

กลุ่มก่อการร้าย

กับแหล่งระดมทุนยุคศตวรรษที่ ๒๑ (Terrorist Use of Cryptocurrencies)

พันเอก พิศาล อมรรัตนานภาพ
นายทหารปฏิบัติการกรมข่าวทหาร

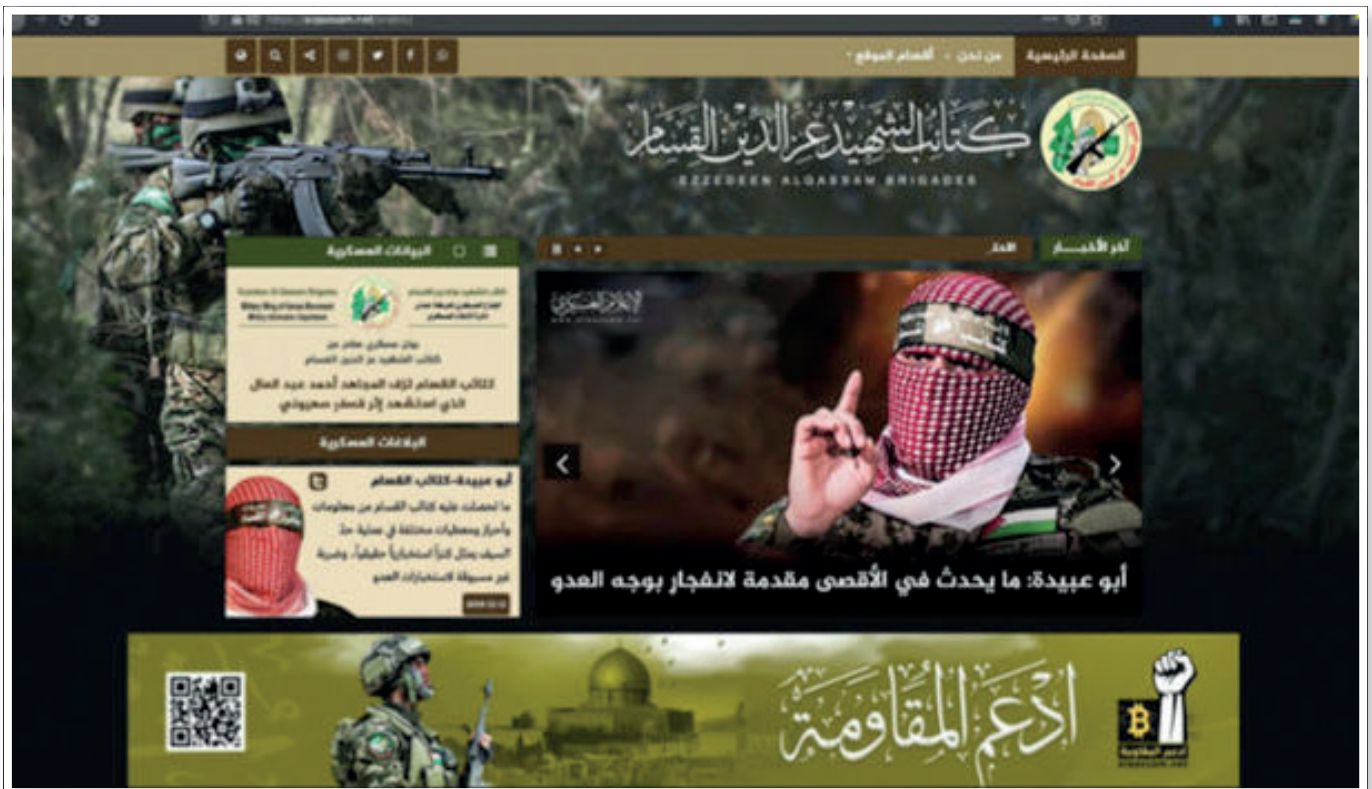


กองพลน้อยอัลกอซซัม (al-Qassam) ภายใต้การบังคับบัญชาของกลุ่มก่อการร้ายฮามาส (Hamas)
ที่มา < <https://www.timesofisrael.com/senior-idf-commander-says-hamas-has-7000-rockets-dozens-of-drones/>>

คำถาม : กลุ่มก่อการร้ายมีการระดมทุนผ่าน blockchain/สกุลเงินดิจิทัล หรือไม่

จากเอกสารงานวิจัยที่เกี่ยวข้องกับสงครามไซเบอร์ (Cyber Warfare) ซึ่งเขียนโดย Mazanec, B. & Whyte, C. (2019), เรื่อง Understanding Cyber Warfare: Politics, Policy and Strategy ได้นิยามคำว่า การก่อการร้ายทางไซเบอร์ หรือ Cyberterrorism หมายถึง “A term used to describe either the use of computer attack for terroristic coercion or the use of the internet to upgrade all parts of the terrorist enterprise.” โดยสามารถสรุปใจความได้ว่า การก่อการร้ายทางไซเบอร์

คือการใช้สงครามคอมพิวเตอร์เชิงรุก (Computer Network Attack: CNA) และ/หรือการใช้ระบบอินเทอร์เน็ต (ดิจิทัล) เพื่อการยกระดับขีดความสามารถขององค์กรฯ ในห้วง ๕ ปีที่ผ่านมาผู้เขียนมักจะกล่าวถึงกลุ่มก่อการร้าย (Terrorist Actor) และตัวแทนรัฐที่ใช้วิธีการก่อการร้าย (Proxy) ซึ่งทั้ง ๒ กลุ่มได้ยกระดับตนเองด้วยการยื่นตระหนักรู้บนคลื่นของการเปลี่ยนแปลงทางเทคโนโลยี ทั้งการใช้การโจมตีต่อระบบคอมพิวเตอร์ ณ โครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) และแบบยิกระบบคอมพิวเตอร์เพื่อเรียกค่าไถ่ด้วย Ransomware รวมถึงการโจมตีระบบเพื่อมิให้ปฏิบัติงานได้อีกต่อไป นอกเหนือไปจากการได้มาซึ่งอาวุธนั้น ยังมีการใช้ช่องทาง



กองพลน้อยอัลกอซซิม (al-Qassam) ภายใต้การบังคับบัญชาของกลุ่มก่อการร้ายฮามาส (Hamas) ประกาศรับการสนับสนุนเงินทุนผ่าน Bitcoin ที่มา กระทรวงยุติธรรมสหรัฐฯ < <https://www.nbcnews.com/tech/tech-news/feds-announce-largest-seizure-cryptocurrency-connected-terrorism-n1236610> >

หลบลีกการตรวจจับจำพวก Deep Web และ Dark Web โดย Deep Web นั้นหมายถึง เว็บไซต์ที่ไม่สามารถค้นเจอได้จากการค้นผ่าน Search Engine สำหรับ Dark Web เป็นเว็บไซต์ที่อยู่บนโลกอินเทอร์เน็ต แต่วิธีการเข้าไปเพื่อเปิดเว็บไซต์เหล่านั้นจะแตกต่างไปจากการใช้งานเว็บไซต์ปกติ โดยสามารถไม่ระบุตัวตนได้ และไม่สามารถสืบค้นต่อ หรือสืบอัตลักษณ์เฉพาะบุคคลของผู้ใช้งานได้ ทำให้เป็นที่รวมแหล่งข้อมูลผิดกฎหมาย จึงเป็นที่ประจักษ์แล้วว่าเหตุการณ์ได้เกิดขึ้นตามคาดการณ์ ทั้งนี้ยังคงเหลืออีกประเด็นที่ยังมิได้กล่าวถึงคือการระดมทุนผ่านโลกดิจิทัลและการใช้เงินสกุลดิจิทัลเพื่อทำการซื้อขายอาวุธผ่าน Deep Web/Dark Web ซึ่งเหตุผลที่น่าสนใจเนื่องจากในการทำสงครามทั้งตามแบบและสงครามนอกแบบ การก่อการร้ายนั้น การปฏิบัติการกิจก่อเหตุรุนแรงจะต้องได้รับการสนับสนุนทางการเงินซึ่งในศตวรรษที่ ๒๑ การเคลื่อนไหวทางการเงินนั้นส่วนใหญ่ดำเนินการบนโลกดิจิทัลโดยบทความนี้จะศึกษาว่ากลุ่มก่อการร้ายฯ ได้มีการเข้าถึงการระดมทุนผ่านแหล่งเงินสกุลดิจิทัลหรือยัง ทั้งนี้คาดหวังว่าหน่วยงานด้านความมั่นคงจะได้ทำการยกระดับเพื่อการป้องกันต่อไป

หากมองเพียงผิวเผินอาจมองว่าสมาชิกกลุ่มก่อการร้ายและผู้ให้การสนับสนุนการก่อเหตุรุนแรงอาจเป็นบุคคลที่ไม่ทันสมัย แต่แท้จริงแล้วบุคคลเหล่านี้ได้มีการพัฒนาตนเองให้ทันสมัยของการเปลี่ยนด้านเทคโนโลยีได้อย่างเหมาะสมและทันสมัย ซึ่งในการเตรียม

ทำสงครามผู้นำ/แกนนำเริ่มจากการระดมสรรพกำลังและระดมทุน ซึ่งในฐานะนักข่าวที่ทำการตรวจสอบอย่างใกล้ชิดพบว่า นับตั้งแต่ศตวรรษที่ ๒๑ กลุ่มก่อการร้าย อาทิ กลุ่มไอซิส (ISIS) ได้มีการระดมสรรพกำลังและระดมทุนผ่าน Platform บนสื่อสังคมออนไลน์มาอย่างต่อเนื่อง อาทิ เหตุการณ์เมื่อปี ๒๐๑๗ แกนนำไอซิสได้เรียกให้บรรดานักรบต่างชาติจากทั่วภูมิภาคทั่วโลก (Foreign Terrorist Fighters: FTFs) เข้ายึดพื้นที่มินดาเนา (Mindanao Attack 2017 (McKirdy & Watson 2017) โดยการระดมทุนในการก่อเหตุนี้ไม่ได้ขึ้นอยู่กับการโอนเงินผ่านระบบธนาคารตามรูปแบบเดิมที่สามารถติดตามเส้นทางการเงินได้ง่าย หรืออีกเหตุการณ์หนึ่งเมื่อปี ๒๐๑๕ มีเยาวชนสหรัฐฯ สร้าง blog “titled: Bitcoin and the Charity of Jihad” เพื่อระดมทุนในการสนับสนุนภารกิจของกลุ่ม





เมื่อ ‘ผู้ก่อการร้าย’ ระดมทุน ‘สกุลเงินดิจิทัล’

ก่อการร้ายไอซิสและยังปรากฏอีก ๓ คดี ที่มีผู้ให้การสนับสนุนเงินให้กับกลุ่มก่อการร้ายต่าง ๆ อาทิ หน่วยข่าวกรองอิสราเอล ออกแถลงความกังวลต่อการติดตามแหล่งที่มาของเงินสนับสนุน กองพลน้อยอัลกอซซัม (al-Qassam) ภายใต้การบังคับบัญชาของกลุ่มก่อการร้ายฮามาส (Hamas) ที่ได้ออกแบบ Software ลักษณะกระเป๋าสตางค์ (wallet) ตั้งแต่ปี ๒๐๑๙ เพื่อรับบริจาคผ่านเงินสกุลดิจิทัลและนำไปจัดหาอาวุธยุทโธปกรณ์จาก Dark Web จากการวิเคราะห์พบว่ากลุ่มก่อการร้ายจะต้องเข้ามาสู่โลกไซเบอร์มากยิ่งขึ้น

อันเนื่องมาจากเป็นระบบการเงินที่ไม่มีตัวกลางในการควบคุม โดยหน่วยงานทางการเงินหรือธนาคารใด ๆ เหมือนสกุลเงินแบบดั้งเดิม (decentralize) ซึ่งการตรวจสอบและสกัดกั้นนั้นเป็นไปได้ยาก

คำถามหลักที่น่าสนใจสำหรับหน่วยงานด้านความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้สามารถแบ่งออกเป็น ๒ ประเด็นหลักคือ ๑) กลุ่มก่อการร้ายที่เคลื่อนไหวในภูมิภาคฯ มีการใช้สกุลเงินคริปโตในการปฏิบัติการหรือไม่ ๒) หน่วยงานด้านความมั่นคงมีการเตรียมตัวในการป้องกันที่เพียงพอ/ดีพอหรือไม่ โดยจากการ

ศึกษาพบว่ากลุ่มก่อการร้ายที่เคลื่อนไหวในพื้นที่นั้นได้เสริมสร้างขีดความสามารถบนโลกไซเบอร์และมีการใช้เงินดิจิทัลเพื่อเป็นต้นทุนในการก่อเหตุรุนแรง ไม่ว่าจะเป็นเหตุการณ์ที่กลุ่มก่อการร้ายไอซิสเข้ายึดพื้นที่มินดาเนา และเหตุการณ์โจมตีสถานitäรวจเมืองโซโล (Solo), ขวากลาง (Central Java) ประเทศอินโดนีเซีย เมื่อกรกฎาคม ๒๐๑๖ (สมาชิกกลุ่มไอซิสในซีเรียเป็นต้นทางส่งเงินดิจิทัล) ซึ่งทั้ง ๒ เหตุการณ์ได้ปรากฏว่าผู้ก่อเหตุได้รับเงินทุนผ่านเงินสกุลดิจิทัล ซึ่งเมื่อวิเคราะห์เปรียบเทียบแนวทางป้องกันการระดมทุนในระบบดิจิทัลระหว่างสหรัฐฯ และหน่วยงานด้านความมั่นคงที่เป็นพันธมิตรกับหน่วยงานต่อต้านการก่อการร้ายในภูมิภาคอาเซียนพบว่ายังมีความแตกต่างอยู่อีกมาก โดยในภูมิภาคยังไม่มีหน่วยงานที่เป็นแกนหลักในการรับมือการต่อต้านการก่อการร้ายในลักษณะเชิงรุกที่ชัดเจนอีก ทั้งยัง





การขับเคลื่อนยุทธศาสตร์ด้านการป้องกัน และปราบปรามการฟอกเงิน และการสนับสนุนทางการเงินแก่การก่อการร้าย (AML/CFT)

กองความร่วมมือระหว่างประเทศ

สำนักงานป้องกันและปราบปรามการฟอกเงิน



ขาดกฎหมายที่สามารถเข้าไปตรวจสอบเส้นทางการเดินทางของ
เงินทุนที่ใช้เพื่อการก่อการร้าย (Digital Footprints) ซึ่งการขาด
องค์ประกอบทั้ง ๒ นี้ย่อมเป็นช่องโหว่สำหรับการเข้ามาเคลื่อนไหว
ในภูมิภาคฯ ได้อย่างง่ายดายเมื่อเทียบกับสหรัฐฯ ซึ่งการแก้ไขปัญหานี้
ในการรับมือกับองค์กรก่อการร้ายที่ทันสมัยเหล่านี้คือการเข้าร่วม
เป็นพันธมิตรกับหน่วยงานที่มีความพร้อม อาทิ คณะทำงานเฉพาะกิจ
เพื่อดำเนินมาตรการทางการเงิน (Financial Action Task Force:
FATF) โดยองค์กรนี้มีมาตรฐานสากลด้านการป้องกันและปราบ
ปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การ
ก่อการร้าย (AML/CFT) ซึ่งไทยได้เข้าร่วมเป็นสมาชิกตั้งแต่ ๑๕
มีนาคม ๒๐๑๒ สุดท้ายนี้สามารถตอบคำถามได้ว่ากลุ่มก่อการร้าย
มีการระดมทุนผ่าน blockchain/สกุลเงินดิจิทัลไปทั่วทุกภูมิภาค
ทั่วโลกเป็นที่เรียบร้อยแล้ว 🕒



References

- Arianti, V. & Kenneth, Y. Y. (2020), How Terrorists Use Cryptocurrency in Southeast Asia, The Diplomat, 30th June, viewed 8th Aug 2023 <<https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia/>>.
- Farivar, C. (2020), Feds announce largest seizure of cryptocurrency connected to terrorism, NBC News, 13th Aug, viewed 8th Aug 2023 <<https://www.nbcnews.com/tech/tech-news/feds-announce-largest-seizure-cryptocurrency-connected-terrorism-n1236610>>.
- Mazanec, B. & Whyte, C. (2019), Understanding Cyber Warfare: Politics, Policy and Strategy, Routledge, New York.
- McKirdy, E. & Watson, I. (2017), Bloodied and broken: Rising toll of Philippines' war with ISIS, CNN News, 24th August, viewed 9th Aug 2023 <<https://edition.cnn.com/2017/06/25/asia/philippines-marawi-isis/index.html>>.
- Rosenberg, D. (2021), The Secret Weapon That Helps Hamas Raise Millions of Dollars, Haaretz, 21st Jun, viewed 8th Aug 2023 <<https://www.haaretz.com/israel-news/2021-06-21/ty-article/premium/hamas-uses-cryptocurrency-for-fundraising-making-it-harder-to-follow-the-money/0000017f-dbe7-d3ff-a7ff-fbe722080000>>.
- กองพลน้อยอัลกอซซัม (al-Qassam) ภายใต้การบังคับบัญชาของกลุ่มก่อการร้ายฮามาส (Hamas) ประกาศรับการสนับสนุนเงินทุนผ่าน Bitcoin ที่มากระทรวงยุติธรรมสหรัฐ <<https://www.nbcnews.com/tech/tech-news/feds-announce-largest-seizure-cryptocurrency-connected-terrorism-n1236610>>
- กองพลน้อยอัลกอซซัม (al-Qassam) ภายใต้การบังคับบัญชาของกลุ่มก่อการร้ายฮามาส (Hamas) ที่มา <<https://www.timesofisrael.com/senior-idf-commander-says-hamas-has-7000-rockets-dozens-of-drones/>>