รายงานสถานการณ์ปิดกั้นอินเทอร์เน็ตของ iMAP ปี 2565

ประเทศไทย

โดย Siti Nurliza Samsudin (โครงการ Sinar), Kelly Koh (โครงการ Sinar) และเครือข่ายพลเมืองเน็ต

แปลจาก iMAP State of Internet Censorship Report 2022 – Thailand
ต้นฉบับ https://ooni.org/post/2022-state-of-internet-censorship-thailand/

ตีพิมพ์/ผลิตโดย Sinar Project
team@sinarproject.org
https://sinarproject.org

แปลโดย เครือข่ายพลเมืองเน็ต

เกี่ยวกับ iMAP

โครงการปฏิบัติการเฝ้าระวังอินเทอร์เน็ต (Internet Monitoring Action Project หรือ iMAP) มีเป้าหมายเพื่อสร้างเครือข่ายระดับภูมิภาคและภายในประเทศเพื่อตรวจสอบการแทรกแซงรบกวนเครือข่ายและการจำกัดเสรีภาพในการแสดงออกทางออนไลน์ใน 9 ประเทศและดินแดน ได้แก่ กัมพูชา ไทย ฟิลิปปินส์ มาเลเซีย เมียนมา เวียดนาม อินเดีย อินโดนีเซีย และฮ่องกง โครงการ Sinar ทำงานร่วมกับพันธมิตรด้านสิทธิดิจิทัลระดับประเทศใน 9 ประเทศนี้ โครงการนี้ดำเนินการผ่านระบบตรวจจับและรายงานของ “โครงการเปิดเพื่อตรวจจับการแทรกแซงเครือข่าย” (Open Observatory Network Interference - OONI) ซึ่งเกี่ยวข้องกับการบำรุงรักษารายการทดสอบและการตรวจวัด

ดูข้อมูลเพิ่มเติมได้ที่ https://imap.sinarproject.org/ สอบถามและเสนอแนะเกี่ยวกับรายงานนี้ได้ที่ team@sinarproject.org

เกี่ยวกับโครงการซีนาร์

โครงการ Sinar เป็นความริเริ่มด้านเทคโนโลยีของพลเมืองโดยใช้เทคโนโลยีเปิด ข้อมูลเปิด และการวิเคราะห์นโยบาย เพื่อทำให้ข้อมูลสำคัญเป็นสาธารณะอย่างเป็นระบบและเข้าถึงได้มากขึ้นสำหรับชาวมาเลเซีย โดยมีจุดมุ่งหมายเพื่อปรับปรุงธรรมาภิบาลและกระตุ้นให้ประชาชนมีส่วนร่วมในกิจการสาธารณะของประเทศมากขึ้น โดยทำให้รัฐสภาและรัฐบาลมาเลเซียเปิดกว้าง โปร่งใส และมีความรับผิดชอบมากขึ้น ดูข้อมูลเพิ่มเติมได้ที่: https://sinarproject.org

เกี่ยวกับเครือข่ายพลเมืองเน็ต

เครือข่ายพลเมืองเน็ต (Thai Netizen Network) เป็นกลุ่มพลเมืองที่รวมตัวกันเพื่อสนับสนุนสิทธิพลเมืองออนไลน์ บนหลักพื้นฐาน 5 ประการ ได้แก่ สิทธิในการเข้าถึงข้อมูล, สิทธิในการคิดและการแสดงออก, สิทธิในความเป็นส่วนตัว, สิทธิในการร่วมออกแบบนโยบาย และสิทธิในการเป็นเจ้าของและใช้ทรัพยากร โดยดำเนินกิจกรรมติดตามประเด็นเทคโนโลยีและการสื่อสารที่เกี่ยวกับสิทธิมนุษยชน วิจัยเชิงนโยบายและรณรงค์ขับเคลื่อนบนฐานงานวิจัย และพัฒนาทักษะผู้ใช้เน็ตและสื่อพลเมือง เครือข่ายพลเมืองเน็ตดำเนินงานภายใต้มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง (Foundation for Internet and Civic Culture) ดูข้อมูลเพิ่มเติมได้ที่: https://thainetizen.org

ประเทศไทยเป็นประเทศที่ตั้งอยู่บนภาคพื้นทวีปของเอเชียตะวันออกเฉียงใต้ อยู่ภายใต้การปกครองของรัฐบาลทหารเป็นเวลาห้าปีตั้งแต่ปี 2557 ถึง 2562 จนถึงการเลือกตั้งทั่วไปในปี 2562 ประเทศนี้ถูกปกครองโดยระบอบราชาธิปไตยภายใต้รัฐธรรมนูญที่ใช้ระบบรัฐสภาแต่เพียงในนาม และประมวลกฎหมายอาญามาตรา 112 (กฎหมายหมิ่นพระบรมเดชานุภาพ) ยังคงถูกใช้อย่างต่อเนื่อง โดยเฉพาะเมื่อเกี่ยวกับการปิดกั้นอินเทอร์เน็ต ในสถานการณ์การแพร่ระบาดของโควิด-19 รัฐบาลไทยได้นำข้อกำหนดที่ออกตามความในมาตรา 9 แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (ฉบับที่ 29) มาบังคับใช้เพื่อควบคุมข่าวปลอม ซึ่งนำไปสู่การรายงานการปิดกั้นอินเทอร์เน็ต

รายงานนี้มีวัตถุประสงค์เพื่อแสดงให้เห็นสถานการณ์ของการปิดกั้นอินเทอร์เน็ตในประเทศไทย โดยอ้างอิงจากเหตุการณ์ที่ถูกรายงานเหล่านี้ ตลอดจนข้อมูลตรวจวัดของ OONI ที่รวบรวมได้ในช่วงครึ่งแรกของปี 2565

สารบัญ

การค้นพบที่สำคัญ 7

บทนำ 8

ภูมิหลัง 9

ภูมิทัศน์ทางการเมือง 9

สภาพแวดล้อมทางกฎหมาย 10

เสรีภาพในการแสดงออก 10

ประมวลกฎหมายอาญา มาตรา 112 (หมิ่นพระบรมเดชานุภาพ) 10

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 10

พ.ร.บ.การรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2551 11

เสรีภาพสื่อมวลชน 11

คำสั่ง คสช. ที่ 97/2557 11

คำสั่งหัวหน้า คสช. ที่ 3/2558 ข้อ 5 11

กำหนดออกตามความในมาตรา 9 แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (ฉบับที่ 29) 12

การเข้าถึงข้อมูล 12

พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540 12

ความเป็นส่วนตัว 13

รัฐธรรมนูญแห่งราชอาณาจักรไทย 13

การปิดกั้นและการเฝ้าสอดส่อง 14

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 20 14

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 14

รายงานการปิดกั้นอินเทอร์เน็ต 14

การประท้วงในปี 2563-2564 14

ภูมิทัศน์เครือข่ายและการเข้าถึงอินเทอร์เน็ต 17

ข้อค้นพบเกี่ยวกับการปิดกั้นอินเทอร์เน็ตในประเทศไทย 19

การปิดกั้นเว็บไซต์ 19

เครื่องมือนิรนามและเครื่องมือหลบเลี่ยง 21

การพนัน 22

ประเด็นสิทธิมนุษยชน 24
สื่อเชิงข่าว 26
สื่ออนาจาร 27
เว็บไซต์ที่น่าสนใจ 29
Change.org 29
No112.org 31
การปิดกั้นแอปพลิเคชันส่งข้อความ 34
การปิดกั้นเครื่องมือหลบเลี่ยง 34

ข้อจำกัดของผลการศึกษา 34

บทสรุป 34
การมีส่วนร่วมในการศึกษา 35

กิตติกรรมประกาศ 35

ภาคผนวก 1: อภิธานศัพท์ 36

ภาคผนวก 2: วิธีการ 39
ข้อมูล 39
ขอบเขตการศึกษา 39
ข้อมูลตรวจวัดเครือข่ายถูกรวบรวมอย่างไร? 39
ข้อมูลตรวจวัดเครือข่ายถูกวิเคราะห์อย่างไร? 40
รหัสประเทศ 40
หมายเลขระบบอิสระ (Autonomous System Number - ASN) 40
วันที่และเวลาตรวจวัด 40
หมวดหมู่ 41
ที่อยู่ IP และข้อมูลอื่น ๆ 45
ข้อมูลตรวจวัดเครือข่าย 45
ข้อมูลตรวจวัดที่ได้ยืนยัน เทียบกับ ฮิวริสติก 48

การค้นพบที่สำคัญ

- มีการรายงานเหตุการณ์การปิดกั้นอินเทอร์เน็ตหลายครั้งระหว่างการประท้วงในปี 2563 - 2564 ในประเทศไทย โดยเฉพาะอย่างยิ่งภายใต้ข้อกำหนดที่ออกตามความในมาตรา 9 แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (ฉบับที่ 29) ซึ่งอ้างว่ามีขึ้นเพื่อแก้ไขปัญหา “ข่าวปลอม” ที่เกี่ยวข้องกับการแพร่ระบาดของโรคโควิด-19
- ในช่วงหกเดือนตั้งแต่เดือนมกราคมถึงมิถุนายน 2565 มีการบันทึกข้อมูลตรวจวัด 3,129,067 ครั้ง ในการทดสอบการเชื่อมต่อเว็บของ OONI จากจุดสำรวจ 30 จุด จากทั้งหมดนี้พบว่าร้อยละ 95.8 (2,996,695) เป็นปกติ ร้อยละ 3.1 (96,626) ผิดปกติ ร้อยละ 0.3 (8,982) ได้รับการยืนยันการปิดกั้น และร้อยละ 0.9 (26,664) เป็นการตรวจวัดที่ล้มเหลว
- รายการโดเมนที่ถูกปิดกั้นที่ได้รับการยืนยันของ OONI มี 76 โดเมนจากหมวดหมู่ต่าง ๆ ในขณะที่การวิเคราะห์เพิ่มเติมโดยฮิวริสติกได้เพิ่ม 43 โดเมนลงในรายการ รวมเป็น 119 โดเมนที่ได้รับการยืนยันการปิดกั้น เมื่อเปรียบเทียบกันแล้ว รายงานปี 2560 พบว่ามี 13 เว็บไซต์ที่ถูกปิดกั้น
- ในรายการข้างต้น หมวดหมู่ที่มีโดเมนมากกว่า 10 โดเมน ได้แก่ เครื่องมือจัดทำข้อมูลนิรนามและเครื่องมือการหลบเลี่ยง การพนัน ประเด็นสิทธิมนุษยชน ข่าวสาร และสื่ออนาจาร

บทนำ

ตามรายงานฉบับก่อนซึ่งใช้ข้อมูลของ OONI ในปี 2560 นั้น การปิดกั้นอินเทอร์เน็ตในประเทศไทยมีสาเหตุหลักมาจากความมั่นคงแห่งชาติ รายงานดังกล่าวเน้นว่า URL 10,000 รายการถูกปิดกั้นในปี 2553 รวมถึงเว็บไซต์ 56 แห่งถูกปิดกั้นระหว่างเดือนพฤษภาคมถึงมิถุนายน 2557 ระหว่างการรัฐประหาร

ในฐานะที่เป็นส่วนหนึ่งของโครงการปฏิบัติการเฝ้าระวังอินเทอร์เน็ต (Internet Monitoring Action Project หรือ iMAP) ซึ่งส่งเสริมและปกป้องเสรีภาพทางอินเทอร์เน็ตในเอเชียใต้และเอเชียตะวันออกเฉียงใต้ รายงานนี้มุ่งที่จะรายงานเกี่ยวกับการเฝ้าระวังการแทรกแซงรบกวนเครือข่ายและการจำกัดเสรีภาพในการแสดงออกทางออนไลน์ โดยแบ่งออกเป็นส่วนต่าง ๆ ดังต่อไปนี้: ข้อมูลภูมิหลังของภูมิทัศน์ทางการเมือง สภาพแวดล้อมทางกฎหมาย และรายงานกรณีการปิดกั้นอินเทอร์เน็ต ตลอดจนภาพรวมของเครือข่ายและการเข้าถึงของอินเทอร์เน็ต ตามด้วยผลสำรวจการปิดกั้นอินเทอร์เน็ตในประเทศไทย การยอมรับข้อจำกัด ข้อสรุป และกิตติกรรมประกาศ

ภูมิหลัง

ประเทศไทย มีชื่ออย่างเป็นทางการว่าราชอาณาจักรไทย ตั้งอยู่ใจกลางเอเชียตะวันออกเฉียงใต้ภาคพื้นทวีป มีประชากรมากกว่า 71 ล้านคน ทิศเหนือติดกับเมียนมาและ สปป.ลาว ทิศตะวันออกติดกับ สปป.ลาว และกัมพูชา ทิศใต้ติดกับอ่าวไทยและมาเลเซีย และทิศตะวันตกติดกับทะเลอันดามัน ประเทศนี้ประกอบด้วยชาวไทยร้อยละ 75 ชาวไทยเชื้อสายจีนร้อยละ 14 และชาวมาเลย์ร้อยละ 3 ภาษาราชการคือภาษาไทย โดยกว่าร้อยละ 90 ของประชากรใช้ภาษานี้ทุกวัน ข้อมูลสำมะโนประชากรประมาณการว่าร้อยละ 93 ของประชากรนับถือศาสนาพุทธ ในขณะที่ร้อยละ 5 นับถือศาสนาอิสลาม และที่เหลือนับถือศาสนาคริสต์ (ร้อยละ 1) และอื่นๆ (น้อยละกว่าร้อยละ 1) นอกจากนี้ ร้อยละ 51 ของประชากรอาศัยอยู่ในเขตเมือง

ตามภาพรวมของธนาคารโลก ในช่วงสี่ทศวรรษที่ผ่านมาประเทศได้ขยับสถานะจากประเทศรายได้ต่ำขึ้นสู่สถานะประเทศรายได้ปานกลางระดับสูง ซึ่งเป็นผลมาจากโครงสร้างเศรษฐกิจที่เน้นการส่งออก อย่างไรก็ตาม ผลผลิตและรายได้ชบเซาตั้งแต่ปี 2558 เนื่องจากความวุ่นวายทางการเมืองภายในประเทศ ตามมาด้วยรายได้ที่หดตัวมากที่สุดในช่วงที่มีโรคโควิด-19 โดย ผลิตภัณฑ์มวลรวมในประเทศลดลงร้อยละ 6.1 ในปี 2563 ในปี 2564 เศรษฐกิจเติบโตร้อยละ 1.6 ตลอดทั้งปี แม้จะประสบปัญหาการระบาดอีกระลอกของโรคโควิด-19 ในช่วงเวลาเดียวกัน อัตราความยากจนล่าสุดอยู่ที่ร้อยละ 6.8 ในปี 2563

ภูมิทัศน์ทางการเมือง

ในด้านการเมือง ในปี 2562 ประเทศไทยเปลี่ยนผ่านไปสู่รัฐบาลกึ่งทหารที่มีการเลือกตั้ง หลังจากการปกครองแบบเผด็จการทหารเป็นเวลาห้าปี พระมหากษัตริย์เป็นพระประมุขแห่งรัฐ นายกรัฐมนตรีเป็นหัวหน้าฝ่ายบริหาร ซึ่งมาจากการเลือกของสมาชิกรัฐสภาทั้งสองสภา (สภาผู้แทนราษฎรและวุฒิสภา) รัฐธรรมนูญฉบับปัจจุบันประกาศใช้ในปี 2560 โดยรัฐสภาเป็นแบบสองสภา ประกอบด้วยวุฒิสภาและสภาผู้แทนราษฎร รัฐสภายังสามารถเลือกบุคคลที่ไม่ใช่สมาชิกสภาหรือนักการเมืองเป็นนายกรัฐมนตรี ซึ่งนักวิจารณ์มองว่าวิธีนี้ช่วยให้กองทัพควบคุมรัฐบาลได้อย่างมีประสิทธิภาพ โดยไม่ต้องคำนึงถึงผลการเลือกตั้ง

จากรายงานประเทศไทยประจำปี 2565 โดย Freedom House ประเทศไทยถูกจัดอยู่ในประเภท “ไม่เสรี” ด้วยคะแนน 29 เกิน 100 ความเสื่อมโทรมของประชาธิปไตยและความไม่พอใจนำไปสู่การเดินขบวนประท้วงครั้งใหญ่ ซึ่งตามมาด้วยระบอบการปกครองที่ใช้กลยุทธ์เผด็จการ รวมถึงการจับกุมตามอำเภอใจ การข่มขู่ การฟ้องร้องคดีหมิ่นพระบรมเดชานุภาพ และคุกคามนักกิจกรรม การจำกัดเสรีภาพสื่อ การไม่เคารพกระบวนการอันควรตามกฎหมาย และการลอยนวลพ้นผิดของอาชญากรรมที่กระทำต่อนัก

เคลื่อนไหว นอกจากนี้ ประเทศไทยได้คะแนน 36/100 ในด้านเสรีภาพทางอินเทอร์เน็ต ในปี 2564 รัฐบาลได้ประกาศใช้ข้อกำหนดที่ออกตามความในมาตรา 9 แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (ฉบับที่ 29) ซึ่งห้ามการพูดที่จะ “ยุยงให้เกิดความกลัว” ข้อบังคับดังกล่าวยังกำหนดให้ผู้ให้บริการอินเทอร์เน็ตต้องยอมมอบที่อยู่โปรโตคอลอินเทอร์เน็ตของผู้ใช้ที่มีส่วนร่วมในการแสดงออกดังกล่าวให้แก่เจ้าหน้าที่ อย่างไรก็ดี ในเดือนสิงหาคม 2564 ศาลแพ่งระงับการใช้ข้อบังคับข้างต้นตามคำร้องของนักเคลื่อนไหวและสื่อต่าง ๆ

สภาพแวดล้อมทางกฎหมาย

เสรีภาพในการแสดงออก

ประมวลกฎหมายอาญา มาตรา 112 (หมิ่นพระบรมเดชานุภาพ)

ประมวลกฎหมายอาญามาตรา 112 บัญญัติบทลงโทษผู้ใดที่ “หมิ่นประมาท ดูหมิ่นหรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์” มีโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี จำเลยคดีหมิ่นพระบรมเดชานุภาพมักถูกปฏิเสธการให้ประกันตัว และหากถูกตัดสินว่าผิด มักถูกพิพากษาลงโทษอย่างหนัก การร้องเรียนคดีหมิ่นพระบรมเดชานุภาพหรือการหมิ่นประมาทสามารถยื่นฟ้องโดยพลเมืองคนใดก็ได้ และการร้องเรียนดังกล่าวจะถูกสอบสวนอย่างเป็นทางการจากเจ้าหน้าที่เสมอ สิ่งนี้นำมาซึ่งศักยภาพในทางที่ผิดในการปิดกั้นข้อมูลอย่างเป็นระบบเพื่อจำกัดการเคลื่อนไหวทางสังคมเกี่ยวกับเหตุการณ์ทางการเมืองที่สำคัญ

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

มาตรา 14 (1) ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ลงโทษบุคคลที่พบว่านำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ “ปลอม” หรือข้อมูลคอมพิวเตอร์ “อันเป็นเท็จ" หรือโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน มีโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท ภาษาที่กว้างและกำกวมดังกล่าวเปิดทางให้ใช้กฎหมายในทางที่ผิดได้ มาตรา 14 (1) ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ถูกนำมาใช้กับนักข่าว นักกิจกรรม และผู้ใช้อินเทอร์เน็ตมานานแล้วสำหรับเนื้อหาที่รัฐบาลพิจารณาว่าสร้างความเสียหาย

การแก้ไขเพิ่มเติมมาตรา 14 (2) ของ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ในปี 2560 ขยายขอบเขตองค์ประกอบความผิดในการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูล "ที่น่าจะเกิดความ

เสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน" และขยายอำนาจที่เจ้าหน้าที่มีในการจำกัดเสรีภาพในการแสดงออกของบุคคล

พ.ร.บ.การรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2551

พระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. 2551 กำหนดให้จัดตั้งกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) ซึ่งมีศูนย์ติดตามสถานการณ์ในทุกจังหวัดและมีอำนาจในการตอบสนองต่อบุคคล/กิจกรรมที่ต้องสงสัยว่าเป็นภัยคุกคามต่อความมั่นคงของชาติ กอ.รมน. มีอำนาจจัดการสถานการณ์ที่กระทบต่อความมั่นคงของชาติซึ่งยังไม่มีการประกาศสถานการณ์ฉุกเฉิน โดยไม่ต้องสนใจบทบาทของรัฐสภาและศาลในการตรวจสอบหรือให้ความเห็นชอบต่อความจำเป็นของการใช้อำนาจในทางมิชอบ

เสรีภาพสื่อมวลชน

เสรีภาพสื่อในประเทศไทยถูกจำกัดอย่างรุนแรงหลังการรัฐประหารโดยกองทัพ และการก่อตั้งคณะรักษาความสงบแห่งชาติ (คสช.) ซึ่งบังคับใช้การปิดกั้นในวงกว้าง

ประกาศ คสช. ที่ 97/2557

ประกาศคณะรักษาความสงบแห่งชาติที่ 97/2557 เรื่อง "การให้ความร่วมมือต่อการปฏิบัติงานของคณะรักษาความสงบแห่งชาติและการเผยแพร่ข้อมูลข่าวสารต่อสาธารณะ" ที่ห้ามเผยแพร่หรือออกอากาศเนื้อหาวิพากษ์วิจารณ์หน่วยงานทหารทางสื่อสิ่งพิมพ์ วิทยุ ทีวีและสื่อออนไลน์ คสช. มีดุลยพินิจแต่เพียงผู้เดียวในการพิจารณาว่าเนื้อหาใดเข้าข่ายประเภทต้องห้าม การละเมิดข้อกำหนดในประกาศนี้อาจส่งผลให้ถูกดำเนินคดีตามกฎหมาย และระงับการเผยแพร่หรือโปรแกรมทันที (ประกาศนี้ยกเลิกแล้ว เมื่อ 9 กรกฎาคม 2562)

คำสั่งหัวหน้า คสช. ที่ 3/2558 ข้อ 5

ภายใต้ข้อ 5 ของคำสั่งหัวหน้าคณะรักษาความสงบแห่งชาติที่ 3/2558 เรื่อง "การรักษาความสงบเรียบร้อยและความมั่นคงของชาติ" เจ้าหน้าที่ คสช. มีอำนาจออกคำสั่งห้ามการเสนอข่าว การจำหน่าย หรือทำให้แพร่หลายซึ่งหนังสือ สิ่งพิมพ์ หรือสื่ออื่นใด ที่มีข้อความอันอาจทำให้ประชาชนเกิดความหวาดกลัวหรือเจตนาบิดเบือนข้อมูลข่าวสารทำให้เกิดความเข้าใจผิดจนกระทบต่อความมั่นคงของชาติหรือความสงบเรียบร้อยของประชาชน (คำสั่งนี้ยกเลิกแล้ว เมื่อ 9 กรกฎาคม 2562)

ข้อกำหนดออกตามความในมาตรา 9 แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. 2548 (ฉบับที่ 29)

ภายใต้ข้อกำหนดฯ ฉบับที่ 29 ห้ามมิให้บุคคลใดนำเสนอหรือเผยแพร่ข้อความที่:

- เจตนาบิดเบือนข้อมูลข่าวสารทำให้เกิดความเข้าใจผิดในสถานการณ์ฉุกเฉินจนกระทบต่อความมั่นคงของรัฐ หรือความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- อาจทำให้ประชาชนเกิดความหวาดกลัว

ที่สำคัญ ข้อกำหนดฯ ฉบับที่ 29 อนุญาตให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สามารถระบุที่อยู่ของโปรโตคอลอินเทอร์เน็ต (IP address) และข้อมูลอื่น ๆ ของเจ้าของเนื้อหาที่ละเมิดระเบียบได้ นอกจากนี้ ยังให้อำนาจสำนักงาน กสทช. ในการสั่งให้ผู้ให้บริการอินเทอร์เน็ต (ISP) ให้ข้อมูลดังกล่าว และยุติการให้บริการอินเทอร์เน็ตสำหรับที่อยู่โปรโตคอลอินเทอร์เน็ตดังกล่าว การฝ่าฝืนข้อกำหนดฯ ฉบับที่ 29 และการที่ผู้ให้บริการ ISP ไม่ปฏิบัติตามคำสั่งที่ออกโดยสำนักงาน กสทช. มีโทษทั้งจำทั้งปรับ

แม้ข้อกำหนดฯ ฉบับที่ 29 จะถูกอ้างว่าเป็นความพยายามของรัฐบาลไทยในการแก้ไขปัญหา “ข่าวปลอม” ที่เกี่ยวข้องกับการแพร่ระบาดของโรคโควิด-19 ในประเทศไทย อย่างไรก็ดี กฎระเบียบดังกล่าวถูกวิพากษ์วิจารณ์อย่างมากว่าให้อำนาจรัฐบาลอย่างกว้างขวางในการควบคุมข้อมูลทุกรูปแบบในพื้นที่สาธารณะ รวมถึงการแทรกแซงหน้าที่สำคัญของสื่อมวลชน ปัญหานี้รุนแรงขึ้นจากการใช้ถ้อยคำที่กำกวมที่ห้ามข้อความ “อันอาจทำให้ประชาชนเกิดความหวาดกลัว” และไม่จำกัดเฉพาะข้อมูลที่เป็นเท็จหรือบิดเบือน

การเข้าถึงข้อมูล

พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ให้สิทธิแก่ประชาชนชาวไทยในการร้องขอให้เปิดเผยข้อมูลข่าวสารของราชการจากหน่วยงานของรัฐ อย่างไรก็ตาม เจ้าหน้าที่มีสิทธิที่จะปฏิเสธคำขอเปิดเผยข้อมูลตามมาตรา 15 ของกฎหมาย ด้วยเหตุผลที่ไม่ชัดเจนและกว้างเกินไป เช่น “การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ ความเสียหายต่อความมั่นคงของประเทศ และอันตรายต่อชีวิตหรือความปลอดภัยของ

บุคคลหนึ่งบุคคลใด" แม้ว่าพลเมืองจะมีสิทธิอุทธรณ์การปฏิเสธ แต่การอุทธรณ์ที่ส่งไปยังคณะกรรมการนั้นใช้เวลานานในการพิจารณาและดำเนินการ ทำให้เข้าถึงได้ยากสำหรับพลเมือง
นอกจากนี้ พระราชบัญญัติดังกล่าวยังไม่ครอบคลุมถึงข้อมูลในครอบครองของเอกชน ซึ่งทำให้เกิดข้อโต้แย้งอย่างต่อเนื่องว่าองค์กรอิสระ เช่น คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ สำนักงานคณะกรรมการการเลือกตั้ง สำนักงานการตรวจเงินแผ่นดินอยู่ภายใต้ขอบเขตของพระราชบัญญัตินี้หรือไม่

ความเป็นส่วนตัว

รัฐธรรมนูญแห่งราชอาณาจักรไทย

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ให้สิทธิในความเป็นส่วนตัวแก่พลเมือง ภายใต้รัฐธรรมนูญมาตรา 35 “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ”

หลังการรัฐประหาร พ.ศ. 2557 รัฐธรรมนูญฉบับชั่วคราวได้ประกาศใช้ ซึ่งบทบัญญัติเกือบทั้งหมดของรัฐธรรมนูญเดิมถูกระงับ ไม่มีข้อกำหนดที่ชัดเจนเกี่ยวกับสิทธิในความเป็นส่วนตัวอีกต่อไป

แม้ประเทศไทยจะยังไม่มีกฎหมายคุ้มครองข้อมูลทั่วไปที่ครอบคลุม[1] แต่ข้อมูลส่วนบุคคลของภาครัฐก็ได้รับการคุ้มครองระดับหนึ่งตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งกำหนดให้หน่วยงานของรัฐต้องอนุญาตให้บุคคลแก้ไขข้อมูลส่วนบุคคลที่หน่วยงานเก็บรักษาไว้ ข้อมูลส่วนบุคคลในภาคเอกชน เช่น ข้อมูลเครดิต ข้อมูลผู้ป่วย และข้อมูลโทรคมนาคม ถูกควบคุมโดยกฎหมายเฉพาะกิจการ เช่น พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2551 พ.ร.บ.สุขภาพแห่งชาติ พ.ศ. 2550 และประกาศคณะกรรมการกิจการโทรคมนาคมแห่งชาติ พ.ศ. 2549 (เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม)

[1] ในช่วงเวลาที่รวบรวมข้อมูลและทำการศึกษาเพื่อจัดทำรายงานฉบับนี้ คาบเกี่ยวกับระยะเวลาที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ยังไม่บังคับใช้ในส่วนของการคุ้มครองสิทธิในความเป็นส่วนตัว โดยกฎหมายดังกล่าวเพิ่งบังคับใช้ทั้งฉบับเมื่อวันที่ 1 มิถุนายน 2565

การปิดกั้นและการเฝ้าสอดส่อง

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 20

ภายใต้มาตรา 20 ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม พ.ศ. 2560 “คณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์” 9 คน ซึ่งได้รับการแต่งตั้งจากรัฐบาลมีอำนาจเสนอแนะให้ศาลระงับหรือลบข้อมูลคอมพิวเตอร์ที่ “มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน” เนื่องจากคำนิยามนี้มีความหมายกว้าง ทำให้เจ้าหน้าที่สามารถทำหน้าที่เป็นผู้ทำสงครามด้านศีลธรรม ให้เจ้าหน้าที่มีดุลพินิจอย่างกว้างขวางในการปราบปรามเนื้อหาออนไลน์ที่พิจารณาว่าเป็นการละเมิดศีลธรรมอันดีของประชาชน แม้จะไม่ละเมิดกฎหมายใด ๆ

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18

มาตรา 18 (2) และ 18 (3) ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แก้ไขเพิ่มเติม พ.ศ. 2560 อนุญาตให้เจ้าหน้าที่เข้าถึงข้อมูลเกี่ยวกับผู้ใช้บริการและข้อมูลจราจรทางคอมพิวเตอร์ได้ภายใต้เหตุอันควรโดยไม่ต้องมีคำสั่งศาลเพื่อช่วยในการสอบสวนเกี่ยวกับความผิดภายใต้พระราชบัญญัติดังกล่าวหรือกฎหมายอื่น ๆ

มาตรา 18 (7) อนุญาตให้เจ้าหน้าที่ที่มีคำสั่งศาลบังคับให้ผู้ให้บริการช่วยเหลือในการถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด ซึ่งเป็นการบ่อนทำลายการใช้เครื่องมือเข้ารหัสเพื่อปกป้องความเป็นส่วนตัวของผู้ใช้

รายงานกรณีการปิดกั้นอินเทอร์เน็ต

การประท้วงในปี 2563-2564

เมื่อต้นปี 2563 มีการเดินขบวนต่อต้านรัฐบาลของนายกรัฐมนตรี พล.อ. ประยุทธ์ จันทร์โอชา ต่อมาได้ขยายไปถึงข้อเรียกร้องที่ไม่เคยเกิดขึ้นมาก่อนในการปฏิรูปสถาบันพระมหากษัตริย์ การประท้วงเริ่มต้นจากการยุบพรรคอนาคตใหม่ ในปลายเดือนกุมภาพันธ์ 2563 พรรคดังกล่าววิพากษ์วิจารณ์ พล.อ. ประยุทธ์ฯ การแก้ไขรัฐธรรมนูญในปี 2560 และภูมิทัศน์ทางการเมืองของประเทศที่รัฐธรรมนูญดังกล่าวก่อให้เกิดขึ้น

จากนั้นในเดือนตุลาคม 2563 ทางการไทยได้ปิดกั้นการเข้าถึงเว็บไซต์รับคำร้องออนไลน์ Change.org หลังจากที่มีผู้เรียกร้องให้พระบาทสมเด็จพระเจ้าอยู่หัวทรงถูกประกาศเป็น "บุคคลไม่พึงปรารถนา" ใน

เยอรมนี ซึ่งเป็นที่ที่พระองค์มักจะเสด็จฯ ไปพักผ่อน คำร้องดังกล่าวมีผู้ลงชื่อเข้าร่วมกว่า 130,000 รายชื่อ ก่อนที่เว็บไซต์จะถูกปิดกั้นโดยผู้ให้บริการรายใหญ่ เช่น เอไอเอส ดีแทค และทรู ในช่วงที่มีการประท้วงเรียกร้องประชาธิปไตย

เว็บไซต์ดังกล่าวเปลี่ยนเส้นทางไปยังหน้าปิดกั้น (block page) โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยอ้างว่าเนื้อหาดังกล่าวผิดกฎหมายไทยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หลังจากนั้น ทีมงาน Change.org ยื่นคำร้องต่อศาล และเว็บไซต์สามารถเข้าถึงได้อีกครั้งหลังจากผ่านไป 6 เดือน

ในระหว่างการประท้วงในเดือนตุลาคม 2563 สื่อต่าง ๆ ก็ถูกปิดกั้น อาทิ BBC, Al Jazeera, และ CNN รวมถึงแพลตฟอร์มข่าวออนไลน์ของไทย 4 แห่ง ได้แก่ Voice TV, The Standard, The Reporters และประชาไท จากข้อมูลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม การรายงานข่าวของสำนักข่าวข้างต้นเกี่ยวกับการประท้วงเรียกร้องประชาธิปไตยในกรุงเทพฯ ละเมิดพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉินฯ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

นอกจากนี้ ในปี 2564 เกมคลิกแมวก็ได้รับความนิยมไปทั่วโลก Popcat.click ผู้เล่นจะได้รับคะแนนจากการคลิกหรือแตะเพื่อทำให้ปากของแมวเปิดออกพร้อมกับเสียงป๊อป ต่อมาโปรแกรมเมอร์ไทยกลุ่มหนึ่งได้เปิดตัวเกมเลียนแบบรุ่นที่มี พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรีไทย (prayut.click) จากนั้นกระทรวงฯ ได้ปิดกั้นเว็บไซต์นี้ นัยว่าละเมิดพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ขณะนี้เว็บไซต์ปิดตัวลง

รูปที่ 1: ภาพหน้าจอเว็บไซต์เกมที่มีนายกรัฐมนตรีไทย (prayut.click)

นอกจากนี้ มีหนังสือราชการรั่วไหลออกมา สรุปแผนของรัฐบาลที่จะสั่งให้ผู้ให้บริการอินเทอร์เน็ตปิดกั้น Telegram ซึ่งเป็นแพลตฟอร์มที่นักเคลื่อนไหวใช้อย่างแพร่หลายเพื่อจัดการประท้วงและระดมผู้สนับสนุน ในเดือนตุลาคม 2563 นับเป็นการพิสูจน์ว่ามีการปิดกั้นระหว่างการประท้วง คาดว่าเอกสารนี้ถูกจัดทำโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมของไทย ซึ่งมีอำนาจในการปิดกั้นอินเทอร์เน็ต และถูกส่งไปยัง สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.)

หนังสือดังกล่าวมีข้อความว่า “กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมขอความร่วมมือให้ท่านดำเนินการแจ้งผู้ให้บริการอินเทอร์เน็ตและผู้ให้บริการเครือข่ายมือถือทุกรายระงับการใช้แอปพลิเคชันเทเลแกรม (Telegram)”

ลับมาก

ด่วนที่สุด

ที่ ดศ ๐๒๐๔/๙๑๓

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๑๙ ตุลาคม ๒๕๖๓

เรื่อง ขอให้ดำเนินการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์

เรียน เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

สิ่งที่ส่งมาด้วย ๑. คำสั่งหัวหน้าผู้รับผิดชอบในการแก้ไขสถานการณ์ฉุกเฉินที่มีความร้ายแรง ที่ ๑๑/๒๕๖๓ เรื่อง ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ที่มีลักษณะฝ่าฝืนข้อกำหนดออกตามความในมาตรา ๙ ประกอบมาตรา ๑๑ แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. ๒๕๔๘
๒. IP Address แอปพลิเคชันเทเลแกรม (Telegram)

ด้วยหัวหน้าผู้รับผิดชอบในการแก้ไขสถานการณ์ฉุกเฉินที่มีความร้ายแรง ได้มีคำสั่งที่ ๑๑/๒๕๖๓ เรื่อง ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ที่มีลักษณะฝ่าฝืนข้อกำหนดออกตามความในมาตรา ๙ ประกอบมาตรา ๑๑ แห่งพระราชกำหนดการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ. ๒๕๔๘ ให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ดำเนินการเพื่อให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ รายละเอียดที่ส่งมาด้วย ๑

ในการนี้ เพื่อให้การดำเนินการเป็นไปตามคำสั่งดังกล่าว กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ขอความร่วมมือให้ท่านดำเนินการแจ้งให้ผู้ให้บริการอินเทอร์เน็ตและผู้ให้บริการเครือข่ายมือถือทุกรายระงับการใช้แอปพลิเคชันเทเลแกรม (Telegram) โดยมีรายละเอียดตามสิ่งที่ส่งมาด้วย ๒

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการเรื่องดังกล่าว จะขอบคุณยิ่ง

ขอแสดงความนับถือ

(นายภุชพงศ์ โนดไธสง)
รองปลัดกระทรวง ปฏิบัติราชการแทน
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ
โทร ๐ ๒๑๔๓ ๙๒๗๔ โทรสาร ๐ ๒๑๔๓ ๘๐๓๔

ลับมาก

รูปที่ 2: หนังสือจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมถึงเลขาธิการ กสทช. เรื่องการระงับการใช้งานแอปพลิเคชัน Telegram

อย่างไรก็ตาม ผู้ที่อยู่ในประเทศไทยได้สังเกตว่า Telegram ยังคงทำงานอยู่ในช่วงเวลาดังกล่าว ซึ่งอาจเป็นไปได้ว่ามาตรการตอบโต้บางอย่างที่ Telegram จัดทำขึ้นนั้นได้ผลในการทำให้ Telegram ยังคงใช้งานได้สำหรับคนไทย

ภูมิทัศน์เครือข่ายและการเข้าถึงอินเทอร์เน็ต

ประเทศไทยเข้าถึงอินเทอร์เน็ตได้ในปี 2539 ซึ่งเป็นประเทศที่สามในเอเชียตะวันออกเฉียงใต้ ปัจจุบันอินเทอร์เน็ต 5G ก็มีให้บริการในประเทศเช่นกัน ประเทศไทยยังติด 1 ใน 10 ประเทศที่มีความเร็วอินเทอร์เน็ตบรอดแบนด์เร็วที่สุดในปี 2564 อีกด้วย

ในแง่ของการเข้าถึงอินเทอร์เน็ต ร้อยละ 85 ของครัวเรือนเข้าถึงได้ที่บ้าน และร้อยละ 98 ของประชากรมีเครือข่ายมือถือ 4G เป็นอย่างน้อย มีความแตกต่างเล็กน้อยในอัตราการเข้าถึงอินเทอร์เน็ตระหว่างพื้นที่ในเมืองและชนบท โดยร้อยละ 89 ของครัวเรือนในเมืองและร้อยละ 82 ของครัวเรือนในชนบทสามารถเข้าถึงอินเทอร์เน็ตได้

คณะกรรมการกิจการโทรคมนาคมแห่งชาติให้ใบอนุญาตดำเนินการแก่ผู้ให้บริการอินเทอร์เน็ตในประเทศไทย ซึ่งผสมผสานระหว่างบริษัทของรัฐและผู้ประกอบการเอกชน โดยบริษัทที่รัฐเป็นเจ้าของคือ กสท โทรคมนาคม และทีโอที[2] ขณะที่ผู้ให้บริการโทรศัพท์เคลื่อนที่รายใหญ่เอกชนสามราย ได้แก่ แอดวานซ์ อินโฟร์ เซอร์วิส (เอไอเอส) ดีแทค และทรู[3]

รายงานปี 2560 เน้นย้ำว่า รัฐบาลไทยมีอำนาจควบคุมอินเทอร์เน็ตอย่างกว้างขวาง โดยอาศัยความสัมพันธ์กับผู้ให้บริการอินเทอร์เน็ตและบริษัทโทรคมนาคม นอกจากนี้ อดีตนักการเมือง นายทหาร หรือสมาชิกครอบครัวของคนเหล่านี้ก็ดำรงตำแหน่งสำคัญในบริษัทเหล่านี้

[2] กสท โทรคมนาคม และ ทีโอที ควบรวมกิจการกันเป็น บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ในวันที่ 7 มกราคม 2564

[3] ดีแทค และทรู ควบรวมกิจการกันเป็น บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) ในช่วงปลายปี 2565 โดยยังทำการตลาดแยกกันเป็นสองตราสินค้าอยู่ตามเงื่อนไขในการอนุมัติให้ควบรวมกิจการได้ของกสทช.

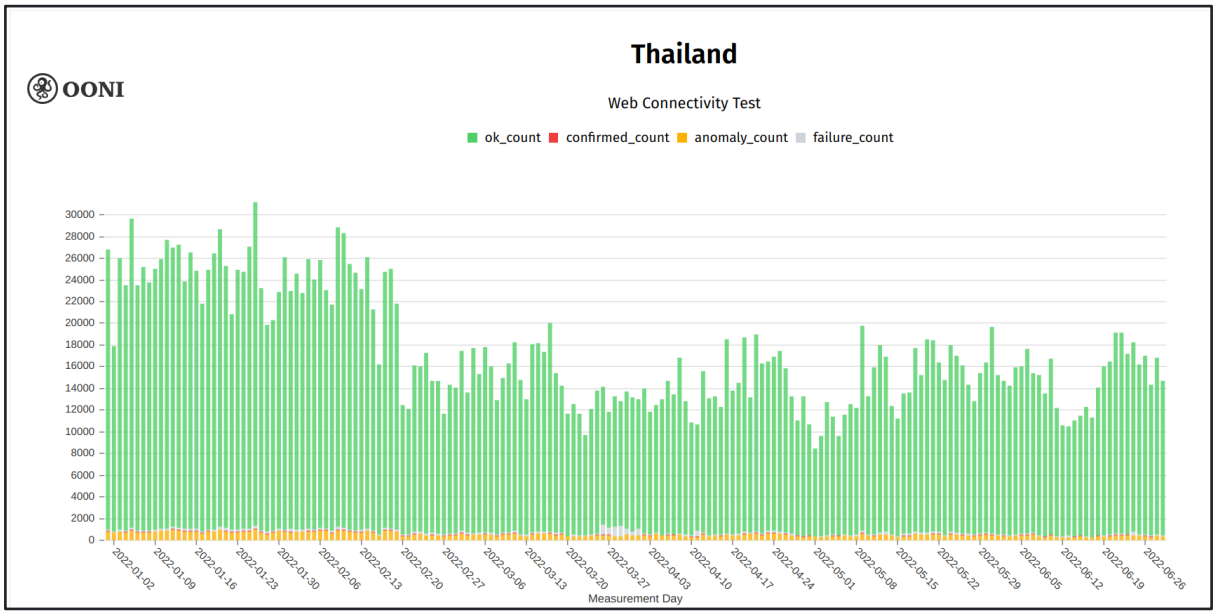
ข้อค้นพบเกี่ยวกับการปิดกั้นอินเทอร์เน็ตในประเทศไทย

การวิเคราะห์ใช้ผลการทดสอบระหว่าง 1 มกราคม 2565 - 30 มิถุนายน 2565

การปิดกั้นเว็บไซต์

ในขณะที่เขียนรายงานนี้ รายชื่อการทดสอบ Citizen Lab ของประเทศไทยประกอบด้วย URL 446 รายการ

ในช่วงหกเดือน มีการบันทึกข้อมูลตรวจวัด 3,129,067 รายการในการทดสอบการเชื่อมต่อเว็บของ OONI จากจุดสำรวจ 30 จุด จากทั้งหมดนี้พบว่าร้อยละ 95.8 (2,996,695) เป็นปกติ ร้อยละ 3.1 (96,626) มีความผิดปกติ ร้อยละ 0.3 (8,982) ได้รับการยืนยันการปิดกั้น และร้อยละ 0.9 (26,664) เป็นการตรวจวัดที่ล้มเหลว นอกจากนี้ ข้อมูลตรวจวัดประมาณร้อยละ 80 ของข้อมูลทั้งหมด หรือเท่ากับข้อมูลตรวจวัด 2.5 ล้านจุด มาจาก ASN 5 แห่ง ได้แก่ JasTel-IIG (บริษัท จัสเทล เน็ทเวิร์ค จำกัด) ร้อยละ 29, TripleT (บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)) ร้อยละ 16, SBN-IIG (บริษัท ซุปเปอร์ บรอดแบนด์ เน็ทเวอร์ค จำกัด) ร้อยละ 14, TOT (บริษัท ทีโอที จำกัด (มหาชน)) ร้อยละ 13, และบริษัท ทรู อินเทอร์เน็ต จำกัด



รูปที่ 3: ข้อมูลตรวจวัด OONI ในประเทศไทย มกราคม-มิถุนายน 2565

รายการโดเมนที่ถูกปิดกั้นที่ได้ยืนยันของ OONI มี 76 โดเมนจากหมวดหมู่ต่าง ๆ ในขณะที่การวิเคราะห์พฤติกรรมเพิ่มเติมโดยฮิวริสติก (heuristics) พบเพิ่ม 43 โดเมน รวมเป็น 119 โดเมนที่ได้รับการยืนยันการปิดกั้น ในขณะที่รายงานปี 2560 พบว่ามี 13 เว็บไซต์ที่ถูกปิดกั้น

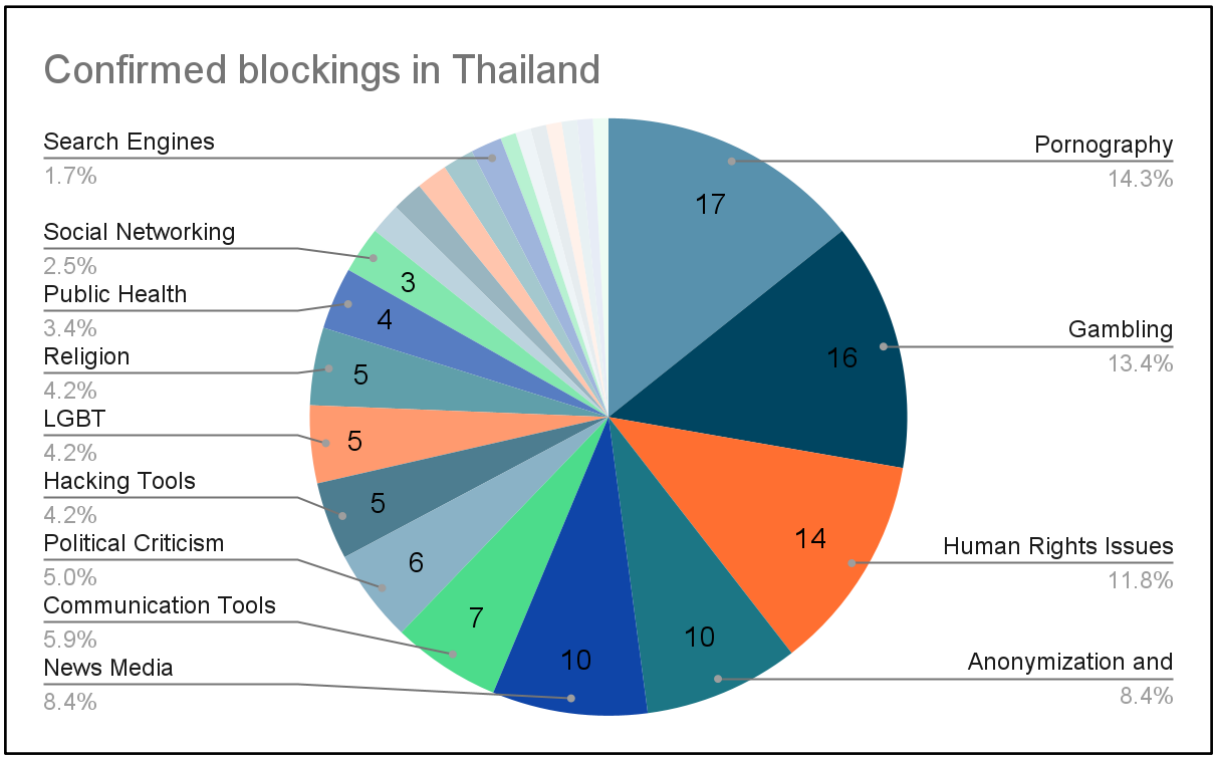
จากการวิเคราะห์พบว่าการปิดกั้นดำเนินการผ่านการแก้ไข DNS ซึ่งเปลี่ยนเส้นทางโดเมนไปยังที่อยู่ไอพี 2 แห่ง คือ ['180.180.255.130'] และ ['125.26.170.3'] ที่อยู่แรกไม่แสดงการปิดกั้นแต่แสดงการหมดเวลาเท่านั้น แต่เนื่องจากที่อยู่ IP นี้เป็นของ บริษัท ทีโอที จำกัด (มหาชน) จึงเป็นไปได้สูงว่าเป็นการปิดกั้นที่ได้รับการยืนยัน

ที่อยู่หลังนำไปสู่หน้าปิดกั้นดังนี้

รูปที่ 4: หน้าปิดกั้น (block page) ในประเทศไทย โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

นอกจากนี้ ยังพบการปิดกั้นจากการปลอมแปลง HTTP โดยการทดสอบให้ผลเป็นส่วนหัว/เนื้อหา ของ HTTP ตามด้านล่าง ซึ่งย้อนกลับไปยังหน้าปิดกั้นเดียวกัน (http://103.288.24.21) หรือหน้าว่างที่รอจนหมดเวลา (http://110.164. 252.137)

รายการปิดกั้นที่ได้รับการยืนยันประกอบด้วยหมวดหมู่ดังนี้



รูปที่ 5: แผนภูมิวงกลมแสดงการปิดกั้นที่ได้ยืนยันในประเทศไทย

รายการเป็นไปตามภาคผนวก 1

หมวดหมู่ที่มีโดเมนมากกว่า 10 โดเมนในรายการข้างต้น ได้แก่ เครื่องมือจัดทำข้อมูลนิรนามและเครื่องมือการหลบเลี่ยง การพนัน ปัญหาสิทธิมนุษยชน ข่าวสาร และสื่ออนาจาร

เครื่องมือนิรนามและเครื่องมือหลบเลี่ยง

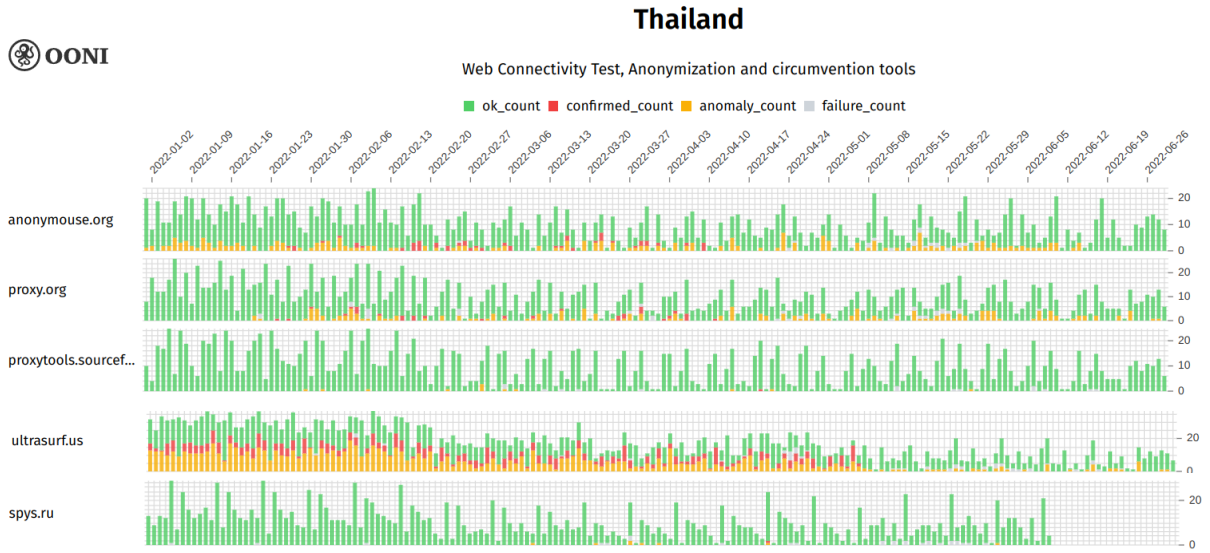
โดเมน 10 รายการที่เกี่ยวข้องกับเครื่องมือนิรนามและเครื่องมือหลบเลี่ยง (anonymization and circumvention tools) ถูกปิดกั้นดังนี้

ยืนยันโดย OONI	ยืนยันโดยฮิวริสติก
anonymouse.org	proxify.com
ultrasurf.us	www.hidemyass.com
proxy.org	www.hotspotshield.com

proxytools.sourceforge.net	www.jmarshall.com
spys.ru	www.peacefire.org

จากข้อมูลของ OONI เพียงอย่างเดียว การทดสอบ 10 โดเมนจะส่งผลดังนี้

ปกติ	ยืนยัน	ผิดปกติ	ล้มเหลว	รวม
20,401 (86%)	563 (2%)	2,270 (10%)	381 (2%)	23,615 (100%)



รูปที่ 6: ข้อมูลตรวจวัด OONI ของโดเมนที่ถูกปิดกั้นที่ได้รับการยืนยันซึ่งเกี่ยวข้องกับเครื่องมือจัดทำข้อมูลนิรนามและเครื่องมือการหลบเลี่ยง

เมื่อพิจารณาที่ 5 โดเมนที่ยืนยันว่าถูกปิดกั้นโดย OONI การปิดกั้นเกิดขึ้นตลอดระยะเวลา ยกเว้น “proxytools.sourceforge.net” และ “spys.ru” ซึ่งการปิดกั้นเกิดขึ้นเพียงไม่กี่ครั้ง

โดเมนที่เหลืออีก 5 โดเมนซึ่งได้รับการยืนยันโดยฮิวริสติกถูกปิดกั้นผ่านการดัดแปลง DNS หรือ HTTP นอกเหนือจากผลที่ปกติ (“OK” measurements) มีการบันทึกการปิดกั้นสูงสุด 25 รายการต่อวันสำหรับ 5 โดเมน โดยส่วนใหญ่เป็นการรีเซ็ตการเชื่อมต่อ TLS รีเซ็ตการเชื่อมต่อ HTTP และ DNS ไม่สอดคล้องกัน

การพนัน

พบการปิดกั้น 16 โดเมนที่เกี่ยวข้องกับการพนัน โดย OONI หรือโดยฮิวริสติก

ยืนยันโดย OONI	ยืนยันโดยฮิวริสติก
Bet365.com	www.betdaq.com
Ibcbet.com	www.ladbrokes.com
www.888casino.com	www.williamhill.com
www.betfair.com	www.grandonline.com
www.casinotropez.com	casino.com
www.europacasino.com	
www.riverbelle.com	
www.spinpalace.com	
www.sportingbet.com	
www.sportsinteraction.com	
www.10bet.com	

จากข้อมูลของ OONI เพียงอย่างเดียว การทดสอบ 16 โดเมนมีผลดังต่อไปนี้

ปกติ	ยืนยัน	ผิดปกติ	ล้มเหลว	รวม
10,931 (69%)	1,453 (9%)	3,412 (21%)	88 (1%)	15,884 (100%)

เมื่อพิจารณาโดเมน 11 โดเมนที่ยืนยันการปิดกั้นโดย OONI การปิดกั้นเกิดขึ้นตลอดช่วงเวลา โดยได้รับการยืนยันและความผิดปกติสูงสุดสำหรับ “bet365.com” “Ibcbet.com” และ www.sportingbet.com

รูปที่ 7: ข้อมูลตรวจวัด OONI ของโดเมนซึ่งเกี่ยวข้องกับการพนันที่ได้รับการยืนยันว่าถูกปิดกั้น

โดเมนที่เหลืออีก 5 โดเมนซึ่งได้รับการยืนยันโดยฮิวริสติกถูกปิดกั้นผ่านการดัดแปลง DNS หรือ HTTP นอกเหนือจากผลที่ปกติ (“OK” measurements) มีการบันทึกการปิดกั้นสูงสุด 10 รายการต่อวันสำหรับ 5 โดเมนดังกล่าว โดยส่วนใหญ่เป็นการรีเซ็ตการเชื่อมต่อ TLS และ DNS ที่ได้ยืนยัน

ประเด็นสิทธิมนุษยชน

มี 14 โดเมนที่เกี่ยวข้องถูกปิดกั้น สอดคล้องกับประเด็นสิทธิมนุษยชนที่รายงานโดย Freedom House เกี่ยวกับสถานการณ์ประเทศไทยปี 2565 ดังนี้

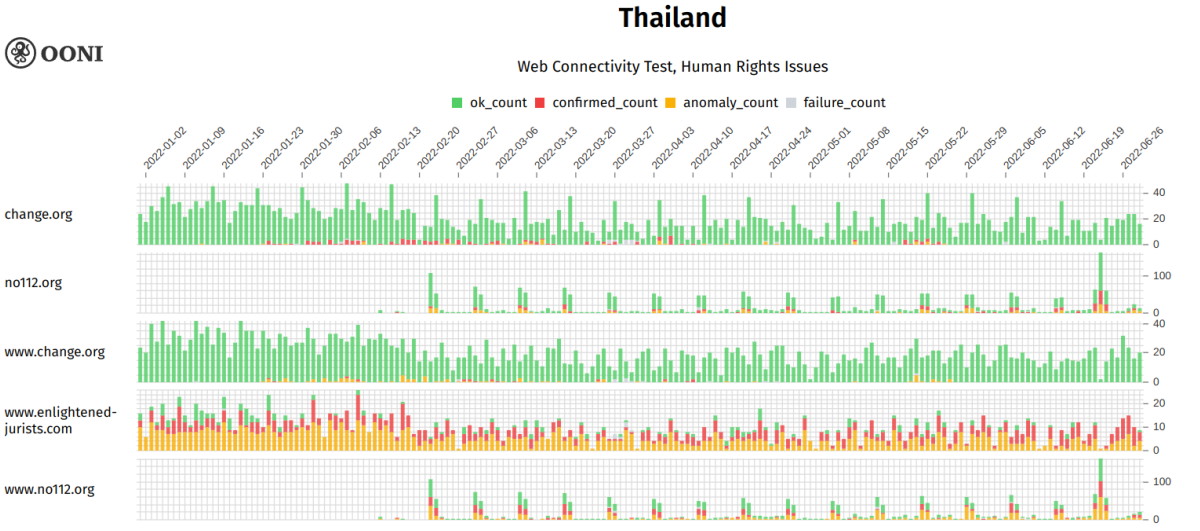
ยืนยันโดย OONI	ยืนยันโดยฮิวริสติก
no112.org	hirvikatu10.net
www.no112.org	hrlibrary.umn.edu

change.org	www.hrw.org
www.enlightened-jurists.com	www.humanrights.asia
laborrights.org	www.ihf-hr.org
	www.ohchr.org
	www.onlinewomeninpolitics.org
	www.mwgthailand.org
	hrw.org

จากข้อมูลของ OONI เพียงอย่างเดียว การทดสอบ 14 โดเมนมีผลดังต่อไปนี้:

ปกติ	ยืนยัน	ผิดปกติ	ล้มเหลว	รวม
42,616 (89%)	1,636 (3%)	2,869 (6%)	584 (1%)	47,705 (100%)

ใน OONI Explorer โดเมนทั้ง 5 ถูกยืนยันว่าถูกปิดกั้นตลอดช่วงเวลานั้น โดยการปิดกั้นส่วนใหญ่เกิดกับ www.enlightened-jurists.com บทความใน The Nation ในปี 2556 "enlightened jurists" หรือคณะนิติราษฎร์คือกลุ่มอาจารย์กฎหมายในมหาวิทยาลัยที่เรียกร้องให้ ส.ส. ที่ลงคะแนนให้วุฒิสภามาจากการเลือกตั้งทั้งหมด เพิกเฉยต่อคำวินิจฉัยของศาลรัฐธรรมนูญที่ไม่อนุญาตให้แก้ไขรัฐธรรมนูญตามข้อเรียกร้องนั้น



รูปที่ 8: ข้อมูลตรวจวัด OONI ของโดเมนเกี่ยวข้องกับปัญหาสิทธิมนุษยชนที่ได้รับการยืนยันว่าถูกปิดกั้น

โดเมนที่เหลือทั้ง 7 โดเมนซึ่งได้รับการยืนยันโดยฮิวริสติกนั้นถูกปิดกั้นผ่านการดัดแปลง DNS หรือ HTTP นอกเหนือจากผลที่ปกติ ("OK" measurements) มีการบันทึกการปิดกั้นสูงสุด 20 รายการต่อวันสำหรับ 7 โดเมนข้างต้น โดยส่วนใหญ่เป็นการรีเซ็ตการเชื่อมต่อ HTTP

สื่อเชิงข่าว

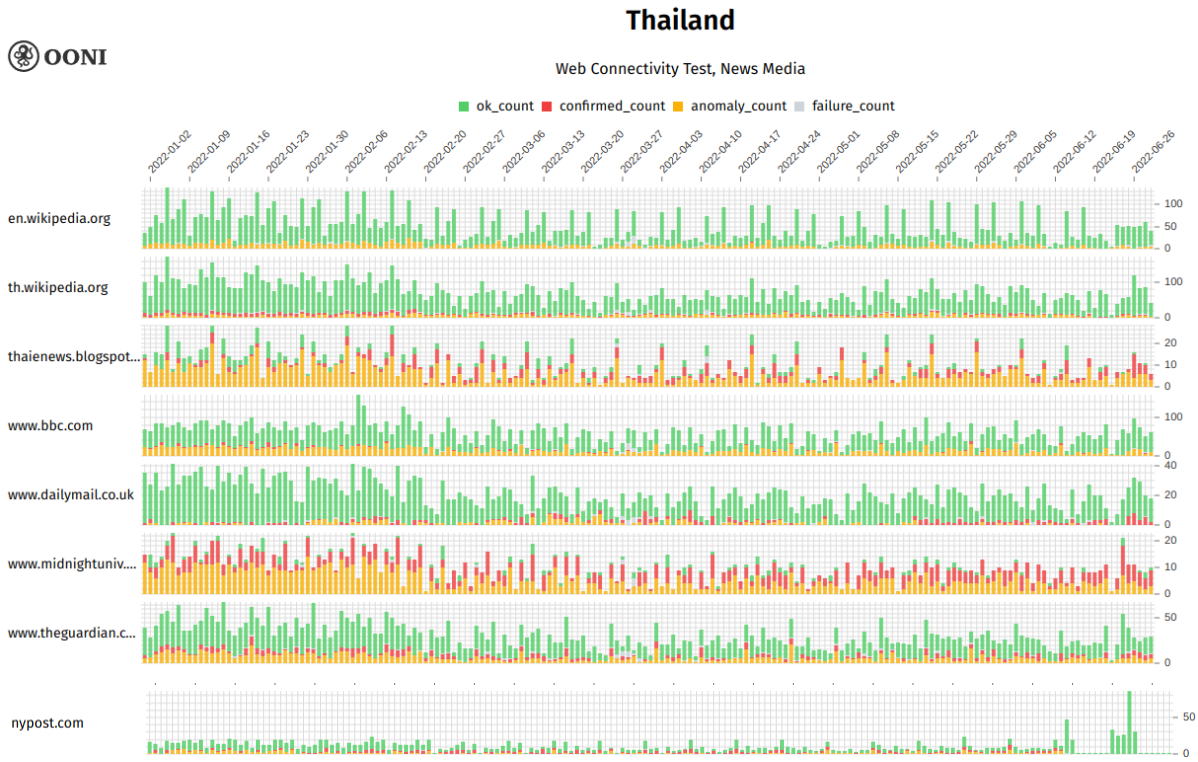
10 โดเมนที่เกี่ยวข้องกับสื่อเชิงข่าว (news media) ถูกยืนยันว่าถูกปิดกั้น ดังนี้

ยืนยันโดย OONI	ยืนยันโดยฮิวริสติก
www.midnightuniv.org	midnightuniv.org
en.wikipedia.org	wartani.com
nypost.com	
th.wikipedia.org	
thaienews.blogspot.com	
www.bbc.com	
www.dailymail.co.uk	
www.theguardian.com	

จากข้อมูลของ OONI เพียงอย่างเดียว การทดสอบ 10 โดเมนมีผล ดังนี้

ปกติ	ยืนยัน	ผิดปกติ	ล้มเหลว	รวม
40,973 (76%)	3,276 (6%)	9,306 (17%)	673 (1%)	54,228 (100%)

เมื่อพิจารณาจาก 8 โดเมนที่ยืนยันว่าถูกปิดกั้นโดย OONI พบว่ามีความผิดปกติที่สำคัญตลอดช่วงเวลาดังกล่าว โดยมีการปิดกั้นที่เห็นได้ชัดบน "thaienews.blogspot.com" และ "www.midnightuniv.org" ในทุกจุดสำรวจ



รูปที่ 9: ข้อมูลตรวจวัด OONI ของโดเมนข่าวสารที่ได้รับการยืนยันว่าถูกปิดกั้น

โดเมนที่เหลืออีก 2 โดเมนซึ่งได้รับการยืนยันโดยฮิวริสติกถูกปิดกั้นผ่านการดัดแปลง DNS หรือ HTTP นอกเหนือจากผลที่ปกติ (“OK” measurements) จะพบการปิดกั้นสูงสุด 10 รายการต่อวันสำหรับ 2 โดเมน โดยส่วนใหญ่ คือ HTTP ล้มเหลวทั่วไป หรือ HTTP ได้รับการยืนยัน

สื่ออนาจาร

17 โดเมนที่เกี่ยวข้องได้รับการยืนยันว่าถูกปิดกั้น ดังนี้

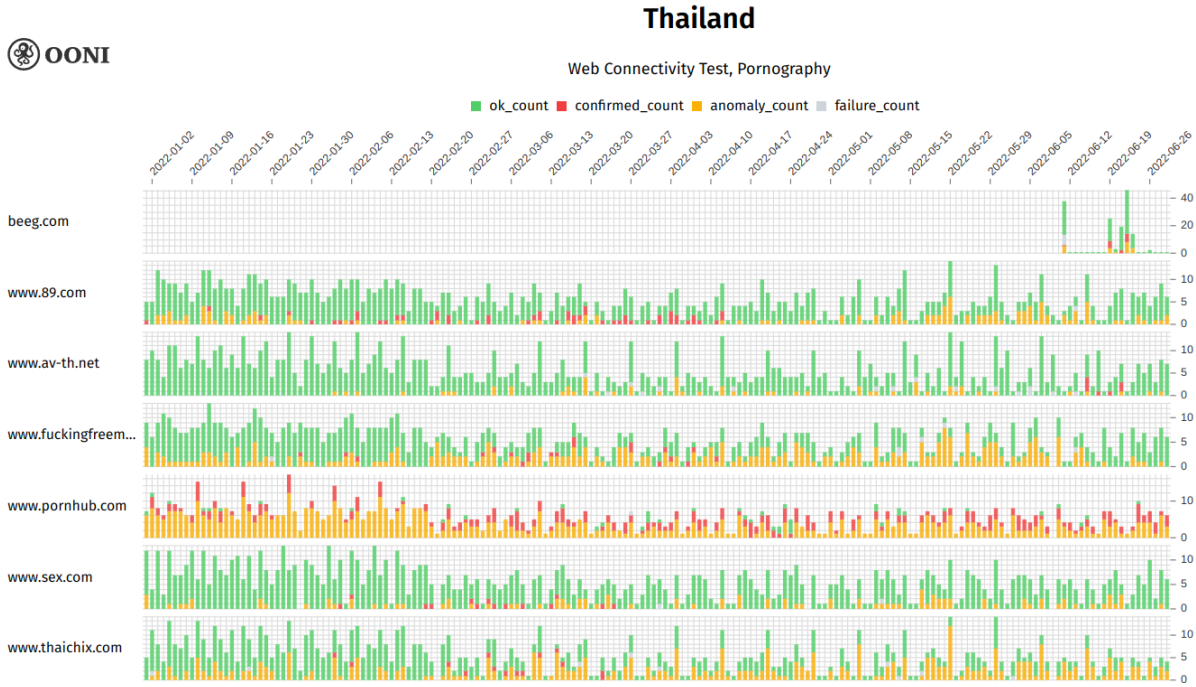
ยืนยันโดย OONI	ยืนยันโดยฮิวริสติก
www.pornhub.com	8thstreetlatinas.com
beeg.com	taknai.com
www.89.com	xhamster.com
www.fuckingfreemovies.com	bravotube.net
www.sex.com	avgle.com
www.thaigirls100.net	

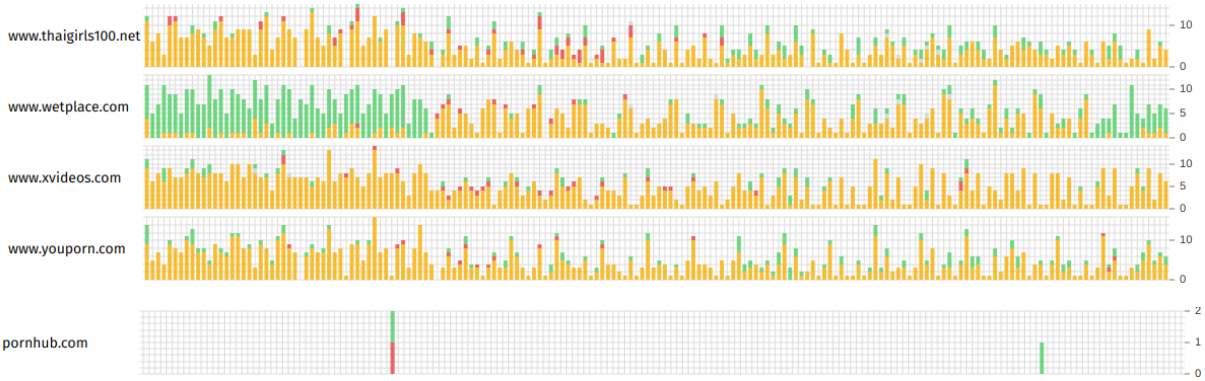
www.wetplace.com	
www.xvideos.com	
www.youporn.com	
www.av-th.net	
www.thaichix.com	
pornhub.com	

จากข้อมูลของ OONI เพียงอย่างเดียว การทดสอบ 17 โดเมนมีผลดังต่อไปนี้

ปกติ	ยืนยัน	ผิดปกติ	ล้มเหลว	รวม
8,038 (58%)	519 (4%)	5,093 (37%)	94 (1%)	13,744 (100%)

เมื่อพิจารณาจาก 12 โดเมนที่ยืนยันว่าถูกปิดกั้นโดย OONI การปิดกั้นที่ได้รับการยืนยันและความผิดปกตินั้นสอดคล้องกันตลอดระยะเวลา





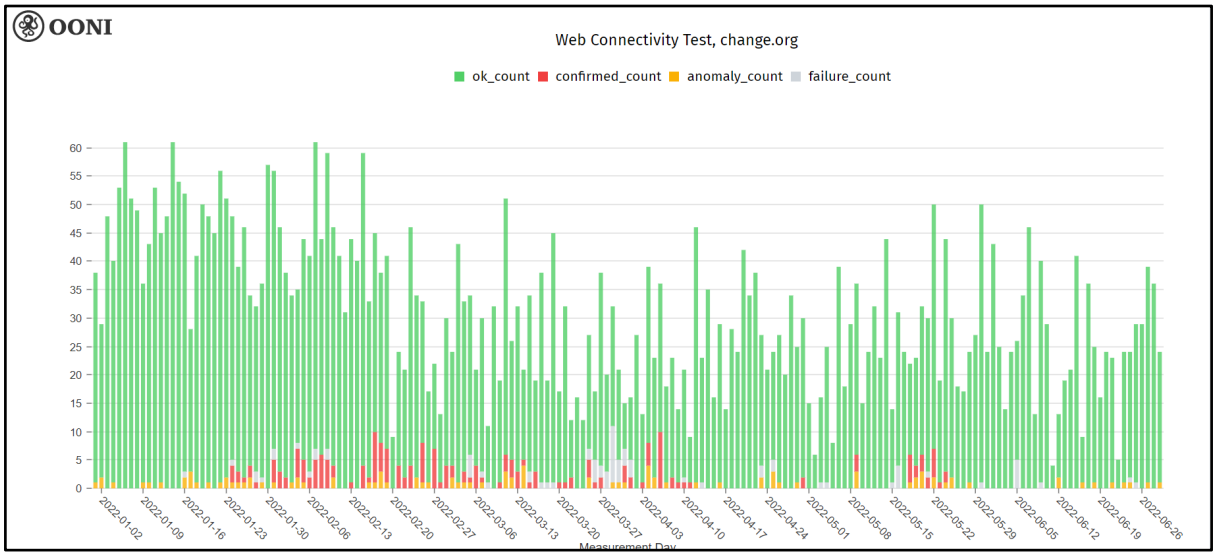
รูปที่ 10: ข้อมูลตรวจวัด OONI ของโดเมนซึ่งเกี่ยวข้องกับสื่ออนาจารที่ได้รับการยืนยันว่าถูกปิดกั้น

โดเมนที่เหลืออีก 5 โดเมนซึ่งได้รับการยืนยันโดยฮิวริสติกถูกปิดกั้นผ่านการดัดแปลง DNS หรือ HTTP นอกเหนือจากผลที่ปกติ (“OK” measurements) มีการปิดกั้นสูงสุด 10 รายการต่อวันสำหรับ 5 โดเมน โดยมีการปิดกั้นประเภทต่าง ๆ

เว็บไซต์ที่น่าสนใจ

การค้นพบด้านล่างแสดงการวิเคราะห์ข้อมูลตรวจวัดกับเว็บไซต์เป้าหมาย 2 แห่ง ได้แก่ Change.org และ No112.org

Change.org



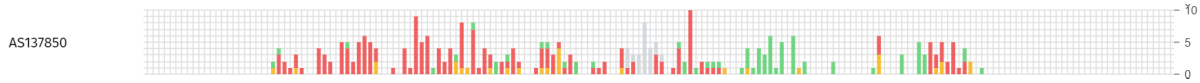
รูปที่ 11: ข้อมูลตรวจวัด OONI ของ Change.org

สัญญาณของการปิดกั้น Change.org ยังคงมีอยู่ในปี 2565 หลังจากถูกปิดกั้นครั้งแรกระหว่างการประท้วงในเดือนตุลาคม 2563 จากข้อมูลของ OONI พบว่ามีการปิดกั้นตั้งแต่เดือนมกราคมถึงพฤษภาคม

ปกติ	ยืนยัน	ผิดปกติ	ล้มเหลว	รวม
5,243 (93%)	187 (2%)	100 (2%)	78 (1%)	5,608 (100%)

เมื่อพิจารณาจากหมายเลขระบบอิสระ (ASN) พบว่าผู้ให้บริการอินเทอร์เน็ตที่แสดงสัญญาณยืนยันการปิดกั้นคือ AS137850 (สำนักงานบริหารเทคโนโลยีเพื่อพัฒนาการศึกษา - UniNet) และ AS4750 (บริษัท ซี เอส ล็อกซอินโฟ จำกัด (มหาชน))

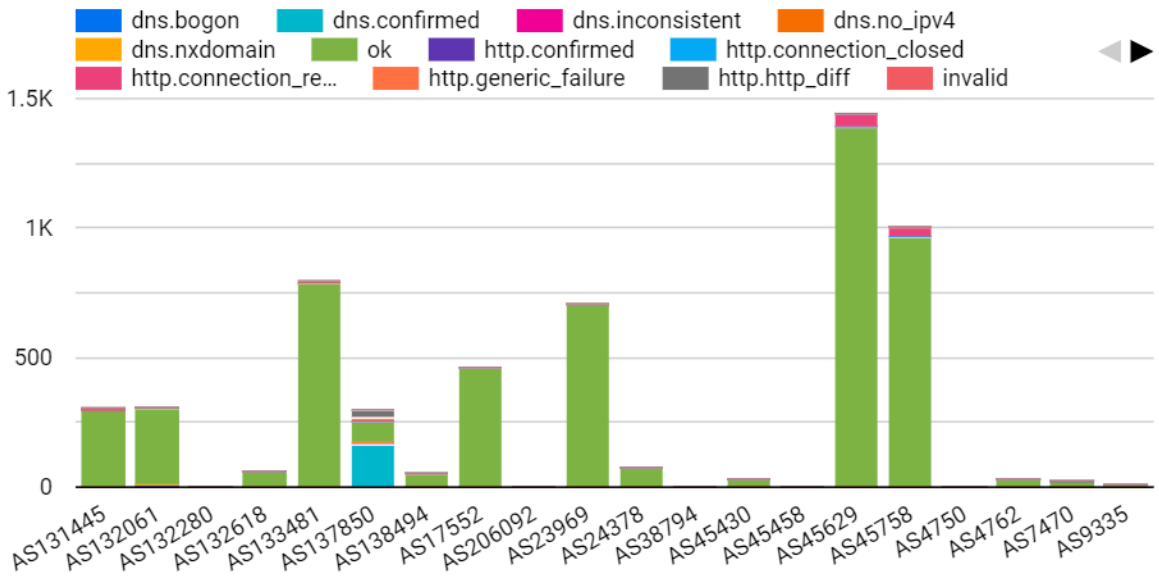
ตรวจพบการปิดกั้นตั้งแต่วันที่ 24 มกราคม 2565 ถึง 24 พฤษภาคม 2565 บน AS137580 จากข้อมูลตรวจวัดดิบ การปิดกั้นได้ดำเนินการผ่านการแก้ไขเปลี่ยนแปลง DNS และแทนที่ด้วยหน้าปิดกั้น (125.26.170.3) โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



รูปที่ 12: **การตรวจวัด** OONI **ของ** Change.org **บน** AS137580

ในขณะที่ AS4750 ตรวจพบการปิดกั้นในวันที่ 30 เมษายน 2565 แม้ว่าจะมีการตรวจวัดเพียง 2 ครั้ง เช่นเดียวกับ AS137850 การปิดกั้นยังดำเนินการผ่านการแก้ไขเปลี่ยนแปลง DNS และแทนที่ด้วยหน้าปิดกั้น (125.26.170.3) โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

รูปที่ 13: **ข้อมูลตรวจวัด** OONI **ของ** Change.org **บน** AS4750



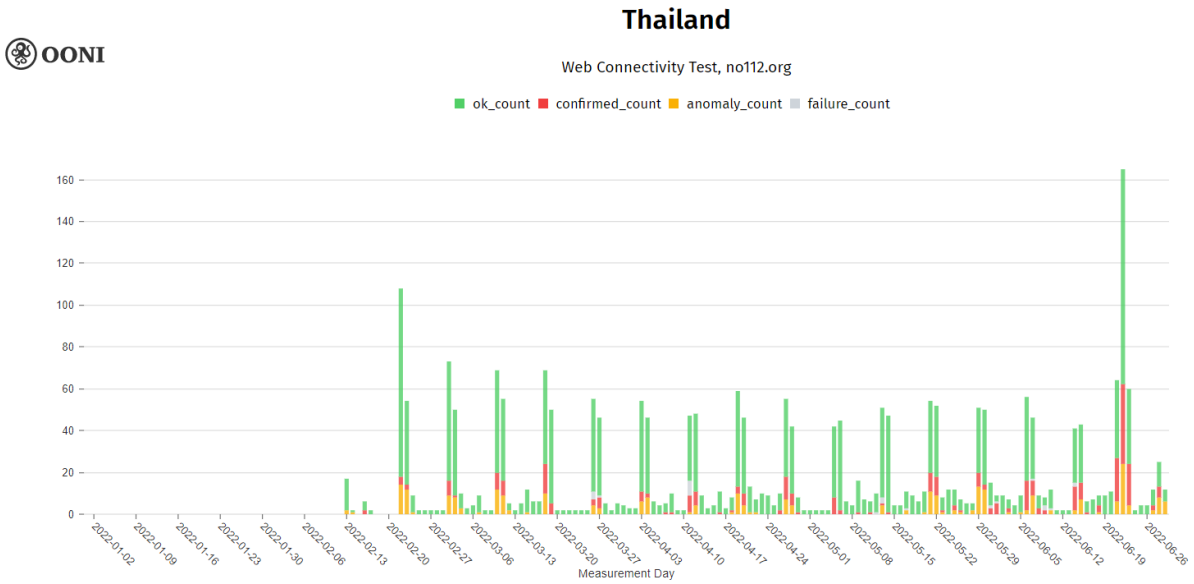
รูปที่ 14: ข้อมูลตรวจวัด OONI ของ Change.org ตามวิธีการปิดกั้น

เมื่อพิจารณาที่ ASN อื่น ๆ ยังมีความไม่สอดคล้องกันของ DNS ที่บันทึกไว้ใน AS45458 (ผู้ให้บริการเชื่อมต่อ SBN-IIG) และ AS45758 (บริษัท ทริปเปิลที อินเทอร์เน็ต จำกัด) อย่างไรก็ตาม สิ่งเหล่านี้อาจเป็นกรณีของผลบวกปลอม (false positive)

No112.org

การหมิ่นพระบรมเดชานุภาพ (การหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี รัชทายาท หรือผู้สำเร็จราชการแทนพระองค์) เป็นการกระทำความผิดอาญาตามมาตรา 112 แห่งประมวลกฎหมายอาญาของไทย No112.org เป็นเว็บไซต์รณรงค์ให้ยกเลิกมาตรานี้ที่จัดโดยคณะก้าวหน้าและกลุ่มราษฎร จนถึงเวลาที่จัดทำรายงานนี้ (กันยายน 2565) มีผู้ลงชื่อมากกว่า 237,000 ราย

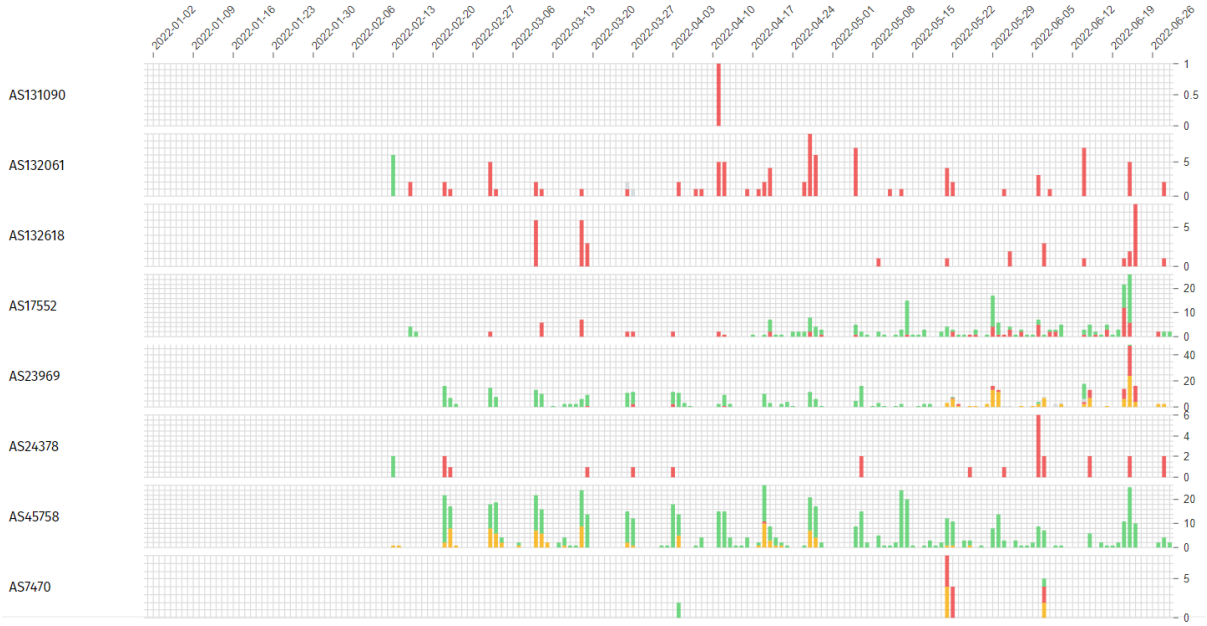
จากข้อมูลของ OONI ตรวจพบการปิดกั้นที่ยืนยันตั้งแต่วันที่ 16 กุมภาพันธ์ 2565 ถึง 28 มิถุนายน 2565 นอกจากนี้ยังมีความผิดปกติที่สำคัญในการตรวจวัดอีกด้วย



รูปที่ 15: **ข้อมูลตรวจวัด** OONI **ของ** No112.org

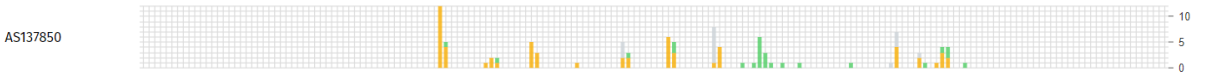
ปกติ	ยืนยัน	ผิดปกติ	ล้มเหลว	รวม
1,909 (76%)	303 (12%)	272 (11%)	25 (1%)	2,509 (100%)

ตรวจพบการปิดกั้นเหล่านี้ที่ยืนยันโดย ASN ใน 8 จุดสำรวจ: AS131090 (บริษัท กสท โทรคมนาคม จำกัด (มหาชน)) AS132061 (บริษัท เรียลมูฟ จำกัด) AS132618 (บริษัท เรียล ฟิวเจอร์ จำกัด) AS17552 (บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด) AS23969 (บริษัท ทีโอที จำกัด (มหาชน)) AS24378 (บริษัท โทเทิ่ล แอ็คเซ็ส คอมมูนิเคชั่น จำกัด (มหาชน)) AS45758 (บริษัท ทริปเปิลที อินเทอร์เน็ต จำกัด) และ AS7470 (บริษัท ทรู อินเทอร์เน็ต คอร์ปอเรชั่น จำกัด)



รูปที่ 16: ข้อมูลตรวจวัด OONI ของ No112.org ตาม ASN

ตรวจพบความผิดปกติสูงบน AS137850 (สำนักงานบริหารเทคโนโลยีเพื่อพัฒนาการศึกษา) จากการตรวจวัดข้อมูลดิบ สิ่งเหล่านี้เกิดจากความไม่สอดคล้องกันของ HTTP และเว็บไซต์ถูกเปลี่ยนเส้นทางไปยังหน้า "307 การเปลี่ยนเส้นทางชั่วคราว"



รูปที่ 17: ข้อมูลตรวจวัด OONI ของ No112.org บน AS137580

นอกเหนือจากการปิดกั้นที่ได้รับการยืนยันผ่านการดัดแปลง DNS แล้ว ยังมีความไม่สอดคล้องของ DNS การรีเซ็ตการเชื่อมต่อ TLS และการรีเซ็ตการเชื่อมต่อ HTTP บน AS23969 (บริษัท ทีโอที จำกัด (มหาชน)) นอกจากนี้ยังมีกรณีของ HTTP ล้มเหลวทั่วไปบน AS45758 (บริษัท ทริปเปิลที อินเทอร์เน็ต จำกัด) ยิ่งไปกว่านั้น บน AS137850 (สำนักงานบริหารเทคโนโลยีเพื่อพัฒนาการศึกษา) มีสัญญาณของการปิดกั้นผ่านความไม่สอดคล้องของ DNS ความล้มเหลวทั่วไปของ HTTP ความไม่สอดคล้องกันของ HTTP และการรีเซ็ตการเชื่อมต่อ TLS

การปิดกั้นแอปพลิเคชันส่งข้อความ

มีการตรวจวัดแอปพลิเคชันส่งข้อความบน OONI 106,595 ครั้ง ในช่วงระยะเวลาหกเดือน แอปพลิเคชันดังกล่าวคือ Facebook, Messenger, Telegram, Signal, และ WhatsApp ดูเหมือนจะไม่มีสัญญาณของการปิดกั้นในประเทศไทย เนื่องจากการทดสอบเหล่านี้ประสบความสำเร็จมากกว่าร้อยละ 99

การปิดกั้นเครื่องมือหลบเลี่ยง

มีการตรวจวัดเครื่องมือหลบเลี่ยงที่ถูกบันทึกบน OONI 55,573 รายการ ในช่วงระยะเวลาหกเดือน เครื่องมือดังกล่าวคือ Psiphon, Tor และ Tor Snowflake ดูเหมือนจะไม่มีสัญญาณของการปิดกั้นในประเทศไทย เนื่องจากการทดสอบเหล่านี้ประสบความสำเร็จมากกว่าร้อยละ 99 อย่างไรก็ตาม สังเกตได้ว่าเครื่องมือเหล่านี้อาจไม่ถูกใช้มากเท่ากับเครื่องมืออื่น ๆ ในประเทศไทย เนื่องจากเมื่อใช้การทดสอบการเชื่อมต่อเว็บ พบว่ามี 10 โดเมนที่เกี่ยวข้องกับเครื่องมือนิรนามและเครื่องมือหลบเลี่ยง ที่ถูกปิดกั้น

ข้อจำกัดของผลการศึกษา

การตรวจสอบข้อค้นพบต่าง ๆ ในการศึกษานี้ จำกัดอยู่เฉพาะกับข้อมูลตรวจวัดเครือข่ายที่รวบรวมระหว่างวันที่ 1 มกราคม ถึง 30 มิถุนายน 2565 เพื่อตรวจสอบแนวโน้มและเหตุการณ์การปิดกั้นล่าสุด

แม้ข้อมูลตรวจวัดเครือข่ายจะถูกรวบรวมจากจุดวัด 30 จุดในประเทศไทย แต่การทดสอบของซอฟต์แวร์ OONI นั้นไม่ได้สม่ำเสมอกันตลอดทั้งเครือข่าย

บทสรุป

นับตั้งแต่มีการเผยแพร่รายงานสถานการณ์ปิดกั้นในประเทศไทยในปี 2560 มีรายงานเหตุการณ์การปิดกั้นหลายครั้ง โดยเฉพาะอย่างยิ่งในช่วงการประท้วงในปี 2563-64 ซึ่งรวมถึงเว็บไซต์ที่เกี่ยวข้องกับสิทธิมนุษยชนและสื่อเชิงข่าว ซึ่งส่งผลกระทบอย่างมากต่อเสรีภาพทางอินเทอร์เน็ตในประเทศ จำนวนโดเมนที่มีรายงานว่าถูกปิดกั้นบน OONI เพิ่มขึ้นจาก 13 โดเมนเป็น 119 โดเมน ซึ่งอาจเป็นเพราะวิธีการศึกษาได้รับการปรับปรุงและข้อมูลตรวจวัดที่เพิ่มขึ้น หมวดหมู่ที่มีโดเมนมากกว่า 10 โดเมนถูกปิดกั้น ได้แก่ เครื่องมือนิรนามและเครื่องมือหลบเลี่ยง การพนัน ปัญหาสิทธิมนุษยชน สื่อเชิงข่าว และสื่ออนาจาร

คาดว่าด้วยการศึกษานี้ ข้อมูลตรวจวัดจะเพิ่มขึ้นอย่างต่อเนื่องด้วยผู้เข้าร่วมเครือข่ายที่กว้างขึ้นและผู้ทดสอบที่มากขึ้น

การมีส่วนร่วมในการศึกษา

มีหลายวิธีในการมีส่วนร่วมตรวจวัด OONI

- การทดสอบ: คุณสามารถทำการทดสอบบนแพลตฟอร์มต่าง ๆ ทั้งบนมือถือ (iOS และ Android) และเครื่องคอมพิวเตอร์ตั้งโต๊ะ รวมถึงบนคอมมานด์ไลน์ (CLI) บนแพลตฟอร์ม Linux https://ooni.org/install/ โดเมนที่คุณทดสอบสามารถเลือกแบบสุ่มจากรายการทดสอบของ Citizen Lab หรือรายการทดสอบแบบกำหนดเองตามความต้องการของคุณ
- มีส่วนร่วมในรายการทดสอบ: คุณสามารถเพิ่มเติมรายการทดสอบบน GitHub https://github.com/citizenlab/test-lists หรือบน OONI https://test-lists.ooni.org/
- แปล OONI Probe เป็นภาษาท้องถิ่นของคุณ https://explore.transifex.com/otf/ooniprobe/
- เข้าร่วมการสนทนาในกลุ่ม OONI บน Slack https://slack.ooni.org/

กิตติกรรมประกาศ

เราขอขอบคุณทีมงาน OONI สำหรับการสนับสนุนต่าง ๆ ในการเขียนรายงานนี้

ภาคผนวก 1: อภิธานศัพท์

ดีเอ็นเอส DNS	DNS ย่อมาจาก “Domain Name System” หรือระบบชื่อโดเมน มันเทียบชื่อโดเมน (domain name) เข้ากับที่อยู่ไอพี (IP address) โดเมนหมายถึงชื่อที่มักจะมอบให้กับเว็บไซต์ (ในตอนที่มันถูกสร้างขึ้น) เพื่อที่มันจะได้ถูกเรียกและจดจำได้ง่ายขึ้น ตัวอย่างเช่น twitter.com เป็นโดเมนสำหรับเว็บไซต์ของทวิตเตอร์ อย่างไรก็ตาม คอมพิวเตอร์ไม่สามารถเชื่อมต่อกับบริการอินเทอร์เน็ตได้ทางชื่อโดเมน แต่ต้องใช้ที่อยู่ไอพี ซึ่งเป็นที่อยู่ดิจิทัลสำหรับบริการแต่ละบริการบนอินเทอร์เน็ต เช่นเดียวกับที่โลกกายภาพจำเป็นต้องมีที่อยู่สำหรับบ้าน เพื่อที่จะได้เดินทางไปหาได้ (แทนที่จะมีเพียงชื่อของบ้านเท่านั้น) ระบบชื่อโดเมน (Domain Name System - DNS) นั้นรับผิดชอบการแปลงชื่อโดเมนที่มนุษย์อ่านเข้าใจ (เช่น ooni.org) ให้เป็นที่อยู่ไอพีที่เป็นตัวเลข (ในกรณีนี้คือ 104.198.14.52) เพื่อให้คอมพิวเตอร์ของคุณสามารถเข้าถึงเว็บไซต์ที่ต้องการได้
เอชทีทีพี HTTP	Hypertext Transfer Protocol (HTTP) เป็นโปรโตคอลพื้นฐานที่เวิลด์ไวด์เว็บใช้เพื่อถ่ายโอนหรือแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต โปรโตคอล HTTP ช่วยให้สามารถสื่อสารระหว่างเครื่องลูกข่าย (ไคลเอนต์) และเครื่องให้บริการ (เซิร์ฟเวอร์) ได้ โดยมันช่วยจัดการคำขอของเครื่องลูกข่ายที่ต้องการเชื่อมต่อกับเซิร์ฟเวอร์ และจัดการคำตอบสนองของเซิร์ฟเวอร์ต่อคำขอของเครื่องลูกข่าย เว็บไซต์ทั้งหมดจะนำหน้าด้วย HTTP (หรือ HTTPS) (เช่น http://example.com/) ซึ่งทำให้คอมพิวเตอร์ของคุณ (ไคลเอนต์) สามารถร้องขอและรับเนื้อหาของเว็บไซต์ (ที่ตั้งอยู่บนเซิร์ฟเวอร์) ได้

	การส่งข้อมูลผ่านโปรโตคอล HTTP นั้นไม่มีการเข้ารหัสลับ
ฮิวริสติก heuristics	วิธีวิเคราะห์พฤติกรรมเพื่อช่วยยืนยันการปิดกั้นเพิ่มเติม นอกเหนือจากที่ตรวจพบตามร่องรอยลายนิ้วมือการปิดกั้นของ OONI ดูคำอธิบายโดยละเอียดเพิ่มเติมที่ภาคผนวก “ข้อมูลตรวจวัดที่ได้ยืนยัน เทียบกับ ฮิวริสติก”
ไอเอสพี ISP	ผู้ให้บริการอินเทอร์เน็ต (ISP) คือองค์กรที่ให้บริการเพื่อเข้าถึงและใช้งานอินเทอร์เน็ต ผู้ให้บริการอินเทอร์เน็ตอาจเป็นของรัฐ เป็นบริการเชิงพาณิชย์ มีชุมชนเป็นเจ้าของ ไม่แสวงหาผลกำไร หรืออาจเป็นของส่วนตัวของเอกชน โวดาโฟน เอทีแอนด์ที แอร์เทล เอไอเอส ทรู ทีโอที เป็นตัวอย่างของไอเอสพี
กล่องตัวกลาง middle boxes	มิดเดิลบ็อกซ์ หรือกล่องตัวกลาง คืออุปกรณ์เครือข่ายคอมพิวเตอร์ที่เปลี่ยนแปลง ตรวจดู กรอง หรือจัดการการจราจรในทางอื่น เพื่อวัตถุประสงค์นอกเหนือจากการส่งต่อแพ็กเก็ต ผู้ให้บริการอินเทอร์เน็ต (ISP) จำนวนมากทั่วโลกใช้มิดเดิลบ็อกซ์เพื่อปรับปรุงประสิทธิภาพเครือข่าย ให้ผู้ใช้เข้าถึงเว็บไซต์ได้เร็วขึ้น และเพื่อวัตถุประสงค์ด้านเครือข่ายอื่นอีกหลายประการ อย่างไรก็ตาม ในบางครั้งกล่องตัวกลางก็ถูกใช้เพื่อจำกัดเนื้อหาและ/หรือสอดส่องอินเทอร์เน็ต แอป OONI Probe มีการทดสอบสองรายการที่ออกแบบมาให้ตรวจวัดเครือข่ายเพื่อระบุการมีอยู่ของกล่องตัวกลาง
ทีซีพี TCP	Transmission Control Protocol (TCP) เป็นหนึ่งในโปรโตคอลหลักบนอินเทอร์เน็ต ในการเชื่อมต่อกับเว็บไซต์ คอมพิวเตอร์ของคุณต้องสร้างการเชื่อมต่อ TCP ไปยังที่อยู่ของเว็บไซต์นั้น

	TCP ทำงานอยู่บน Internet Protocol (IP) ซึ่งกำหนดวิธีระบุที่อยู่คอมพิวเตอร์บนอินเทอร์เน็ต เมื่อติดต่อกับเครื่องคอมพิวเตอร์ผ่านโปรโตคอล TCP คุณจะใช้ที่อยู่ไอพีคู่กับหมายเลขพอร์ต ซึ่งมีลักษณะดังนี้: 10.20.1.1:8080 ข้อแตกต่างที่สำคัญระหว่าง TCP และ (อีกโปรโตคอลที่ได้รับความนิยมมาก ชื่อ) UDP คือ TCP มีแนวคิดเกี่ยวกับ “การเชื่อมต่อ” ทำให้เป็นโปรโตคอลรับส่งที่ “วางใจได้”
ทีแอลเอส TLS	Transport Layer Security (TLS) – หรือถูกอ้างถึงเช่นกันด้วยชื่อ “SSL” – เป็นโปรโตคอลการเข้ารหัสลับที่อนุญาตให้คุณสามารถคงการเชื่อมต่อที่ถูกเข้ารหัสลับและปลอดภัยระหว่างคอมพิวเตอร์ของคุณและบริการอินเทอร์เน็ต เมื่อคุณเชื่อมต่อกับเว็บไซต์ผ่าน TLS ที่อยู่ของเว็บไซต์จะเริ่มต้นด้วย HTTPS (เช่น https://www.facebook.com/) แทนที่จะเป็น HTTP

อภิธานศัพท์ที่เกี่ยวกับ OONI โดยละเอียด สามารถดูได้ที่: https://ooni.org/support/glossary/

ภาคผนวก 2: วิธีการ

ข้อมูล

ข้อมูลที่คำนวณตามฮิวริสติกสำหรับรายงานชิ้นนี้ สามารถดาวน์โหลดได้ที่: https://github.com/Sinar/imap-data ขณะที่ข้อมูลที่รวมกันแล้วสามารถดาวน์โหลดได้จาก OONI Explorer: https://explorer.ooni.org/

ขอบเขตการศึกษา

รายงาน iMAP State of Internet Censorship Country Report ครอบคลุมผลตรวจวัดเครือข่ายที่รวบรวมผ่าน Open Observatory of Network Interference (OONI) แอป OONI Probe[4] ที่ตรวจวัดการปิดกั้นเว็บไซต์ แอปส่งข้อความ เครื่องมือหลบเลี่ยง และการปลอมแปลงเครือข่าย ข้อค้นพบนั้นเน้นไปที่เว็บไซต์แอปส่งข้อความ และเครื่องมือหลบเลี่ยง ที่ได้รับการยืนยันว่าถูกปิดกั้น, ASN ที่ตรวจพบการเซ็นเซอร์, และวิธีการแทรกแซงรบกวนเครือข่าย รายงานยังให้บริบทภูมิหลังเกี่ยวกับภูมิทัศน์ของเครือข่าย พร้อมกับประเด็นและเหตุการณ์ทางกฎหมาย สังคม และการเมืองล่าสุด ซึ่งอาจส่งผลต่อการดำเนินการจำกัดอินเทอร์เน็ตในประเทศ

ในแง่ของลำดับเวลา รายงาน iMAP ฉบับแรกนี้ครอบคลุมการตรวจวัดในช่วงหกเดือนตั้งแต่ 1 มกราคม 2565 ถึง 30 มิถุนายน 2565 ประเทศที่ครอบคลุมในรอบนี้ได้แก่ กัมพูชา ไทย ฟิลิปปินส์ มาเลเซีย เมียนมา เวียดนาม อินโดนีเซีย และฮ่องกง ส่วนอินเดียจะรวมอยู่ในการรายงานรอบถัดไป

ข้อมูลตรวจวัดเครือข่ายถูกรวบรวมอย่างไร?

ข้อมูลตรวจวัดเครือข่ายถูกรวบรวมผ่านการใช้แอป OONI Probe ซึ่งเป็นเครื่องมือซอฟต์แวร์เสรีที่พัฒนาโดย Open Observatory of Network Interference (OONI)[5] หากต้องการรู้เพิ่มเติมเกี่ยวว่าการทดสอบของ OONI Probe นั้นทำงานอย่างไร โปรดไปที่ https://ooni.org/nettest/

[4] https://ooni.org/install/
[5] https://ooni.org/

นักวิจัยประจำประเทศของ iMAP และอาสาสมัครนิรนามเรียกใช้แอป OONI Probe เพื่อตรวจสอบการเข้าถึงเว็บไซต์ในรายการทดสอบของ Citizen Lab [6] นักวิจัยประจำประเทศของ iMAP ทบทวนรายการทดสอบที่ทำขึ้นสำหรับประเทศนั้นอย่างแข็งขัน เพื่อให้แน่ใจว่าได้รวมเว็บไซต์ที่เป็นปัจจุบัน และเว็บไซต์ที่ขึ้นกับบริบทได้รับการจัดหมวดหมู่อย่างเหมาะสม ทั้งนี้โดยการปรึกษาหารือกับชุมชนท้องถิ่นและพันธมิตรเครือข่ายสิทธิดิจิทัล เราใช้แนวทางของ Netalitica [7] ในการทบทวนรายการทดสอบของแต่ละประเทศ

เป็นเรื่องสำคัญที่ต้องระลึกว่า ข้อค้นพบดังกล่าวใช้ได้กับเว็บไซต์ที่ได้รับการตรวจสอบเท่านั้น และไม่ได้สะท้อนถึงกรณีการจำกัดอินเทอร์เน็ตทั้งหมดที่อาจเกิดขึ้นในระหว่างเวลาของการทดสอบ

ข้อมูลตรวจวัดเครือข่ายถูกวิเคราะห์อย่างไร?

OONI ประมวลผลข้อมูลชนิดดังต่อไปนี้ ผ่านท่อลำเลียงข้อมูล (data pipeline)[8] ของ OONI เอง:

รหัสประเทศ

ตามค่าปริยาย OONI จะเก็บรวบรวมรหัสที่ระบุถึงประเทศที่ผู้ใช้ใช้งานการทดสอบบน OONI Probe รหัสนี้ได้มาโดยอัตโนมัติด้วยการค้นที่อยู่ไอพีของผู้ใช้จากฐานข้อมูล ASN[9] ซึ่งใช้ข้อมูลรูปแบบเดียวกับฐานข้อมูล MaxMind GeoIP[10]

หมายเลขระบบอิสระ (Autonomous System Number - ASN)

ตามค่าปริยาย OONI จะรวบรวมหมายเลขระบบอิสระ (Autonomous System Number - ASN) ของเครือข่ายที่ใช้เพื่อเรียกให้แอป OONI Probe ทำงาน ซึ่งจะเปิดเผยผู้ให้บริการเครือข่ายของผู้ใช้

วันที่และเวลาตรวจวัด

ตามค่าปริยาย OONI จะรวบรวมเวลาและวันที่ที่การทดสอบถูกเรียกให้ทำงาน เพื่อดูว่าเกิดการแทรกแซงเครือข่ายขึ้นเมื่อใด และเพื่อให้สามารถเปรียบเทียบข้ามเวลาได้ เวลาสากลเชิงพิกัด (UTC) ถูกใช้เป็นเขต

---

[6] https://github.com/citizenlab/test-lists/tree/master/lists

[7] https://netalitica.com/wp-content/uploads/2021/10/Guideline-for-Test-List-Researchers-V7.pdf

[8] https://github.com/ooni/pipeline

[9] https://github.com/ooni/asn-db-generator

[10] https://www.maxmind.com/

เวลามาตรฐานในข้อมูลเวลาและวันที่ นอกจากนี้ โดยค่าปริยาย แผนภูมิที่สร้างขึ้นบน OONI MAT จะไม่รวมข้อมูลตรวจวัดในวันสุดท้าย

หมวดหมู่

หมวดหมู่เว็บไซต์ 32 อย่างดังต่อไปนี้ มาจากรายการทดสอบของ Citizen Lab: https://github.com/citizenlab/test-lists ไม่ใช่ทุกเว็บไซต์ที่ทดสอบโดย OONI นั้นจะอยู่ในรายการนี้ เว็บไซต์เหล่านั้นจะปรากฏเป็นหมวดหมู่ “unclassified”

#	หมวดหมู่	รหัส	คำอธิบาย
1	แอลกอฮอล์และยาเสพติด Alcohol & Drugs	ALDR	เว็บไซต์ที่ทำขึ้นโดยเฉพาะเพื่อเสนอวิธีการเสพ ของใช้เกี่ยวกับการเสพ และการขายยาเสพติดและแอลกอฮอล์ ทั้งนี้ไม่เกี่ยวกับว่ามันถูกกฎหมายท้องถิ่นหรือไม่
2	ศาสนา Religion	REL	เว็บไซต์ที่ทำขึ้นโดยเฉพาะเพื่อพูดคุยเรื่องศาสนา ทั้งในทางสนับสนุนและวิพากษ์วิจารณ์ รวมทั้งการสนทนาของกลุ่มศาสนากลุ่มน้อย
3	สื่ออนาจาร Pornography	PORN	สื่ออนาจารทั้งฮาร์ดคอร์และซอฟต์คอร์
4	เครื่องแต่งกายเร้าใจ Provocative Attire	PROV	เว็บไซต์ที่แสดงเครื่องแต่งกายที่เร้าใจและจัดแสดงผู้หญิงในลักษณะยั่วยวนทางเพศ ใส่เสื้อผ้าน้อยชิ้น
5	การวิพากษ์วิจารณ์การเมือง Political Criticism	POLR	เนื้อหาที่นำเสนอมุมมองทางการเมืองเชิงวิพากษ์ รวมถึงนักเขียนและบล็อกเกอร์ที่วิพากษ์วิจารณ์ ตลอดจนองค์กรทางการเมืองฝ่ายค้าน รวมถึงเนื้อหาสนับสนุนประชาธิปไตย เนื้อหาต่อต้านการทุจริต ตลอดจนเนื้อหาที่เรียกร้องให้เปลี่ยนแปลงผู้นำ ปัญหาธรรมาภิบาล การปฏิรูปกฎหมาย เป็นต้น

#	หมวดหมู่	รหัส	คำอธิบาย
6	ประเด็นสิทธิมนุษยชน Human Rights Issues	HUMR	เว็บไซต์ที่อุทิศให้กับการอภิปรายประเด็นสิทธิมนุษยชนในรูปแบบต่างๆ รวมถึงสิทธิสตรีและสิทธิของชนกลุ่มน้อย
7	สิ่งแวดล้อม Environment	ENV	มลภาวะ สนธิสัญญาสิ่งแวดล้อมระหว่างประเทศ การตัดไม้ทำลายป่า ความยุติธรรมด้านสิ่งแวดล้อม ภัยพิบัติ ฯลฯ
8	การก่อการร้ายและกองกำลัง Terrorism and Militants	MILX	เว็บไซต์ที่รณรงค์การก่อการร้าย กองกำลังที่ใช้ความรุนแรงหรือขบวนการแบ่งแยกดินแดน
9	ประทุษวาจา Hate Speech	HATE	เนื้อหาที่ดูหมิ่นบุคคลหรือกลุ่มบุคคลเฉพาะเจาะจง บนฐานของเชื้อชาติ เพศ เพศวิถี หรือคุณสมบัติอื่น
10	สื่อเชิงข่าว News Media	NEWS	หมวดหมู่นี้รวมช่องข่าวใหญ่ (เช่น บีบีซี ซีเอ็นเอ็น) เช่นเดียวกับสื่อท้องถิ่น และสื่ออิสระ
11	เพศศึกษา Sex Education	XED	รวมถึงการคุมกำเนิด การงดเว้นการมีเพศสัมพันธ์ โรคติดต่อทางเพศสัมพันธ์ (STD) เพศวิถีที่เป็นสุข การตั้งครรภ์ในวัยรุ่น การป้องกันการข่มขืน การทำแท้ง สิทธิทางเพศ และบริการสุขภาพทางเพศ
12	สาธารณสุข Public Health	PUBH	เอชไอวี ซาร์ส หวัดนก ศูนย์ควบคุมโรค องค์การอนามัยโลก ฯลฯ
13	การพนัน Gambling	GMB	เว็บไซต์พนันออนไลน์ รวมถึงเกมคาสิโนที่มีการใช้เงินจริง การแทงพนันกีฬา ฯลฯ
14	เครื่องมือนิรนามและเครื่องมือหลบเลี่ยง Anonymization and circumvention tools	ANON	เว็บไซต์ที่เปิดให้เข้าถึงเครื่องมือสำหรับการปกปิดตัวตน การหลบเลี่ยงการปิดกั้น พร็อกซี และการเข้ารหัสลับ

#	หมวดหมู่	รหัส	คำอธิบาย
15	การหาคู่ออนไลน์ Online Dating	DATE	บริการหาคู่ออนไลน์ที่ใช้เพื่อนัดเจอคน แสดงโปรไฟล์ แชต พูดคุย ฯลฯ
16	เครือข่ายสังคม Social Networking	GRP	เครื่องมือและแพลตฟอร์มเครือข่ายสังคม
17	แอลจีบีที LGBT	LGBT	ประเด็นเกย์-เลสเบียน-ไบเซ็กชวล-ทรานส์เจนเดอร์ (ไม่รวมภาพอนาจาร)
18	แบ่งปันแฟ้ม File-sharing	FILE	เว็บไซต์และเครื่องมือที่ใช้เพื่อแบ่งปันแฟ้ม รวมถึงที่จัดเก็บแฟ้มแบบคลาวด์ ทอร์เรนต์ และเครื่องมือแบ่งปันแฟ้มแบบ P2P
19	เครื่องมือเจาะระบบ Hacking Tools	HACK	เว็บไซต์ที่เน้นเนื้อหาเกี่ยวกับความปลอดภัยทางคอมพิวเตอร์ รวมถึงข่าวสารและเครื่องมือ รวมทั้งเนื้อหาที่มีเจตนาร้ายและไม่มีเจตนาร้าย
20	เครื่องมือสื่อสาร Communication Tools	COMT	เว็บไซต์และเครื่องมือสำหรับการสื่อสารระหว่างบุคคลและในกลุ่ม รวมถึงอีเมลทางเว็บ โทรศัพท์อินเทอร์เน็ต (VoIP) บริการข้อความด่วน แชต และแอปส่งข้อความ
21	แบ่งปันสื่อ Media sharing	MMED	แพลตฟอร์มแบ่งปันวิดีโด เสียง และภาพ
22	โฮสติ้งและแพลตฟอร์มบล็อก Hosting and Blogging Platforms	HOST	บริการรับฝากเว็บ แพลตฟอร์มเขียนบล็อก (blogging) และแพลตฟอร์มตีพิมพ์เนื้อหาออนไลน์อื่น
23	เครื่องมือค้นหา Search Engines	SRCH	เครื่องมือค้นหาและเว็บท่า

#	หมวดหมู่	รหัส	คำอธิบาย
24	เกม Gaming	GAME	เกมออนไลน์และแพลตฟอร์มสำหรับเล่นเกม แต่ไม่รวมเว็บไซต์พนัน
25	วัฒนธรรม Culture	CULTR	เนื้อหาเกี่ยวกับความบันเทิง ประวัติศาสตร์ วรรณกรรม ดนตรี หนังสือ การเสียดสีและอารมณ์ขัน
26	เศรษฐกิจ Economics	ECON	เนื้อหา หน่วยงาน และโอกาสเข้าถึงเงินทุน ในหัวข้อการพัฒนาเศรษฐกิจและความยากจนโดยทั่วไป
27	รัฐบาล Government	GOVT	เว็บไซต์ที่ดำเนินงานโดยรัฐบาล รวมถึงเว็บไซต์ของกองทัพ
28	การค้าอิเล็กทรอนิกส์ E-commerce	COMM	เว็บไซต์สำหรับสินค้าและบริการเชิงพาณิชย์
29	เนื้อหาควบคุม Control content	CTRL	เนื้อหาทั่วไปที่ไม่มีประเด็นให้ปิดกั้น ใช้เพื่อเป็นตัวแปรควบคุม
30	องค์การระหว่างประเทศ Intergovernmental Organizations	IGO	เว็บไซต์ขององค์การระหว่างประเทศ เช่น สหประชาชาติ
31	เนื้อหาเบ็ดเตล็ด Miscellaneous content	MISC	เว็บไซต์ที่ไม่ถูกจัดอยู่ในหมวดหมู่ใดเลย

ที่อยู่ IP และข้อมูลอื่น ๆ

OONI ไม่เจตนารวบรวมหรือจัดเก็บที่อยู่ไอพีของผู้ใช้ OONI มีมาตรการเพื่อลบพวกมันออกจากข้อมูลตรวจวัดที่ถูกเก็บรวบรวมมา เพื่อปกป้องผู้ใช้จากความเสี่ยงที่อาจเกิดขึ้น[11] อย่างไรก็ตาม อาจมีบางกรณีที่ที่อยู่ไอพีของผู้ใช้และข้อมูลอื่นๆ ที่อาจระบุตัวตนได้นั้นถูกรวบรวมโดยไม่ได้ตั้งใจ หากข้อมูลดังกล่าวรวมอยู่ในส่วนหัว HTTP หรือข้อมูลเมทาดาทาอื่นๆ ของข้อมูลตรวจวัด ตัวอย่างเช่น กรณีนี้อาจเกิดขึ้นได้หากเว็บไซต์ที่ถูกทดสอบมีเทคโนโลยีการติดตามหรือเนื้อหาที่ปรับเปลี่ยนตามตำแหน่งเครือข่ายของผู้ใช้

ข้อมูลตรวจวัดเครือข่าย

ชนิดของข้อมูลตรวจวัดเครือข่ายที่ OONI รวบรวมนั้นขึ้นอยู่กับชนิดของการทดสอบที่เรียกใช้ ข้อมูลจำเพาะเกี่ยวกับการทดสอบ OONI แต่ละอย่าง สามารถดูได้ที่ที่เก็บข้อมูล git[12] ของ OONI รายละเอียดว่าข้อมูลตรวจวัดเครือข่ายที่รวบรวมมานั้นบอกอะไร สามารถดูได้ผ่าน OONI Explorer หรือผ่าน API ข้อมูลตรวจวัดของ OONI[13]

เพื่อให้รู้ถึงความหมายจากข้อมูลตรวจวัดที่ได้รวบรวมมา OONI จะประมวลผลข้อมูลชนิดที่กล่าวถึงข้างต้นเพื่อตอบคำถามต่อไปนี้:

- มีการทดสอบ OONI ชนิดใดบ้าง?
- การทดสอบเหล่านั้นดำเนินการในประเทศใดบ้าง?
- การทดสอบเหล่านั้นดำเนินการในเครือข่ายใด?
- การทดสอบเหล่านั้นดำเนินการเมื่อใด?
- การแทรกแซงเครือข่ายที่เกิดขึ้นเป็นชนิดใด?
- การแทรกแซงเครือข่ายเกิดขึ้นในประเทศใดบ้าง?
- การแทรกแซงเครือข่ายเกิดขึ้นในเครือข่ายใด?
- การแทรกแซงเครือข่ายเกิดขึ้นเมื่อใด?
- การแทรกแซงเครือข่ายเกิดขึ้นได้อย่างไร?

[11] https://ooni.org/about/risks/
[12] https://github.com/ooni/spec
[13] https://api.ooni.io/

ท่อลำเลียงข้อมูลของ OONI ถูกออกแบบมาเพื่อตอบคำถามดังกล่าว โดยประมวลผลข้อมูลตรวจวัดเครือข่าย เพื่อให้สามารถทำสิ่งเหล่านี้:

- ระบุแหล่งที่มาของข้อมูลตรวจวัดไปยังประเทศใดประเทศหนึ่งโดยเจาะจง
- ระบุแหล่งที่มาของข้อมูลตรวจวัดไปยังเครือข่ายใดเครือข่ายหนึ่งภายในประเทศหนึ่งโดยเจาะจง
- แยกแยะข้อมูลตรวจวัดตามการทดสอบที่เจาะจง ซึ่งถูกเรียกใช้ในการรวบรวมข้อมูล
- แยกแยะความแตกต่างระหว่างข้อมูลตรวจวัด "ปกติ" และ "ผิดปกติ" (อย่างหลังบ่งชี้ว่ามีแนวโน้มว่าจะมีการปลอมแปลงเครือข่ายในบางรูปแบบ)
- ระบุชนิดของการแทรกแซงเครือข่าย ตามชุดของฮิวริสติกสำหรับการดัดแปลง DNS, การปิดกั้น TCP/IP และการปิดกั้น HTTP
- ระบุบหน้าปิดกั้น (block page) ตามชุดของฮิวริสติกสำหรับการปิดกั้น HTTP
- ระบุการมีอยู่ของ “กล่องตัวกลาง” ภายในเครือข่ายที่ทดสอบ

อ้างอิงจาก OONI ผลบวกปลอม (false positive) อาจเกิดขึ้นกับข้อมูลที่ถูกประมวลแล้วด้วยสาเหตุหลายประการ DNS resolver (ดำเนินการโดยกูเกิล หรือผู้ให้บริการอินเทอร์เน็ตท้องถิ่น) มักจะให้ที่อยู่ไอพีที่ใกล้ที่ตั้งทางภูมิศาสตร์ของผู้ใช้ที่สุด แม้สิ่งนี้อาจดูเหมือนเป็นกรณีของการดัดแปลง DNS แต่จริง ๆ แล้วทำด้วยความตั้งใจที่จะให้ผู้ใช้เข้าถึงเว็บไซต์ได้เร็วขึ้น ในทำนองเดียวกัน ผลบวกปลอมอาจเกิดขึ้นเมื่อเว็บไซต์ที่ถูกทดสอบแสดงเนื้อหาที่แตกต่างกันโดยขึ้นอยู่กับประเทศที่ผู้ใช้เชื่อมต่อ หรือในกรณีที่เว็บไซต์ส่งความผิดพลาดกลับมา แม้มันจะไม่ได้ถูกปลอมแปลงเลยก็ตาม

นอกจากนี้ ข้อมูลตรวจวัดที่ระบุการปิดกั้น HTTP หรือ TCP/IP อาจเกิดจากความล้มเหลวชั่วคราวของ HTTP หรือ TCP/IP และอาจไม่ใช่สัญญาณที่แน่ชัดของการแทรกแซงเครือข่าย ดังนั้นจึงเป็นสิ่งสำคัญในการทดสอบเว็บไซต์ชุดเดียวกันในช่วงเวลาต่างๆ และตรวจสอบข้อมูลยันข้ามกัน ก่อนที่จะสรุปว่าเว็บไซต์ถูกปิดกั้นจริงหรือไม่

เนื่องจากหน้าปิดกั้น (block page) นั้นแตกต่างกันไปในแต่ละประเทศ และบางครั้งแม้แต่จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง การระบุหน้าปิดกั้นให้ถูกต้องนั้นจึงค่อนข้างท้าทาย OONI ใช้ชุดของการวิเคราะห์พฤติกรรม (ฮิวริสติก) เพื่อพยายามคาดเดาว่าหน้าเว็บที่กำลังพิจารณานั้นแตกต่างจากตัวอย่างที่รู้จักอยู่ก่อนหรือไม่ แต่การวิเคราะห์พฤติกรรมเหล่านี้มักมากับผลบวกปลอม ด้วยเหตุนี้ OONI จึงจะระบุว่ามีการปิดกั้นที่ได้ยืนยันแล้วก็ต่อเมื่อตรวจพบหน้าปิดกั้น
จากข้อมูลตรวจวัดเครือข่ายที่รวบรวมได้มากขึ้น OONI ยังคงพัฒนาฮิวริสติกสำหรับการวิเคราะห์ข้อมูลอย่างต่อเนื่อง โดยพิจารณาจากความแม่นยำของการระบุเหตุการณ์การเซ็นเซอร์

รายการทดสอบที่เจาะจงสำหรับแต่ละประเทศ ซึ่งมีเว็บไซต์ที่ได้รับการยืนยันแล้วว่าถูกปิดกั้นใน กัมพูชา ไทย ฟิลิปปินส์ มาเลเซีย เมียนมา เวียดนาม อินโดนีเซีย และฮ่องกง สามารถดูได้ที่: https://github.com/citizenlab/test-lists

ข้อมูลตรวจวัดที่ได้ยืนยัน เทียบกับ ฮิวริสติก

ข้อมูลตรวจวัด OONI ที่ได้รับการยืนยันนั้น ดูจากหน้าปิดกั้น (block page) ซึ่งลายนิ้วมือถูกบันทึกไว้ที่ https://github.com/ooni/blocking-fingerprints

จากนั้นฮิวริสติกด้านล่างจะถูกใช้กับข้อมูลตรวจวัดดิบจากทุกประเทศภายใต้โครงการ iMAP เพื่อยืนยันการปิดกั้นเพิ่มเติม

ในชั้นแรก ที่อยู่ไอพีที่มีมากกว่า 10 โดเมนจะถูกระบุ จากนั้น ที่อยู่ไอพีแต่ละรายการจะถูกตรวจสอบกับคำถามต่อไปนี้:

<table>
<tr><td colspan="5">IP ดังกล่าวชี้ไปยังหน้าปิดกั้น (block page) ของรัฐบาลหรือไม่?</td></tr>
<tr><td>ใช่</td><td colspan="4">ไม่ใช่ - หมดเวลาเรียกดูหน้า หรือแสดงหน้าของ Content Delivery Network (CDN)</td></tr>
<tr><td>⬇</td><td colspan="4">⬇</td></tr>
<tr><td>การปิดกั้นที่ได้ยืนยัน</td><td colspan="4">เมื่อดูข้อมูลจาก whois เราได้ข้อมูลอะไรเกี่ยวกับ IP นี้?</td></tr>
<tr><td rowspan="6"></td><td>ISP ท้องถิ่น</td><td colspan="3">CDN / Private IP</td></tr>
<tr><td>⬇</td><td colspan="3">⬇</td></tr>
<tr><td>การปิดกั้นที่ได้ยืนยัน</td><td colspan="3">เราได้รับใบรับรอง TLS ที่ถูกต้องของโดเมนที่กำลังตรวจสอบอยู่หรือไม่ หลังจากที่ได้ทำ TLS handshake และระบุ SNI?</td></tr>
<tr><td rowspan="3"></td><td>ใช่</td><td>ไม่ใช่ - พบลายนิ้วมือของการปิดกั้น</td><td>ไม่ใช่ - หมดเวลา</td></tr>
<tr><td>⬇</td><td>⬇</td><td>⬇</td></tr>
<tr><td>ผลบวกปลอม</td><td>การปิดกั้นที่ได้ยืนยัน</td><td>ตัวอย่างข้อมูลตรวจวัดจะถูกวิเคราะห์บน OONI Explorer</td></tr>
</table>

เมื่อตัดสินได้ว่ามีการปิดกั้น โดเมนใด ๆ ที่เปลี่ยนทางไปหาที่อยู่ไอพีเหล่านี้จะถูกทำเครื่องหมายเป็น ‘dns.confirmed’

ในชั้นที่สอง หัวเรื่องและตัวเนื้อความของ HTTP ได้ถูกวิเคราะห์เพื่อระบุหาหน้าปิดกั้น (block page) ตัวอย่างนี้แสดงให้เห็นว่า HTTP ส่งคืนข้อความ ‘The URL has been blocked as per the instructions of the DoT in compliance to the orders of Court of Law’ (“URL ดังกล่าวถูกปิดกั้นโดยทำตามคำแนะนำของกระทรวงโทรคมนาคม เพื่อทำตามคำสั่งของศาลยุติธรรม”)[14] โดเมนใด ๆ ที่เปลี่ยนเส้นทางไปหัวเรื่องและตัวเนื้อความ HTTP เหล่านี้จะถูกทำเครื่องหมายเป็น ‘http.confirmed’

ด้วยวิธีการนี้ ทำให้ผลบวกปลอม (false positive) ถูกกำจัดออก และการปิดกั้นได้รับการยืนยันมากขึ้น รวมถึงในประเทศเช่น กัมพูชา เวียดนาม และฟิลิปปินส์ ซึ่งไม่มีร่องรอยการปิดกั้นที่ได้ยืนยันบน OONI

ในกรณีของฮ่องกง ผลของฮิวริสติกแสดงให้เห็นการเซ็นเซอร์จากภายนอกประเทศแทนที่จะเป็นการเซ็นเซอร์จากภายในท้องถิ่น เมื่อเป็นเช่นนั้น นักวิจัยท้องถิ่นจึงวิเคราะห์ข้อมูลตรวจวัด OONI ด้วยมือ เพื่อระบุการปิดกั้นที่ได้ยืนยัน โดเมนที่ถูกระบุนั้นอยู่บนฐานของการเชื่อมต่อที่พยายามจนหมดเวลา (timed-out)

[14] https://explorer.ooni.org/m/20220411130348.256418_IN_webconnectivity_56d89076f8fb71ac