สงครามไซเบอร์ : หนึ่งในมุมมองของ Richard A. Clarke (Cyber warfare : Richard A. Clarke's Point of view)

โดย พลตรี ฤทธี อินทราวุธ ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก

วันสื่อสารแห่งชาติ ประจำปี ๒๕๖๐ สำนักงานปลัดกระทรวงกลาโหมร่วมกับคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) จัดสัมมนาวิชาการ ในหัวข้อ " สงครามไซเบอร์ในยุคเศรษฐกิจดิจิตอลการพิจารณาเชิงยุทธศาสตร์ของประเทศไทย " (Cyber warfare in Digital Economy Era: Strategic Considerations for Thailand) เมื่อ ๓ ส.ค.๖๐ ซึ่งมี พล.อ.ประวิตร วงษ์สุวรรณ รองนายกรัฐมนตรี / รมว.กระทรวงกลาโหม เป็นประธานเปิดงาน ฯ พร้อมด้วย ปลัดกระทรวงกลาโหม และผบ.เหล่าทัพ มาร่วมงานกันอย่างคับคั่ง โดยมีนาย Richard A. Clarke ผู้เขียนหนังสือ Cyber War : The Next Threat to National Security and What to Do About It และทำงานเป็นที่ปรึกษาพิเศษของสภาความมั่นคงแห่งชาติของสหรัฐอเมริกา ได้บรรยายเรื่อง Cyber Security

นาย Richard A. Clarke ได้บรรยายเรื่อง Cyber Security โดยกล่าวถึงในปี ๑๙๙๗ ทางสหรัฐ ได้มีการฝึกเสนาธิการร่วมในระยะเวลา ๑ สัปดาห์ ซึ่งมีเรื่องของการรับมือการโจมตีทางไซเบอร์ คนที่รู้บ่งการดังกล่าวมีเพียง รมว.กห. และ หน.เสนาธิการร่วม ซึ่งผู้โจมตีก็ไม่รู้ว่าเป้าหมายตามสถานการณ์ฝึกฯ เป็น เพนตากอน ซึ่งเป็นที่ตั้งของ กห.สหรัฐฯ ว่ามีระบบฯอะไรอยู่บ้าง? ทีมผู้โจมตีเป็นแค่ทีมเล็กๆ สามารถใช้เวลาเพียง ๓๖ ชม. เท่านั้นก็สามารถเข้าควบคุมระบบสั่งการของเพนตากอนได้ การฝึกดังกล่าวจบลงแสดงให้เห็นว่า Hacker สามารถเข้าถึงกองบัญชาการต่างๆได้ทั่วโลกเช่นเดียวกัน

ผลจากการฝึกดังกล่าวทำให้ รมว.กห. สหรัฐฯ ต้องเรียกประชุมฉุกเฉินในเรื่องดังกล่าว ต่อมาสหรัฐฯ จึงต้องมีการติดตั้งระบบป้องกันการบุกรุกโจมตีไซเบอร์ (Intrusion Prevention System : IPS) ขึ้นมาควบคุมดูแลเครือข่ายของกองทัพทั้งหมด และมีการประเมินติดตามผลในทุก ๓ เดือน ว่ายังมีความปลอดภัยอยู่หรือไม่? ซึ่งตอบพบว่ายังไม่มีความปลอดภัย เพราะการโจมตีอาจจะมีมาก่อนหน้านี้แล้ว แต่เรายังไม่รู้ตัวเท่านั้นเอง

ทางด้านประธานาธิบดีบิล คลินตัน ได้มีการร่างแผนยุทธศาสตร์ไซเบอร์ และเกิดแผนยุทธศาสตร์ฯ ในอีก ๔๐ ประเทศตามมา เป็นการกำหนดความชัดเจนว่าใครเป็นผู้รับผิดชอบในการบัญชาการ และงบประมาณมาจากไหน หากประเทศไม่มี Roadmap ด้านไซเบอร์ เราก็จะไม่มีแผนการดำเนินการและจะขาดความมั่นคงปลอดภัยในที่สุด เมื่อเกิดการโจมตี ก็จะมีคำถามว่าเกิดอะไรขึ้น โดยมีด้านหรือมิติที่เกี่ยวข้อง ๔ อย่าง คือ CHEW (Crime , Hacktivism , Espionage , War)

C อาชญากรรม (Crime) กรณีเกาหลีเหนือขโมยเงินทางธุรกรรมจากประเทศฟิลิปปินส์ และบังกลาเทศ Hacker สามารถเจาะเข้าไปในระบบและทำการโอนเงินไปในหลายๆ ที่ ทำให้การตามหาผู้กระทำผิดหรือได้เงินคืนเป็นเรื่องยาก ในภาพรวมองค์การอาชญากรรมทางไซเบอร์มีศักยภาพในการขโมยเงินได้มากกว่ากลุ่มค้ายาเสพติดหลายเท่า ถึงจะส่งผลกระทบแต่ไม่สามารถจับกุมได้ เนื่องจากมีการติดสินบนทั้งตำรวจหรือคนในระดับรัฐบาล ขณะที่ทั้ง NSA และ FBI มีการระบุว่าเป็นคนๆ

หนึ่งทราบชื่อแล้ว แต่เมื่อให้ทางประเทศรัสเซีย หรือประเทศอื่นๆ ช่วยตามจับกุมก็จะไม่สามารถพบตัวตนที่แท้จริงได้ ทำให้ประเทศเหล่านั้นเป็นพื้นที่หลบซ่อน การโจมตีทางไซเบอร์จึงยังคงอยู่ต่อไป ในขณะเกิดการโจมตีอย่างธนาคารก็จะประเมินความเสียหาย หากไม่สามารถนำกลับมาได้ เขาก็ต้องหาทางชดเชยกับลูกค้าอื่นๆ นั่นก็คือ ถึงแม้ว่าธนาคารจะโดนโจมตี แต่ประชาชนหรือลูกค้าก็ถูกขโมยเงินเช่นกัน

H แฮกติวิสซึม (Hacktivism) การเจาะข้อมูลเพื่อการเผยแพร่ต่อสาธารณะ เพื่อให้เกิดความอับอายทั้งภาครัฐและเอกชน โดยจะถูกนำไปตีพิมพ์ไว้ที่ Wikileak ซึ่งผู้บรรยายเคยมีการส่ง E-mail ลับ ระหว่างเอกอัครราชทูตฯ เนื้อหาบางส่วนเป็นการตำนิประธานาธิบดีฯ หากถูกเผยแพร่ออกไป ตัวเขาคงกลับไปทำงานในทำเนียบขาวไม่ได้แล้ว ในกรณี E-mail ของนาง ฮิลลารี คลินตัน ที่ถูกเปิดเผยออกมาทำให้ส่งผลเสียในการเลือกตั้ง ทำให้แพ้การเลือกตั้ง ซึ่งข้อมูลลับที่เปิดเผยออกมาทำลายทั้งองค์กร หรือถึงขั้นการไม่ได้เป็นประธานาธิบดี ได้เช่นกัน

E จารกรรม (Espionage) การจ้างสายลับเพื่อขโมยเอกสารลับออกมาเปิดเผย หรือส่งไปให้สายลับอีกคนหนึ่ง แต่ทุกวันนี้การขโมยข้อมูลลับ สามารถเจาะข้อมูลจากที่บ้านได้เลย ตอนนี้เรามีโดรน (Drone) และผู้บรรยายเคยไปงานเกี่ยวกับอากาศยานแล้วพบว่าแบบแปลนดังกล่าว ทางเราไม่เคยขายออกไป แต่เราพบโดรนที่มาจากประเทศจีนซึ่งจีนอาจจะมีนักเจาะข้อมูลเพื่อขโมยแบบแปลนดังกล่าว ดังนั้นบริษัทมักจะถูกเจาะระบบทุกวัน โดยเฉพาะคู่แข่งทางการค้า บางบริษัทฯ ต้องลงทุกวิจัยใช้งบประมาณมากมาย แต่ก็ต้องโดนคู่แข่งผลิตของเลียนแบบ ซึ่งถือเป็นอาชญากรรมทางเศรษฐกิจ

W สงคราม (War) ในห้วง ๗ ปี ที่ผู้บรรยายได้เขียนหนังสือ Cyber War มีหลายคนบอกว่ามันไม่มีทางเป็นไปได้ แต่ก็มีเหตุการณ์ที่รัสเซียบุกจอร์เจีย และก่อนที่จะบุกโดยรถถัง ระบบสื่อสาร ธนาคารของประเทศล่มหมด ทำให้ไม่สามารถเผยแพร่หรือรายงานการโจมตีออกไปสู่ภายนอกได้ ในเรื่องของ Stuxnet virus ที่มีการโจมตีโรงงานไฟฟ้านิวเคลียร์ประเทศอิหร่าน ถึงแม้ว่าเป็นระบบภายใน (Intranet) ไม่ได้ต่อออกสู่ภายนอก แต่ทั้งสหรัฐและอิสราเอลก็สามารถหาทางเจาะเข้าไปได้ ส่งผลให้เครื่องคอมพิวเตอร์ของโรงงานฯกว่า ๘๐๐ เครื่องถูกทำลาย ถือเป็นการทำลายทางกายภาพโดยตรง สำหรับคำสั่งการโจมตีดังกล่าวเป็นเพียงหนอนไวรัส (Worm) และโปรแกรมไม่พึงประสงค์ (Malware) ซึ่งมีการกระจายไปทั่วโลก

สำหรับการจัดทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถาม ๖ คำถาม เพื่อให้เกิดการพิจารณาดังนี้

๑. เราจะรุกอะไร? รับอะไร? สำหรับการรุกเป็นวิธีที่รวดเร็ว ประหยัดได้ผลที่สุด แต่ไม่สำคัญเท่าการรับ ในยุทธการระดับประเทศ การป้องกันถือเป็นยุทธศาสตร์แรก การโจมตีหรือรุกอาจจะมีค่าใช้จ่ายจัดตั้งทีมเจาะระบบสูงกว่า ๒ ล้านเหรียญสหรัฐ แต่การป้องกันต้องใช้งบประมาณเป็น ๑,๐๐๐ ล้านเหรียญสหรัฐ ในเดือน ธ.ค.๕๙ มีการโจมตีโครงข่ายการไฟฟ้าของยูเครน โดยรัสเซีย ทั้งฝ่ายยูเครนต้องใช้เวลาถึง ๖ ชม.ในการฟื้นฟูระบบฯ และหากเกิดเหตุการณ์แบบนี้ในประเทศไทย เราไม่มีไฟฟ้าใช้ ๖ เดือน อะไรจะเกิดขึ้น ดังนั้นการตั้งรับจึงเป็นสิ่งสำคัญเป็นอันดับแรก

๒. คำถามเกี่ยวกับภาคเอกชน ซึ่งมีทั้งการแพทย์ ตลาดหุ้น หน่วยงานเหล่านี้ มีการพิจารณาด้านความปลอดภัยกันเองหรือไม่? หรือให้ภาครัฐเข้าไปกำกับดูแล ซึ่งโดยปกติเอกชนไม่อยากให้ภาครัฐเข้าไปยุ่งเกี่ยวด้านความปลอดภัย จริงๆแล้วการกำกับดูแลของภาครัฐก็มีข้อจำกัด เพราะไม่รู้ว่าเอกชนทำงานอย่างไร? จึงควรมีความร่วมมือระหว่างกัน รัฐจะต้องกำหนดเป้าหมายด้านความปลอดภัยร่วมกับภาคเอกชน และมีการตรวจสอบจากภาครัฐอีกครั้งหนึ่ง ในอุตสาหกรรมสำคัญ เช่น โรงไฟฟ้า, โรงพยาบาล เป็นต้น ในห้วงที่ผ่านมาโรงพยาบาลในสหรัฐถูกโจมตีด้วย WannaCry, PetYa ต้องปิดการให้บริการทางโรงพยาบาลเองก็ไม่ทราบจะจัดการเรื่องดังกล่าวอย่างไร ดังนั้นรัฐต้องควบคุมแต่ไม่ได้บังคับ หรือจะบังคับต้องอาศัยวิธีการที่ชาญฉลาดพร้อมการตรวจสอบไปในตัว

๓. ประเด็นเรื่องความเป็นส่วนตัว ในองค์กรประเภท NGO อยากจะได้รับการคุ้มครองในเรื่องความเป็นส่วนตัว หากภาครัฐเข้ามากำกับดูแลก็ถูกมองว่าเป็นการควบคุมนั่นเอง ซึ่งในด้านความมั่นคงและด้านความเป็นส่วนตัวมีความขัดแย้งกันในตัว กรณีประวัติการรักษาพยาบาลถูกเจาะข้อมูลนำไปเผยแพร่ทางอินเทอร์เน็ตก็คือเรื่องการละเมิดความเป็นส่วนตัว การป้องกันเรื่องดังกล่าวก็ต้องใช้ด้านความมั่นคงเข้าไปจัดการ ดังนั้นไม่ต้องมีความคิดเห็นที่ขัดแย้งกันเพราะทั้งสองด้านไม่มีใครผิดไม่มีใครถูก รัฐต้องดูแลทั้งความปลอดภัยและความเป็นส่วนตัวไปพร้อมกันด้วย เช่น กรณีรัฐบาลสหรัฐมีการดักฟังโทรศัพท์ โดยดูข้อมูลที่เป็น Meta Data เมื่อมีการร้องเรียนก็ต้องมีหมายศาลในเรื่องดังกล่าว โดยศาลเองก็ต้องมีกระบวนการที่รวดเร็วในการออกหมาย ศาลโดยปกติจะไม่เข้าใจเรื่องไซเบอร์ ทางสหรัฐมีการจัดตั้งศาลเฉพาะด้านที่มีความรู้ความเข้าใจด้วยทั้งด้านโทรคมนาคมและการสื่อสาร ศาลจึงต้องเข้าสู่ยุคสารสนเทศเช่นเดียวกัน ถือเป็นบริการของภาครัฐในการป้องกันข้อมูลส่วนบุคคลและระบบสารสนเทศ

๔. เวลาที่เราต้องลงทุน ในการลงทุนไปกับซอฟต์แวร์ในการค้นหาข้อมูลสินค้าเมื่อลูกค้าหาสินค้าที่ต้องการเจอและสั่งสินค้า บริษัทมีการส่งสินค้าไปถึงมือลูกค้าให้ปลอดภัยไม่เสียหาย คำถามคือ เป็นเรื่องซอฟต์แวร์หรือเรื่องบุคคล ตอบก็คือ เราต้องลงทุนในเรื่องคน ซึ่งสามารถช่วยป้องกันระบบเครือข่ายขายสินค้าของเราได้ หากเราไม่มีผู้เชี่ยวชาญ เราจะปกป้องสิ่งเหล่านี้ได้อย่างไร โดยเฉพาะด้านการทหาร บุคคลที่เก่งมักจะไม่เข้ามาในวงการทหาร สาเหตุเพราะไม่อยากเป็นทหาร ไม่อยากแต่งเครื่องแบบ หากเราต้องการคนที่มีความเชี่ยวชาญก็ต้องเปิดใจ เปิดรับคนใหม่ๆ ทั้งประเทศรัสเซีย และอิสราเอล หากเขาจับกุมวัยรุ่นที่เป็น Hacker เขาจะส่งไปเป็นทหาร เราจึงควรมีการฝึกอบรมคนเหล่านี้เป็นพันๆ คน เพื่อรับมือภัยคุกคามใหม่ๆ จากการสำรวจตำแหน่งงานที่ว่างโดยเฉพาะการทหาร ซึ่งมีเป็นแสนตำแหน่งที่ต้องการผู้เชี่ยวชาญทางไซเบอร์ที่จะเข้ามาทำงานในตำแหน่งนี้อีกมาก ขนาดว่าเราส่งเสริมทั้งการศึกษามีทุนเรียนด้านไซเบอร์เพื่อให้เข้ามาทำงานภาครัฐ แต่สุดท้ายก็ยังมีตำแหน่งว่างอยู่ดี

๕. นวัตกรรม ทุกคนมักจะผลิตสิ่งใหม่ๆ เพื่อขายในตลาด โดยไม่สนใจความปลอดภัย มีอุปกรณ์นับพันล้านชิ้นที่ต่อเชื่อมอินเตอร์เน็ต และในอีก ๓ ปีข้างหน้า อาจจะเพิ่มขึ้นในระดับพันล้านชิ้น สำหรับแนวคิดเรื่อง IoT -Internet of Thing ทุก

อุปกรณ์สามารถเชื่อมต่อเข้าสู่อินเตอร์เน็ตด้วยตัวมันเอง เช่นเครื่องขายน้ำอัดลมแบบหยอดเหรียญ ก็ต้องต่ออินเตอร์เน็ตเพื่อจะได้ทราบว่าสินค้าหมดแล้วหรือยัง นอกจากนั้นแม้แต่ลิฟต์ก็ต้องมีการต่อเชื่อมอินเตอร์เน็ตเพื่อจะทราบข้อมูลการเข้าไปดูแลรักษาตามห้วงเวลา ถ้านวัตกรรมเชื่อถือไม่ได้จะเกิดปัญหา เช่น มีการเจาะเข้าไปในคาสิโน โดยอาศัยเครื่องคอมพิวเตอร์ที่ควบคุมอ่างเลี้ยงปลาในการควบคุมปริมาณออกซิเจนและใช้มันเป็นเครื่องมือเจาะเครื่องอื่นๆต่อไป นอกจากเครื่องควบคุม CCTV ก็มีโอกาสเป็นเหยื่อด้วยเช่นกัน ถ้าให้เลือกน้ำหนักของนวัตกรรม กับความน่าเชื่อถือ ผู้บรรยายให้น้ำหนักทางความน่าเชื่อถือมากกว่า

๖. ด้านการออกแบบยุทธศาสตร์ เราจะเน้นในเรื่องการป้องกันหรือฟื้นฟูหลังการโจมตี ในระบบคอมพิวเตอร์ทุกเครื่องถูกโจมตี ในเครือข่ายลับก็ถูกโจมตี หน่วยงานลับ CIA ก็ถูกโจมตี ซึ่งประเทศต่างๆ ต้องเผชิญกับฝ่ายตรงข้ามอย่างรัสเซีย จีน ที่มีขีดความสามารถสูง ซึ่งเชื่อว่าเขาทำได้อย่างแน่นอน เราอาจจะป้องกัน Hacker ทั่วไปได้ แต่มืออาชีพนั้นไม่มีทางป้องกันได้ หลังถูกโจมตีต้องฟื้นฟูให้เร็วที่สุด โดยปกติทุกภาคส่วนมักจะคิดป้องกันการเจาะระบบ ลดความเสียหาย การแบ่งแยกระบบงานและเครือข่าย และต้องมีการฟื้นฟู มีระบบสำรอง (Backup) ให้ระบบกลับมาใช้งานตามปกติให้เร็วที่สุด

หากทุกคนต้องทำยุทธศาสตร์ด้านไซเบอร์ ต้องตอบคำถามทั้ง ๖ ข้อให้ได้ แผนที่มีไม่ได้สั่งจากบนลงล่างอย่างเดียว ทั้งหมดต้องมีส่วนร่วมในการวางแผน มีการโต้เถียงกันให้ได้ข้อยุติ ในประเทศไทยเรามีทหารที่เข้มแข็ง แต่จะไม่ปลอดภัยหากไม่มีการป้องกันทางไซเบอร์

คำถามเกี่ยวกับหน่วยบัญชาการไซเบอร์ (Cyber Command) สหรัฐมีการรวมทั้ง ๓ เหล่าทัพขึ้นตรงต่อ รมว.กห.สหรัฐฯ ในประเทศกว่า ๒๐ ประเทศที่มีการจัดตั้งหน่วยดังกล่าว มีทั้งเล็กใหญ่ตามรูปแบบของแต่ละประเทศ หากเรามี Cyber Command ไม่ได้หมายความว่าหน่วยอื่นๆจะไม่สนใจด้านไซเบอร์ ประเทศไทยต้องออกแบบการพัฒนาไซเบอร์ และมองให้ออกว่ามันได้ประโยชน์ต่อประเทศอย่างไร ต้องหาคนมาเป็นผู้เชี่ยวชาญ รวมคนเหล่านั้นเข้าด้วยกัน

คำถามกรณี 9/11 เราให้ความสำคัญหน่วยงานที่เป็นโครงสร้างพื้นฐาน สร้าง Red Team เพื่อการซักซ้อมแผนเผชิญเหตุ ซักซ้อมการโจมตี การวางแผนสำรองกรณีฉุกเฉิน ให้กระทรวงทั้งหมดปรับการทำงาน โดยไม่ต้องมีการสั่งการจากศูนย์บัญชาการเพียงอย่างเดียว แต่ถึงอย่างไรศูนย์บัญชาการสำรองก็อาจจะไม่มีคนเพียงพอ ถึงแม้จะมีคนไม่พอก็ต้องพยายามเฝ้าระวังในทุกๆวันอย่างต่อเนื่อง การฝึกด้านไซเบอร์ต้องทำบ่อยๆ แผนในเอกสารไม่มีประโยชน์ คนต้องได้ทำจริง ปฏิบัติจริง สำหรับเรื่องอาชญากรรมข้ามชาติต้องมีความร่วมมือในการติดตามจับกุมตัวและมีมาตรการลงโทษประเทศที่ไม่ให้ความร่วมมือ

คำถามเรื่อง สงครามสารสนเทศและสงครามไซเบอร์ ในสหรัฐมองว่า Information Warfare ไม่ค่อยได้ใช้แล้ว เพราะแยกไม่ออกระหว่างสงครามจิตวิทยาหรือไซเบอร์กันแน่ เช่นในกรณีของการ์ต้าที่ถูกการเจาะระบบและเปิดเผยข้อมูล เป็นการใช้สงครามไซเบอร์เพื่อยึดครองเครือข่าย และใช้การโฆษณาชวนเชื่อเพื่อการขยายผลดังกล่าว

คำถามขอให้ผู้บรรยายกล่าวถึงหนังสือใหม่ชื่อที่ว่า Warnings เล่าถึงการแจ้งเตือน ซึ่งจะมีขึ้นทุกๆ ครั้งที่มีภัยพิบัติขนาดใหญ่ โดยปกติมักจะมีคนทำนายว่าเกิดเหตุการณ์ใหญ่ขึ้นแต่คนไม่สนใจ เรามักจะไปแสวงหาผู้เชี่ยวชาญมาให้ความเห็น แต่อาจจะมีบางความเห็นซึ่งไม่สอดคล้องกับส่วนใหญ่คนก็ไม่สนใจ อย่างกรณีของโรงงานไฟฟ้านิวเคลียร์ของญี่ปุ่น มีที่ตั้งอยู่ในพื้นที่ราบติดริมทะเล มีคนบอกว่าอาจจะเกิดแผ่นดินไหวและเกิดสึนามิ ซึ่งไม่มีใครเชื่อ แต่ปรากฏว่ามีเหตุการณ์จริง มีคนถามว่าท่านรู้ได้อย่างไร เขาก็บอกว่าได้เดินสำรวจบนภูเขาและมีป้ายศาลาหลักเขียนเตือนว่าอย่างสร้างสิ่งก่อสร้างที่มีระดับต่ำกว่านี้และเป็นการเตือนเมื่อ ๔๐๐ ปีมาแล้ว เป็นต้น

จริงๆ แล้วเรื่องเหล่านี้ ในบ้านเมืองเราได้มีการหยิบยกมาพูดคุยกันซ้ำแล้วซ้ำเล่ากันนานแล้วในหลายๆ เวที รวมถึงบทความและสื่อต่างๆ แต่ด้วยความเป็นวัฒนธรรมของเรา ที่มักจะไม่ค่อยจะให้ความสำคัญกับเรื่องราวพวกนี้รวมถึงเครดิตคนไทยด้วยกันเองมากนัก จึงจำเป็นต้องเชิญผู้เชี่ยวชาญจากต่างประเทศมาบรรยาย อาจจะได้รับความเชื่อถือและความสนใจใส่ใจจากผู้หลักผู้ใหญ่ที่เกี่ยวข้องมากขึ้น ที่ผ่านมามักมีแต่การสร้างกระแส เกาะกระแส ไม่ค่อยเอาจริงเอาจังกันเท่าไหร่ ปล่อยให้ผู้ปฏิบัติงานจริง ตัวจริง เสียงจริง ดิ้นรนกันไป แต่บทเรียนในอดีตที่ผ่านมา พอมีการสนใจใส่ใจเอาจริงเอาจังของผู้หลักผู้ใหญ่ในการผลักดันส่งเสริมสนับสนุนจนเกิดหน่วยงาน Cyber Command อย่างเป็นรูปธรรมขึ้นมา ก็จะมีองค์เทพลงมาจุติ ทำนองว่า คนรู้ไม่ได้ทำ คนที่มาทำไม่ค่อยจะรู้ หรือรู้แบบงูๆ ปลาๆ พากันเข้าป่าเข้าดงไป และขอขอบคุณ พ.อ.นิพัฒน์ เล็กฉลาด จากศูนย์ไซเบอร์กองทัพบก ที่สรุปประเด็นสาระการบรรยายของ Richard A. Clarke ที่เป็นประโยชน์เพื่อนำมาเผยแพร่ในครั้งนี้