

**บทวิเคราะห์ร่างพรบ.ว่าด้วยการรักษามันคง  
ปลอดภัยไซเบอร์แห่งชาติ พ.ศ.....:**  
**เปรียบเทียบกลยุทธ์และกฎการรักษาความมันคง  
ปลอดภัยไซเบอร์ของสหภาพยุโรป**

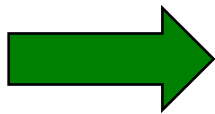
*รองศาสตราจารย์ ดร.สราวุธ ปิตียาศักดิ์  
สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช*

## ขอบเขตการบรรยาย

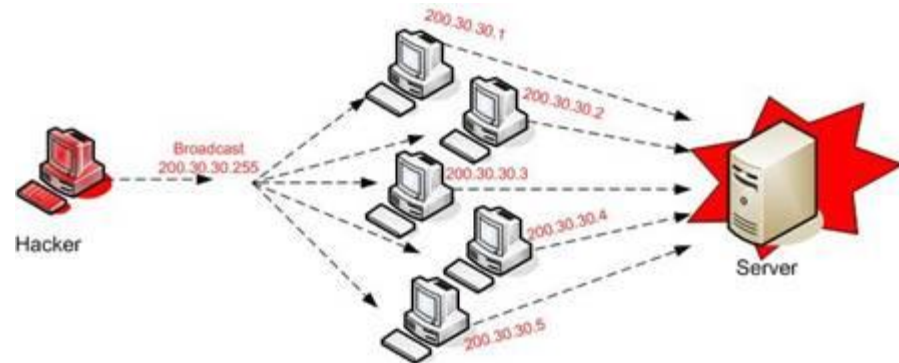
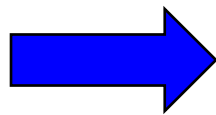
1. การโจมตีทางไซเบอร์
2. แนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์
3. EU Security Strategy and National and Information Security Directive
4. วิเคราะห์ร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.....

# การโจมตีทางไซเบอร์

(1) โจมตีวัตถุ



โจมตีระบบ (Network) /  
ข้อมูล (Information)

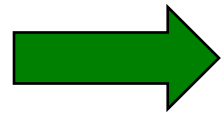


<http://hilight.kapook.com/view/56931>

<http://www.mvt.co.th/viewarticle.php?cid=3&nid=82&page=>



## (2) National Boundary



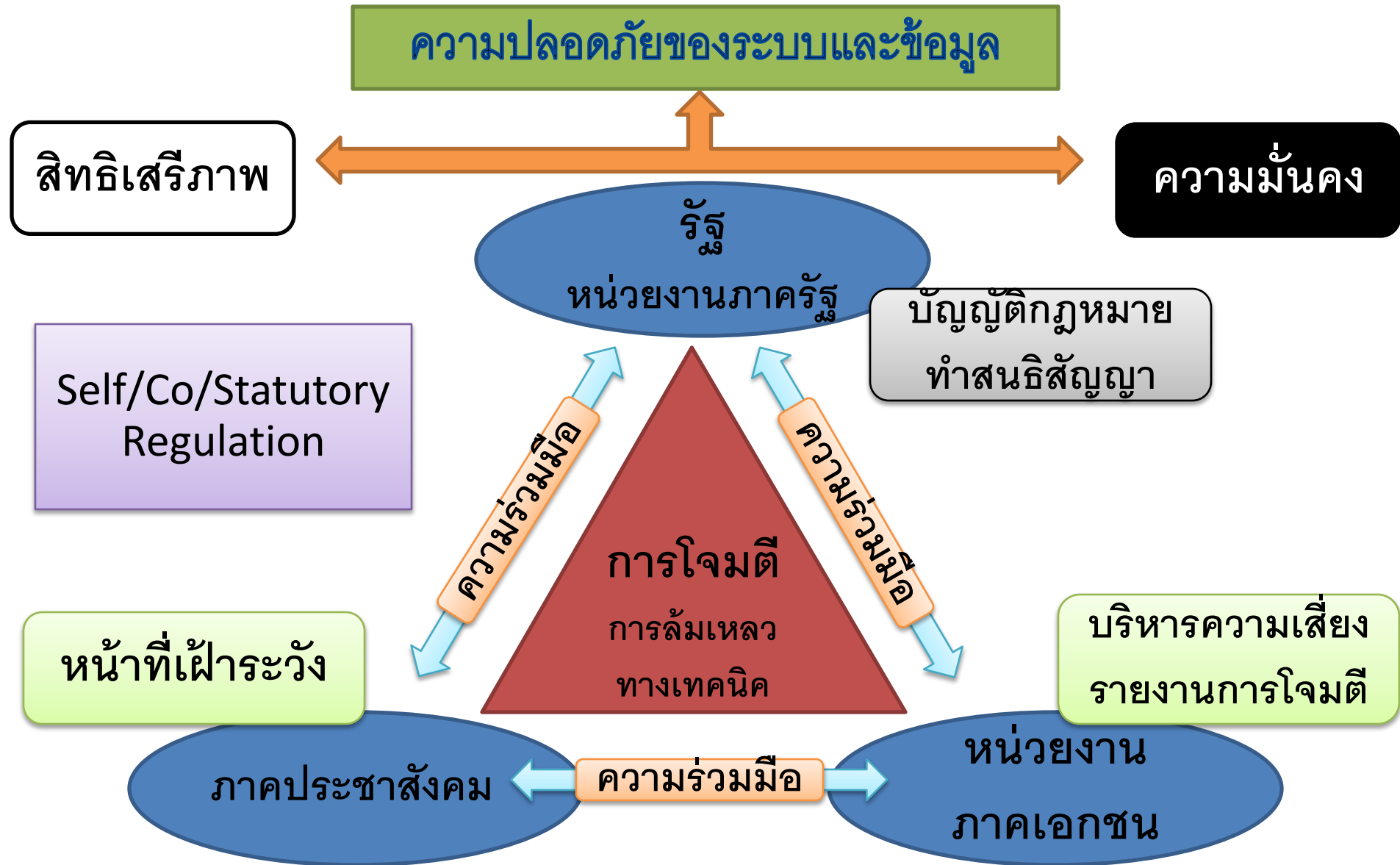
Without Boundary



# รูปแบบการโจมตีไซเบอร์

1. การเจาะระบบคอมพิวเตอร์ (Hacking)
2. การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ (Spyware)
3. การดักจับข้อมูลคอมพิวเตอร์ (Sniffing)
4. การทำลายระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ (Malicious Software: Malware)
5. การรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack: DOS)

# กรอบแนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์



# EU Security Strategy and National and Information Security Directive

- Digital Single Market
- EU Security Strategy
- EU National and Information Security Directive
  - ปรับปรุงประสิทธิภาพทางเทคนิคในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศสมาชิกแห่งสหภาพยุโรป
  - เสริมสร้างความร่วมมือระหว่างประเทศสมาชิก รวมถึงหน่วยงานภาครัฐและเอกชนเพื่อจัดการกับการโจมตีไซเบอร์
  - กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับผู้ประกอบกิจการเกี่ยวกับโครงสร้างพื้นฐานที่สำคัญ

# ร่าง พรบ. ว่าด้วยการรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ.....

## เหตุผล

- การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัยความร่วมมือและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง



# นิยามศัพท์

- “ความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้าน ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

- “หน่วยงานของรัฐ” หมายความว่า กระทรวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น องค์การมหาชน รัฐวิสาหกิจ และหน่วยงานที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่ากรณีใด ๆ

# คณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ

- มาตรา 6 ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กปช.” และให้ใช้ชื่อภาษาอังกฤษว่า “**National Cybersecurity Committee**” เรียกโดยย่อว่า “**NCSC**” ประกอบด้วย

(1) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

(2) กรรมการโดยตำแหน่งจํานวนสี่คน ได้แก่ เลขาธิการสภาความมั่นคงแห่งชาติ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงกลาโหม ผู้บังคับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ

(3) กรรมการผู้ทรงคุณวุฒิจํานวนไม่เกินเจ็ดคนซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ด้านนิติศาสตร์ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

## อำนาจหน้าที่ กปช.

มาตรา 7 ให้ กปช. มีอำนาจหน้าที่ ดังต่อไปนี้

(8) ส่งเสริมหรือประสานความร่วมมือกับหน่วยงานภาครัฐ และภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ

# อำนาจสั่งการหน่วยงานของรัฐ

- มาตรา 34 เมื่อมีเหตุฉุกเฉินหรือภัยอันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดผลกระทบต่อความมั่นคงของประเทศ ให้ กปช. มีอำนาจสั่งการให้หน่วยงานของรัฐทุกแห่งดำเนินการอย่างหนึ่งอย่างใดเพื่อป้องกัน แก้ไขปัญหา หรือบรรเทาความเสียหายที่เกิดหรืออาจจะเกิดขึ้นได้ตามที่เห็นสมควร และอาจให้หน่วยงานของรัฐ หรือบุคคลใด รวมทั้งบุคคลซึ่งได้รับอันตรายหรืออาจได้รับอันตรายหรือความเสียหายดังกล่าว กระทำหรือร่วมกันกระทำการใด ๆ อันจะมีผลเป็นการควบคุม ระงับ หรือบรรเทาผลร้ายจากอันตรายและความเสียหายที่เกิดขึ้นนั้นได้อย่างทันที่

## อำนาจสั่งการหน่วยงานภาคเอกชน

- มาตรา 33 ในกรณีที่มีความจำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ กปช. อาจสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง และให้รายงานผลการปฏิบัติการต่อ กปช. ตามที่ กปช. ประกาศกำหนด

# พนักงานเจ้าหน้าที่

มาตรา 35 เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ มีอำนาจดังต่อไปนี้

(1) มีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติการตามพระราชบัญญัตินี้

(2) มีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช.



**(3)** เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

การดำเนินการตาม **(3)** ให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะรัฐมนตรีกำหนด

# สรุป

**1** กฎไซเบอร์ของสหภาพยุโรปมุ่งรักษาความมั่นคงปลอดภัยของระบบและข้อมูลในโลกไซเบอร์ แต่ร่างกฎหมายไซเบอร์ไทยมุ่งรักษาความมั่นคงของรัฐจากการกระทำในโลกไซเบอร์

**2** กฎไซเบอร์ของสหภาพยุโรปเน้นการปรับปรุงความร่วมมือระหว่างประเทศสมาชิกและระหว่างภาครัฐและเอกชน แต่ร่างกฎหมายไซเบอร์ของไทย แม้จะได้มีการกำหนดในเหตุผลการยกร่างกฎหมาย แต่ในเนื้อหาของกฎหมายยังไม่มี ความชัดเจนในประเด็นดังกล่าว

**3** กฎไซเบอร์ของสหภาพยุโรปกำหนดให้บริษัทที่อยู่ในภาคธุรกิจที่สำคัญ เช่น พลังงาน การขนส่ง การธนาคาร และสุขภาพ รวมถึงธุรกิจการให้บริการอินเทอร์เน็ตต้องปฏิบัติตามการบริหารความเสี่ยง และรายงานเหตุการณ์สำคัญที่เกิดขึ้นทางไซเบอร์แก่หน่วยงานของรัฐ แต่ร่างกฎหมายไซเบอร์ของไทยกำหนดให้หน่วยงานภาคธุรกิจทุกประเภทต้องรายงานเหตุการณ์ทางไซเบอร์ต่อรัฐ

**4** ร่างกฎหมายไซเบอร์ของไทยให้อำนาจพิเศษแก่ กปช. อย่างมาก กปช. มีอำนาจสั่งการได้หน่วยงานภาครัฐทุกแห่ง แต่มีรัฐมนตรีเป็นประธาน สมควรให้นายกรัฐมนตรีซึ่งเป็นผู้บังคับบัญชาสูงสุดฝ่ายบริหารเป็นประธาน

**5** กฎไซเบอร์ของสหภาพยุโรปให้อำนาจการเข้าถึงการติดต่อสื่อสารเฉพาะข้อมูลคอมพิวเตอร์เท่านั้น แต่ร่างกฎหมายไซเบอร์ไทยให้อำนาจการเข้าถึงการติดต่อสื่อสารทุกรูปแบบ เช่น ไปรษณีย์ โทรเลข ฯ ซึ่งอาจเป็นการนอกกรอบวัตถุประสงค์ของการรักษาความมั่นคงปลอดภัยไซเบอร์และอาจขัดสิทธิส่วนบุคคล

**6** การให้เจ้าพนักงานเข้าถึงข้อมูลคอมพิวเตอร์ซึ่งเป็นข้อมูลส่วนบุคคลในหน่วยงานเอกชนโดยไม่ต้องขออำนาจศาล (**warrant**) ควรมีการกำหนดให้กระทำได้เฉพาะกรณีจำเป็นเร่งด่วนและเฉพาะหน่วยงานเอกชนประเภทที่มีความสำคัญต่อความมั่นคงของชาติเท่านั้น (**Critical Infrastructures**)

7 ร่างกฎหมายไซเบอร์ของไทยควรมุ่งเน้นในการสร้างความร่วมมือ (**Cooperation**) ระหว่างรัฐ หน่วยงานภาคเอกชน และภาคประชาสังคม ในลักษณะของการกำกับดูแลตนเอง (**Self-Regulation**) และการกำกับดูแลร่วมกัน (**Co-Regulation**) มากกว่าการใช้ตัวบทกฎหมาย (**Statutory Regulation**) ที่เข้มงวดเกินไปอันอาจกระทบถึงสิทธิเสรีภาพของประชาชนในการติดต่อสื่อสาร

