประเทศยุโรปมาแล้วเป็นต้น

กรณีศึกษาการสืบสวนคดีอาชญากรรมทางไซเบอร์จาก Europol (Cybercrime cases)

เมื่อวันที่ 6 ก.ค. 58 ศูนย์ EC3 ได้ร่วมโอเปเรชั่นภายใต้รหัสวอกเกอร์กับตำรวจแห่งชาติสเปนในการทลายกลุ่มแฮกเกอร์ที่จัดตั้งคอลเซนเตอร์แบบผิดกฎหมาย ณ เมืองบาเซโลนา กลุ่มอาชญากรนี้เป็นส่วนหนึ่งของกลุ่มอาชญากรทางไซเบอร์โดยใช้ช่องโหว่ของการบริการผ่านทางระบบโทรคมนาคมเป็นหลัก จากปฏิบัติการนี้เจ้าหน้าที่ตำรวจบุกค้นบ้านจำนวน 6 หลังและยึดโทรศัพท์มือถือกว่า 100 เครื่อง, ซิมโทรศัพท์มือถือที่ถูกโจรกรรม, อุปกรณ์คอมพิวเตอร์, เงินสด และบัตรเครดิตจำนวนมาก ซึ่งจากการสืบสวนของเจ้าหน้าที่ทราบว่ามีกลุ่มอาชญากรที่รับโทรศัพท์มือถือที่ถูกขโมยจากนักท่องเที่ยวในประเทศสเปน จากนั้นได้มีการนำโทรศัพท์นั้นมาสมัครใช้บริการโทรที่มีบริการพิเศษหรือบริการเสริม ทำให้เหยื่อหรือผู้เสียหาย ได้รับใบแจ้งค่าบริการที่สูงกว่าปกติ การดำเนินการในขั้นนี้โดยกลุ่มองค์กรอาชญากรรมทางไซเบอร์ซึ่งมีที่ตั้งอยู่นอกสหภาพยุโรป ซึ่งหัวใจหลักสำคัญในความสำเร็จของการปฏิบัติการนี้ของเจ้าหน้าที่ตำรวจยูโรโปล (Europol) คือความร่วมมือและการประสานงานที่ดีระหว่างเจ้าหน้าที่ตำรวจประเทศต่าง ๆ, เจ้าหน้าที่จากยูโรโปล และบริษัทโทรคมนาคมต่าง ๆ ในการรับมือกับอาชญากรรมทางดิจิทัลในรูปแบบนี้ ทางยูโรโปลก็ใช้เทคนิคที่เรียกว่าการสนับสนุนในพื้นที่ปฏิบัติการ (On-the-spot support) กับเจ้าหน้าที่ตำรวจของสเปนในการปฏิบัติการนี้โดยสามารถจับกุมผู้ต้องสงสัยรวมทั้งสิ้น 9 ราย เป้าหมายในการดำเนินการครั้งนี้คืออาชญากรทางไซเบอร์ที่เกี่ยวของกับการหลอกลวงผู้เสียหายผ่านทางการบริการโทรคมนาคม ซึ่งกลุ่มอาชญากรนี้มีส่วนในการสนับสนุนและการถ่ายโอนทรัพย์ที่ได้จากการฉ้อโกงทางโทรคมนาคม ซึ่งมูลค่าความเสียหายรวมของอาชญากรกลุ่มนี้กว่าสองล้านยูโร และมีผู้เสียหายจากหลายประเทศ

ย้อนกลับไปเมื่อเดือนกุมภาพันธ์ 2558 ศูนย์ EC3 ของยูโรโปลมีการทำบันทึกความร่วมมือกับบริษัทผู้เชี่ยวชาญในการบุกทลายกลุ่มแฮกเกอร์ที่สร้างซอฟแวร์เรียกค่าไถ่ (Ransomware)[7] ซึ่งเป็นบริษัททางด้านป้องกันภัยคุกคามทางไซเบอร์ของประเทศโปรตุเกส ชื่อว่าบริษัทอานุบิสเน็ตเวิร์ค (AnubisNetworks) โดยเมื่อปีที่แล้วบริษัทนี้เป็นหนึ่งในอีกหลายบริษัทที่ได้ช่วยเอฟบีไอ (FBI) ภายใต้ปฏิบัติการโทวาร์ (FBI-led Operation Tovar) ในการสืบสวนโทรจันเซอัส (Zeus Trojan) และคริปโตลอกเกอร์ (Cryptolocker) ซึ่งเป็นหนึ่งในซอฟแวร์เรียกค่าไถ่ที่แพร่กระจายไปทั่วโลก

[7] ซอฟแวร์เรียกค่าไถ่ (Ransomware) ซึ่งได้ระบาดมาถึงประเทศไทยแล้ว โดยมัลแวร์นี้จะเข้ารหัสของคอมพิวเตอร์ของเหยื่อโดยจะไม่สามารถเปิดใช้ไฟล์ใดๆได้เลยจนกว่าจะมีการจ่ายเงินให้กับอาชญากร ซึ่งการป้องกันทำได้โดยการไม่กดลิงค์ที่ไม่แน่ใจ และมีการสำรองข้อมูลอย่างสม่ำเสมอ มีการติดตั้งซอฟแวร์ป้องกันระบบคอมพิวเตอร์ให้อัพเดทเสมอ

โดยปฏิบัติการโทวาร์นี้นำไปสู่การกวาดล้างจับกุมแฮกเกอร์ชาวรัสเซีย ซึ่งความสำเร็จของปฏิบัติการโทวาร์นี้เกิดจากความร่วมมือและประสานของบริษัททางด้านความปลอดภัยทางไซเบอร์หลายบริษัท เช่น เดลล์, ไมโครซอฟท์, เอฟ-ซีเคียว, แมคอาฟี, ไซแมนเทค, และเทรนด์ไมโคร แม้ว่าการปฏิบัติการนี้ยังไม่สามารถยับยั้งซอฟแวร์เรียกค่าไถ่ได้อย่างถาวร แต่สิ่งหนึ่งที่หัวหน้าศูนย์ EC3 ได้กล่าวไว้คือ การปฏิบัติการได้รับความร่วมมือจากหลายฝ่ายหลายประเทศ ซึ่งเป็นมากกว่าการแบ่งปันข้อมูลทางการสืบสวนแต่ถึงขั้นไว้เนื้อเชื่อใจ (Trust) จึงทำให้การปฏิบัติการสำเร็จลุล่วงได้ ซึ่งคุณโกดาร์ทได้กล่าวว่า เป็นการปฏิวัติทางวัฒนธรรมการทำงานของเหล่าผู้บังคับใช้กฎหมายก็ว่าได้ (โกดาร์ท, 2558)

จะเห็นได้ว่าความสำเร็จของศูนย์อาชญากรรมทางไซเบอร์ของยุโรปหรือศูนย์ EC3 นี้ไม่ได้เกิดขึ้นจากเจ้าหน้าที่ภายในศูนย์เท่านั้น หากแต่เป็นการร่วมมือร่วมใจ และประสานงานการทำงานของทางศูนย์นี้กับหน่วยงานภายในประเทศและต่างประเทศของยุโรป ทั้งในส่วนของหน่วยงานบังคับใช้กฎหมายในภาครัฐบาลและจากบริษัทเอกชนที่มีความเชี่ยวชาญทางเทคโนโลยีและโดยเฉพาะทางด้านการรักษาความปลอดภัยทางไซเบอร์ ไม่เพียงแต่จะมีการแบ่งปันข้อมูลทางการสืบสวนอาชญากรรมทางไซเบอร์ แต่ทุกภาคส่วนมีความไว้เนื้อเชื่อใจกัน เพื่อนำไปสู่เป้าหมายของการเกิดความปลอดภัยของประชาชนส่วนรวม ดังนั้นหากประชาคมอาเซียนจะนำรูปแบบการดำเนินการของศูนย์ EC3 นี้ มาจัดตั้งภายใต้ตำรวจอาเซียน (ASEANAPOL) เพื่อให้เป็นศูนย์กลางทางด้านอาชญากรรมทางไซเบอร์ (Cybercrime Hub) ของประชาคมอาเซียน ซึ่งจะทำให้การสืบสวนสอบสวนและดำเนินคดีต่ออาชญากรทางไซเบอร์ที่เกิดขึ้นได้ผลสัมฤทธิ์ดังเช่นตัวอย่างของการจัดตั้งศูนย์อาชญากรรมทางไซเบอร์ของยุโรป

อ้างอิง

ตำรวจสากลภาคพื้นยุโรปทลายกลุ่มอาชญากรไซเบอร์ของสเปน. (13 ก.ค. 2558). จากเว็บไซต์ http://www.scmagazineuk.com/europol-dismantles-spanish-cyber-crime-group/article/425983/

ประชาคมอาเซียนกับสำนักงานตำรวจแห่งชาติ. (2558). จากเว็บไซต์ http://www.sbpolice.go.th/file-notification/AEC.pdf

ยูโรโปลวางแผนในการปราบมัลแวร์. (3 ก.พ. 2558). จากเว็บไซต์ http://www.scmagazineuk.com/europol-plans-more-malware-takedowns/article/396089/

ยูโรโปลสนับสนุนตำรวจสเปนในการทลายกลุ่มอาชญากรทางไซเบอร์. (10 ก.ค. 2558). จากเว็บไซต์ https://www.europol.europa.eu/content/europol-supports-spanish-police-dismantle-serious-cybercriminal-group

โครงสร้างกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี.(2558). จากเว็บไซต์ http://www.hightechcrime.org/

โครงสร้างการทำงานของศูนย์อาชญากรรมทางไซเบอร์ของยุโรป (2558). จากเว็บไซต์ https://www.europol.europa.eu/ec3old