# Cyber Warrior Hackathon 2025 – Project Proposal

**1. Team Name:** Exodia

**2. Team Members:** นายชาญณรงค์ จันทร์สุดสุข Computer Engineering, SIIT TU นายชลบดินทร์ เชียงทอง Digital Engineering, SIIT TU นายพีรพงษ์ วิพิธกาญจน์ Computer Engineering, SIIT TU น.ส.ทยิดา จันทร์ไทสกุล M.Sc Forensic, RCPA และ นายสุทธิกานต์ ขันทอง Computer Engineering, MUIC

**3. ผู้ติดต่อหลักของทีม:** น.ส.ทยิดา จันทร์ไทสกุล 0869273272 thayida.jan@gmail.com

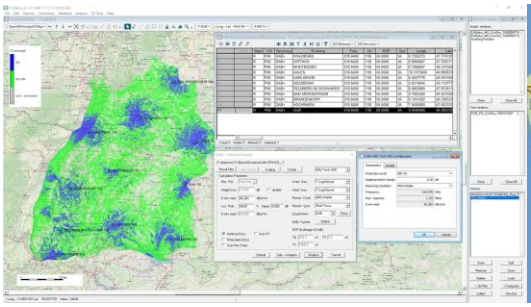
**4. ชื่อโครงการ:** “ระบบระบุตำแหน่งและติดตาม Simbox ด้วยเทคโนโลยี GIS, IMSI Catcher และ Cellular Triangulation”

**5. ปัญหาที่โครงการต้องการแก้ไข:** ปัจจุบันกลุ่มมิจฉาชีพหรือแก๊งคอลเซ็นเตอร์หลอกลวง มักใช้ “Simbox” หรืออุปกรณ์ประเภท GSM Gateway
ที่สามารถบรรจุซิมการ์ดจำนวนมากและปลอมแปลงสัญญาณให้เหมือนโทรศัพท์หรือส่งข้อความจากภายในประเทศไทย ทั้งที่ต้นทางจริงมาจากต่างประเทศ เช่น ลาว กัมพูชา หรือเมียนมา วิธีนี้ช่วยให้คนร้ายสามารถหมุนเวียนซิม ซ่อนตัวตน และหลีกเลี่ยงการตรวจจับของเจ้าหน้าที่ได้อย่างมีประสิทธิภาพ ส่งผลให้การติดตามและระบุตำแหน่งที่ตั้งของ Simbox ทำได้ยาก ส่งผลกระทบต่อความมั่นคงของประเทศและสร้างความเสียหายต่อประชาชนอย่างกว้างขวาง
ด้วยความท้าทายในการตรวจสอบและติดตาม Simbox ในปัจจุบัน
ทีมของเราจึงเห็นความจำเป็นในการพัฒนานวัตกรรมที่สามารถช่วยให้หน่วยงานรัฐและผู้ให้บริการเครือข่าย สามารถวิเคราะห์และระบุจุดที่มีการใช้งาน Simbox ได้อย่างรวดเร็ว แม่นยำ และมีประสิทธิภาพมากขึ้น

**6. แนวทางแก้ไขที่เสนอ:** เพื่อตอบสนองต่อปัญหาการใช้งานอุปกรณ์ Simbox
ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ ทีมของเราจึงนำเสนอแนวคิดในการพัฒนา **แพลตฟอร์มระบุตำแหน่งและติดตาม Simbox ด้วยข้อมูลเชิงพื้นที่ (Geo-locating Simbox Platform)**
โดยบูรณาการข้อมูลจากหลายแหล่ง ร่วมกับการใช้เทคโนโลยีเชิงแผนที่ (GIS) และอุปกรณ์ภาคสนาม
เพื่อเพิ่มความแม่นยำและประสิทธิภาพในการตรวจจับ**แนวคิดหลักของระบบประกอบด้วย 2 ระยะ ดังนี้:**

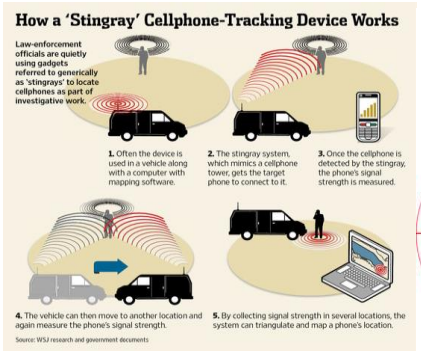
**ระยะที่ 1: วิเคราะห์พื้นที่ต้องสงสัยด้วย GIS**

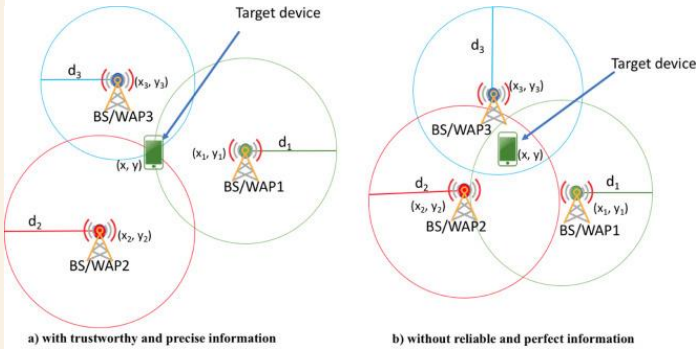
- ระบบจะรวบรวมและวิเคราะห์ข้อมูลจากผู้ให้บริการเครือข่าย (AIS) และระบบของรัฐ เช่น ข้อมูลจากเสาสัญญาณและ Cell ID ปริมาณการโทรออกหรือหมุนเวียนซิมในแต่ละพื้นที่ รวมถึงพฤติกรรมผิดปกติที่บ่งชี้การใช้งาน Simbox
- ข้อมูลทั้งหมดจะถูกนำมาวิเคราะห์ร่วมกันบนระบบ GIS และแสดงผลเป็น Heatmap หรือ ArcMap เพื่อระบุพื้นที่ที่มีความเสี่ยงหรือมีแนวโน้มว่ามี Simbox ดำเนินการอยู่



**ระยะที่ 2: เข้าตรวจสอบภาคสนามด้วย IMSI Catcher (StingRay) -** เมื่อระบบระบุพื้นที่ต้องสงสัยแล้ว เจ้าหน้าที่สามารถนำอุปกรณ์ IMSI Catcher หรือตัวจำลองสถานีฐาน (Fake Base Station) เช่น StingRay เข้าพื้นที่ โดยกระบวนการทำงานประกอบด้วย:

- FBS จะปล่อยสัญญาณเลียนแบบสถานีฐานจริง โดยมีความแรงของสัญญาณมากกว่าหรือใกล้เคียงกับสถานีฐานเดิมในพื้นที่
- เมื่อซิมการ์ดหรืออุปกรณ์ Simbox ตรวจพบ FBS ที่มีสัญญาณแรงกว่า จะเชื่อมต่อเข้ากับ FBS ของเราโดยอัตโนมัติ แทนที่จะเชื่อมต่อกับสถานีฐานจริง
- ระบบจะดักจับข้อมูลรหัสประจำตัว (IMSI) ของซิมการ์ดหรืออุปกรณ์ที่เชื่อมต่อเข้ามา เพื่อยืนยันตัวตนและวิเคราะห์พฤติกรรม
- ใช้เทคนิค **Cellular Triangulation หรือ Trilateration** เพื่อคำนวณตำแหน่งที่แม่นยำของ Simbox จากข้อมูลที่เก็บได้
- ยืนยันพฤติกรรมการหมุนเวียนซิมหรือส่งสัญญาณผิดปกติ และระบุตำแหน่ง Simbox เพื่อเตรียมการเข้าตรวจค้นและดำเนินการทางกฎหมาย




a) with trustworthy and precise information b) without reliable and perfect information

แนวทางนี้จะช่วยให้สามารถตรวจจับและติดตาม Simbox ได้แม่นยำยิ่งขึ้น ลดระยะเวลาการสืบสวน และช่วยให้หน่วยงานความมั่นคงตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

**7. ฟีเจอร์หลักที่วางแผนจะพัฒนา:** โครงการวางแผนพัฒนาแพลตฟอร์มที่สามารถตรวจจับและวิเคราะห์การใช้งานอุปกรณ์ Simbox โดยมีฟีเจอร์หลักดังต่อไปนี้

1. ระบบวิเคราะห์พฤติกรรมการโทรผิดปกติ (Suspicious Call Behavior Detection)
    - ตรวจสอบจำนวนและความถี่ของการโทรออกจากซิมการ์ดหรืออุปกรณ์ในแต่ละพื้นที่
    - ตรวจจับพฤติกรรมผิดปกติ เช่น มีการโทรออกจำนวนมากผิดปกติ หรือการหมุนเวียนซิมในจุดเดียว
2. การระบุตำแหน่งผ่านข้อมูล Cell ID และพิกัดสัญญาณ (Location Approximation)
    - วิเคราะห์ข้อมูลจากเสาสัญญาณโทรศัพท์มือถือเพื่อประมาณตำแหน่งซิม เพื่อตรวจสอบพื้นที่ที่มีแนวโน้มมีอุปกรณ์ Simbox
    - รองรับการวิเคราะห์ตำแหน่งทั้งจากเสาเดี่ยว และการประเมินตำแหน่งแบบ Triangulation หรือ Trilateration เพื่อเพิ่มความแม่นยำ
3. Heatmap Visualization และการวิเคราะห์พื้นที่เสี่ยง (Risk Area Mapping and Visualization)
    - แสดงพื้นที่ที่มีความถี่ในการโทรออกหรือเปลี่ยนซิมผิดปกติ

- ใช้ระบบแผนที่ดิจิทัลพร้อม Heatmap เพื่อช่วยให้เจ้าหน้าที่เห็นภาพรวมของพื้นที่เสี่ยงได้อย่างชัดเจน

4. ระบบแจ้งเตือนอัตโนมัติ (Alert System)
    - ส่งการแจ้งเตือนไปยังเจ้าหน้าที่เมื่อพบพฤติกรรมที่เข้าเกณฑ์ต้องสงสัย
5. การสร้าง Cluster Visualization ของซิมต้องสงสัย
    - จำแนกกลุ่มของเบอร์โทรศัพท์หรือซิมที่มีพฤติกรรมคล้ายคลึงกัน เช่น เปลี่ยนซิมถี่ หรือเชื่อมต่อจากตำแหน่งเดียว
6. ฟีเจอร์รองรับการใช้งานภาคสนาม
    - รองรับการเชื่อมต่อกับอุปกรณ์ IMSI Catcher หรือ Fake Base Station (เช่น StingRay) เพื่อเข้าสู่พื้นที่จริงและตรวจจับตำแหน่งของ Simbox ได้อย่างแม่นยำ

**8. กลุ่มเป้าหมายหรือผู้ใช้:** โครงการนี้มุ่งเน้นการให้ประโยชน์แก่กลุ่มผู้ใช้งานหลัก ดังต่อไปนี้

1. เจ้าหน้าที่ตำรวจ และฝ่ายสืบสวนสอบสวน
    - ใช้แพลตฟอร์มเพื่อวางแผนการตรวจค้นและระบุตำแหน่ง Simbox อย่างแม่นยำ
    - ช่วยวางแผนการตรวจค้นภาคสนามอย่างแม่นยำ ลดระยะเวลาและทรัพยากรในการสืบสวน
2. หน่วยงานความมั่นคงและหน่วยงานรัฐที่เกี่ยวข้อง
    - เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, สำนักงานตำรวจแห่งชาติ, หรือ กสทช.
    - ใช้เพื่อเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ Simbox
3. ผู้ให้บริการเครือข่ายโทรศัพท์มือถือ (AIS, DTAC, TRUE, NT)
    - ใช้เพื่อช่วยตรวจสอบการใช้งานซิมที่ผิดปกติภายในระบบของตน
    - ทำงานร่วมกับรัฐเพื่อป้องกันการนำเบอร์โทรศัพท์ไปใช้ในกิจกรรมที่ผิดกฎหมาย
4. ประชาชนทั่วไป (ในระยะยาว)
    - ได้รับประโยชน์จากการลดความเสี่ยงในการตกเป็นเหยื่อของการหลอกลวงผ่านโทรศัพท์

**9. Minimum Viable Product (MVP):** เวอร์ชันขั้นต่ำที่สามารถใช้งานได้จริงของโครงการนี้ (MVP) คือ **ระบบแผนที่วิเคราะห์พื้นที่ต้องสงสัย (Suspicious Area Analysis Platform)**
ที่สามารถแสดงพื้นที่ที่มีแนวโน้มการใช้งาน Simbox หรือ GSM Gateway ซึ่งมีพฤติกรรมเข้าข่ายผิดปกติ
โดยมีองค์ประกอบหลักดังนี้:

- ข้อมูล Cell ID และพิกัดสัญญาณ จากผู้ให้บริการเครือข่ายโทรศัพท์มือถือ
- การระบุ Cluster หรือจุดรวมความผิดปกติบนแผนที่ด้วยการใช้ Heatmap Visualization
- ระบบแผนที่เชิงโต้ตอบ (Interactive Map) ที่ช่วยให้เจ้าหน้าที่เห็นภาพรวมพื้นที่เสี่ยง สามารถวิเคราะห์และวางแผนการตรวจสอบภาคสนามได้อย่างมีประสิทธิภาพ

MVP นี้จะแสดงให้เห็นว่าแนวคิดของโครงการสามารถทำงานได้จริง มีความเป็นไปได้ในทางเทคนิค และสามารถนำไปพัฒนาต่อยอดได้ เช่น การเชื่อมต่อกับระบบภาคสนาม (IMSI Catcher), การใช้ AI วิเคราะห์พฤติกรรมการใช้งานซิม หรือการเชื่อมโยงกับฐานข้อมูลอาชญากรรมข้ามชาติ โดยการทดสอบ MVP ในพื้นที่จริง จะเป็นจุดเริ่มต้นของการพัฒนาเครื่องมือที่สามารถประยุกต์ใช้ได้ทั้งในระดับจังหวัด ระดับประเทศ และในอนาคตอาจขยายสู่ความร่วมมือกับประเทศเพื่อนบ้านในระดับภูมิภาคได้อีกด้วย