ความมั่นคงของมนุษย์: ศึกษากรณีความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดน

Human Security: a Case Study on Cybersecurity in A Borderless World

สุธีราภรณ์ แสงจันทร์ศรี[1] สลิลา กลั่นเรืองแสง[2]

Suteeraporn Saengchansri and Salila Klanreaungseang

Article History

Received: December 2, 2020

Revised: September 1, 2021

Accepted: September 13, 2021

บทคัดย่อ

บทความนี้มีวัตถุประสงค์เพื่อชี้ให้เห็นถึงความเสี่ยงที่จะเกิดภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศหรือระบบดิจิทัลอย่างไม่ถูกต้อง ซึ่งประเทศไทยอาจเป็นเป้าหมายของอาชญากรรมทางไซเบอร์โดยเฉพาะอย่างยิ่งในรูปแบบที่เรียกว่า “Advanced Persistent Threats (APT) Actors” ซึ่งถือเป็นปัญหาใหม่ในโลกแห่งการเปลี่ยนแปลง และเป็นความท้าทายสำคัญในการพัฒนากฎหมายให้มีมาตรการรองรับที่เพียงพอ ทั้งนี้จากการวิจัยเชิงเอกสาร (Documentary Research) ชี้ให้เห็นถึงความสำคัญของกฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งย่อมจะเป็นเครื่องมือหนึ่งเพื่อเป็นหลักประกันความปลอดภัยต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งภาครัฐและภาคเอกชน รองรับการใช้ชีวิตในโลกที่ไร้พรมแดน อีกทั้งเป็นหลักประกันความมั่นคงของชาติต่อไป

โดยจากผลการศึกษาแสดงให้เห็นว่า ในประเด็นด้านความมั่นคงของมนุษย์ ตลอดจนเพื่อการรักษาไว้ซึ่ง ความมั่นคงของรัฐจำเป็นต้องสร้างสมดุลระหว่างเสรีภาพของปัจเจกบุคคลกับประโยชน์สาธารณะ ซึ่งการกำหนดยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดนนี้ ควรดำเนินการโดยหน่วยงานที่เชี่ยวชาญเฉพาะด้าน บนพื้นฐานความโปร่งใสและการไม่เลือกปฏิบัติ ยิ่งไปกว่านั้นกรณีความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดนย่อมต้องมีระบบกำกับดูแลที่กำหนดกรอบการดำเนินการที่ชัดเจนเพราะย่อมส่งผลกระทบโดยตรงกับภาคประชาสังคมทั้งระดับประเทศและระดับโลก ทั้งนี้ ต้องบูรณาการความร่วมมือระหว่างหน่วยงานระดับประเทศกับระดับภูมิภาคโดยหากต้องยุติข้อขัดแย้งอาจจำเป็นต้องจัดตั้งหน่วยงานด้านการยุติธรรมหรือกึ่งตุลาการ อย่างไรก็ตาม การที่จะรับมือกับกิจกรรมไซเบอร์ในโลกไร้พรมแดนได้ทั้งหมด ยุทธศาสตร์ในการรับมือการคุกคามทางไซเบอร์ในแต่ละประเทศควรสอดคล้องกับมาตรฐานที่องค์การระหว่างประเทศแนะนำไว้ อีกทั้งควรให้ประเด็นด้านความมั่นคงปลอดภัยในโลกไซเบอร์เป็นประเด็นสำคัญในการดำเนินนโยบายต่างประเทศ โดยต้องส่งเสริมทักษะด้านการทูตทางไซเบอร์ รวมถึงพัฒนาองค์กรที่มีวัตถุประสงค์เฉพาะเจาะจง เน้นการมีส่วนร่วมของประชาคมโลกในประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดน รวมถึงต้องมีกลไกที่สร้างบรรทัดฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นสากลซึ่งนำไปปฏิบัติได้อย่างเป็นรูปธรรมอันส่งผลโดยตรงต่อความมั่นคงของมนุษย์

คำสำคัญ: ภาวะโลกไร้พรมแดน ความมั่นคงปลอดภัยไซเบอร์ ความมั่นคงของข้อมูล ความมั่นคงของมนุษย์

[1-2] คณะนิติศาสตร์ มหาวิทยาลัยราชภัฏรำไพพรรณี

Faculty of Law, Rambhai Barni Rajabhat University Email: pickki_k@hotmail.com *Corresponding author

Abstract

This article aims to propose the risk of threat exposure if information technologies or digital world systems are misused. In this case, Thailand can likely become the target of cyber criminals, especially so-called “Advanced Persistent Threats (APT) Actors”. In this regard, it is not only a new problem in the world but also as the challenge of law development to compatible with relevant problems. The analysis in this documentary research reveals the importance of cybersecurity protection law. The particular law can then be one of the tools to ensure the safety of vital information infrastructure of public and private sectors. Also, it can serve for the human being in a borderless world and national security.

In sum, this study suggests, for human security issues, it is necessary to balance the freedom of the individual and the public interest for maintaining the security of the state. Cybersecurity strategies in the borderless world should thus be formulated by a specialized agency based on transparency and indiscrimination. Moreover, cybersecurity in the borderless world needs a clear-defined monitoring framework due to its direct impact on national and global civil society actors. Meanwhile, collaborations between national and regional agencies must be integrated and, in case of dispute settlement, the establishment of judicial or quasi-judicial bodies is required. However, to cope with all global activities during the borderless digital world, strategies for addressing cyber threats in an individual country should be in line with the standards or guidelines as recommended by international organizations. Furthermore, “cybersecurity” issues should be defined as a key component of foreign policy. The promotion of cyber diplomacy skills and the development of an organization with a specific objective of “global community involvement in cyber-security issues in the borderless world”, which directly affect human security, are important. Also, a mechanism to concretely create universal cyber security norms must be introduced.

Keywords: Borderless, Cyber Security, Information Security, Human Security

บทนำ

ในช่วงหลายปีที่ผ่านโลกได้วิวัฒนาการเข้าสู่ยุคดิจิทัล (Digital Age) และมนุษย์เจริญเติบโตท่ามกลางความสะดวกสบายจากการที่มีเทคโนโลยีด้านสารสนเทศที่ทันสมัยและพัฒนาต่อเนื่องอย่างรวดเร็วและแพร่ขยายไปทั่วโลก ส่งผลให้เกิดการแลกเปลี่ยนความก้าวหน้าทางเทคโนโลยีในสังคมโลกอย่างรวดเร็ว ซึ่งรวมถึงในเอเชียตะวันออกเฉียงใต้ที่เกิดเป็นปรากฏการณ์ของสภาวะทางสังคมที่มีการเปิดรับเทคโนโลยีสารสนเทศมากขึ้น ซึ่งจะเป็นผลดีก็ต่อเมื่อมีการใช้เทคโนโลยีเหล่านี้ในการพัฒนาศักยภาพ สนับสนุนหรือเสริมสร้างความอยู่ดีกินดีให้กับประชาชนหรือทำให้ประชาชนมีคุณภาพชีวิตที่ดีขึ้น โดยเฉพาะอย่างยิ่ง การเข้าถึงซึ่งความรู้ในปัจจัยพื้นฐานด้านการดำรงชีพ อาทิยารักษาโรคและความปลอดภัยในการบริโภคอาหาร ในขณะเดียวกัน การนำเทคโนโลยีด้านสารสนเทศมาใช้ในการจัดการกับงานที่เคยทำเป็นกิจวัตรของมนุษย์ เช่น การใช้ปัญญาประดิษฐ์ (AI) เข้ามาช่วยในการทำกิจกรรมซ้ำ ๆ ที่เน้นความถูกต้อง หรือการที่ข้อมูลสำคัญที่เป็นข้อมูลส่วนบุคคลหรือเป็นข้อมูลของส่วนราชการที่จัดอยู่ชั้นความลับ ได้ถูกนำมาจัดเก็บในระบบดิจิทัลมากขึ้น โดยหากมองในมุมที่ดีย่อมเป็นการทำให้เกิดกระบวนการจัดการความรู้ที่เป็นระบบ การรักษาข้อมูลให้ถูกต้อง เข้าถึงได้สะดวก ลดโอกาสสูญหาย หรือถูกทำลาย แต่ในขณะเดียวกันย่อมจะเป็นช่องทางใหม่ ๆ ให้กลุ่มอาชญากรรมทางไซเบอร์มีช่องทางหรือโอกาสในการสร้างภัยคุกคามที่ย่อม

กระทบต่อความมั่นคง การแสวงประโยชน์โดยมิชอบ ตลอดจนการทำลายระบบโครงสร้างพื้นฐานสำคัญของชาติได้

กล่าวได้ว่า ภาวะไร้พรมแดน (Borderless) ในโลกปัจจุบัน (Deloitte, 2012) ขณะนี้ ถือเป็นความเสี่ยงหนึ่งหากมีการใช้เทคโนโลยีสารสนเทศหรือระบบดิจิทัลในทางที่ไม่ถูกต้อง ซึ่งความเสี่ยงที่เกิดขึ้นเหล่านี้มักเกิดขึ้นแล้วจจะเริ่มต้นสร้างผลเสียหรือส่งผลกระทบมาสักระยะหนึ่งแต่ยังไม่เห็นอย่างเด่นชัด ด้วยเหตุนี้ สมควรที่ประเทศไทยจะมีมาตรการรับมือ อีกทั้งมีกลไกในการส่งเสริมให้เกิดความตระหนักรู้ให้แก่พลเมืองของรัฐ เพื่อเตรียมพร้อมสำหรับภัยคุกคามและการรับมือด้วยความรอบคอบ หากวันใดวันหนึ่งที่ประเทศอาจเป็นเป้าหมายของอาชญากรไซเบอร์ได้ โดยเฉพาะอย่างยิ่ง ในรูปแบบที่เรียกว่า “Advanced Persistent Threats (APT) Actors” ซึ่งถือเป็นความท้าทายใหม่ในโลกแห่งการเปลี่ยนแปลง และถือเป็นหน้าที่สำคัญของรัฐในการพัฒนากฎเกณฑ์ต่าง ๆ เพื่อจัดให้มีมาตรการที่เหมาะสมครอบคลุมไปถึงความเสี่ยงทางไซเบอร์ข้ามประเทศอันเกิดจากภาวะไร้พรมแดนเช่นนี้ (Cyber Cross-Jurisdictional Risks) (Henning Schaloske, Kathrin Feldmann and AmreiZürn, 2018)

อย่างไรก็ตาม โดยที่ภูมิสถาปัตย์ของภัยคุกคามทางไซเบอร์ (Cyber Threat Landscape) (ENISA, 2018) เปลี่ยนแปลงไปรวดเร็ว โดยเฉพาะอย่างยิ่ง การลงทุนในระบบจัดการด้านความมั่นคงในระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructures) ซึ่งส่วนใหญ่ได้ถูกเชื่อมกับอินเตอร์เน็ต จึงมีแนวโน้มเกิดความเสี่ยงที่จะมีการคุกคามหรือการถูกโจมตีทางไซเบอร์ การแฮกเกอร์โดยใช้มัลแวร์ (Malwares) ที่ซับซ้อนเพื่อเข้าถึงและขโมยข้อมูลสำคัญ ครอบคลุมทั้งด้านเศรษฐกิจ การเมือง และการทหาร ยิ่งไปกว่านั้น เมื่อพิจารณาโดยภาพรวมในเอเชียตะวันออกเฉียงใต้นั้น ควรจัดให้มีกรอบการป้องกันทางไซเบอร์เชิงเทคนิคและเชิงกฎหมายที่ยืดหยุ่น (Resilient Legal and Technical Cyber Protection Framework) สามารถปรับใช้ได้ในภูมิภาค รวมถึงมีการจัดการประชุมหรือทำความตกลงระหว่างประเทศเพื่อให้มีประสานงานที่เป็นรูปธรรม โดยควรจัดให้มีระบบกำกับดูแลที่เป็นรูปธรรมรวมถึงกลไกการรายงาน หากเกิดกรณีการโจมตีทางไซเบอร์ในระดับภูมิภาค

วัตถุประสงค์

เพื่อสะท้อนมุมมองของการใช้ชีวิตในโลกไร้พรมแดน โดยการให้ความรู้เบื้องต้นซึ่งจะเป็นองค์ความรู้ที่จำเป็นในการส่งเสริมให้เกิดการมีส่วนร่วม (Participation) ในภาพรวมของพลเมืองตลอดจนแนะนำค่านิยมเกี่ยวกับการตระหนักรู้ร่วมกันในการป้องกันหรือยับยั้งภัยคุกคามทางไซเบอร์ทั้งในระดับปัจเจกบุคคลและในระดับความมั่นคงของชาติต่อไป

นิยามศัพท์

ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) (ITU, 2010) คือ ภาพรวมของเครื่องมือ นโยบาย แนวคิดการรักษาความปลอดภัย การรักษาความปลอดภัย แนวทาง วิธีการบริหารความเสี่ยง การปฏิบัติ การอบรม วิธีการปฏิบัติที่เป็นเลิศ การับประกัน และเทคโนโลยี ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กรและสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับที่เชื่อมต่อคอมพิวเตอร์ ข้อมูลส่วนตัว โครงสร้างพื้นฐาน แอปพลิเคชั่น บริหาร ระบบสารสนเทศและภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ (สำนักงานรัฐบาลอิเล็กทรอนิกส์, 2559)

ความมั่นคงปลอดภัยสารสนเทศ (Information Security) คือ การปกป้องข้อมูลและระบบสารสนเทศจากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้ การเปิดเผย การขัดขวาง การดัดแปลง หรือการทำลาย (United States Government Publishing Office, 2020)

Advanced Persistent Threat (APT) คือ อาชญากรรมทางคอมพิวเตอร์ประเภทหนึ่งที่มีเป้าหมายเพื่อโจมตีหน่วยงานที่มีข้อมูลสำคัญ เช่น หน่วยงานทางทหารหรือหน่วยงานทางด้านความมั่นคงปลอดภัยของประเทศ หน่วยงานทางการเมือง หรือองค์กรธุรกิจขนาดใหญ่ รูปแบบการโจมตีแบบ APT ส่วนใหญ่ผู้ดำเนินการมักจะเป็นกลุ่มบุคคลมากกว่าเป็นการดำเนินการของบุคคลใดบุคคลหนึ่ง ซึ่งอาจเป็นไปได้ว่า กลุ่มบุคคลนี้มักจะมีองค์กรหรือรัฐบาลของประเทศใดประเทศหนึ่งคอยให้การสนับสนุนอยู่เบื้องหลัง การโจมตีมีเป้าหมายที่แน่ชัด ผู้โจมตีมักพยายามแฝงตัวอยู่ในระบบของเป้าหมายให้ได้นานที่สุด และใช้ทุกวิถีทางเพื่อให้การโจมตีสำเร็จผล (ThaiCERT, 2019)

APT (ไทยเซิร์ต, 2554) อธิบายได้ดังนี้

A - Advanced คือ ผู้ที่โจมตี หรือมีความสามารถและมีทรัพยากรที่พร้อมสำหรับการโจมตี วิธีการโจมตีจะใช้เครื่องมือและเทคนิคหลายอย่างด้วยกัน ซึ่งเป็นไปได้ตั้งแต่การใช้ความรู้ทางคอมพิวเตอร์ขั้นสูงเพื่อเจาะระบบ รวมถึงการใช้เทคนิคพื้นฐาน เช่น Social Engineering ซึ่งเป็นการโจมตีโดยอาศัยหลักจิตวิทยาเพื่อหลอกลวงคนให้เปิดเผยข้อมูลสำคัญ

P - Persistent คือ การโจมตีจะเป็นแบบค่อยเป็นค่อยไปและสม่ำเสมอ เนื่องจากผู้โจมตีต้องแฝงเข้าไปอยู่ในระบบโดยไม่ให้เป้าหมายรู้ตัว เพื่อสร้างความเสียหายหรือรวบรวมข้อมูลที่ต้องการให้ได้มากที่สุด

T -Threat คือ ภัยคุกคามที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

แนวคิดและทฤษฎี

การคุกคามความมั่นคงปลอดภัยไซเบอร์ คือ ภาวะความเสี่ยงที่เกิดขึ้นจากเหตุการณ์ที่เริ่มเป็นภัยคุกคาม (Threat) ประกอบกับการมีช่องโหว่ หรือข้อบกพร่อง ซึ่งสร้างผลกระทบทางเศรษฐกิจ เหตุการณ์ที่สามารถเปลี่ยนเส้นทางไปจากที่คาดหวังได้ โดยแล้วแต่สถานการณ์ ทั้งนี้ ภัยคุกคามและช่องโหว่ต่าง ๆ จะเป็นตัวกำหนดและส่งผลต่อการวางแผนการดำเนินการ หากไม่มีภัยคุกคาม หรือไม่มีช่องโหว่ ย่อมไม่เพิ่มความเสี่ยง

กรอบแนวคิดเกี่ยวกับความมั่นคงของมนุษย์ในระบบดิจิทัล

ความมั่นคงของมนุษย์ (Human security) คือ แนวทางที่ยึดมนุษย์เป็นศูนย์กลาง โดยมุ่งเน้นไปที่ปัจเจกชนโดยพิจารณาถึงสิทธิและความต้องการของพวกเขา (Costanzo, Charles E., 2011) ซึ่งมีความเชื่อมโยงกับแนวคิดด้านความปลอดภัยดิจิทัล ซึ่งความเสี่ยงทางดิจิทัล แตกต่างจากความเสี่ยงประเภทอื่น ๆ ทั้งนี้อาจใช้คำว่า"ความปลอดภัยในโลกไซเบอร์" ซึ่งคำว่า "ไซเบอร์" เป็นคำที่คุ้นเคยที่ช่วยทำให้เข้าใจได้ง่าย (OECD, 2015) โดยต้องยอมรับความจริงที่ว่า การจัดการด้านความมั่นคงปลอดภัยในโลกไซเบอร์อาจจะลดระดับลง หากกระทบต่อผลประโยชน์ทางเศรษฐกิจหรือประโยชน์เชิงเศรษฐศาสตร์

นอกจากนี้เมื่อกล่าวถึง "ความเสี่ยง" ความเสี่ยงเป็นผลของความไม่แน่นอนต่อวัตถุประสงค์ ทั้งนี้ "ความเสี่ยงด้านความปลอดภัยดิจิทัล (Digital Security Risk)" คือ การอธิบายถึงความเสี่ยงที่เกี่ยวข้องกับการใช้ การพัฒนา และการจัดการทางดิจิทัล รวมถึงสภาพแวดล้อมทางดิจิทัล (Digital Environment) ซึ่งอาจรวมถึงภัยคุกคามและช่องโหว่ ในสภาพแวดล้อมดิจิทัลโดยประเด็นเหล่านี้เชื่อมโยงและส่งผลต่อเศรษฐกิจและสังคมในแง่ของการรักษาความลับ อย่างไรก็ตาม ความเสี่ยงด้านความปลอดภัยดิจิทัลมีการเปลี่ยนแปลงอย่างต่อเนื่อง โดยมีปัจจัยสำคัญ ได้แก่สภาพแวดล้อมทางดิจิทัล กิจกรรม และกระบวนการขององค์กรที่สนับสนุน อย่างไรก็ตาม เมื่อพิจารณาในแง่ของความมั่งคั่งทางเศรษฐกิจและสังคม การสร้างความมั่งคั่งจากการสร้างนวัตกรรมการเติบโตของตลาดดิจิทัล ความสามารถในการแข่งขัน การจ้างงานในทุกภาคส่วน ตลอดจนความเป็นอยู่ที่ดีขึ้น ย่อมส่งผลโดยตรงต้องสภาพแวดล้อมดิจิทัลที่ขับเคลื่อนให้เกิดการดำเนินการสิ่งต่าง ๆ บนโลกดิจิทัล

ข้อสังเกตระหว่างคำว่า ความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยสารสนเทศ

เมื่อมีการกล่าวถึงความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) และความมั่นคงของข้อมูล (Information Security) ผู้เขียนเห็นว่า การใช้คำกลาง ๆ ว่า ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) มักใช้ในบริบทของการอธิบายถึงข้อมูลดิจิทัลหรือการส่งผ่านข้อมูลบนอินเตอร์เน็ต ซึ่งเป็นไปเพื่อการอธิบายถึงมาตรการทางเทคนิคเพื่อป้องกันข้อมูลไม่ให้สูญหาย แต่ประสงค์ให้เป็นความลับ

แต่ในบริบทเมื่อต้องการกำหนดเงื่อนไขในการเข้าถึง (Access) หรือการจำกัดการเข้าถึง กล่าวคือ ต้องมีมาตรการด้านความมั่นคงของข้อมูล จึงต้องใช้คำที่ครอบคลุมกว่า คือ ความมั่นคงของข้อมูล (Information Security) ซึ่งในความเป็นจริงย่อมหมายถึงข้อมูลในอินเตอร์เน็ตหรือข้อมูลดิจิทัลเป็นส่วนใหญ่ ทั้งนี้ความเปลี่ยนแปลงในโลกปัจจุบัน จากการส่งผ่านข้อมูลถึงกันได้อย่างรวดเร็ว พบว่า ข้อมูลส่วนใหญ่เป็นประโยชน์ต่อการใช้ชีวิตในโลกยุคดิจิทัล ซึ่งล้วนมีการนำเสนอ ค้นหาได้ง่ายทาง Search Engine ซึ่งแน่นอนว่า สัดส่วนของข้อมูลที่ต้องการให้ได้รับการปกปิดหรือคุ้มครองในสังคมแห่งการเปลี่ยนแปลงนี้ ย่อมมีจำนวนมากเช่นกัน ดังนั้น ข้อมูลส่วนใหญ่ในปัจจุบันนั้น จึงไม่ได้อยู่เพียงแค่ในแฟ้มหรือตู้เอกสารของทางราชการอีกต่อไป หากแต่อยู่ในรูปของการเก็บไว้ผ่านเครือข่ายขององค์กรต่าง ๆ เช่น ระบบ

อินทราเน็ตภายในองค์กร หรือการจัดเก็บไฟล์ในรูปแบบดิจิทัล ดังนั้น เพื่อให้เข้าใจถึงความมั่นคงของข้อมูลในโลกที่ไร้พรมแดน และเมื่อพิจารณาตามคำจำกัดความของ สหภาพโทรคมนาคมระหว่างประเทศ หรือ ITU ซึ่งอธิบายถึงคำว่า Cybersecurity (ITU, 2019) หมายถึง ภาพรวมของเครื่องมือ นโยบาย แนวคิดการรักษาความปลอดภัยการรักษาความปลอดภัย แนวทาง วิธีการบริหารความเสี่ยง การปฏิบัติ การอบรม วิธีการปฏิบัติที่เป็นเลิศ การับประกัน และเทคโนโลยี ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กรและสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับที่เชื่อมต่อคอมพิวเตอร์ ข้อมูลส่วนตัว และการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ (สำนักรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (EGA), 2016) จะเห็นได้ว่า การใช้ศัพท์ดังกล่าวนั้น มุ่งหมายเพื่อการอธิบายภาพรวมของข้อมูลที่อยู่ในระบบอินเตอร์เน็ตว่าต้องมีความปลอดภัย (ทั้งการเข้าถึงและการสูญหาย) โดยจากบทนิยามจะเห็นว่า ความมั่นคงปลอดภัยไซเบอร์จะมีขอบเขตที่กว้างกว่า ถ้าพิจารณาในแง่ของพื้นที่บนเครือข่ายอินเตอร์เน็ตเพราะครอบคลุมทุกการกระทำ และทุกรูปแบบที่เกิดขึ้นบนไซเบอร์

อย่างไรก็ตาม หากพิจารณาในอีกบริบท แม้ว่าคำสองคำนี้จะมีความหมายใกล้เคียงกัน แต่การจะใช้แทนกันได้นั้นย่อมไม่ถูกต้องนัก เพราะแม้ว่าทั้งสองคำนั้น มีความมุ่งหมายในทำนองเดียวกันก็ตาม กล่าวคือ สื่อให้เห็นถึงคำความมั่นคงและการปกป้อง (Security and Protecting) จากการกระทำละเมิดและการคุกคามต่อข้อมูล (Information Breaches and Threats) แต่พบว่ามีความแตกต่างอันมีนัยสำคัญในสองคำนี้ คือ การที่คำหนึ่ง คือ “Cybersecurity” จะใช้อธิบายลักษณะเฉพาะในไซเบอร์สเปซ ในขณะที่ “Information Security” สามารถใช้กับข้อมูลทั้งที่อยู่ในไซเบอร์สเปซ (Cyberspace) และที่มีการเก็บในรูปแบบทั่วไป เช่น จัดใส่แฟ้มในตู้เก็บเอกสาร เป็นต้น

จากการอธิบายข้างต้น จะพบว่า มีความแตกต่างระหว่างความมั่นคงปลอดภัยไซเบอร์และความมั่นคงทางสารสนเทศ (Luke Irwin, 2020) แม้ว่าจะมีการนำไปใช้ในทำนองอย่างเดียวกันและมักใช้ปะปนกัน แต่แท้จริงนั้น ทั้ง 2 คำต่างกัน โดยใช้อธิบายถึงขีดความสามารถ (Capabilities) ที่แตกต่างกัน ทั้งนี้ สารสนเทศไม่จำเป็นต้องเก็บในคอมพิวเตอร์ เพราะฉะนั้น ระบบความมั่นคงทางสารสนเทศ (Information Security System) จึงมีความหมายที่กว้างกว่าในแง่ของรูปแบบของข้อมูลและรูปแบบของการจัดเก็บ โดยที่สารสนเทศนั้นอาจจัดเก็บในตู้เก็บเอกสารซึ่งก็ต้องการความปลอดภัยทางกายภาพเพื่อให้เกิดความมั่นคงทางสารสนเทศที่ดี (Good Information Security) ในขณะที่ความมั่นคงทางไซเบอร์ (Cybersecurity) เป็นเรื่องของการปกป้องข้อมูลและสารสนเทศจากแหล่งภายนอก (Outsides Sources) โดยพื้นที่ที่ต้องปกป้องนั้นจำกัดไว้ในไซเบอร์สเปซ (Cyberspace) หรือในอินเตอร์เน็ต

กรอบแนวคิดเกี่ยวกับความมั่นคงของข้อมูล (CIA Triad)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้อธิบายถึง CIA Triad ว่า เป็นส่วนประกอบหนึ่งของ INFOSEC (Information Security) ซึ่งมากจากคำว่า

1) Confidentiality (การรักษาความลับของข้อมูล)

2) Integrity (ความแท้จริงของข้อมูล) และ

3) Availability (การใช้งานได้ของระบบ)

โดยเป็นสิ่งที่ Security Professional ต้องรู้และสามารถอธิบายได้ โดยถือว่าเป็นสิ่งสำคัญในการวิเคราะห์ระหว่างสภาวะความปลอดภัยกับสภาวะความตื่นตระหนก (panic) เกี่ยวกับความเสี่ยงทางไซเบอร์ เพื่อสร้างความมั่นใจ น่าเชื่อถือ และสามารถใช้ประโยชน์ได้ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2012)

ในสหรัฐอเมริกาตามบทบัญญัติที่ปรากฏใน Federal Information Security Management Act (FISMA) (United States Government Publishing Office, 2020) ได้อธิบายถึงความสัมพันธ์ระหว่าง “ความปลอดภัยของข้อมูล (information Security)” และ “CIA Triad” สรุปได้ดังนี้

คำว่า “ความปลอดภัยของข้อมูล” หมายถึง การปกป้องข้อมูลและระบบสารสนเทศจากการเข้าถึง การใช้การเปิดเผย การหยุดชะงัก การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต ในบริบทของ CIA Triad ดังต่อไปนี้

C- (Confidentiality) การรักษาความลับ หมายถึง การจำกัดการได้รับอนุญาตในการเข้าถึงการอนุญาตให้เปิดเผยข้อมูล รวมถึงการกำหนดวิธีการหรือกลไกปกป้องความเป็นส่วนตัว

I - (Integrity) ความซื่อตรง หมายถึง การป้องกันไม่ให้เกิดการแก้ไขหรือการทำลายข้อมูลที่ไม่เหมาะสมและรวมถึงการรับประกันว่าข้อมูลจะไม่มีการแก้ไขโดยไม่มีอำนาจ

A - (Availability) การง่ายต่อการเข้าถึง หมายถึง ระยะเวลาที่เหมาะสมในการเข้าถึงข้อมูล รวดเร็ว ทันเวลา

ทั้งนี้ ข้อมูลอาจเกิดภัยคุกคามโดยไม่ได้คาดหมายล่วงหน้า เช่น ระบบ หรือซอฟต์แวร์ทำงานผิดพลาด ในขณะที่การคุกคามโดยเจตนาคือ สิ่งที่เกิดขึ้นจากผู้คุกคาม กระทำการโดยเจตนา โดยที่ภัยคุกคามโดยเจตนาอาจตรวจสอบแบบไม่เป็นทางการจากการใช้เครื่องมือตรวจสอบพื้นฐาน ตลอดจนการโจมตีที่ซับซ้อน เช่น การดักฟัง เป็นต้น ทั้งนี้ สภาวการณ์ที่มีการเข้าถึงอินเทอร์เน็ตทั่วโลกทำให้ความปลอดภัยในโลกไซเบอร์มีลักษณะเฉพาะ กล่าวคือ ในขณะที่ระบบส่วนใหญ่เดิมทีเดียวนั้นเป็นแบบ Stand Alone และไม่ค่อยมีการข้ามเขตการรักษาความปลอดภัยทางไซเบอร์แต่ในปัจจุบัน ปรากฏการณ์โลกไร้พรมแดน (Borderless World) ที่เกิดขึ้นอย่างหลีกเลี่ยงไม่ได้นั้น ย่อมมีแนวโน้มที่จะสร้างภัยคุกคามซึ่งแพร่ขยาย (Proliferation) ทั่วโลก โดยที่กฎหมายหรือกฎเกณฑ์ที่สร้างขึ้นในระบบการปกครองของโลก (Global Administration) สำหรับความมั่นคงปลอดภัยของข้อมูลที่มีอยู่แล้วนั้น อาจไม่เพียงพอเพื่อรักษาไว้ ซึ่งความมั่นคงของมนุษย์ (Human Security) ได้อีกต่อไป ส่งผลให้รัฐต่าง ๆ ต้องมีการปรับปรุงมาตรการทางกฎหมายตลอดจนเพิ่มการอธิบายหรือกำหนดนิยามศัพท์ใหม่จากการมี Actor ใหม่ ๆ ซึ่งเกิดขึ้นอย่างต่อเนื่อง ให้ทันสมัยและเท่าทันต่อเทคโนโลยีดิจิทัลที่เปลี่ยนแปลงอย่างรวดเร็ว

กรอบแนวคิดเกี่ยวกับภาวะการคุกคามความมั่นคงปลอดภัยไซเบอร์

ภัยคุกคามทางไซเบอร์ หรือ Cyber Threats หมายถึง การละเมิดคุณสมบัติด้านความปลอดภัยที่อาจจะเกิดขึ้นทั้งที่เป็นการคุกคามโดยเจตนา (Intentional Threats) และการคุกคามโดยอ้อม (Passive Threats) อย่างไรก็ตามเป้าหมายของการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ การช่วยปกป้องทรัพย์สินและทรัพยากรขององค์กรในแง่ของทรัพยากรมนุษย์ การเงิน และข้อมูล โดยอาศัยกระบวนการรักษาความปลอดภัยทางไซเบอร์ที่ต้องตอบสนองต่อความกังวลของคนในสังคมซึ่งสามารถสร้างขึ้นได้จากการส่งเสริมให้มีการปฏิบัติตามประมวลจรรยาบรรณทางไซเบอร์เพื่อการใช้อย่างเหมาะสมซึ่งเป็นไปตามกรอบที่เป็นแนวทางแนะนำ (Guideline) อันเป็นที่ยอมรับจากนานาอารยประเทศ ที่แนะนำให้รัฐต่าง ๆ สามารถกำหนดนโยบายด้านความปลอดภัยที่มีมาตรฐาน ตลอดจนเป็นหน้าที่สำคัญของนักยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่ต้องตระหนักและให้ความสำคัญกับการโจมตีแบบกำหนดเป้าหมายหรือภัยคุกคามต่อเนื่อง ตลอดจนส่งเสริมและปลูกฝังให้ประชาชนได้ตระหนักถึงบทบาทในฐานะพลเมืองของรัฐที่จะต้องรับผิดชอบต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ร่วมกันกับภาครัฐ

กรอบแนวคิดเกี่ยวกับนโยบายของโลก (Global Policy) ด้านความมั่นคงปลอดภัยไซเบอร์ระดับโลก

ในระดับโลก การกำหนดนโยบายของโลกดิจิทัล อาจจำเป็นต้องสอดคล้องกับนโยบายของโลก (Global Policy) ซึ่งกำกับด้วยหลักนิติธรรม ที่ถือได้ว่าเป็นบรรทัดฐานในการวางระเบียบกฎหมาย (Legal Order) ที่เป็นที่ยอมรับทั่วภูมิภาคของโลก ถือเป็นหลักการทั่วไปที่แน่นอนและมีเสถียรภาพ ทั้งนี้ หลักนิติธรรม (The Rule of Law) อาจเป็นเครื่องมือหนึ่งที่นำไปสู่ขั้นตอนการสร้างธรรมนูญของโลกด้านดิจิทัลต่อไปในอนาคต

“หลักนิติธรรม/นิติรัฐ” (Rule of Law) เป็นหลักการที่กำหนดความสัมพันธ์ระหว่างรัฐกับเอกชน เอกชนกับเอกชน และรัฐกับรัฐ หากเป็นความสัมพันธ์ระหว่างรัฐกับเอกชนจะเป็นความสัมพันธ์ภายใต้กฎหมายมหาชน ส่วนความสัมพันธ์ระหว่างเอกชนกับเอกชนจะอยู่ภายใต้กฎหมายเอกชน และความสัมพันธ์ระหว่างรัฐกับรัฐจะอยู่ภายใต้กฎหมายระหว่างประเทศ ดังนั้น จึงอาจกล่าวได้ว่าหลักนิติธรรม/นิติรัฐเป็นหลักการที่ใช้กับกฎหมายทุกสาขาทั้งกฎหมายมหาชน กฎหมายเอกชน และกฎหมายระหว่างประเทศ (สถาบันวิจัยเพื่อการพัฒนาประเทศไทย, 2559) จะเห็นได้ว่า หลักนิติธรรม เป็นกฎเกณฑ์ที่เป็นสากล อย่างไรก็ตาม เพียงแค่หลักนิติธรรมอย่างเดียวนั้นย่อมไม่เพียงพอ เพราะนอกจากจะต้องมีหลักการที่มีลักษณะทั่วไปที่แน่นอนและมีเสถียรภาพ (Fixed and Stable General Principles) ย่อมต้องมีกระบวนการยุติธรรมเพื่อการแก้ไขข้อขัดแย้งแบบข้ามประเทศหรือระดับโลก (Authority of a Transnational or Global) ซึ่งการตัดสินย่อมจะก้าวล่วงเข้าไปในระบบกฎหมายภายในรัฐหรือในระดับประเทศ (National Legal Systems) ทั้งนี้มีข้อโต้แย้ง

ว่า การตัดสินซึ่งก้าวล่วงและกระทบต่ออำนาจอธิปไตยดังกล่าวนั้นจะมีความชอบธรรมมากน้อยเพียงใด โดยย่อมต้องคำนึงถึงความมั่นคงของมนุษย์ ซึ่งต้องชั่งน้ำหนักระหว่างประโยชน์ของปัจเจกบุคคลกับประโยชน์สาธารณะ อย่างไรก็ตาม ต้องอยู่บนหลักการอย่างน้อยที่สุดคือต้องมีความโปร่งใส (Transparency) รวมทั้งมีกลไกของการมีส่วนร่วม ซึ่งมักจะเกิดข้อสงสัยในเรื่องของการตรวจสอบได้ เมื่อกระทบต่ออำนาจอธิปไตยของแต่ละรัฐ

อย่างไรก็ตาม การที่มนุษย์ใช้ชีวิตที่ยึดติดกับโลกดิจิทัลมากขึ้น นำไปสู่ปรากฏการณ์ “ภายใน” (“In Here” Phenomenon) ที่กระทบต่ออัตลักษณ์ส่วนบุคคล (Personal Identity) อาทิ การใช้ชีวิตในโลกที่หลายคนจะคุ้นกับรูปของนายเนลสัน แมนเดลา (Nelson Mandela) มากกว่าหน้าตาของเพื่อนบ้าน (Anthony Giddens, 1996) สะท้อนให้เห็นถึงโลกที่เปลี่ยนแปลงไปสู่สังคมโลกที่กลมกลืนเข้ากันยิ่งขึ้น นอกจากนี้ การที่โลกมีภาวะไร้เขตแดน (Borderless) ย่อมสะท้อนถึงความสำคัญของรัฐชาติ (Nation State) ที่จำเป็นต้องมีความเข้มแข็ง ในบริบทที่ว่า โลกไร้พรมแดนทำให้มีการตัดสินใจของรัฐระดับระหว่างประเทศมากขึ้น ซึ่งยังคงต้องคำนึงถึงสิทธิมนุษยชนและการปฏิบัติตามพันธกรณีระหว่างประเทศ ทั้งนี้ แนวคิดในการรองรับภัยคุกคามทางไซเบอร์ (Cyber-threats) จากการปาฐกถาพิเศษในหัวข้อ “Protecting and Defending against Cyberthreats in Uncertain Times” โดยนาย Brad Smith, President of Microsoft (Brad Smith, 2017) สรุปได้ว่า ปัญหาที่เกิดขึ้นมักต้องการทางออกใหม่ ๆ (A growing problem in need of new solutions) โดยที่การโจมตีทางไซเบอร์ (Cyber-attack) เป็นสงครามรูปแบบใหม่ ซึ่งสนามรบไม่ได้เป็นแบบที่เราเคยเข้าใจอีกต่อไป โลกไซเบอร์สามารถกลายเป็นสมรภูมิรบได้ตลอดเวลา ทั้งนี้ อาจต้องเปลี่ยนจากการปกป้องพลเมืองในเวลาสงครามเป็นการปกป้องพลเมืองในเวลาที่โลกสงบสุข (From Protection Civilians in Time of War to Attacking Civilian in Time of Peace) โดยที่การเข้าถึงชุดข้อมูลจะเป็นจุดแข็งสำหรับใช้ในการต่อสู้ (Data Strengthens our Defense) เพราะในการต่อสู้รับมือกับภัยคุกคาม “ข้อมูลเป็นสิ่งที่จำเป็น” อย่างมากในการรับมือและแก้ไขปัญหา

นอกจากนี้ เมื่อกล่าวถึงความร่วมมือในระดับโลก (UN, 2018) หัวข้อสำคัญในการอภิปรายเกี่ยวกับความปลอดภัยในโลกไซเบอร์และสิทธิออนไลน์ มักจะเป็นสิ่งที่ได้รับการพิจารณาโดยให้ความสำคัญในระดับแรก ๆ โดยที่ผู้มีส่วนได้เสียจากภาครัฐ ภาคเอกชนหรือภาคประชาสังคม จะให้ความสำคัญกับ Fake News โดยประสงค์ให้มีมาตรการเพื่อจัดการกับการบิดเบือนข้อมูลในหลายสถานการณ์ อาทิ การแทรกแซงผลการเลือกตั้ง การปลุกระดมความเกลียดชังหรือสร้างความขัดแย้ง รวมถึงการนำเสนอเนื้อหาประเภทที่ทำให้เข้าใจผิดหรือปิดบังวัตถุประสงค์ที่แท้จริง เป็นต้น

กล่าวได้ว่า แนวคิดเกี่ยวกับระบบการกำกับดูแลของโลก (Global Regulatory Regimes) เป็นการกำกับดูแล ในรูปแบบใหม่ที่เกิดขึ้นในสังคมโลก เป็นผลมาจากการที่องค์การระหว่างประเทศสามารถกำหนดบรรทัดฐานของตนเองและกำกับดูแลกิจกรรมต่าง ๆ รวมทั้งปฏิบัติตามกระบวนการทางกฎหมายของตนเองได้ โดยประเด็นสำคัญ คือ การให้ “สิทธิในการมีส่วนร่วม (Participatory Rights)” ในการกำหนดมาตรฐานระดับระหว่างประเทศ เพื่อเป็นแนวทางปฏิบัติที่สำคัญให้ทั้งกับภาครัฐและเอกชน ทั้งนี้ การกำกับดูแลขององค์การระหว่างประเทศมักอยู่ในรูปของข้อแนะนำ แนวปฏิบัติ หลักปฏิบัติที่ดีที่สุด (Best Practices) คำแนะนำทางเทคนิค ระเบียบของคณะกรรมการหรือสิ่งที่เป็นกฎเกณฑ์ต่าง ๆ ในหลากหลายรูปแบบ (ไม่ว่าจะเป็นการเผยแพร่ต่อสาธารณชนหรือเป็นการเผยแพร่ไม่เป็นทางการ) จึงมีข้อถกเถียงเกี่ยวกับผลในทางกฎหมายของกฎเกณฑ์ดังกล่าว (ที่เรียกว่า Soft Law ฯลฯ) ด้วยเหตุนี้ การนำหลักนิติธรรมมาปรับใช้ในการสร้างระบบกำกับดูแลจึงมีความสำคัญมากขึ้น บนหลักการของการให้เหตุผล การทบทวน อีกทั้งต้องอาศัยการมีส่วนร่วม โดยต้องอยู่บนพื้นฐานของความโปร่งใสและการตรวจสอบได้ ทั้งนี้ แนวคิดเกี่ยวกับระบบการกำกับดูแลของโลกดิจิทัลย่อมต้องเข้มงวดมากขึ้นกว่าเดิม เพราะเป็นภัยคุกคามที่อาจมองไม่เห็นซึ่งเป็นความท้าทายของสังคมโลกในการสร้างกลไกที่ครอบคลุมกับทุกการใช้ประโยชน์จากโลกไซเบอร์ต่อไป

กรอบแนวคิดเกี่ยวกับคุณค่าของสิทธิมนุษยชน (Human Rights Values) บทโลกไร้พรมแดน

ภาวะไร้พรมแดนเป็นสัญลักษณ์ของการเพิ่มขึ้นของอิทธิพลของความร่วมมือระดับโลก (Global Corporations) การสื่อสารรูปแบบใหม่ และแนวคิดบริโภคนิยม (Consumerism) การตัดสินใจทั้งในระดับท้องถิ่นหรือในระดับประเทศ ล้วนส่งผล

ต่อเนื่องในวงกว้างต่อการรวมกลุ่มระดับโลกในลักษณะเหนือรัฐ (Supranational Global Gathering) ทั้งนี้สิ่งสำคัญอีกประการหนึ่ง คือ การที่พลเมืองของโลกได้สร้างเครือข่ายและเกิดการเคลื่อนไหวด้านสิทธิมนุษยชนที่มีมีอิทธิพลในระดับโลกมากขึ้น

กล่าวได้ว่า ความเป็นสากลของสิทธิมนุษยชน (Universality of the Human Rights) ขึ้นอยู่กับพื้นฐานของรัฐที่ต้องตระหนักและให้ความสำคัญกับการพัฒนาทรัพยากรมนุษย์ โดยการคำนึงถึงสิทธิมนุษยชนในประเทศต่าง ๆ มักเกี่ยวข้องกับโครงสร้างทางเศรษฐกิจหรือเชื่อมโยงกับสถาบันทางการเงินระหว่างประเทศซึ่งเป็นสถาบันที่มีอิทธิพลมาก ซึ่งในบริบทนี้ ศาลยุติธรรมระหว่างประเทศ (ICJ) เป็นตัวอย่างที่ดี ในฐานะที่เป็นองค์การที่มีบทบาทสำคัญในการแก้ไขปัญหาเชิงโครงสร้างที่เกี่ยวข้องกับการปฏิเสธสิทธิมนุษยชน (Denial of Human Rights) บทพื้นฐานที่สอดคล้องกับหลักนิติธรรม (Philip Alston, 1981)

ทั้งนี้ สภาพความเป็นจริงที่รัฐต่าง ๆ หรือสภาวการณ์ที่นานาอารยประเทศกำลังเผชิญนั้น คือ การที่รัฐต้องเตรียมพร้อมต่อการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยีที่ทำให้เกิดปรากฏการณ์ “Disruption” ในปัจจุบัน ซึ่งบางส่วนเป็นผลจากการเข้าถึงทุกพื้นที่ในสังคมโลกได้รวดเร็ว เป็นความท้าทายต่อการควบคุมสังคมและการปกป้องสิทธิมนุษยชนที่เกี่ยวข้องกับระบบดิจิทัลมากยิ่งขึ้น

อย่างไรก็ตาม แม้ว่าระบบความมั่นคงและปลอดภัยของชาตินั้น ต้องคำนึงถึงเรื่องอาณาเขตซึ่งเป็นองค์ประกอบสำคัญประการหนึ่งของความเป็นรัฐ แต่ทว่าปัจจุบัน อาณาเขตของรัฐในความเป็นจริงนั้น เริ่มไร้ขอบเขต จนการรักษาดินแดนซึ่งเป็นองค์ประกอบหนึ่งที่สำคัญในการคงความเป็นรัฐ อาจต้องพิจารณาถึงอาณาเขตทาง Cyber Space ด้วย ดังนั้น การสร้างกรอบหรือกฎเกณฑ์ที่เกี่ยวข้องจึงมีความจำเป็นอย่างเร่งด่วน เพื่อให้มั่นใจว่า สิทธิและเสรีภาพของมนุษย์ ซึ่งเป็นแก่นของความมั่นคงของมนุษย์นั้นจะยังคงได้รับการคุ้มครองตามหลักการด้านสิทธิมนุษยชน

ตัวอย่างมาตรการที่ส่งผลต่อความมั่นคงของมนุษย์ในโลกไซเบอร์ในระดับระหว่างประเทศ

ในประชาคมยุโรปมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation (GDPR)) ซึ่งกฎหมายฉบับนี้เป็นตัวอย่างมาตการทางกฎหมายที่เป็นเอกภาพ โดยนำไปบังคับใช้โดยตรง ในทุกประเทศที่เป็นสมาชิกสหภาพยุโรปโดยไม่ต้องมีการแปลง (Transpose) เป็นกฎหมายระดับประเทศ (National Law) โดยที่กฎหมายคุ้มครองข้อมูลทั่วไป (GDPR) มีข้อกำหนดเกี่ยวกับการแจ้งเมื่อมีการละเมิดข้อมูล (Data Breach Notification) ระบบจัดการการคุ้มครองข้อมูล (Data Protection Management Systems) ค่าปรับและบทลงโทษ รวมทั้งการเรียกร้องจากบุคคลที่สาม (Third Party Claims) (กรมเจรจาทางการค้าระหว่างประเทศ, 2561) โดยมีข้อกำหนดบางส่วนที่เข้มงวดกว่ากฎหมายภายในรัฐหรือระดับประเทศ ส่งผลต่อภาคเอกชนหรือบริษัทต่าง ๆ ให้ต้องคำนึงถึงกฎหมายคุ้มครองข้อมูลทั่วไป (GDPR) ฉบับนี้เป็นหลักสำคัญ แทนที่จะต้องคำนึงถึงกฎหมายคุ้มครองข้อมูลภายในของรัฐสมาชิกของสหภาพยุโรป ซึ่งทำให้เกิดเป็นมาตรฐานกลางสำหรับการป้องกันความเสี่ยงที่จะเกิดภัยคุกคามทางไซเบอร์ข้ามประเทศ การจัดการความเสี่ยงทางเทคโนโลยีสารสนเทศทั่วไป (General IT Risk Management) ตลอดจนการป้องกันการโจมตีทางไซเบอร์ที่สามารถควบคุมได้เป็นเอกภาพมากยิ่งขึ้น

บทวิเคราะห์

โลกดิจิทัลส่งผลให้มีการเปลี่ยนแปลงในการดำเนินชีวิตของมนุษย์ ทั้งคนรุ่นปัจจุบันและคนรุ่นต่อไป กล่าวคือคือ ทำให้มนุษย์สามารถศึกษา เรียนรู้ เข้าใจ ในภูมิศาสตร์ วัฒนธรรม และค่านิยมของอีกประเทศหนึ่งได้โดยสะดวก เข้าถึงง่าย อีกทั้งใช้เวลาน้อยและง่ายต่อการแลกเปลี่ยน ซึ่งหากเกิดแนวคิดในด้านลบอาจส่งผลให้เกิดเป็นคุกคามต่อความมั่นคงของมนุษย์ (Human Security) ได้ โดยอาจมีการสร้างบุคลากรด้านไซเบอร์ที่ทำงานในเชิงลบ การเพิ่มขีดความสามารถให้แฮกเกอร์ในการเอาไปซึ่งข้อมูล หรือการทำให้เสื่อมสียจากการเผยแพร่ข้อมูลของบุคคลหรือขององค์กร เช่นนี้ ทำให้การสู้รบในยุคปัจจุบันอาจไม่ใช่การสู้ด้วยอาวุธเหมือนในอดีต แต่ได้เปลี่ยนแปลงรูปแบบของการโจมตีในลักษณะของการขโมยข้อมูลหรือการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐาน ตลอดจนการให้ข้อมูลที่ผิดหรือการสร้างข่าวที่เป็นเท็จ (Fake News) อันเป็นเครื่องมือที่ก่อให้เกิดการทำลายความมั่นคงของข้อมูล (Information Security) ข้อมูล

จึงเป็นเสมือนอาวุธในสนามรบดิจิทัล (Digital Battlefield) ซึ่งทำให้เกิดความได้เปรียบหรือเสียเปรียบ

วิเคราะห์ภัยคุกคามทางไซเบอร์จากสภาพโดยทั่วไป

ภัยคุกคามทางไซเบอร์ มักจะเกิดจากช่องว่างหรือความแตกต่างด้านศักยภาพในการพัฒนาด้านเทคโนโลยีสารสนเทศ ส่งผลให้เกิดความแตกต่างในการเพิ่มขีดความสามารถในการป้องกันหรือรักษาข้อมูลสำคัญในระดับเป็นความมั่นคงของประเทศ

เมื่อวิเคราะห์จากสภาพแวดล้อมทั่วไป (เศรษฐพงค์ มะลิสุวรรณ, 2560) สรุปได้ว่า ปัจจัยด้านสิ่งแวดล้อมที่มี ผลต่อความมั่นคงปลอดภัยไซเบอร์ อาทิ การที่เทคโนโลยีสารสนเทศเข้ากับวิถีชีวิตของมนุษย์ การปฏิวัติทางดิจิทัล (Digital Revolution) ทำให้เกิดตัวแปรใหม่ที่ประเทศต้องพึ่งพาเทคโนโลยีดิจิทัล เช่น ในการทำงานของบุคลากรภาครัฐ บริหารราชการแผ่นดิน นอกจากนี้การขยายขอบเขตการใช้งานกับโครงสร้างพื้นฐานที่จำเป็นต่อการดำรงชีวิต ยิ่งเป็นการเพิ่มอาณาเขตของการคุกคามทางไซเบอร์ เช่น ระบบการผลิตไฟฟ้า ระบบน้ำประปา ระบบควบคุมจราจรดาวเทียม และระบบการขนส่งสาธารณะ เป็นต้น

ทั้งนี้ เพื่อให้มีมาตรการรองรับอย่างเท่าทันต่อภัยคุกคามไซเบอร์ดังที่อธิบายมาข้างต้น มีข้อพิจารณาสำคัญ สรุปได้ดังนี้

1. เมื่อพิจารณาขนาดและลักษณะของภัยคุกคามทางไซเบอร์และช่องโหว่ของประเทศ การใช้แนวทางในปัจจุบันอาจจะทำให้ประเทศมีความมั่นคงปลอดภัยไซเบอร์ที่ยังไม่เพียงพอ

2. ควรกำหนดแนวทางโดยคำนึงถึงความต้องการของตลาด (Market Based Approach) เพราะความต้องการและความนิยมอย่างมากจากการใช้ประโยชน์บนโลกไซเบอร์ ทำให้เกิดการลงทุนในภาคเอกชนเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์มีขึ้นอย่างต่อเนื่อง แต่อาจยังไม่มีนัยสำคัญที่ทำให้เกิดการเปลี่ยนแปลง ในระดับที่รองรับกับปัญหาได้ ดังนั้น รัฐบาลต้องเป็นผู้นำและแทรกแซงโดยการสร้างกลไกด้านการลงทุนและการนำทรัพยากรที่มีอยู่ไปใช้เพื่อการเตรียมพร้อมและรองรับกับปัญหา

3. การที่รัฐบาลดำเนินการฝ่ายเดียว จะไม่สามารถแก้ไขได้ในทุกด้าน ต้องสร้างความร่วมมือกับทุกภาคส่วน

4. ประเทศไทยจำเป็นต้องมีหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เน้นการสร้างความเข้าใจให้ความรู้ สร้างความตระหนักและตื่นตัวให้กับประชาชน และมีกลไกสนับสนุนทักษะและสร้างขีดความสามารถต่าง ๆ ที่สามารถก้าวทันและเผชิญกับภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว และต่อเนื่องได้

วิเคราะห์ผลการประเมินด้านความมั่นคงปลอดภัยไซเบอร์ในระดับโลก

ปัจจุบันประเทศไทยมียุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy) (สำนักงานสภามั่นคงแห่งชาติ, 2561) อีกทั้งมีกระทรวงดิจิทัล เศรษฐกิจและสังคม ซึ่งมีบทบาทสำคัญในการประสานการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับระหว่างประเทศ บทบาทที่สำคัญประการหนึ่งคือการพัฒนาด้านบุคลากร อาทิ การได้รับเลือกให้เป็นเจ้าภาพจัดตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre : AJCCBC) (ตามมติที่ประชุม TELMIN-Japan การประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศร่วมกับประเทศญี่ปุ่น ที่ประเทศกัมพูชา) โดยมีสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA เป็นหน่วยงานหลักในการดำเนินงาน เนื่องจากเป็นหน่วยงานที่มีประสบการณ์ในการพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ของประเทศมาอย่างต่อเนื่อง โดยศูนย์ดังกล่าวนี้ได้รับการสนับสนุนจากประเทศญี่ปุ่นเป็นผู้ถ่ายทอดองค์ความรู้ต่าง ๆ ทำให้สามารถดำเนินการฝึกอบรมให้แก่ประเทศสมาชิกอาเซียนเป็นไปอย่างมีประสิทธิภาพ

อย่างไรก็ตาม ในการพิจารณาความมั่นคงปลอดภัยทางไซเบอร์ในระดับโลก ดัชนีความปลอดภัยทางไซเบอร์ทั่วโลกหรือ GCI ซึ่งมีรากฐานมาจาก ITU Global Cybersecurity Agenda (GCA) สะท้อนถึงกฎหมายเทคนิคกับองค์กรที่เสริมสร้างขีดความสามารถและความร่วมมือที่เกี่ยวข้อง

โดยที่สหภาพโทรคมนาคมระหว่างประเทศ หรือ ITU กำหนดตัวชี้วัดไว้ 25 ตัวชี้วัด ในมาตรฐานเดียวทั่วโลก เพื่อตรวจสอบความมั่นคงและความปลอดภัยในโลกไซเบอร์ของรัฐสมาชิก ITU (193 ประเทศ) ซึ่งผลสำรวจในปี 2018 (ITU, 2019) สรุปได้ดังนี้

Member State	Score	Global Rank
United Kingdom	0.931	**1**
United States of America	0.926	2
France	0.918	3
Lithuania	0.908	4
Estonia	0.905	5
Singapore	0.898	**6**
Spain	0.896	7
Malaysia	0.893	8
Canada	0.892	9
Norway	0.892	9
Australia	0.890	10
Thailand	**0.796**	**35**

จากตารางแสดงข้อมูลข้างต้น ย่อมเป็นการสะท้อนให้เห็นถึงศักยภาพและการดำเนินนโยบายที่เป็นรูปธรรมในประเทศนั้น ๆ โดยประเทศที่มีกลยุทธ์ด้านความปลอดภัยทางไซเบอร์ที่ดีที่สุดในเอเชียตะวันออกเฉียงใต้ คือ สิงคโปร์ ซึ่งได้อันดับที่ 6 ในขณะที่ประเทศไทยได้อันดับที่ 35 ทั้งนี้ ท่ามกลางการเผชิญกับปัญหาการคุกคามทางไซเบอร์ที่กระทบต่อสิทธิมนุษยชน การดูแลความมั่นคงปลอดภัยไซเบอร์จึงเป็นสิ่งจำเป็นต้องดำเนินการอย่างต่อเนื่อง เพื่อให้แน่ใจว่า พลเมืองของประเทศได้ใช้ชีวิตอยู่ท่ามกลางสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัย โดยจะเห็นได้ว่า การจัดอันดับดังกล่าวของ ITU นั้น เป็นไปเพื่อให้รัฐต่าง ๆ ตระหนักถึงความสำคัญในการสร้างกลไกที่จำเป็นเพื่อการรักษาไว้ซึ่งความปลอดภัยของพลเมืองของรัฐในโลกดิจิทัลที่ภัยคุกคามอาจมาในรูปแบบของสิ่งที่มองไม่เห็น

กล่าวได้ว่า การประเมินผลในระดับความร่วมมือระหว่างประเทศยังคงเป็นสิ่งที่จำเป็น แต่ทว่าเป็นหน้าที่ของรัฐบาลของแต่ละประเทศที่จะต้องพัฒนากลไกหรือจัดให้มีแผนยุทธศาสตร์ที่เป็นรากฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยต้องมีการประสานงานที่มีประสิทธิภาพและการประสานความร่วมมือระหว่างหน่วยงานของรัฐในระดับชาติและระดับท้องถิ่น รวมถึงภาคเอกชนและภาคประชาสังคมอีกด้วย (Artur Appazov, 2014)

วิเคราะห์การกำกับดูแลของสังคมโลกในประเด็นด้านสิทธิมนุษยชน

กล่าวได้ว่า กิจกรรมในโลกยุคปัจจุบันเกือบแทบทั้งหมดแท้จริงแล้วย่อมอยู่ภายใต้ “การกำกับดูแลระดับโลก (Global Regulation)” ในรูปแบบใดรูปแบบหนึ่ง กล่าวคือ สินค้าและกิจกรรมต่าง ๆ ที่นอกจากจะมีกลไกการควบคุมมาตรฐานโดยรัฐใดรัฐหนึ่งแล้ว เมื่อสินค้าและกิจกรรมเหล่านั้นต้องข้ามพรมแดนหรือมีการขนส่งข้ามประเทศ ย่อมต้องอยู่ภายใต้กลไกการกำกับดูแลหรือมาตรฐานระดับโลกหรือระดับระหว่างประเทศ

จะเห็นได้ว่า การสร้างมาตรฐานสากลที่ได้รับการยอมรับในระดับโลก หรือการสร้างระบบการกำกับดูแลครอบคลุมทั่วโลก (Global Regulatory Regimes) ในหลากหลายกิจกรรม เช่น การอนุรักษ์ป่า การประมง การจัดการทรัพยากรน้ำ การคุ้มครองสิ่งแวดล้อม การควบคุมอาวุธ ความปลอดภัยของอาหาร มาตรฐานทางการเงินและการบัญชี เภสัชกรรม การคุ้มครองทรัพย์สินทางปัญญา การปกป้องผู้อพยพ มาตรฐานด้านแรงงาน และมาตรการป้องกันการผูกขาด เป็นต้น โดยที่ระบบการกำกับดูแลที่ครอบคลุมหลายภาคส่วนเหล่านี้มีแนวโน้มได้รับการยอมรับโดยมีขอบเขตการบังคับใช้มากยิ่งขึ้น จากการขับเคลื่อนผ่านกลไกความร่วมมือ

โดยองค์การระหว่างประเทศ ทั้งที่เป็นองค์การระหว่างรัฐบาล (Intergovernmental Organizations หรือ IGOs) รวมถึงองค์การที่จัดตั้งขึ้นโดยภาคเอกชน (Non-Governmental Organizations หรือ NGOs)

ทั้งนี้ เรื่องความมั่นคงของมนุษย์ โดยเฉพาะอย่างยิ่ง ด้านความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดน ย่อมต้องมีระบบกำกับดูแล ซึ่งในเบื้องต้นอาจกำหนดกรอบสำหรับการดำเนินการของรัฐ หรือการกำหนดแนวทางสำหรับหน่วยงานปกครองภายในประเทศ (Domestic Administrative Agencies) ซึ่งส่งผลกระทบโดยตรงกับภาคประชาสังคมระดับประเทศ (National Civil Society Actors) ทั้งนี้ ระบบกำกับดูแลอาจจะมีกลไกเป็นของตนเองในการนำไปปฏิบัติ ซึ่งอาจต้องอาศัยหน่วยงานระดับประเทศหรือระดับภูมิภาคเป็นผู้ดำเนินการ โดยที่ในกรณีต้องยุติข้อขัดแย้ง ระบบกำกับดูแลบางระบบอาจจัดตั้งหน่วยงานด้านยุติธรรม (หรือกึ่งศาล) (Judicial or Quasi - Judicial Bodies) หรือจะใช้รูปแบบที่ “นุ่มนวล” มากกว่า (Softer Forms) เช่น การเจรจา การไกล่เกลี่ย ซึ่งเป็นกลไกดั้งเดิมที่บนพื้นฐานของการยินยอมของรัฐ (State Consent) ซึ่งมักได้รับความนิยม อย่างไรก็ตาม ท่ามกลางโลกดิจิทัลที่ไร้พรมแดนเช่นนี้ วิธีการดั้งเดิมอาจไม่เพียงพอที่จะรับมือกับกิจกรรมในระดับโลก (Global Activities) ได้ทั้งหมด ดังนั้น ยุทธศาสตร์ในการรับมือกับปัญหาการคุกคามทางไซเบอร์ในแต่ละประเทศควรสอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติที่องค์การระหว่างประเทศแนะนำไว้ (ITU, 2018) อีกทั้งควรตระหนักว่าความมั่นคงปลอดภัยในโลกไซเบอร์เป็นองค์ประกอบสำคัญของนโยบายต่างประเทศ โดยเห็นว่าเป็นสิ่งสำคัญที่จะต้องส่งเสริมทักษะด้านการทูตทางไซเบอร์ (Cyber Diplomacy) เพื่อเสริมสร้างวิธีการแบบดั้งเดิม รวมถึงพัฒนาโครงสร้างองค์กรที่เฉพาะเจาะจงซึ่งมีเป้าหมายหลักคือ การมีส่วนร่วมทางการทูตในประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ในโลกพรมแดนที่ส่งผลต่อความมั่นคงของมนุษย์ ซึ่งต้องกำหนดแผนดำเนินการระยะยาวด้านความร่วมมือระหว่างประเทศ การกำหนดผู้มีส่วนได้ส่วนเสีย รวมถึงกลไก ในการสร้างบรรทัดฐานด้านการรักษาความปลอดภัยทางไซเบอร์สากลและการบังคับใช้ที่เป็นรูปธรรม

ข้อเสนอแนะ

ข้อเสนอแนะในมุมมองของผู้เขียนเพื่อสร้างความมั่นคงปลอดภัยทางไซเบอร์ในสังคมไทย อาทิ

1. ส่งเสริมให้มีกลไกการจัดการความรู้ด้านดิจิทัลให้กับพลเมืองของประเทศที่เป็นรูปธรรม

ทรัพยากรมนุษย์ในโลกดิจิทัล เป็นเรื่องที่ต้องเร่งดำเนินการเพื่อสร้างบุคคลที่มีศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Professionals) โดยเฉพาะผู้มีหน้าที่ด้านการบังคับใช้กฎหมาย (Law Enforcement Community) ซึ่งต้องเป็นผู้ที่มีความเชี่ยวชาญทางเทคนิคด้วย อาทิ การสอบสวนออนไลน์ (Online Investigation) และการชันสูตรทางดิจิทัล (Digital Forensics) โดยที่ผู้สอบสวน (Investigators) ต้องมีศักยภาพเพื่อความพร้อมในการเสริมสร้างความมั่นคงของมนุษย์

2. ปลูกฝังค่านิยมด้านการรู้เท่าทันและการตระหนักรู้ทางดิจิทัล

ค่านิยมด้านการรู้เท่าทันและการตระหนักรู้ทางดิจิทัล (Digital Literacy and Awareness) เป็นเรื่องสำคัญที่ต้องส่งเสริมให้เจ้าหน้าที่ของรัฐและประชาชน ซึ่งบางส่วนอาจขาดความตระหนักรู้เกี่ยวกับอาชญากรรมทางไซเบอร์ เนื่องจากเป็นภัยคุกคามที่มองไม่เห็นจนกว่าจะปรากฏความเสียหายที่ชัดเจน จึงต้องมีกระบวนการเพื่อให้ความรู้และสร้างความเข้าใจ ตลอดจนปลูกฝังค่านิยมด้านการรู้เท่าทันและการตระหนักรู้ทางดิจิทัลให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็วในโลกดิจิทัล

3. บูรณาการความร่วมมือระหว่างหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานอื่น ๆ ที่เกี่ยวข้องสิทธิมนุษยชนกับความมั่นคงของมนุษย์

ควรกำหนดยุทธศาสตร์ด้านอาชญากรรมไซเบอร์ให้ครอบคลุมกับปัญหาด้านสิทธิมนุษยชน อาทิ การแสวงประโยชน์ทางเพศจากเด็กทางออนไลน์ (Online Child Sexual Exploitation) ทั้งนี้ การดำเนินการในประเทศไทย มีการกำหนดยุทธศาสตร์คณะกรรมการสิทธิมนุษยชนแห่งชาติ (พ.ศ. 2560 - 2565) ที่วางหลักการให้ต้องส่งเสริมและติดตามให้ทุกภาคส่วนของสังคมให้เกิดการเคารพสิทธิมนุษยชนตามที่ได้รับการรับรองตามรัฐธรรมนูญ ดังนั้น การคุ้มครองสิทธิมนุษยชนในปัจจุบัน จึงจำเป็นต้องครอบคลุมการละเมิดสิทธิมนุษยชนในช่องทางที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์หรือใช้ประโยชน์

จากช่องทางดิจิทัลด้วย เพราะอาจเป็นช่องทางที่ “ประชาชนกลุ่มเปราะบาง” เช่น เด็กและเยาวชน ที่อาจเข้าถึงข้อมูลจากสื่อออนไลน์และนำความไม่ปลอดภัยมาสู่ตนเองและครอบครัวได้ ทั้งนี้ การกำหนดนโยบายด้านอาชญากรรมไซเบอร์ (Lack of Proper Regulatory/Policy Regarding Cybercrime) ในประเด็นดังกล่าวนี้ ถือเป็นความท้าทายอีกประการหนึ่ง โดยควรศึกษาวิจัยอย่างต่อเนื่องในประเด็นที่เกี่ยวข้องโดยละเอียดต่อไปในอนาคต อาทิ การติดตามผลลัพธ์ หรือ Feedback จากการกำหนดนโยบายของรัฐบาลวางโครงสร้างทางกฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ประกาศและมีผลใช้บังคับแล้ว เพื่อแก้ไขความกังวลของประชาชนเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ควบคู่กับการส่งเสริมคุณค่าความเป็นมนุษย์โดยการเคารพต่อหลักเกณฑ์พื้นฐานด้านสิทธิมนุษยชนที่เป็นหลักการสากล

4. พัฒนาระบบกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมโดยมุ่งเน้นความเป็นอิสระ

ควรกำหนดกรอบการกำกับดูแลโดยสร้างองค์กรด้านการกำกับดูแล (Regulatory Body) ความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมระดับรัฐ ซึ่งต้องมีความอิสระ โดยอาจจัดตั้งในรูปของคณะกรรมการ เช่น คณะกรรมการกำกับกิจการพลังงาน เป็นต้น) เพื่อทำหน้าที่ประสานความร่วมมือในระดับระหว่างประเทศ การรับข้อร้องเรียนจากประชาชน รวมถึงมีกลไกระงับข้อพิพาทหรือไกล่เกลี่ยปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ในเบื้องต้น

5. ดำเนินนโยบายด้านการต่างประเทศอย่างเป็นรูปธรรม เพื่อให้เกิดความร่วมมือด้านความมั่นคงทางไซเบอร์ (Cyber Protection Framework) และระบบกำกับดูแลทางไซเบอร์ในภูมิภาคอาเซียน

เพื่อแก้ไขประเด็นข้ามเขตอำนาจศาล (Cross-Jurisdictional Issues) ตลอดจนเป็นการบูรณาการความร่วมมือในภูมิภาคเอเชียตะวันออกเฉียงใต้อย่างเป็นรูปธรรม ควรจัดการเจรจาหรือการประชุมเพื่อการตกลงร่วมกันในการสร้างกลไกในการแบ่งปันข้อมูลและสร้างช่องทางในการขอหลักฐานอิเล็กทรอนิกส์จากประเทศอื่น ๆ ได้ เพื่อสร้างมาตรการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งถือเป็นประเด็นที่เชื่อมโยงต่อการธำรงไว้ซึ่งสันติภาพและความมั่นคงของมนุษย์

บทส่งท้าย

ท่ามกลางความเจริญก้าวหน้าทางเทคโนโลยีที่โลกดิจิทัลครอบคลุมและแพร่ขยาย (Proliferation) ไปทั่วโลกแทบทุกพื้นที่ และในบางครั้งก็เป็นประหนึ่งโลกเสมือนจริง (Visual World) โดยเป็นกิจวัตรประจำวันของคนส่วนใหญ่ในโลกปัจจุบัน อย่างไรก็ตาม ในทุกกครั้งที่เราใช้เป็นเครื่องมืออำนวยความสะดวก หรือใช้เป็นอุปกรณ์สำคัญในการเรียน หรือใช้ประกอบการทำงาน ตลอดจนใช้เป็นช่องทางในการสร้างความบันเทิงซึ่งในบางครั้งอาจเกินจริง (Surreal) จะเห็นได้ว่าในทุกกิจกรรมดังที่กล่าวมา ย่อมต้องเผชิญความจริงที่ว่า ในทุก ๆ ครั้งที่มีการเข้าถึง (Access) ย่อมเสี่ยงที่จะมีการคุกคาม (Threat) กลับมาได้เสมอ

กล่าวโดยสรุป ในประเด็นด้านความมั่นคงของมนุษย์ การสร้างสมดุลระหว่างรัฐกับปัจเจกบุคคลเพื่อรักษาไว้เสรีภาพของปัจเจกบุคคล กับการต้องคำนึงถึงประโยชน์สาธารณะ ตลอดจนการรักษาไว้ซึ่งความมั่นคงของรัฐ การกำหนดยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ในโลกไร้พรมแดนนี้ ควรตรวจสอบให้แน่ใจว่ามีการเฝ้าระวังและการรวบรวมข้อมูลซึ่งต้องดำเนินการภายในบริบทของหน่วยงานที่เชี่ยวชาญเฉพาะด้าน บนพื้นฐานของประโยชน์สาธารณะที่ชัดเจนโปร่งใส (Transparency) และไม่มีการเลือกปฏิบัติ (Discrimination) โดยที่ความเชื่อมโยงอย่างไร้ขอบเขตบนไซเบอร์สเปซ (Cyberspace) เป็นสภาวะความเปลี่ยนแปลงซึ่งไม่เพียงแต่ให้ประโยชน์มหาศาลแก่มนุษยชาติ แต่ในบริบทของความมั่นคงทางดิจิทัลของมนุษย์ (Digital Human Security) ย่อมนำมาซึ่งภัยคุกคาม อันเป็นโทษต่อมนุษย์ โดยเป็นภัยคุกคามในภาวะสันติ (Peace Time Threats) ต่อมนุษยชาติได้เช่นกัน

บรรณานุกรม

กรมเจรจาทางการค้าระหว่างประเทศ. (2561, 23 มกราคม). *กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป.* https://www.moc.go.th/images/633/GDPR-3-5.pdf

ไทยเซิร์ต (2554, 3 พฤศจิกายน). *APT ภัยคุกคามใหม่หรือแค่ชื่อใหม่ของภัยเดิม.* https://www.thaicert.or.th/papers/technical/2011/pa2011te002.html

เศรษฐพงค์ มะลิสุวรรณ. (2560, 22 มิถุนายน). *เอกสารเรื่อง National Cybersecurity Strategy ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ*. http://nbtc.go.th/getattachment/News/Information/National-Cybersecurity-Strategy-ยุทธศาสตร์ความมั่น/เอกสารแนบ.pdf.aspx

สถาบันวิจัยเพื่อการพัฒนาประเทศไทย. (2559, 11 พฤษภาคม). *กรอบแนวคิดและกรอบยุทธศาสตร์ในการพัฒนาดัชนีชี้วัดด้านหลักนิติธรรม/นิติรัฐ (Rule of Law Index/Indicators) ในประเทศไทย*. https://tdri.or.th/wp-content/uploads/2016/11/Rule_of_Law_Index_resize.pdf

สำนักงานรัฐบาลอิเล็กทรอนิกส์. (2559). *ความมั่นคงปลอดภัยทางไซเบอร์.* สืบค้นจาก https://dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf

สำนักงานสภาความมั่นคงแห่งชาติ. (2561). *ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2561-2564.* (สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา, มิถุนายน 2561) สืบค้นจาก http://www.nsc.go.th/Download1/ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐-๒๕๖๔.pdf

Anthony Giddens. (1996). *Affluence, Poverty and the Idea of a Post-Scarcity Society.* Retrieved from https://www.files.ethz.ch/isn/29014/dp63.pdf

Artur Appazov. (2014). *Legal Aspects of Cybersecurity.* Retrieved from https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

Brad Smith. (2017). *Protecting and Defending against Cyberthreats in Uncertain Times.* Retrieved from https://www.rsaconference.com/industry-topics/presentation/protecting-and-defending-against-cyberthreats-in-uncertain-timesdefending-against-cyberthreats-in-uncertain-times

Charles E. Costanzo. (2011). *Human Security in a Borderless World.* Retrieved from https://digital-commons.usnwc.edu/nwc-eview/vol64/iss3/11

Deloitte. (2012). *Cyber Security in a Borderless World*. Retrieved from https://deloitte.wsj.com/cio/2012/05/23/cyber-security-in-a-borderless-world/

ENISA. (2018). *Threat Landscape Report*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport

Henning Schaloske, Kathrin Feldmann and AmreiZürn. (2018). *Cyber cross-jurisdictional risks and the impact of GDPR: Europe*. Retrieved from https://www.mondaq.com/uk/data-protection/683016/cyber-cross-jurisdictional-risks-and-the-impact-of-gdpr-europe

ITU. (2010). *Introduction to Security Cyberspace, Cybercrime and Cybersecurity*. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf

ITU. (2018). *Guide to Developing a National Cybersecurity Strategy*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

ITU. (2019). *Global Cybersecurity Index (GCI) 2018*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Luke Irwin. (2020). *What's the difference between information security and cyber security?.* Retrieved from https://www.itgovernance.eu/blog/en/whats-the-difference-between-information-security-and-cyber-security

OECD. (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECDRecommendation and Companion.* Retrieved from https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en#page5

Philip Alston. (1981). *Development and the Rule of Law: Prevention Versus Cure as a Human Rights Strategy.* Retrieved from https://www.icj.org/wp-content/uploads/2013/06/Universal-rule-of-law-development-working-paper-1981-eng.pdf

ThaiCERT. (2019). *Threat Group Cards: A Threat Actor Encyclopedia.* Retrieved from https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf

UN. (2018). *Consensus on The Application of Rule of Law and UN Charter to Make Cyberspace Safe.* Retrieved from https://www.un.org/sustainabledevelopment/blog/2018/11 /consensus-on-the-application-of-rule-of-law-and-un-charter-to-make-cyberspace-safe/

United States Government Publishing Office (GPO). (2020). *Federal Information Security Modernization Act of 2014 (Public Law 113-283; December 18, 2014).* Retrieved from https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf