# ปัญหาการบังคับใช้เขตอำนาจรัฐเหนือพื้นที่ไซเบอร์ : ศึกษากรณีการก่อการร้ายทางไซเบอร์

# PROBLEMS IN ENFORCEMENT OF STATE JURISDICTION OVER CYBERTERRITORIES: STUDIES OF CYBERTERRORISM

**จิตราภรณ์ โสตถิกุล**

**Jittraphorn Sotthikul**

นักศึกษาปริญญาโท หลักสูตรนิติศาสตรมหาบัณฑิต สาขากฎหมายระหว่างประเทศ

คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ : jittraphorn@outlook.com

Graduate student of Master of Laws Program in International Law,

Faculty of Law, Thammasat University : jittraphorn@outlook.com

Received : July 04, 2021

Revised : October 03, 2021

Accepted : November 02, 2021

**บทคัดย่อ**

บทความนี้มุ่งศึกษาปัญหาการบังคับใช้เขตอำนาจรัฐตามกฎหมายระหว่างประเทศเหนือการกระทำผิดที่เกิดขึ้นบนพื้นที่ไซเบอร์ เนื่องจากเป็นพื้นที่ที่มิได้ตั้งอยู่บนเขตแดนทางกายภาพที่แน่นอนจึงทำให้การกระทำผิดที่เกิดขึ้นอาจมีความเชื่อมโยงกับรัฐต่าง ๆ ทั่วโลก ซึ่งทำให้การกระทำผิดเหล่านี้มีลักษณะระหว่างประเทศ อันทำให้การบังคับใช้อำนาจรัฐเหนือการกระทำผิดดังกล่าวต้องเป็นไปตามหลักกฎหมายระหว่างประเทศ อย่างไรก็ตามแนวคิดเกี่ยวกับการบังคับใช้เขตอำนาจรัฐในปัจจุบันยึดโยงกับเขตแดนทางกายภาพ จึงทำให้เกิดปัญหาการอ้างเขตอำนาจรัฐเหนือการกระทำความผิดบนพื้นที่ไซเบอร์ทับซ้อนกัน ด้วยเหตุนี้ผู้เขียนจึงได้ศึกษาการบังคับใช้เขตอำนาจรัฐตามหลักกฎหมายระหว่างประเทศ เพื่อวิเคราะห์ถึงปัญหาในการปรับใช้กับการกระทำผิดที่เกิดขึ้นบนพื้นที่ไซเบอร์โดยเฉพาะในส่วนของการก่อการร้ายทางไซเบอร์ เนื่องจากถือเป็นภัยคุกคามทางไซเบอร์ที่กระทบต่อเสถียรภาพและความมั่นคงระหว่างประเทศ ซึ่งจากผลการศึกษาพบว่าการนำหลักป้องกันมาปรับใช้กับการบังคับใช้เขตอำนาจรัฐเหนือการก่อการร้ายทางไซเบอร์จะช่วยลดจำนวนรัฐที่สามารถอ้างการใช้เขตอำนาจเหนือการกระทำความผิดที่เกิดขึ้นบนพื้นที่ไซเบอร์ได้อย่างเหมาะสมที่สุด ทั้งนี้ผู้เขียนเสนอให้มีการนิยามการก่อการร้ายทางไซเบอร์ที่ชัดเจนในกฎหมายภายในเพื่อที่จะช่วยส่งเสริมให้รัฐสามารถบังคับใช้อำนาจรัฐเหนือการกระทำผิดดังกล่าวอย่างมีประสิทธิภาพ

**คำสำคัญ**

พื้นที่ไซเบอร์, เขตอำนาจรัฐ, การก่อการร้ายทางไซเบอร์

**ABSTRACT**

This article studies on the problems in enforcement of state jurisdiction in international law over offences occurring in cyberspace. As the cyberspace territory does not exist with a precise physical aspect or location, offences committed are therefore connected to nations worldwide, rendering these acts as international and enforcement of state jurisdiction over them in accordance with international law principles. However, concepts of enforcing state jurisdiction are currently tied to physical terrains, causing problems when states claim overlapping jurisdiction over offences committed on cyberspace. For these reasons, the enforcement of state jurisdiction was examined in accordance with international law principles to analyze different issues when enforcing jurisdiction over offences committed in cyberspace, especially cyberterrorism, as cyberthreats against international stability and security. Results are that using the principle of protective jurisdiction over cyberterrorism most appropriately reduces the number of states that can exert jurisdiction over the offences committed on cyberspace. These findings suggest that cyberterrorism should be clearly defined in domestic legislation to support efficient enforcement by state jurisdiction over such offences.

**Keywords**

Cyberspace, State Jurisdiction, Cyber Terrorism.

**1. บทนำ**

การก่อการร้ายทางไซเบอร์ถือเป็นภัยคุกคามทางไซเบอร์รูปแบบใหม่ที่ท้าทายสังคมระหว่างประเทศ โดยภัยคุกคามนี้เกิดขึ้นจากการรวมสองคำเข้าด้วยกัน คือ “ไซเบอร์” และ “การก่อการร้าย” ซึ่งไซเบอร์หรือพื้นที่ไซเบอร์ถือเป็นเครือข่ายที่เชื่อมต่อกันระหว่างโครงสร้างพื้นฐานด้านข้อมูลดิจิทัลและการสื่อสารทั่วโลก และโดยปกติจะเป็นที่เข้าใจว่าหมายถึงอินเทอร์เน็ต หรือในแง่ที่กว้างกว่าจะหมายถึงเครือข่ายคอมพิวเตอร์[1] สำหรับคำว่าการก่อการร้ายที่แม้ว่าประชาคมระหว่างประเทศจะยังไม่มีคำนิยามที่เป็นสากล แต่ก็เป็นที่เข้าใจโดยทั่วไปว่าหมายถึง การกระทำความรุนแรงที่มุ่งเป้าไปยังประชาชนเพื่อให้บรรลุวัตถุประสงค์ทางการเมืองหรือความเชื่อ[2] ด้วยเหตุนี้การก่อการร้ายทางไซเบอร์จึงหมายถึงการกระทำที่หลากหลาย ตั้งแต่การเผยแพร่การโฆษณาชวนเชื่อออนไลน์ไปจนถึงการเปลี่ยนแปลงหรือการทำลายข้อมูล หรือแม้กระทั่งการวางแผนและการโจมตีของผู้ก่อการร้ายผ่านเครือข่ายคอมพิวเตอร์[3] ด้วยลักษณะเช่นนี้ทำให้การกระทำที่ถือเป็นก่อการร้ายทางไซเบอร์มีทั้งลักษณะของการโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์ กล่าวคือ หากการกระทำการก่อการร้ายทางไซเบอร์ใดที่เกิดขึ้นเพื่อบ่อนทำลายการทำงานของเครือข่ายคอมพิวเตอร์เพื่อวัตถุประสงค์ทางการเมืองหรือความมั่นคงของรัฐ[4] ก็จะมีลักษณะของการโจมตีทางไซเบอร์ เช่น การโจมตีต่อเครือข่ายควบคุมระบบโทรคมนาคมของรัฐผ่านการใช้เครือข่ายคอมพิวเตอร์ เป็นต้น หรือหากเป็นการกระทำความผิดอาญาที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ที่ถูกขับเคลื่อนด้วยผลประโยชน์ทางเศรษฐกิจของผู้กระทำความผิด[5] ก็จะเป็นลักษณะการกระทำความผิดของอาชญากรรมทางไซเบอร์ เช่น การทำธุรกรรมออนไลน์เพื่อฟอกเงินที่ใช้ในการสนับสนุนการก่อการร้าย เป็นต้น เนื่องจากลักษณะการกระทำความผิดของการก่อการร้ายทางไซเบอร์ที่หลากหลายเช่นนี้ทำให้ในปัจจุบันยังไม่ปรากฏคำนิยามการก่อการร้ายทางไซเบอร์ที่เป็นสากลซึ่งนำไปสู่ปัญหาการดำเนินคดีกับผู้กระทำความผิดในลักษณะดังกล่าว อย่างไรก็ตาม Dorothy E. Denning ได้ให้คำนิยามของการก่อการร้ายทางไซเบอร์ที่ได้รับการยอมรับทางวิชาการมากที่สุดในปัจจุบัน[6]

---

[1] Laura Mayer Lux, ‘Defining cyberterrorism’ (2018) 7 Revista Chilena De Derecho Y Tecnologia 5, 5.

[2] OHCHR ‘Fact Sheet No. 32, Human Rights, Terrorism and Counter-terrorism’ (July 2008) UN Doc GE.08-41872.

[3] Laura Mayer Lux (เชิงอรรถ 1) 6.

[4] Oona A Hathaway and others, ‘The Law of Cyber-Attack’ (2012) 4 California Law Review 817, 826.

[5] Convention on cybercrime (Budapest Convention) art 2-11.

[6] Dorothy E. Denning, ‘Cyberterrorism’ (Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representative, 23 May 2000) <https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm?fbclid=IwAR0fwDSjm35f2WjzmfMTHaOBxqTsp6vJ9vapr_6E82YQ_MRKP-Bd1KAV3qA> สืบค้นเมื่อ 26 กุมภาพันธ์ 2564.

> “การก่อการร้ายทางไซเบอร์เป็นการรวมกันของการก่อการร้ายและพื้นที่ไซเบอร์ ซึ่งเป็นที่เข้าใจโดยทั่วไปว่าหมายถึงการโจมตีที่ผิดกฎหมายและเป็นการคุกคามด้วยการโจมตีต่อคอมพิวเตอร์ เครือข่าย และข้อมูลที่ถูกจัดเก็บไว้ เพื่อข่มขู่หรือบีบบังคับรัฐบาลหรือประชาชนของรัฐเพื่อให้บรรลุถึงวัตถุประสงค์ทางการเมืองหรือสังคม โดยจะต้องเป็นการโจมตีที่เป็นการใช้ความรุนแรงต่อบุคคลหรือทรัพย์สิน หรืออย่างน้อยที่สุดได้ก่อให้เกิดความเสียหายที่เพียงพอที่จะทำให้เกิดความหวาดกลัว” (แปลโดยผู้เขียน)

การนิยามเช่นนี้ยังเป็นแนวทางในการอธิบายถึงการก่อการร้ายทางไซเบอร์ของสหประชาชาติว่า “เป็นการเปลี่ยนแปลงข้อมูลในระบบคอมพิวเตอร์จากระยะไกล หรือเป็นการขัดขวางการเคลื่อนย้ายข้อมูลระหว่างระบบคอมพิวเตอร์เพื่อก่อการโจมตีของผู้ก่อการร้าย”[7] จะเห็นได้ว่าลักษณะที่สำคัญของการก่อการร้ายทางไซเบอร์เป็นความผิดอาญา อีกทั้งเป็นความผิดที่กระทำบนพื้นที่ไซเบอร์ซึ่งมิได้ตั้งอยู่บนเขตแดนทางกายภาพที่แน่นอน ดังนั้นจึงทำให้เกิดปัญหาการบังคับใช้เขตอำนาจรัฐเหนือการก่อการร้ายทางไซเบอร์ กล่าวคือ แนวคิดเรื่องเขตอำนาจรัฐที่มีในปัจจุบันตั้งอยู่บนพื้นฐานของการใช้เขตอำนาจรัฐเหนือดินแดนที่มีลักษณะทางกายภาพปกติ[8] และเนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีและการสื่อสารที่มากขึ้นทำให้กิจกรรมต่าง ๆ ที่เกิดขึ้นมิได้จำกัดอยู่แต่ภายในดินแดนของรัฐใดรัฐหนึ่งโดยเฉพาะอีกต่อไป ทำให้เกิดความพยายามในการขยายขอบเขตการใช้อำนาจรัฐออกไป[9] ไม่ว่าจะด้วยการใช้เขตอำนาจรัฐตามหลักสัญชาติ หลักผู้ถูกกระทำ หลักสากล หรือหลักป้องกัน แต่การก่อการร้ายทางไซเบอร์เป็นการกระทำความผิดที่เกิดขึ้นบนพื้นที่ไซเบอร์ที่อาจทำให้มีรัฐมากกว่าหนึ่งรัฐสามารถอ้างการใช้เขตอำนาจรัฐตามหลักต่าง ๆ เหนือการกระทำดังกล่าวได้ ซึ่งจากการศึกษาจะพบว่าการใช้เขตอำนาจรัฐเหนือการก่อการร้ายทางไซเบอร์ตามหลักการแต่ละหลักจะนำไปสู่ปัญหาที่แตกต่างกัน โดยสามารถแบ่งประเด็นที่จะพิจารณาได้ 2 ส่วน ได้แก่ ส่วนแรกเป็นการศึกษาปัญหาการใช้เขตอำนาจรัฐตามกฎหมายระหว่างประเทศเหนือพื้นที่ไซเบอร์ในกรณีของการก่อการร้ายทางไซเบอร์ ซึ่งแบ่งออกเป็นการใช้เขตอำนาจรัฐตามหลักดินแดน หลักผู้ถูกกระทำ หลักสัญชาติ และหลักสากลตามลำดับ และในส่วนที่สองจะเป็นการพิจารณาถึงแนวทางการแก้ไขปัญหาการใช้เขตอำนาจรัฐเหนือพื้นที่ไซเบอร์ในกรณีของการก่อการร้ายทางไซเบอร์โดยใช้หลักป้องกัน

---

[7] UNODC ‘Counter-Terrorism Legal Training Curriculum: Module 1 Counter-Terrorism in the International Law Context’ (2021) UN Doc V.21-02319 อ้างถึงใน ‘Cyberterrorism’ (UNODC) <http://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html> สืบค้นเมื่อ 26 กันยายน 2564.

[8] Malcolm N. Shaw, *International law* (Cambridge: Grotius Publications Limited, 1991) 276.

[9] Cristos Velasco, Julia Hörnle and Anna-Maria Osula, ‘Global Views on Internet Jurisdiction and Trans-Border Access’ (2016) < https://rm.coe.int/16806b8a7c> สืบค้นเมื่อ 26 กันยายน 2564.

**2. ปัญหาการใช้เขตอำนาจรัฐเหนือพื้นที่ไซเบอร์ในกรณีของการก่อการร้ายทางไซเบอร์**

การก่อการร้ายทางไซเบอร์เป็นการดำเนินการบนเครือข่ายคอมพิวเตอร์ซึ่งมิได้ยึดโยงอยู่กับเขตแดนทางกายภาพที่แน่นอน กล่าวคือสามารถดำเนินการในเวลาใดก็ได้บนพื้นที่ไซเบอร์ โดยไม่จำเป็นต้องเข้าไปสู่พื้นที่ทางกายภาพจริงเพื่อดำเนินการ[10] เช่น ผู้ก่อการร้ายชาวฝรั่งเศสได้ดำเนินการผ่านเครือข่ายอินเทอร์เน็ตของประเทศไทยในขณะที่อยู่ในประเทศสหรัฐอเมริกาเพื่อโจมตีระบบการทำงานเครือข่ายคอมพิวเตอร์ของประเทศจีน เป็นต้น จากกรณีตัวอย่างนี้ประเทศที่อาจอ้างการใช้เขตอำนาจรัฐเหนือความผิดที่เกิดขึ้นได้แก่ ประเทศฝรั่งเศสอ้างตามหลักสัญชาติ ประเทศสหรัฐอเมริกา และประเทศจีนอ้างการใช้เขตอำนาจรัฐตามหลักดินแดน ซึ่งถือเป็นการอ้างการใช้เขตอำนาจรัฐทับซ้อนกันเหนือการกระทำความผิดเดียว ดังนั้นการก่อการร้ายทางไซเบอร์จึงเป็นการกระทำความผิดที่ผู้ดำเนินการสามารถปฏิบัติการโจมตีต่อเป้าหมายที่อยู่ในระยะไกลได้โดยไม่จำเป็นจะต้องเข้าไปถึงพื้นที่เป้าหมายจริง เนื่องจากเป็นการปฏิบัติการผ่านเครือข่ายคอมพิวเตอร์โดยจะใช้วิธีการโจมตีในลักษณะของการสั่งการระยะไกล (remote) รวมถึงทำให้สามารถโจมตีต่อเป้าหมายที่หลากหลายได้อีกด้วย[11] นอกจากนี้การระบุแหล่งที่มาของการกระทำความผิดรวมถึงการระบุข้อมูลของผู้กระทำความผิดเป็นไปได้ยาก เพราะการดำเนินการบนพื้นที่ไซเบอร์สามารถปกปิดตัวตน รวมไปถึงสามารถอำพรางที่มาของการกระทำความผิดได้[12] จะเห็นได้ว่าลักษณะการกระทำความผิดของการก่อการร้ายทางไซเบอร์ที่เกิดขึ้นนอกเหนือเขตแดนทางกายภาพปกติทำให้เกิดปัญหาในการใช้เขตอำนาจรัฐขึ้น และโดยเฉพาะอย่างยิ่งในกรณีตัวอย่างที่กล่าวมานี้ก็แสดงให้เห็นถึงปัญหาการใช้เขตอำนาจรัฐตามหลักดินแดนที่นำไปสู่ปัญหาการอ้างเขตอำนาจรัฐไม่มีที่สิ้นสุด เนื่องจากไม่สามารถระบุตำแหน่งของสถานที่ที่เกิดการกระทำความผิดได้อย่างแน่นอนบนดินแดนทางกายภาพ เช่นเดียวกับการอ้างเขตอำนาจรัฐตามหลักผู้ถูกกระทำที่แม้ว่าจะมิได้คำนึงถึงสถานที่ที่เกิดความผิดขึ้น แต่โดยส่วนใหญ่มักสร้างผลกระทบเป็นวงกว้างซึ่งทำให้มีผู้เสียหายจำนวนมากและสามารถนำไปสู่การอ้างเขตอำนาจรัฐไม่มีที่สิ้นสุดได้เช่นเดียวกัน เช่นกรณีของไวรัส WannaCry ที่เป็นการปล่อยมัลแวร์เข้าไปในระบบคอมพิวเตอร์เพื่อเข้าถึงข้อมูลที่สำคัญเพื่อใช้สำหรับการเรียกค่าไถ่ โดยในปี ค.ศ.2017 พบว่ามีคอมพิวเตอร์ใน 74 ประเทศที่ถูกไวรัสดังกล่าวโจมตี ซึ่งถึงแม้ว่าคอมพิวเตอร์ในประเทศรัสเซียจะถูกโจมตีมากที่สุด แต่การโจมตีที่เกิดขึ้นในยูเครน อินเดีย และไต้หวันก็มีความเสียหายที่รุนแรงเช่นเดียวกัน[13] ดังนั้นในกรณีนี้จะทำให้มีรัฐจำนวนมากสามารถอ้างการใช้เขตอำนาจรัฐตามหลักผู้ถูกกระทำได้

---

[10] Mohammad Iqbal, 'Defining Cyberterrorism' (2004) 12 Journal of Computer & Information Law 397, 403.

[11] Anna C. Mourlam, 'Unarmed Attacks: Cyber Combatants and the Right to Defend' (2018) 26 The California International Law Journal 19, 19.

[12] Gabriel Weimann, 'Cyberterrorism: How Real Is the Threat?' (Submitted to United States Institute of Peace, December 2004) 6.

[13] Alex Perekalin, 'WannaCry: Are you safe?' (Kaspersky Daily, 13 May 2017) <https://www.kaspersky.com/blog/wannacry-ransomware/16518/> สืบค้นเมื่อ 26 กันยายน 2564.

2.1 ปัญหาการใช้เขตอำนาจรัฐตามหลักดินแดน (Territorial Jurisdiction) กับการก่อการร้ายทางไซเบอร์

เขตอำนาจรัฐตามหลักดินแดนเป็นแนวคิดการใช้เขตอำนาจรัฐที่พิจารณาถึงสถานที่ที่การกระทำความผิดเกิดขึ้น ไม่ว่าบุคคลผู้กระทำความผิดจะเป็นคนชาติของรัฐนั้นหรือไม่ก็ตาม[14] โดยการพิจารณาเขตอำนาจรัฐตามหลักดินแดนแบ่งออกเป็น 2 ลักษณะ[15] คือ การใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัย (Subjective Territorial Jurisdiction) ที่เป็นการใช้เขตอำนาจรัฐเหนือการกระทำความผิดอาญาที่เริ่มต้นกระทำในรัฐหนึ่ง แต่ผลของการกระทำนั้นไปสิ้นสุดในดินแดนของรัฐอื่น และการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นภาวะวิสัย (Objective Territorial Jurisdiction) ที่เป็นการใช้เขตอำนาจรัฐเหนือการกระทำความผิดอาญาที่ผลของการกระทำความผิดได้สิ้นสุดในดินแดนของตน แม้ว่าองค์ประกอบของความผิดหรือความผิดนั้นจะได้เริ่มกระทำที่รัฐอื่นก็ตาม จากหลักการใช้เขตอำนาจรัฐตามหลักดินแดนทั้งสองลักษณะนี้เมื่อพิจารณาตามตัวอย่างที่ได้ยกไว้ข้างต้นจะเห็นได้ว่ากรณีที่ผู้ก่อการร้ายชาวฝรั่งเศสอยู่ในประเทศสหรัฐอเมริกาได้ดำเนินการ ผ่านเครือข่ายอินเทอร์เน็ตของประเทศไทยเพื่อโจมตีระบบการทำงานเครือข่ายคอมพิวเตอร์ของประเทศจีน การที่ประเทศสหรัฐอเมริกาอ้างการใช้เขตอำนาจรัฐเหนือการกระทำดังกล่าวก็เป็นไปตามหลักดินแดนที่เป็นอัตวิสัย เนื่องจากเป็นกรณีที่ผู้ก่อการร้ายได้เริ่มดำเนินการเมื่ออยู่ในดินแดนของประเทศสหรัฐอเมริกา[16] เช่นเดียวกับประเทศจีนที่สามารถอ้างการใช้เขตอำนาจรัฐเหนือการกระทำนี้ได้ตามหลักดินแดนที่เป็นภาวะวิสัย เนื่องจากผลของการดำเนินการดังกล่าวได้สิ้นสุดลงในประเทศจีน อย่างไรก็ตามก็เป็นปัญหาที่ต้องพิจารณาว่าประเทศไทยสามารถอ้างการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยได้หรือไม่ เนื่องจากเมื่อผู้ก่อการร้ายใช้เครือข่ายอินเทอร์เน็ตของประเทศไทยในการดำเนินการ จะถือว่าการกระทำความผิดได้เริ่มต้นในดินแดนของไทยได้หรือไม่ เพราะหากวิเคราะห์ว่าที่ตั้งของผู้ให้บริการเครือข่ายอินเทอร์เน็ตถือเป็นที่ตั้งทางกายภาพที่สามารถใช้อ้างอิงเขตอำนาจรัฐได้ ก็จะทำให้ประเทศไทยซึ่งถือเป็นดินแดนซึ่งมีการตั้งอยู่ของที่ทำการของผู้ให้บริการเครือข่ายอินเทอร์เน็ตที่ถูกใช้ในการกระทำความผิด เป็นรัฐที่มีเขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยเช่นกัน ด้วยเหตุนี้จึงเห็นได้ว่าแม้การใช้เขตอำนาจรัฐตามหลักดินแดนถือเป็นหลักที่ได้รับความนิยมมากที่สุดและเป็นที่โต้เถียงน้อยที่สุดแต่เมื่อนำมาปรับใช้กับการก่อการร้ายทางไซเบอร์กลับก่อให้เกิดปัญหาที่สำคัญ 3 ประการ[17]

ประการแรก คือ แนวคิดเกี่ยวกับเส้นเขตแดนของรัฐไม่เหมาะสมกับบริบทของพื้นที่ไซเบอร์ เนื่องจากพื้นที่ไซเบอร์มิใช่พื้นที่ที่ตั้งอยู่บนดินแดนทางกายภาพ อีกทั้งยังมิใช่สิ่งที่สามารถจับต้องได้ จึงทำให้พื้นที่ไซเบอร์มีลักษณะของการไร้พรมแดนและการข้ามชาติ ซึ่งเปิดโอกาสให้บางประเทศสามารถอ้างการใช้เขตอำนาจรัฐเหนือการกระทำผิดบนพื้นที่

[14] จุมพต สายสุนทร, *กฎหมายระหว่างประเทศเล่ม 1* (พิมพ์ครั้งที่ 5, วิญญูชน, 2547) 244.

[15] เพิ่งอ้าง.

[16] CNN, 'Hackers shut down Palestinian Internet network' (1 November 2011) <https://edition.cnn.com/2011/11/01/world/meast/mideast-cyber-attack/index.html> สืบค้นเมื่อ 26 กันยายน 2564.

[17] Paul N. Stockton & Michele Golabek-Goldman, 'Prosecuting Cyberterrorists: Applying Traditional Jurisdiction Frameworks to a Modern Threat' (2014) 25 Stanford Law & Policy Review 211, 231-235.

ไซเบอร์ได้[18] ดังเช่นประเด็นของประเทศไทยที่ได้ยกตัวอย่างไปข้างต้นที่เป็นการใช้ที่ตั้งของผู้ให้บริการเครือข่ายอินเทอร์เน็ตที่ถูกใช้ในการดำเนินการก่อการร้ายทางไซเบอร์ถือเป็นพื้นที่ที่การกระทำความผิดได้เกิดขึ้นซึ่งทำให้รัฐมีเขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัย เป็นต้น ประการที่สอง การอ้างเขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยอาจกระตุ้นให้กลุ่มก่อการร้ายเลือก forum shopping คือ ในกรณีที่มีศาลมากกว่าหนึ่งศาลที่มีเขตอำนาจเหนือคดีเดียวกันที่เกิดขึ้น คู่ความสามารถเลือกที่จะฟ้องคดีต่อศาลในประเทศที่มีกฎหมายซึ่งเป็นประโยชน์แก่คดีของตนได้แม้ในคดีที่มีจุดเกาะเกี่ยวในประเทศเพียงเล็กน้อยก็ตาม[19] ดังนั้นหากใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยเป็นเกณฑ์ในการพิจารณาเขตอำนาจศาล จะทำให้ผู้ก่อการร้ายตัดสินใจดำเนินการโจมตีจากภายในรัฐที่ไม่มีกฎหมายว่าด้วยการก่อการร้ายทางไซเบอร์ เพื่อที่จะหลีกเลี่ยงการถูกดำเนินคดี กล่าวคือ เมื่อมีหลายรัฐที่สามารถอ้างการใช้เขตอำนาจรัฐเหนือการโจมตีครั้งหนึ่งได้ แต่หากปรากฏว่าผู้ก่อการร้ายได้ดำเนินการโจมตีจากรัฐที่มีกฎหมายเกี่ยวกับการก่อการร้ายทางไซเบอร์อ่อนแอ จะทำให้รัฐดังกล่าวสามารถอ้างการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยได้ แต่ก็ไม่อาจนำไปสู่การลงโทษผู้ก่อการร้ายดังกล่าวได้อย่างแท้จริง เนื่องจากกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์หรือความผิดบนพื้นที่ไซเบอร์ในแต่ละประเทศมีความแตกต่างกัน และในหลาย ๆ ประเทศก็ไม่สามารถบังคับใช้กฎหมายที่เกี่ยวกับอาชญากรรมทางไซเบอร์ได้ ด้วยเหตุนี้การใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยอาจกระตุ้นให้กลุ่มก่อการร้ายตัดสินใจกระทำความผิดในประเทศที่กฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ยังมีไม่เพียงพอหรือไม่มีประสิทธิภาพได้[20] ซึ่งปัญหานี้ก็สะท้อนให้เห็นถึงปัญหาความไม่มีประสิทธิผลในการป้องกันการก่อการร้ายทางไซเบอร์ด้วยเช่นกัน ประการที่สาม การใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นภาวะวิสัยจะก่อให้เกิดความยุ่งยากและทำให้ความสัมพันธ์ระหว่างรัฐมีความไม่แน่นอน เพราะจะทำให้เกิดการแข่งขันของรัฐต่าง ๆ ในการอ้างการใช้เขตอำนาจรัฐอย่างไม่มีที่สิ้นสุด เนื่องจากโดยทั่วไปกลุ่มก่อการร้ายมักจะมีแนวคิดในการดำเนินการโจมตีต่อเป้าหมายจำนวนมาก อีกทั้งการใช้อาวุธไซเบอร์ยังง่ายและมีค่าใช้จ่ายน้อยกว่าที่จะทำให้เกิดความเสียหายอย่างมากในหลายสถานที่พร้อม ๆ กัน ดังนั้นการดำเนินการหนึ่งครั้งของการก่อการร้ายทางไซเบอร์อาจส่งผลให้เกิดความเสียหายอย่างมากในหลาย ๆ ประเทศ[21] ด้วยเหตุนี้จึงทำให้มีรัฐจำนวนมากที่สามารถอ้างการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นภาวะวิสัยได้ ในขณะที่การใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยอาจส่งผลให้เกิดการอ้างการใช้เขตอำนาจของรัฐต่าง ๆ ไม่มีที่สิ้นสุดได้เช่นเดียวกัน เพราะการก่อการ

[18] เพิ่งอ้าง 232.

[19] Jan-Peter Ewert and David Weslow, 'Forum Shopping in Europe and the United States' (2011) 9 International Trademark Association Bulletin 9, 9.

[20] Paul N. Stockton & Michele Golabek-Goldman (เชิงอรรถ 17) 234.

[21] Brian K. Houghton & Jonathan M. Schachter, 'Coordinated Terrorist Attacks: Implications for Local Responders' (2005) 74 FBI Law enforcement Bulletin 11, 12-15.

ร้ายทางไซเบอร์หนึ่งครั้งอาจเป็นการดำเนินการที่เกิดขึ้นพร้อม ๆ กันในหลาย ๆ รัฐ เช่น การใช้ robot botnets[22] ที่ทำให้คอมพิวเตอร์จำนวนมากในหลาย ๆ ประเทศถูกสั่งการให้โจมตีต่อเป้าหมาย เป็นต้น

2.2 ปัญหาการใช้เขตอำนาจรัฐตามหลักผู้ถูกกระทำ (Passive Personality Jurisdiction) กับการก่อการร้ายทางไซเบอร์

เขตอำนาจรัฐตามหลักผู้ถูกกระทำเป็นแนวคิดการใช้เขตอำนาจรัฐโดยอ้างจากสัญชาติของเหยื่อหรือผู้ถูกกระทำ เนื่องจากเป็นแนวคิดที่ว่ารัฐมีหน้าที่ในการคุ้มครองคนชาติของตน ไม่ว่าคนเหล่านั้นจะอยู่ในดินแดนของรัฐตนหรือไม่ก็ตาม ด้วยเหตุนี้สัญชาติของผู้ถูกกระทำจะเป็นเงื่อนไขในการกำหนดการใช้เขตอำนาจของรัฐ[23] อย่างไรก็ตามแนวคิดนี้ยังมิได้รับความนิยมและยังคงเป็นที่โต้เถียงอยู่มาก[24] ดังนั้นการอ้างเขตอำนาจรัฐตามหลักนี้กับการก่อการร้ายทางไซเบอร์ก็ยังมีความไม่เหมาะสม เพราะจะทำให้เกิดการอ้างเขตอำนาจรัฐไม่มีที่สิ้นสุดเช่นเดียวกับการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นภาวะวิสัย เนื่องจากผลกระทบของการก่อการร้ายทางไซเบอร์อาจส่งผลให้เกิดความเสียหายไปทั่วโลก หรือในกรณีที่เกิดความเสียหายในประเทศหนึ่งโดยเฉพาะ แต่ผลกระทบจากการก่อการร้ายทางไซเบอร์มิได้จำกัดอยู่เพียงคนชาติของรัฐดังกล่าว แต่ยังส่งผลกระทบต่อคนชาติของรัฐอื่นที่อาศัยอยู่ในรัฐดังกล่าวด้วย อันทำให้มีรัฐจำนวนมากสามารถอ้างสิทธิในการดำเนินคดีกับการกระทำดังกล่าวได้ ซึ่งเป็นปัญหาการอ้างการใช้อำนาจรัฐที่ไม่มีที่สิ้นสุด ในขณะเดียวกัน การใช้เขตอำนาจรัฐตามหลักผู้ถูกกระทำเหนือการก่อการร้ายทางไซเบอร์ยังส่งผลให้กระบวนการยุติธรรมระหว่างประเทศเป็นไปได้ยาก เพราะหากรัฐใดเชื่อว่ารัฐผู้ร้องขอความช่วยเหลือหรือขอส่งผู้ร้ายข้ามแดนกำลังก้าวล่วงอธิปไตยของรัฐตนโดยมิได้มีภัยคุกคามเช่นว่านั้นอยู่จริง ย่อมทำให้รัฐที่เชื่อเช่นนี้จะไม่ช่วยเหลือรัฐผู้ร้องขอ ซึ่งทำให้กระบวนการยุติธรรมในการดำเนินการกับการก่อการร้ายทางไซเบอร์ที่จะต้องพึ่งพาความร่วมมือระหว่างประเทศประสบปัญหาขึ้น[25] ด้วยเหตุนี้นอกจากปัญหาที่ทำให้เกิดการอ้างเขตอำนาจรัฐไม่มีที่สิ้นสุดแล้ว การใช้เขตอำนาจรัฐตามหลักผู้ถูกกระทำเหนือการก่อการร้ายทางไซเบอร์ก็สะท้อนให้เห็นถึงความไม่มีประสิทธิผลในการป้องกันภัยคุกคามดังกล่าวด้วยเช่นกัน

---

[22] Botnets คือเครื่องคอมพิวเตอร์ชุดหนึ่งที่มีฐานจากอินเทอร์เน็ตภายใต้ผู้ควบคุมคนเดียวกัน ถึงแม้ว่าคำดังกล่าวสามารถรวมถึงเครือข่ายคอมพิวเตอร์ที่ถูกต้องตามกฎหมาย แต่มักมีการใช้คำดังกล่าวสำหรับคอมพิวเตอร์ที่ถูกแฮก และอยู่ภายใต้การควบคุมของแฮกเกอร์ที่เป็นอาชญากร ดู Ira Winkler and Araceli Treu Gomes, Advanced Persistent Security (Elsevier 2017) 75-76.

[23] Sanjana Sahu, 'Passive Personality Principle: An Overview' (Academike) <http://www.lawctopus.com/academike/passive-personality-principle-overview/> สืบค้นเมื่อ 27 มิถุนายน 2564.

[24] Geoffrey R. Watson, 'The Passive Personality Principle' (1993) 28 Texas International Law Journal 1, 2.

[25] Paul N. Stockton & Michele Golabek-Goldman (เชิงอรรถ 17) 243-245.

2.3 ปัญหาการใช้เขตอำนาจรัฐตามหลักสัญชาติ (Nationality Jurisdiction) กับการก่อการร้ายทางไซเบอร์

การใช้เขตอำนาจรัฐตามหลักสัญชาติเป็นการอ้างเขตอำนาจรัฐตามสัญชาติของผู้กระทำความผิด โดยไม่คำนึงถึงสถานที่ที่เกิดอาชญากรรม[26] เป็นแนวคิดที่มองว่ารัฐย่อมมีเขตอำนาจรัฐเหนือบุคคลที่ถือสัญชาติของรัฐไม่ว่าบุคคลนั้นจะอยู่ที่ใดก็ตาม แม้ว่าหลักการนี้ดูเหมือนว่าจะสามารถปรับใช้ได้กับการดำเนินการบนพื้นที่ไซเบอร์ได้อย่างมีประสิทธิภาพ เพราะสามารถสันนิษฐานได้ว่าคนชาติของรัฐย่อมทราบถึงหน้าที่และสิทธิพลเมืองของตนโดยไม่กระทำการใดที่ถือเป็นความผิดตามสัญชาติของตนไม่ว่าจะอาศัยอยู่ที่ใด[27] อีกทั้งยังเป็นการรับประกันว่าแม้ความผิดจะเกิดขึ้นนอกอธิปไตยของรัฐต่าง ๆ แต่ผู้กระทำความผิดก็ผูกพันภายใต้กฎหมายของรัฐสัญชาติตน อย่างไรก็ตามการอ้างเขตอำนาจรัฐตามหลักสัญชาติถือเป็นสิ่งที่ล้าสมัยในบริบทของการก่อการร้ายทางไซเบอร์[28] เพราะเป็นการดำเนินการผ่านเครือข่ายคอมพิวเตอร์ที่ผู้กระทำความผิดสามารถปกปิดตัวตนหรือไม่ระบุตัวตนได้[29] ดังนั้นการพิสูจน์สัญชาติของผู้กระทำความผิดจึงเป็นไปได้ยาก ยิ่งไปกว่านั้นหากเป็นกรณีที่ผู้กระทำความผิดปลอมแปลงตัวตนในการดำเนินการเช่น ผู้ก่อการร้ายทางไซเบอร์ยึด botnets ในหลาย ๆ ประเทศผ่าน proxy servers[30] และหลอกให้เชื่อว่าการกระทำดังกล่าวมาจากประชาชน หรือรัฐบาลย่อมทำให้การพิสูจน์สัญชาติที่ใช้ในการอ้างเขตอำนาจรัฐตามหลักสัญชาติเกิดความผิดพลาด อีกทั้งการดำเนินคดีโดยอาศัยสัญชาติของผู้กระทำผิดเป็นฐาน ทำให้ประชาคมระหว่างประเทศจำเป็นที่จะต้องมีการจัดสรรเขตอำนาจรัฐใหม่เมื่อมีการค้นพบข้อมูลหรือแหล่งที่มาที่แท้จริงและสัญชาติของผู้กระทำความผิด เพื่อมิให้รัฐใช้เขตอำนาจของตนโดยไม่คำนึงถึงเขตอำนาจของรัฐอื่นจึงจำเป็นต้องมีการจัดสรรความสามารถระหว่างรัฐต่าง ๆ ที่อาจอ้างการใช้เขตอำนาจรัฐเหนือกรณีเดียวกัน เช่น รัฐ ก ใช้อำนาจรัฐตามหลักสัญชาติในการสืบสวนการก่อการร้ายทางไซเบอร์ที่เกิดขึ้นจากการดำเนินการโดยคนชาติของรัฐ ก แต่ผลปรากฏว่านาย ข ซึ่งเป็นคนชาติของรัฐอื่นเป็นผู้ดำเนินการโดยปลอมแปลงตัวตนเป็นนาย ก ทำให้รัฐเจ้าของสัญชาติของนาย ข เป็นรัฐที่มีสิทธิดีกว่าในการสืบสวนการกระทำความผิดที่เกิดขึ้น ด้วยเหตุนี้จึงต้องมีการจัดสรรอำนาจรัฐใหม่ให้รัฐเจ้าของสัญชาติของนาย ข เป็นรัฐที่มีอำนาจในการ

---

[26] จุมพต สายสุนทร (เชิงอรรถ 14) 255-258.

[27] Joanna Kulesza, 'Internet Governance and the Jurisdiction of States: Justification of the need for and International Regulation of Cyberspace' (GigaNet: Global Internet Governance Academic Network, 2 December 2008) < https://ssrn.com/abstract=1445452> สืบค้นเมื่อ 29 กันยายน 2564.

[28] Paul N. Stockton & Michele Golabek-Goldman (เชิงอรรถ 17) 242.

[29] Adria Allen, 'Internet Jurisdiction Today' (2001) 22 Northwestern Journal of International Law & Business 69, 87.

[30] คือ เครื่องมือใด ๆ ที่แปลการรับ-ส่งข้อมูลระหว่างเครือข่ายหรือโปรโตคอล ทำหน้าที่เสมือนประตูเข้าออกระหว่างผู้ใช้และอินเทอร์เน็ต โดยเป็นเครื่องมือที่จะให้ระดับความปลอดภัย ความเป็นส่วนตัวที่แตกต่างกันไปขึ้นอยู่กับการใช้งาน ดูประกอบ Jeff Petters, 'What is a Proxy Server and How Does it Work?' (Varonis, 7 พฤษภาคม 2564) <https://www.varonis.com/blog/what-is-a-proxy-server/> สืบค้นเมื่อ 25 พฤษภาคม 2564.

สืบสวนการกระทำความผิดที่เกิดขึ้น ซึ่งการจัดสรรเขตอำนาจรัฐใหม่นี้จะทำให้รัฐมีแรงจูงใจน้อยในการค้นหาแหล่งที่มาของการกระทำความผิดในการดำเนินคดีกับผู้ก่อการร้ายเพราะมีความเชื่อว่ารัฐอื่นอาจชิงการใช้เขตอำนาจรัฐไปได้หากพบข้อมูลใหม่ที่เกี่ยวข้องกับสัญชาติของผู้กระทำความผิด[31] นอกจากนี้การใช้เขตอำนาจรัฐตามหลักสัญชาติยังใช้ได้กับนิติบุคคลเช่นเดียวกับบุคคลธรรมดา ดังนั้นจึงเป็นปัญหาที่ต้องพิจารณาต่ออีกว่าผู้ให้บริการอินเทอร์เน็ตหรือเครือข่ายที่ถูกนำมาใช้เป็นเครื่องมือในการกระทำความผิดของผู้ก่อการร้ายจะอยู่ภายใต้หลักสัญชาติที่ต้องผูกพันตามภาระหน้าที่และการกระทำผิดเหล่านั้นหรือไม่ หากปรากฏว่ารัฐที่นิติบุคคลนั้นตั้งอยู่กำหนดให้การกระทำของการก่อการร้ายทางไซเบอร์เป็นความผิด[32]

2.4 ปัญหาการใช้เขตอำนาจรัฐตามหลักสากล (Universal Jurisdiction) กับการก่อการร้ายทางไซเบอร์

การใช้เขตอำนาจรัฐตามหลักสากลเป็นการอ้างการใช้อำนาจของรัฐเหนืออาชญากรรมที่เกิดขึ้นไม่ว่าความผิดดังกล่าวจะเกิดขึ้นที่ใด ไม่ว่าสัญชาติของผู้กระทำความผิดและเหยื่อจะเป็นสัญชาติใดก็ตาม และไม่ว่ารัฐที่อ้างใช้เขตอำนาจรัฐดังกล่าวนี้จะเกี่ยวข้องกับการกระทำความผิดดังกล่าวหรือไม่ ซึ่งจะทำให้ทุกรัฐสามารถกล่าวอ้างการใช้เขตอำนาจรัฐเหนือการกระทำผิดใด ๆ ได้ แต่การใช้เขตอำนาจรัฐตามหลักสากลจะเกี่ยวข้องกับอาชญากรรมที่ร้ายแรงอย่างมาก กล่าวคืออาชญากรรมที่เกิดขึ้นจะมีความร้ายแรงที่ถึงกับเป็นภัยต่อมนุษยชาติและทำให้สังคมระหว่างประเทศตกอยู่ในอันตราย ผู้กระทำความผิดเช่นนี้จะถือเป็นศัตรูของมนุษยชาติ ด้วยเหตุนี้จึงทำให้ทุก ๆ รัฐมีอำนาจในการบังคับคดีกับผู้กระทำความผิดในลักษณะดังกล่าว[33] การใช้เขตอำนาจรัฐตามหลักสากลจะพิจารณาถึงสถานที่ที่เกิดการกระทำผิด เนื่องจากการกระทำผิดเหล่านี้มักจะเกิดขึ้นนอกเขตอำนาจอธิปไตยของรัฐต่าง ๆ เช่น ดินแดนที่ไม่มีเจ้าของ (no man's land) หรือทะเลหลวง นอกจากนี้อาจเป็นอาชญากรรมที่เกิดขึ้นบนดินแดนของรัฐที่ล้มเหลว (failed states) ซึ่งเป็นรัฐที่ไม่มีความสามารถในการบังคับกฎหมายหรือบังคับคดีกับอาชญากรรมดังกล่าวได้อย่างมีประสิทธิภาพ แม้กระทั่งอาจเป็นอาชญากรรมที่เกิดขึ้นในรัฐที่รัฐบาลต้องการปกป้องผู้ถูกกล่าวหาจากการถูกดำเนินคดี โดยอาจดำเนินการพิจารณาโดยหลอกลวง (sham trials) ด้วยเหตุนี้การใช้เขตอำนาจรัฐตามหลักสากลจึงเป็นการป้องกันมิให้ผู้กระทำความผิดดังกล่าวสามารถหลบหนีโดยไม่ต้องรับโทษได้[34] ดังนั้นการใช้เขตอำนาจรัฐตามหลักสากลจึงเป็นการรับประกันว่าผู้กระทำความผิดจะได้รับการลงโทษ ซึ่งทำให้มีนักวิชาการบางส่วนมองว่าการปรับใช้หลักสากลกับการก่อการร้ายทางไซเบอร์เป็นแนวทางที่

[31] Paul N. Stockton & Michele Golabek-Goldman (เชิงอรรถ 17) 241-243.

[32] Abdelmonem Mohamed Magdy Khalifa, 'Overcoming the conflict of jurisdiction in cybercrime' (LL.M. Thesis The American University in Cairo) 32.

[33] OpenLearn, 'Jurisdiction' (The Open University) <https://www.open.edu/openlearn/ society-politics-law/exploring-the-boundaries-international-law/content-section-4.3.1?fbclid=IwAR0A4dhV7z03by8SC_8npmLtgtSFHAELmWXRhd4lUAWrCmXIOyc7OmSEIg> สืบค้นเมื่อ 1 มีนาคม 2564.

[34] Isidoro Blanco Cordero, 'Universal Jurisdiction' (2008) 79 International Review of Penal Law 59, 85.

เหมาะสมที่สุด[35] เนื่องจากการปรับใช้เขตอำนาจรัฐตามหลักสากลมีขอบเขตที่กว้างซึ่งสอดคล้องกับลักษณะของการปฏิบัติการของการก่อการร้ายทางไซเบอร์ที่มีความซับซ้อน จึงทำให้การใช้เขตอำนาจรัฐตามหลักสากลเป็นวิธีที่มีประสิทธิภาพที่สุดในการยับยั้งการก่อการร้ายทางไซเบอร์ เพราะก่อให้เกิดความรับผิดและเป็นการสนับสนุนความยุติธรรมและสันติภาพระหว่างประเทศ อย่างไรก็ตามการปรับใช้หลักดังกล่าวกับการก่อการร้ายทางไซเบอร์ก็เป็นที่โต้เถียงอย่างมากเนื่องจากการก่อการร้ายทางไซเบอร์มิได้ถูกกำหนดเป็นอาชญากรรมที่อยู่ภายใต้เขตอำนาจรัฐตามหลักสากล เพราะอาชญากรรมที่อยู่ภายใต้เขตอำนาจรัฐตามหลักสากลจะต้องถูกกำหนดโดยจารีตประเพณีระหว่างประเทศหรือสนธิสัญญาเท่านั้น[36] แต่ในปัจจุบันจารีตประเพณีระหว่างประเทศและสนธิสัญญาที่มีอยู่ได้กำหนดประเภทอาชญากรรมสากลครอบคลุมเฉพาะการกระทำผิดที่มีลักษณะเลวทรามตามธรรมชาติ (heinous in nature) ได้แก่ การกระทำโจรสลัด การฆ่าล้างเผ่าพันธุ์ การทรมาน อาชญากรรมสงคราม อาชญากรรมต่อมนุษยชาติ เป็นต้น ซึ่งถือเป็นความผิดที่มีความร้ายแรงถึงขนาดที่กระทบกับมโนธรรมของมนุษย์ (conscience of humanity) อันถือเป็นความผิดอาญาร้ายแรงระหว่างประเทศ[37] และแม้ว่าจะพิจารณาให้การก่อการร้ายทางไซเบอร์มีลักษณะที่เลวทรามตามธรรมชาติเช่นเดียวกับอาชญากรรมต่อมวลมนุษยชาติซึ่งทำให้สามารถใช้เขตอำนาจรัฐตามหลักสากลได้[38] แต่ก็มีปัญหาที่จะต้องกำหนดขอบเขตของภัยคุกคามให้กว้างพอที่จะครอบคลุมการใช้เขตอำนาจรัฐตามหลักสากลและแคบเพียงพอที่จะหลีกเลี่ยงมิให้มีรัฐใดใช้ประโยชน์จากการใช้เขตอำนาจรัฐเพียงเพื่อยุติความขัดแย้งในพื้นที่ออนไลน์[39] อันจะส่งผลให้การใช้เขตอำนาจตามหลักสากลเป็นการสร้างความขัดแย้งระหว่างประเทศ

เมื่อพิจารณาการก่อการร้ายทางไซเบอร์กับอาชญากรรมเหล่านี้จะเห็นได้ว่าการโจมตีของก่อการร้ายทางไซเบอร์จำนวนมากไม่ได้ก่อให้เกิดผลถึงขนาดที่เป็นความเลวทรามที่จะกระทบกับมโนธรรมของมนุษย์ ดังนั้นผลลัพธ์ของการก่อการร้ายทางไซเบอร์จึงมีน้อยมากเมื่อเทียบกับการกระทำผิดในลักษณะที่เป็นการละเมิด *jus cogens* เช่น การฆ่าล้างเผ่าพันธุ์ หรือการทรมาน และถึงแม้ว่ามีการโจมตีโดยการก่อการร้ายทางไซเบอร์ใดที่ถือว่าเป็นความเลวทรามตามธรรมชาติ แต่ก็ยังไม่เพียงพอตามกฎหมายจารีตประเพณีระหว่างประเทศและระบอบสนธิสัญญาที่จะก่อให้เกิดการใช้เขตอำนาจรัฐตามหลักสากล เพราะยังไม่ปรากฏว่ามีแนวทางของรัฐที่เชื่อว่าการป้องกันการก่อการร้ายทางไซเบอร์หรือการ

---

[35] Kelly A. Gable, 'Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and using Universal Jurisdiction as a Deterrent' (2009) 43 Vanderbilt Journal of Transnational Law 57, 118.

[36] Lee A. Steven, 'Genocide and the Duty to Extradite or Prosecute: Why the United States is in Breach of Its International Obligations' (1999) 39 Virginia Journal of International Law 425,436.

[37] สมบูรณ์ เสงี่ยมบุตร และพรชัย ด่านวิวัฒน์, *กฎหมายอาญาระหว่างประเทศ* (วิญญูชน 2555) 19.

[38] Abdelmonem Mohamed Magdy Khalifa (เชิงอรรถ 32) 39.

[39] Alexandra Perloff-Gilest, 'Transnational Cyber Offenses: Overcoming Jurisdictional Challenges' (2018) 43 The Yale Journal of International Law 191, 224-225.

โจมตีทางไซเบอร์ในรูปแบบอื่นจะเทียบเท่ากับพันธกรณีตามกฎหมายระหว่างประเทศ[40] อีกทั้งในระบอบสนธิสัญญาที่แม้ว่าจะมีอนุสัญญาระหว่างประเทศยอมรับการก่อการร้ายเป็นอาชญากรรมสากล แต่ส่วนใหญ่แล้วก็ไม่ครอบคลุมถึงการก่อการร้ายทางไซเบอร์[41] อีกทั้งอนุสัญญาว่าด้วยอาชญากรรมทางไซเบอร์ของสหภาพยุโรปที่มีการกำหนดแนวทางความร่วมมือระหว่างประเทศซึ่งครอบคลุมถึงการก่อการร้ายทางไซเบอร์ แต่ก็ไม่เพียงพอที่จะสรุปได้ว่าอนุสัญญาดังกล่าวยอมรับให้การก่อการร้ายทางไซเบอร์เป็นอาชญากรรมสากลที่จะส่งผลให้สามารถอ้างการใช้เขตอำนาจรัฐตามหลักสากลได้

**3. แนวทางการแก้ปัญหาการใช้เขตอำนาจรัฐเหนือพื้นที่ไซเบอร์ในกรณีของการก่อการร้ายทางไซเบอร์**

จากปัญหาการใช้เขตอำนาจรัฐตามหลักต่าง ๆ ดังที่ได้กล่าวมาแล้วข้างต้น แสดงให้เห็นว่าการใช้เขตอำนาจรัฐตามหลักดินแดนและหลักผู้ถูกกระทำก่อให้เกิดปัญหาการอ้างการใช้เขตอำนาจรัฐไม่มีที่สิ้นสุด เนื่องจากทำให้รัฐจำนวนมากสามารถอ้างการใช้เขตอำนาจรัฐเหนือการกระทำผิดหนึ่งที่เกิดขึ้นได้ เพราะลักษณะเฉพาะของการก่อการร้ายทางไซเบอร์ที่มิได้เกิดขึ้นบนอาณาเขตทางกายภาพปกติ อีกทั้งผลที่เกิดจากการดำเนินการก็เกิดขึ้นเป็นวงกว้างซึ่งส่งผลให้มีผู้ได้รับผลกระทบจำนวนมาก อีกทั้งลักษณะเฉพาะของการก่อการร้ายทางไซเบอร์ที่สามารถดำเนินการโดยปกปิดหรือปลอมแปลงตัวตนทำให้การสืบสวนหาผู้กระทำความผิดที่แท้จริงเพื่อที่รัฐจะใช้เขตอำนาจตามหลักสัญชาติก็เป็นไปได้ยาก นอกจากนี้การก่อการร้ายทางไซเบอร์มิได้ถูกกำหนดให้เป็นอาชญากรรมสากลอันจะทำให้รัฐสามารถใช้เขตอำนาจรัฐตามหลักสากลได้ ด้วยเหตุนี้การใช้เขตอำนาจรัฐตามหลักป้องกันจึงอาจเป็นแนวทางการแก้ไขปัญหาการใช้เขตอำนาจรัฐเหนือพื้นที่ไซเบอร์ในกรณีของการก่อการร้ายทางไซเบอร์ได้

การใช้เขตอำนาจรัฐตามหลักป้องกัน (Protective Jurisdiction) เป็นการใช้เขตอำนาจรัฐที่พิจารณาถึงผลประโยชน์และความมั่นคงของรัฐเป็นสำคัญ กล่าวคือ เป็นการใช้อำนาจของรัฐที่ครอบคลุมไปถึงอาชญากรรมใด ๆ ที่ได้กระทำขึ้นนอกดินแดนของรัฐนั้นและโดยคนชาติของรัฐอื่นที่ได้กระทำความผิดอันกระทบต่อความมั่นคง เอกภาพของดินแดน หรือความเป็นอิสระทางการเมืองของรัฐที่ได้ใช้เขตอำนาจดังกล่าว หลักป้องกันเกิดขึ้นตามพื้นฐานที่ว่ารัฐทุกรัฐต่างมีหน้าที่ในการป้องกันตัวเอง จึงเป็นหลักการที่รัฐได้มาซึ่งเขตอำนาจจากการที่ผลประโยชน์ของรัฐถูกละเมิดหรือสูญเสียไปจากการกระทำความผิด[42] โดยส่วนใหญ่แล้วหลักการนี้จะถูกใช้ในการดำเนินคดีกับความผิดที่เกี่ยวข้องกับการปลอมแปลงสกุลเงิน การปลอมแปลงเอกสารราชการซึ่งสะท้อนให้เห็นว่าเป็นความผิดที่ทุกรัฐยอมรับว่ากระทบกับความมั่นคงและผลประโยชน์ของรัฐ[43] แต่ในขณะเดียวกันการอ้างถึงความมั่นคงและผลประโยชน์แห่งรัฐอาจเปิดช่องให้รัฐเกิดการใช้อำนาจโดยมิชอบได้ เช่น ในกรณีของศาลเยอรมันที่อ้างการใช้เขตอำนาจรัฐนอกดินแดนเหนือชาวยิวต่างชาติที่

[40] Pardis Molsemzadeh Tehrani and Nazura Abdul Manap, 'A rational jurisdiction for cyber terrorism' (2013) 29 Computer Law & Security Review 689, 695.

[41] เพิ่งอ้าง 696.

[42] OpenLearn (เชิงอรรถ 33).

[43] Danielle Ireland-Piper, 'Extraterritorial Criminal Jurisdiction: Does the long arm of the law undermine the rule of law?' (2012) 13 Melbourne Journal of International Law 1, 16.

เกี่ยวข้องกับการมีเพศสัมพันธ์กับหญิงชาวเยอรมันในเชคโกสโลวาเกีย ในคดีดังกล่าวศาลได้อ้างว่าการกระทำของชาวยิวผู้นั้นเป็นอันตรายต่อความบริสุทธิ์ทางเชื้อชาติของเยอรมัน[44] ถือเป็นการกระทำที่กระทบกับอุดมการณ์ของรัฐซึ่งเป็นผลประโยชน์แห่งชาติ การอ้างผลประโยชน์แห่งชาติเช่นนี้ส่งผลให้การใช้เขตอำนาจตามหลักป้องกันเป็นที่ถกเถียงอย่างมาก อย่างไรก็ตามโดยทั่วไปแล้วการใช้เขตอำนาจดังกล่าวก็จำกัดอยู่เฉพาะความผิดบางประเภทเท่านั้น อีกทั้งความตระหนักถึงปัญหาเกี่ยวกับการก่อการร้ายก็ทำให้การใช้เขตอำนาจรัฐตามหลักป้องกันได้รับการยอมรับมากขึ้นในสังคมระหว่างประเทศ[45] นอกจากนี้ Donald Neuchterlein ได้วางหลักการพิจารณาสถานการณ์ความรุนแรงที่ถือว่ากระทบกับผลประโยชน์แห่งชาติที่สำคัญโดยพิจารณาจากเงื่อนไข 8 ประการคือ 1.ระดับของภัยอันตราย คือการพิจารณาระดับความรู้สึกว่ารัฐถูกคุกคามความมั่นคงมากเพียงใด 2.ธรรมชาติของภัยคุกคาม คือ การพิจารณาว่าเป็นการกระทำที่ถือเป็นการใช้ความรุนแรงอย่างชัดเจนหรือไม่ 3.ความเสี่ยงทางเศรษฐกิจ คือการพิจารณาผลกระทบทางเศรษฐกิจของรัฐ 4.ความผูกพันทางอารมณ์ คือการพิจารณาว่าการกระทำดังกล่าวมีอิทธิพลต่อความรู้สึกของประชาชนในรัฐมากเพียงใด 5.รูปแบบของรัฐบาล คือการพิจารณาอุดมการณ์ของรัฐในประเด็นดังกล่าวว่าจะผ่อนปรนการใช้อุดมการณ์ของรัฐเพื่อสนับสนุนความร่วมมือระหว่างประเทศ หรือเน้นการใช้อุดมการณ์ของรัฐเพื่อสนับสนุนความเป็นปึกแผ่นของรัฐ 6.ความสงบเรียบร้อยในสังคมโลก คือการพิจารณาว่าการกระทำดังกล่าวกระทบต่อความสงบเรียบร้อยของสังคมระหว่างประเทศหรือไม่ 7.ศักดิ์ศรีของรัฐ คือการพิจารณาว่าการกระทำดังกล่าวกระทบกับความน่าเชื่อถือของรัฐหรือไม่ 8.มุมมองของสังคมระหว่างประเทศที่มีต่อการกระทำดังกล่าว ซึ่งถือเป็นหนึ่งในปัจจัยสำคัญในการเมืองระหว่างประเทศในปัจจุบัน[46] จากเงื่อนไขทั้ง 8 ประการนี้ทำให้เกิดการจำกัดการอ้างใช้เขตอำนาจรัฐตามหลักป้องกันได้มากขึ้น เนื่องจากทำให้รัฐไม่สามารถอ้างเรื่องผลประโยชน์แห่งชาติที่คลุมเครือได้ กล่าวคือหากเปรียบเทียบกับกรณีของศาลเยอรมนีในตัวอย่างข้างต้นจะเห็นได้ว่า เมื่อลักษณะของการกระทำของชาวยิวไม่ถือเป็นการใช้ความรุนแรงอย่างชัดเจน ประกอบกับไม่ส่งผลกระทบต่อเศรษฐกิจของเยอรมนี อีกทั้งยังไม่กระทบต่อความสงบเรียบร้อยของสังคมระหว่างประเทศ ยิ่งไปกว่านั้นคือมุมมองของสังคมระหว่างประเทศในเรื่องดังกล่าวตรงข้ามกับอุดมการณ์ของเยอรมนี ด้วยเหตุนี้จึงทำให้เยอรมนีไม่สามารถอ้างการใช้เขตอำนาจรัฐตามหลักป้องกันเหนือการกระทำดังกล่าวได้เพราะมิใช่ภัยคุกคามที่กระทบต่อผลประโยชน์แห่งชาติ

การใช้เขตอำนาจรัฐตามหลักป้องกันถือเป็นแนวทางที่มีประสิทธิภาพที่สุดในการลดจำนวนการอ้างเขตอำนาจรัฐที่ขัดแย้งกันและช่วยบรรเทาความขัดแย้งระหว่างประเทศในกรณีของการก่อการร้ายทางไซเบอร์ได้ เนื่องจากลักษณะของอาวุธไซเบอร์ที่มีความไม่แน่นอน ทำให้การโจมตีโดยการก่อการร้ายทางไซเบอร์ที่กระทำต่อรัฐหนึ่งอาจส่งผลให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ในอีกหลาย ๆ รัฐได้ หากเป็นการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นภาวะวิสัยจะทำให้รัฐที่ได้รับความเสียหายเหล่านี้สามารถอ้างการใช้เขตอำนาจรัฐของตนเหนือการโจมตีที่เกิดขึ้นได้ แต่หากเป็นการใช้เขต

---

[44] Michael Akehurst, 'Jurisdiction in International Law' (1974) 46 British Year Book of International Law Akehurst 145, 158.

[45] Danielle Ireland-Piper, 'Accountability in Extraterritoriality: Principles, Means and Ends' (LL.M. Thesis The University of Queensland 2014) 64-65.

[46] Donald E. Nuechterlein, 'National Interests and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making' (1976) 2 British Journal of International Studies 246, 253-256.

อำนาจรัฐตามหลักป้องกันจะช่วยลดจำนวนรัฐที่สามารถอ้างการใช้เขตอำนาจรัฐเหนือการโจมตีดังกล่าวได้ เพราะความเสียหายที่เกิดขึ้นในรัฐเหล่านี้ก็ไม่รุนแรงเพียงพอที่จะเป็นการคุกคามต่อความมั่นคงหรืออธิปไตยของรัฐถึงขนาดที่จะก่อให้เกิดสิทธิการใช้เขตอำนาจรัฐตามหลักป้องกันได้ ตัวอย่างเช่น กรณีของ Stuxnet ที่มีผลทำให้เกิดการแพร่ระบาดของไวรัสคอมพิวเตอร์ไปในระบบคอมพิวเตอร์กว่า 11 ประเทศนอกเหนือจากประเทศอิหร่าน แต่ผลที่เกิดขึ้นใน 11 ประเทศนั้นก็น้อยและสามารถย้อนกลับได้[47] ซึ่งแสดงให้เห็นว่าผลกระทบที่เกิดขึ้นในประเทศเหล่านี้ไม่ได้ส่งผลในระดับที่เป็นการคุกคามความมั่นคงของรัฐ ด้วยเหตุนี้หากพิจารณาการใช้เขตอำนาจรัฐตามหลักป้องกันกับกรณีของ Stuxnet ก็จะทำให้มีเพียงประเทศอิหร่านเท่านั้นที่สามารถอ้างเขตอำนาจรัฐตามหลักนี้ได้ เนื่องจากเป็นประเทศเดียวที่ผลของการโจมตีถือเป็นการคุกคามอธิปไตยของรัฐ[48] นอกจากนี้การบังคับใช้เขตอำนาจรัฐตามหลักป้องกันจะช่วยให้รัฐมีอำนาจในการดำเนินคดีเชิงป้องกันและสามารถจับกุมผู้ก่อการร้ายทางไซเบอร์ได้ก่อนที่การโจมตีจะเกิดขึ้น เนื่องจากการอ้างเขตอำนาจรัฐตามหลักป้องกันเป็นเพียงหลักการเดียวในกฎหมายระหว่างประเทศที่ให้รัฐสามารถใช้เขตอำนาจนอกดินแดนเหนืออาชญากรรมที่ก่อให้เกิดความเสียหายอย่างรุนแรงต่อความมั่นคงของรัฐ[49] ในขณะเดียวกันการบังคับใช้เขตอำนาจรัฐตามหลักป้องกันจะช่วยกระตุ้นให้รัฐที่มีกฎหมายเกี่ยวกับการก่อการร้ายทางไซเบอร์ที่ไม่มีประสิทธิภาพรับเอาแบบอย่างของกฎหมายที่กำหนดให้การกระทำดังกล่าวเป็นอาชญากรรมไปปรับใช้ กล่าวคือหากเป็นการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัยจะทำให้ผู้ก่อการร้ายทางไซเบอร์สามารถหนีการลงโทษไปยังประเทศที่ไม่มีมาตรการทางกฎหมายเกี่ยวกับความผิดดังกล่าว ซึ่งทำให้รัฐต่าง ๆ ที่มีแนวโน้มที่จะตกเป็นเหยื่อของการก่อการร้ายทางไซเบอร์ก็จะมีแรงกระตุ้นน้อยในการผลักดันให้การกระทำดังกล่าวเป็นอาชญากรรม เช่น หากการดำเนินคดีเป็นไปตามหลักการใช้เขตอำนาจรัฐตามหลักดินแดนที่เป็นอัตวิสัย ผู้ก่อการร้ายจะตัดสินใจกระทำความผิดหรือดำเนินการในประเทศที่กฎหมายที่เกี่ยวกับความผิดในลักษณะดังกล่าวไม่เข้มงวดแทนเพื่อหลีกเลี่ยงการถูกดำเนินคดี เมื่อเป็นเช่นนี้อาจทำให้ประเทศซึ่งมักจะถูกโจมตีจากกลุ่มก่อการร้ายทางไซเบอร์ไม่มีแรงผลักดันในการกำหนดกฎหมายในเรื่องดังกล่าวให้มีประสิทธิภาพ เพราะประเทศที่ถูกโจมตีไม่สามารถอ้างการใช้เขตอำนาจรัฐเหนือการกระทำความผิดดังกล่าวได้ เป็นต้น ในทางกลับกันหากเป็นการใช้เขตอำนาจรัฐตามหลักป้องกันก็จะทำให้รัฐต่าง ๆ มีแรงกระตุ้นที่จะกำหนดให้การกระทำดังกล่าวเป็นอาชญากรรม เพราะเมื่อรัฐถูกโจมตีจากการก่อการร้ายทางไซเบอร์อันเป็นผลให้เกิดความเสียหายเป็นวงกว้าง รัฐดังกล่าวก็จะมีสิทธิตามกฎหมายในการดำเนินคดีกับผู้กระทำผิดได้หากรัฐนั้นมีการกำหนดในกฎหมายที่ถือให้การกระทำเหล่านั้นเป็นความผิดและกระทบกับผลประโยชน์แห่งชาติ ด้วยเหตุนี้การนำหลักป้องกันมาปรับใช้กับการก่อการร้ายทางไซเบอร์จะส่งผลให้การดำเนินคดีกับความผิดดังกล่าวในทางระหว่างประเทศมีความก้าวหน้ามากขึ้น อย่างไรก็ตามเนื่องจากในปัจจุบันมิได้มีแบบแผนในการดำเนินคดีกับความผิดดังกล่าวไว้อย่างชัดเจน ทำให้อาจเกิดกรณีที่การโจมตีก่อให้เกิดความเสียหายจนส่งผลในระดับที่เป็นการคุกคามความมั่นคงของรัฐมากกว่าหนึ่งรัฐ ซึ่งทำให้มีหลายรัฐที่สามารถใช้เขตอำนาจรัฐตามหลักป้องกันเหนือการโจมตีที่เกิดขึ้นได้ ดังนั้นอาจแก้ไขได้ตามแนวทางความร่วมมือของสหภาพยุโรปที่มาจากพื้นฐานความไว้วางใจซึ่งกันและกัน

[47] Mikko Hypponen, 'Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet' <http://www.wired.com/2012/06/internet-security-fail/> สืบค้นเมื่อ 12 กุมภาพันธ์ 2564.

[48] Paul N. Stockton & Michele Golabek-Goldman (เชิงอรรถ 17) 250-251.

[49] Danielle Ireland-Piper (เชิงอรรถ 43) 6.

ระหว่างรัฐสมาชิกซึ่งทำให้เกิดการยอมรับร่วมกันของคำตัดสินของศาลต่างประเทศ[50] กล่าวคือ หากระหว่างรัฐที่ใช้เขตอำนาจตามหลักป้องกันใดสามารถจับกุมตัวผู้กระทำความผิดมาลงโทษได้ รัฐอื่นที่อ้างเขตอำนาจเดียวกันก็ต้องยอมรับคำตัดสินของศาลนั้น ด้วยเหตุนี้ในทรรศนะของผู้เขียนจึงเห็นว่าประชาคมระหว่างประเทศจะต้องสร้างหลักประกันสำหรับการปรับใช้หลักป้องกันกับการก่อการร้ายทางไซเบอร์ โดยการกำหนดให้รัฐต่าง ๆ มีการประกาศใช้คำนิยามที่ก่อให้เกิดความรับผิดเกี่ยวกับการกระทำที่ถือเป็นการก่อการร้ายทางไซเบอร์ โดยให้การกระทำดังกล่าวถือเป็นความผิดที่กระทบต่อความมั่นคงและเศรษฐกิจของรัฐก่อน จึงจะเป็นหลักประกันที่ทำให้รัฐมีเขตอำนาจเหนือการกระทำดังกล่าวตามหลักป้องกัน และสร้างบรรทัดฐานในการกำหนดบทลงโทษของการกระทำความผิดดังกล่าวในสังคมระหว่างประเทศเพื่อให้ทุกรัฐต่างสามารถยอมรับคำตัดสินในความผิดเรื่องดังกล่าวได้

**บทสรุป**

การก่อการร้ายทางไซเบอร์ถือเป็นอาชญากรรมระหว่างประเทศรูปแบบใหม่ซึ่งในปัจจุบันยังไม่มีปรากฏคำนิยามและขอบเขตความผิดดังกล่าวในทางระหว่างประเทศอย่างเป็นสากล อีกทั้งการกระทำความผิดดังกล่าวที่เกิดขึ้นบนพื้นที่ไซเบอร์สามารถก่อให้เกิดผลกระทบแก่หลาย ๆ ประเทศได้ จึงหลีกเลี่ยงไม่ได้ที่จะเกิดการใช้เขตอำนาจรัฐทับซ้อนเหนือความผิดเดียวกัน ด้วยเหตุนี้เมื่อพิจารณาการใช้เขตอำนาจรัฐตามแนวคิดแบบดั้งเดิมกับการก่อการร้ายทางไซเบอร์จึงอาจก่อให้เกิดความตึงเครียดระหว่างประเทศขึ้นได้ กล่าวคือ การใช้เขตอำนาจรัฐตามหลักดินแดน ไม่ว่าจะเป็นหลักดินแดนที่เป็นอัตวิสัยหรือหลักดินแดนที่เป็นภาวะวิสัยก็จะทำให้มีรัฐจำนวนมากสามารถอ้างการใช้เขตอำนาจรัฐเหนือการกระทำความผิดเดียวกันได้ ซึ่งส่งผลให้เกิดความตึงเครียดระหว่างประเทศขึ้น แต่การนำหลักป้องกันมาปรับใช้กับการก่อการร้ายทางไซเบอร์จะลดจำนวนรัฐที่สามารถอ้างเขตอำนาจเหนือความผิดดังกล่าวได้ เพราะมิใช่ทุกรัฐที่จะได้รับความเสียหายถึงขนาดที่เป็นการคุกคามถึงผลประโยชน์ที่สำคัญของรัฐ เช่นเดียวกับการใช้เขตอำนาจรัฐตามหลักผู้ถูกกระทำ เนื่องจากการกระทำผิดดังกล่าวจะส่งผลกระทบต่อรัฐจำนวนมาก ซึ่งทำให้รัฐเหล่านั้นสามารถอ้างการใช้เขตอำนาจรัฐเหนือการกระทำความผิดดังกล่าวได้ เพราะหลักผู้ถูกกระทำมิได้คำนึงว่าผลกระทบที่ได้รับจะมากน้อยเพียงใด คำนึงถึงเพียงว่าได้รับผลกระทบหรือผลการกระทำความผิดเกิดขึ้นในรัฐที่กล่าวอ้างการใช้เขตอำนาจเช่นว่านั้นก็เพียงพอแล้ว แต่หากเป็นการใช้เขตอำนาจตามหลักป้องกันจะคำนึงถึงผลกระทบต่อผลประโยชน์แห่งชาติของรัฐที่สำคัญเท่านั้น ซึ่งทำให้ลดจำนวนของรัฐที่สามารถใช้เขตอำนาจเหนือการกระทำความผิดดังกล่าวได้ ในขณะที่การใช้เขตอำนาจรัฐตามหลักสัญชาติไม่ส่งเสริมให้เกิดความร่วมมือระหว่างประเทศในการดำเนินคดีกับการกระทำความผิดที่เกิดขึ้น เพราะเป็นหลักการที่ทำให้รัฐเชื่อว่าอาจทำให้รัฐถูกช่วงชิงการใช้เขตอำนาจรัฐไปได้ ซึ่งจะส่งผลให้การดำเนินคดีกับการก่อการร้ายทางไซเบอร์เป็นไปได้ยาก แต่การใช้หลักป้องกันจะทำให้ทุกรัฐพยายามกำหนดขอบเขตความผิดและการดำเนินคดีกับความผิดดังกล่าวมากขึ้น เพื่อให้รัฐของตนสามารถใช้สิทธิในการป้องกันตนเองจากการกระทำที่ถือว่าเป็นการละเมิดต่อความมั่นคงและผลประโยชน์

[50] Pedro Caeiro, 'Jurisdiction in criminal matters in the EU: negative and positive conflicts, and beyond' (2010) 4 Nomos Verlagsgesellschaft mbH 366, 375.

แห่งชาติได้ ซึ่งจะช่วยส่งเสริมให้เกิดการดำเนินคดีกับการก่อการร้ายทางไซเบอร์ในทางระหว่างประเทศมากขึ้น ประกอบกับหลักป้องกันมิได้คำนึงถึงสัญชาติของผู้กระทำผิด ดังนั้นไม่ว่าผู้กระทำความผิดจะปลอมแปลงตัวตนบนพื้นที่ไซเบอร์อย่างไร ก็มิได้ทำให้รัฐที่อ้างการใช้เขตอำนาจตามหลักป้องกันเสียสิทธิในการดำเนินคดีกับความผิดดังกล่าวแต่อย่างใด นอกจากนี้การใช้เขตอำนาจรัฐตามหลักสากลกับการก่อการร้ายทางไซเบอร์ก็เป็นแนวทางที่ไม่เหมาะสมนักเนื่องจากความผิดดังกล่าวยังมิได้ถูกยอมรับว่าเป็นอาชญากรรมสากลที่จะถือว่าเป็นพันธกรณีของรัฐต่าง ๆ ในการใช้เขตอำนาจรัฐเหนือการกระทำความผิดนี้ แต่ในขณะที่การใช้เขตอำนาจรัฐตามหลักป้องกันมิได้คำนึงว่าความผิดดังกล่าวถือเป็นอาชญากรรมสากลหรือไม่ พิจารณาเพียงว่าการกระทำดังกล่าวก่อให้เกิดความเสียหายถึงขนาดที่เป็นการคุกคามต่อผลประโยชน์แห่งชาติและความมั่นคงของรัฐหรือไม่เท่านั้น ดังนั้นจึงทำให้เกิดความเป็นไปได้มากกว่าในการดำเนินคดีกับการก่อการร้ายทางไซเบอร์ ด้วยเหตุนี้จากผลการศึกษาทั้งหมดจะพบว่าการปรับใช้เขตอำนาจรัฐตามหลักป้องกันเหนือการก่อการร้ายทางไซเบอร์ถือเป็นแนวทางที่มีประสิทธิภาพที่สุด เพราะนอกจากจะช่วยลดจำนวนรัฐที่สามารถอ้างการใช้เขตอำนาจรัฐเหนือการกระทำความผิดที่เกิดขึ้นได้แล้ว ยังสามารถกระตุ้นให้รัฐต่าง ๆ ปรับปรุงกฎหมายภายในของรัฐตนที่เกี่ยวข้องกับความผิดดังกล่าวให้มีความชัดเจนและมีประสิทธิภาพมากยิ่งขึ้น เนื่องจากการกำหนดความผิดเกี่ยวกับการก่อการร้ายทางไซเบอร์ว่าเป็นภัยคุกคามความมั่นคงของรัฐจะเปิดโอกาสให้รัฐสามารถใช้เขตอำนาจของรัฐตามหลักป้องกันได้และลดการเกิด forum shopping เพราะเมื่อทุกรัฐต่างกำหนดความผิดดังกล่าวไว้ในมาตรฐานเดียวกัน ไม่ว่าผู้ก่อการร้ายจะดำเนินการดังกล่าวจากรัฐใด ก็ไม่อาจหลีกเลี่ยงการถูกดำเนินคดีได้ อีกทั้งการใช้หลักป้องกันจะทำให้เกิดความเป็นไปได้ในการนิยามและกำหนดแนวทางการจัดการกับการก่อการร้ายทางไซเบอร์ที่เป็นสากลมากยิ่งขึ้น อย่างไรก็ตามเนื่องจากในปัจจุบันมิได้มีกำหนดแนวทางการดำเนินคดีกับผู้ก่อการร้ายทางไซเบอร์อย่างชัดเจน ดังนั้นในความคิดเห็นของผู้เขียนจึงมองว่าควรกำหนดนิยามและขอบเขตของการก่อการร้ายทางไซเบอร์ให้มีความชัดเจนในกฎหมายภายในและกำหนดให้การกระทำเช่นว่านั้นถือเป็นการกระทำที่กระทบต่อความมั่นคงของรัฐหรือความมั่นคงทางเศรษฐกิจของรัฐอย่างร้ายแรง เพื่อที่จะช่วยส่งเสริมให้รัฐสามารถบังคับใช้อำนาจรัฐเหนือการกระทำผิดดังกล่าวอย่างมีประสิทธิภาพ เนื่องจากการใช้เขตอำนาจรัฐตามหลักป้องกันจะเปิดโอกาสให้รัฐสามารถใช้เขตอำนาจนอกดินแดนเหนืออาชญากรรมที่ก่อให้เกิดความเสียหายอย่างรุนแรงต่อความมั่นคงของรัฐได้ แต่การกระทำดังกล่าวจะต้องถูกกำหนดว่าเป็นความผิดที่มุ่งต่อความมั่นคงของรัฐหรือความมั่นคงทางเศรษฐกิจของรัฐเท่านั้น

สำหรับประเทศไทยแม้จะมีการกำหนดความผิดที่ได้กระทำบนพื้นที่ไซเบอร์ไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 แต่เนื่องจากประเทศไทยมิได้มีอธิปไตยบนพื้นที่ไซเบอร์[51] เนื่องจากคนไทยใช้ platform จากต่างประเทศ ดังนั้นเมื่อผู้ก่อการร้ายดำเนินการโจมตีผ่าน platform ต่างประเทศเหล่านั้นมายังประเทศไทย จึงทำให้รัฐเจ้าของ platform เป็นรัฐผู้มีเขตอำนาจเหนือการกระทำดังกล่าว ซึ่งการขาดอธิปไตยบนพื้นที่ไซเบอร์ยังส่งผลให้การบังคับใช้เขตอำนาจรัฐตามหลักสัญชาติเป็นไปได้ยาก เพราะในปัจจุบันไม่สามารถตรวจสอบ IP Address ที่อยู่ใน

[51] ปริญญา หอมเอนก,ประธานกรรมการบริหาร บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด, ‘RoLD Virtual Forum : Living with COVID-19 ตอน ภัยคุกคามไซเบอร์ ชีวิต(ไม่)ปกติใหม่ ยุคโควิด-19’ (เสวนา,สถาบันเพื่อการยุติธรรมแห่งประเทศไทย, 18 มิถุนายน 2563) <https://www.moj.go.th/view/45017> สืบค้นเมื่อ 2 ตุลาคม 2564.

ต่างประเทศได้เนื่องจากผู้ให้บริการปิดกั้นมิให้มีการตรวจสอบข้อมูลเหล่านั้น[52] ดังนั้นจึงไม่สามารถรวบรวมพยานหลักฐานเพื่อนำไปสู่การพิสูจน์สัญชาติของผู้กระทำความผิดที่จะนำไปสู่การอ้างเขตอำนาจรัฐตามหลักสัญชาติได้ ด้วยเหตุนี้ประเทศไทยจึงควรใช้เขตอำนาจรัฐตามหลักป้องกันเหนือการโจมตีบนพื้นที่ไซเบอร์ที่เกิดจากการก่อการร้ายทางไซเบอร์ เนื่องจากประเทศไทยได้กำหนดการกระทำความผิดบางประการซึ่งกระทำนอกราชญอาณาจักรแต่ต้องรับโทษในราชอาณาจักรไว้ในมาตรา 7 แห่งประมวลกฎหมายอาญา โดยระบุถึงความผิดเกี่ยวกับการก่อการร้ายในมาตรา 135/1 ถึงมาตรา 135/4 ซึ่งเมื่อวิเคราะห์แล้วจะเห็นได้ว่าการก่อการร้ายทางไซเบอร์ถือเป็นการกระทำความผิดอาญาซึ่งแม้จะกระทำนอกราชอาณาจักรแต่ต้องรับโทษในราชอาณาจักรได้ในกรณีที่การก่อการร้ายทางไซเบอร์นั้นเป็น “การกระทำการใดอันก่อให้เกิดความเสียหายอย่างร้ายแรงแก่ระบบการขนส่งสาธารณะ ระบบโทรคมนาคม หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ”[53] หรือเป็น “การกระทำการใดอันก่อให้เกิดความเสียหายแก่ทรัพย์สินของรัฐหนึ่งรัฐใด หรือของบุคคลใด หรือต่อสิ่งแวดล้อม อันก่อให้เกิดหรือน่าจะก่อให้เกิดความเสียหายทางเศรษฐกิจอย่างสำคัญ”[54] ดังนั้นแม้ว่าประเทศไทยจะมิได้นิยามความหมายของการก่อการร้ายทางไซเบอร์ไว้โดยตรง แต่หากผลของการกระทำดังกล่าวก่อให้เกิดผลในลักษณะที่กระทบต่อความมั่นคงของรัฐหรือเศรษฐกิจของรัฐแล้ว รัฐไทยก็สามารถใช้เขตอำนาจรัฐตามหลักป้องกันเหนือการกระทำความผิดดังกล่าวได้

[52] พงศ์พจน์ ธรรมากุลวิชช์, ‘ฉ้อโกง ขายของทางออนไลน์’ (เสวนา, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 20 ธันวาคม 2562) <https://www.law.tu.ac.th/summary-seminar-online-fraudulent/> สืบค้นเมื่อ 2 ตุลาคม 2564.

[53] ประมวลกฎหมายอาญามาตรา 135/1 (2).

[54] ประมวลกฎหมายอาญามาตรา 135/1 (3).

**บรรณานุกรม**

**หนังสือ**

**ภาษาไทย**

จุมพต สายสุนทร, *กฎหมายระหว่างประเทศเล่ม 1* (พิมพ์ครั้งที่ 5, วิญญูชน, 2547).

สมบูรณ์ เสงี่ยมบุตร และพรชัย ด่านวิวัฒน์, *กฎหมายอาญาระหว่างประเทศ* (วิญญูชน 2555).

**ภาษาต่างประเทศ**

Malcolm N. Shaw, *International law* (Cambridge: Grotius Publications Limited, 1991).

**บทความวารสาร**

Adria Allen, 'Internet Jurisdiction Today' (2001) 22 Northwestern Journal of International Law & Business 69.

Alexandra Perloff-Gilest, 'Transnational Cyber Offenses: Overcoming Jurisdictional Challenges' (2018) 43 The Yale Journal of International Law 191.

Anna C. Mourlam, 'Unarmed Attacks: Cyber Combatants and the Right to Defend' (2018) 26 The California International Law Journal 19.

Brian K. Houghton & Jonathan M. Schachter, 'Coordinated Terrorist Attacks: Implications for Local Responders' (2005) 74 FBI Law enforcement Bulletin 11.

Danielle Ireland-Piper, 'Extraterritorial Criminal Jurisdiction: Does the long arm of the law undermine the rule of law?' (2012) 13 Melbourne Journal of International Law 1.

Donald E. Nuechterlein, 'National Interests and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making' (1976) 2 British Journal of International Studies 246.

Geoffrey R. Watson, 'The Passive Personality Principle' (1993) 28 Texas International Law Journal 1.

Isidoro Blanco Cordero, 'Universal Jurisdiction' (2008) 79 International Review of Penal Law 59.

Jan-Peter Ewert and David Weslow, 'Forum Shopping in Europe and the United States' (2011) 9 International Trademark Association Bulletin 9.

Kelly A. Gable, 'Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and using Universal Jurisdiction as a Deterrent' (2009) 43 Vanderbilt Journal of Transnational Law 57.

Laura Mayer Lux, 'Defining cyberterrorism' (2018) 7 Revista Chilena De Derecho Y Tecnologia 5.

Lee A. Steven, 'Genocide and the Duty to Extradite or Prosecute: Why the United States is in Breach of Its International Obligations' (1999) 39 Virginia Journal of International Law 425.

Michael Akehurst, 'Jurisdiction in International Law' (1974) 46 British Year Book of International Law Akehurst 145.

Mohammad Iqbal, 'Defining Cyberterrorism' (2004) 12 Journal of Computer & Information Law 397.

Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 4 California Law Review 817.

Pardis Molsemzadeh Tehrani and Nazura Abdul Manap, 'A rational jurisdiction for cyber terrorism' (2013) 29 Computer Law & Security Review 689.

Paul N. Stockton & Michele Golabek-Goldman, 'Prosecuting Cyberterrorists: Applying Traditional Jurisdiction Frameworks to a Modern Threat' (2014) 25 Stanford Law & Policy Review 211.

Pedro Caeiro, 'Jurisdiction in criminal matters in the EU: negative and positive conflicts, and beyond' (2010) 4 Nomos Verlagsgesellschaft mbH.

**วิทยานิพนธ์**

**ภาษาไทย**

เขมชาติ ธีรพงษ์, 'ปัญหากฎหมายและแนวทางแก้ไขปัญหาอันเกิดจากการประกอบกิจกรรมบนเครือข่ายอิเล็กทรอนิกส์ : ปัญหาการใช้เขตอำนาจรัฐ และปัญหาที่สืบเนื่องมาจากความไม่เพียงพอของกฎหมายที่มีอยู่ในปัจจุบัน' (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2543).

**ภาษาต่างประเทศ**

Abdelmonem Mohamed Magdy Khalifa, 'Overcoming the conflict of jurisdiction in cybercrime' (LL.M. Thesis The American University in Cairo) 32.

Danielle Ireland-Piper, 'Accountability in Extraterritoriality: Principles, Means and Ends' (LL.M. Thesis The University of Queensland 2014) 64-65.

**รายงานภาษาต่างประเทศ**

Gabriel Weimann, 'Cyberterrorism: How Real Is the Threat?' (Submitted to United States Institute of Peace, December 2004) 6.

**สื่ออิเล็กทรอนิกส์**

Alex Perekalin, 'WannaCry: Are you safe?' (Kaspersky Daily, 13 May 2017) <https://www.kaspersky.com/blog/wannacry-ransomware/16518/> สืบค้นเมื่อ 26 กันยายน 2564.

Cristos Velasco, Julia Hörnle and Anna-Maria Osula, 'Global Views on Internet Jurisdiction and Trans-Border Access' (2016) < https://rm.coe.int/16806b8a7c> สืบค้นเมื่อ 26 กันยายน 2564.

Dorothy E. Denning, 'Cyberterrorism' (Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representative, 23 May 2000) <https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm?fbclid=IwAR0fwDSjm35f2WjzmfMTHaOBxqTsp6vJ9vapr_6E82YQ_MRKP-Bd1KAV3qA> สืบค้นเมื่อ 26 กุมภาพันธ์ 2564.

Joanna Kulesza, 'Internet Governance and the Jurisdiction of States: Justification of the need for and International Regulation of Cyberspace' (GigaNet: Global Internet Governance Academic Network, 2 December 2008) < https://ssrn.com/abstract=1445452> สืบค้นเมื่อ 29 กันยายน 2564.

Mikko Hypponen, 'Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet' <http://www.wired.com/2012/06/internet-security-fail/> สืบค้นเมื่อ 12 กุมภาพันธ์ 2564.

OpenLearn, 'Jurisdiction' (The Open University) <https://www.open.edu/openlearn/ society-politics-law/exploring-the-boundaries-international-law/content-section-4.3.1?fbclid=IwAR0A4dhV-7z03by8SC_8npmLtgtSFHAELmWXRhd4lUAWrCmXIOyc7OmSEIg> สืบค้นเมื่อ 1 มีนาคม 2564.

Sanjana Sahu, 'Passive Personality Principle: An Overview' (Academike) <http://www.lawctopus.com/academike/passive-personality-principle-overview/> สืบค้นเมื่อ 27 มิถุนายน 2564.