สงครามไซเบอร์

โดย นาวาเอก ธงชัย คุ้มกัน

บทคัดย่อ

สงครามไซเบอร์ (CYBER WAR) คือ การใช้ช่องทางดิจิทัลเพื่อโจมตีประเทศศัตรู โดยหวังผลให้เกิดความเสียหายพอๆ กับการทำสงครามจริงๆ โดยใช้โลกไซเบอร์เป็นเครื่องมือ ทำให้เกิดความเสียหายด้านกายภาพ ทำอันตรายต่อผู้คนหรือวัตถุในโลกจริง รวมถึงไปขัดขวางการทำงานหรือทำลายระบบคอมพิวเตอร์ที่สำคัญ อีกทั้งสงครามไซเบอร์ยังเป็นเรื่องของการใช้อานุภาพทางไซเบอร์ของชาติใดชาติหนึ่ง เพื่อโจมตีอีกชาติหนึ่ง ทั้งเพื่อข่มขู่ คุกคาม จนกระทั่งทำลายล้างอีกชาติหนึ่ง เนื่องจากความก้าวหน้าทางเทคโนโลยีทำให้ มีการเชื่อมโยงเครือข่ายคอมพิวเตอร์หลายล้านเครื่องทั่วโลกเข้าด้วยกัน หรือที่เรียกว่าเครือข่ายอินเตอร์เน็ต นอกจากจะมีประโยชน์ในด้านของการติดต่อสื่อสารกันได้ทั่วโลกแล้ว อินเตอร์เน็ตยังสามารถใช้เป็นอาวุธ ในทางการทหาร และการสงครามด้วย เป็นผลทำให้การทำสงครามเปลี่ยนไปจากสงครามรูปแบบเดิม ๆ ไปอย่างมาก

สงครามรูปแบบใหม่จะมาในรูปของการทำสงครามผ่านทางระบบเครือข่ายอินเตอร์เน็ต หรือที่เรียกว่า CYBER WAR ซึ่งสงครามนี้อาจไม่จำเป็นต้องเคลื่อนกำลังทหารหรือยุทโธปกรณ์ไปโจมตีข้าศึก เพียงแต่นั่งอยู่หน้าจอคอมพิวเตอร์ แล้วเคาะแป้นคีย์บอร์ดเท่านั้น ก็สามารถทำลายข้าศึกให้เกิดความเสียหายได้ แม้ว่าจะไม่มีการทิ้งระเบิดถล่มอาคาร หรืออะไรก็ตามสหรัฐอเมริกาได้ชื่อว่าเป็นผู้นำด้านสงครามไซเบอร์ มีนักรบไซเบอร์ที่เก่งกาจ แต่ก็มีหลายประเทศที่มีศักยภาพด้านสงครามไซเบอร์สูง เช่น จีน รัสเซีย ก็มีศักยภาพเพียงพอสามารถที่จะแฮกระบบของสหรัฐได้เช่นกัน แม้สหรัฐจะดูเหมือนว่ามีความเหนือกว่าในด้านสงครามไซเบอร์ แต่อาจไม่ลงเอยด้วยการเป็นผู้ชนะเสมอไป และหากสงครามไซเบอร์เกิดขึ้นเต็มรูปแบบจะก่อความสูญเสียอย่างไรต่อประเทศที่ถูกโจมตี เนื่องจากโลกในปัจจุบันมีการพึ่งพาระบบเครือข่ายคอมพิวเตอร์ ในการทำธุรกิจ และกิจกรรมอยู่ตลอดเวลา ซึ่งมีความเปราะบางมากที่จะถูกโจมตีจากแฮกเกอร์

ซึ่งสามารถสร้างความเสียหายให้เกิดขึ้นได้ เช่น เงินในบัญชีของผู้ถูกแฮกอาจสูญหายไป ความลับทางการค้าอาจถูกขโมยไป หรืออื่นๆ อีกมากมาย

สงครามไซเบอร์ นั้นมีอิทธิพลอย่างยิ่งต่อการกำหนดยุทธศาสตร์ในหลายๆประเทศได้มีการเตรียมการให้ประเทศมีความพร้อม และมีขีดความสามารถในการทำสงครามไซเบอร์ ดังนั้นประเทศไทย ควรเตรียมการให้ประเทศมีความพร้อมและพัฒนาขีดความสามารถในการทำสงครามไซเบอร์ให้อยู่ในระดับสูง

บทนำ

ในทศวรรษแรกของศตวรรษที่ ๒๑ สหรัฐอเมริกาได้พัฒนาและนำอาวุธชนิดใหม่เข้าประจำการ ได้ก่อตั้งกองบัญชาการทหารหน่วยใหม่ขึ้นมาเพื่อให้ทำหน้าที่ปฏิบัติการในสงครามไฮเทครูปแบบใหม่ โดยในปี ๒๐๐๙ สหรัฐอเมริกาได้ตั้งกองบัญชาการไซเบอร์ ซึ่งเป็นหน่วยงานทางทหารมีภารกิจในการปฏิบัติการทางสงคราม ไซเบอร์ แต่ยังมีกองบัญชาการเช่นเดียวกันนี้ในหลายประเทศ เช่น รัสเซีย จีน เกาหลีใต้ องค์กรด้านการข่าวและการทหารเหล่านี้กำลังเตรียมพร้อมในการทำสงครามไซเบอร์ ด้วยหลายสิ่งที่เรียกกันว่า “Logic Bomb” (ซอฟต์แวร์ หรือชุดคำสั่งที่ปิดระบบหรือเครือข่าย และ/หรือลบข้อมูลหรือซอฟต์แวร์ในเครือข่าย) และ “Trapdoor” (ซอฟต์แวร์ประสงค์ร้าย ที่ถูกเพิ่มในระบบโดยไม่ได้รับอนุญาต เป็นตัวที่จะเปิดการเข้าถึงเครือข่าย หรือโปรแกรมนั้นโดยไม่ได้รับอนุญาตในภายหลัง)

ที่มา https://newstextarea.com/cyber-wars-of-the-future-what-experts-warn-of/

เมื่อใช้อุปกรณ์เชื่อมต่อเครือข่าย ในการติดตั้งโปรแกรม สามารถพบภัยคุกคามมากมาย มีมัลแวร์หลายประเภทที่อาจทำให้ ระบบความปลอดภัยตกอยู่ในความเสี่ยง และอาจส่งผลกระทบต่อการทำงานของระบบคอมพิวเตอร์ การโจมตีด้วย “Logic Bomb Attack” ซึ่งเป็นมัลแวร์ประเภทหนึ่งที่ทำให้เกิดผลกระทบต่อเป้าหมายอย่างร้ายแรงได้ มัลแวร์ Logic Bomb (ซอฟต์แวร์ หรือชุดคำสั่งที่สามารถปิดระบบหรือเครือข่าย และ/หรือลบข้อมูลหรือซอฟต์แวร์ในเครือข่ายได้) ขึ้นอยู่กับการเขียนโค้ดที่เป็นอันตรายลงในโปรแกรม โดยแฝงตัวอยู่ในโปรแกรมนั้น จนกว่าจะถึงเวลาที่กำหนดไว้ให้ดำเนินการโจมตีเป้าหมาย ในกรณีนี้แฮ็กเกอร์จะกำหนดให้ มัลแวร์ดำเนินการโจมตีเป้าหมาย เมื่อตรงตามเงื่อนไขบางประการ อาจเป็นการโจมตีที่ทำให้เกิดความเสียหายมาก เนื่องจากเป้าหมายที่ติดตั้งซอฟต์แวร์นี้ไม่รู้ว่าเครื่องคอมพิวเตอร์นั้นติดไวรัสหรือมัลแวร์ เนื่องจากไม่สังเกตเห็นว่าคอมพิวเตอร์ทำงานผิดปกติ หรือปิดเครื่องไม่มีโปรแกรมที่ติดตั้งเพิ่มเติมปรากฏขึ้นหรือมีอะไรแปลกๆ จนกว่าจะถึงเวลาที่กำหนดไว้ให้โจมตี มัลแวร์ Logic Bomb นั้นมีขีดความสามารถหลายอย่าง เช่น ลบไฟล์ ขโมยข้อมูล ป้องกันการเข้าถึงโปรแกรมหรือบริการใช้บัญชีของเรา หรือใช้ทรัพยากรระบบ “Trapdoor” หรือ “Backdoor” (ซอฟต์แวร์ประสงค์ร้าย ที่ถูกเพิ่มในระบบโดยไม่ได้รับอนุญาต เป็นตัวที่จะเปิดการเข้าถึงเครือข่าย หรือโปรแกรมนั้นโดยไม่ได้รับอนุญาตในภายหลัง) โปรแกรมที่จัดทำขึ้นนั้นจะมีส่วนที่เป็นความลับในโปรแกรม เป็นพิเศษเพื่อเข้าสู่โปรแกรม หรือโมดูลได้โดยตรง จึงเป็นช่องโหว่ในการถูกโจมตีได้ โดยลอบติดตั้งมัลแวร์เอาไว้ในยามสันติ ในการทำสงครามไซเบอร์นั้นการลงมือโจมตีก่อนนั้นดีที่สุดโดยส่วนมาก เป้าหมายการโจมตีนั้นสามารถถูกโจมตีได้ ไม่ว่าจะอยู่ที่ใดในโลก ทำให้มีโอกาสกลายเป็นวิกฤตการณ์ที่สูงได้มากอย่างยิ่ง ดังนั้นการทำสงครามไซเบอร์นั้นจึงถูกปกปิดเป็นความลับอย่างมาก

ประเทศที่เป็นผู้คิดค้นเทคโนโลยีใหม่ ใช้ยุทธวิธีใหม่ ๆ ขึ้นมาใช้งาน อาจไม่ใช่ผู้พิชิตเสมอไป ถ้าหากกองทัพของประเทศนั้นยังคงหลงติดอยู่กับวิธีการที่เคยใช้มาในอดีต ความเชื่อมั่นในยุทโธปกรณ์ที่คิดว่ามีพลานุภาพเหนือใคร ผู้ที่เป็นต้นกำเนิดของอาวุธเชิงรุกใหม่อาจกลายเป็นผู้แพ้ได้ เว้นเสียแต่ว่าจะสามารถดำเนินการป้องกันอาวุธเหล่านี้ได้

จุดเริ่มต้นสงครามไซเบอร์

การทำสงครามไซเบอร์? มีอะไรบ้างที่นำมาใช้เป็นอาวุธในการโจมตี

อันดับแรก อาวุธที่ว่านี้ได้ถูกนำมาใช้ในการก่ออาชญากรรมบนโลกไซเบอร์ ซึ่งเกิดขึ้นอยู่ตลอดเวลา โดยจะมี Botnet (เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot) ที่พร้อมจะดำเนินการโจมตีเป้าหมาย แบบ DDoS (Distribute Denial of Service) คือ การปฏิเสธการให้บริการ ซึ่งเป็นการทำให้เครื่อง หรือทรัพยากรเครือข่าย สำหรับเป้าหมายที่ถูกโจมตีใช้บริการไม่ได้ หรืออาจทำให้การบริการต่างๆ หยุดชะงัก หรือทำหน้าที่เบี่ยงเบนความสนใจจากผู้ดูแลระบบ เพื่อให้สามารถโจมตีเป้าหมายที่แท้จริงได้ง่ายขึ้น (Smoke Screen DDoS) หรืออาจจะเป็นได้ทั้งสองอย่าง นอกจากเทคนิคการ Hacking ของ Hacker ยังมีการโจมตีอีกหลากหลาย เช่น เทคนิคการโจมตีแบบ Social engineering ซึ่งไม่ได้โจมตีที่ระบบ แต่เป็นการโจมตีที่ผู้ใช้ระบบ หรือเทคนิค Spear Phishing เป็นการสร้างสถานการณ์ให้เป้าหมายหลงเชื่อ เช่น การส่งข้อความ อีเมล หรือเว็บไซต์ปลอม เพื่อเป็นเหยื่อล่อให้เป้าหมายหลงเชื่อ และหลอกล่อเป้าหมายให้กรอกข้อมูลส่วนตัวต่าง ๆ หรือ ส่งโปรแกรมให้ติดตั้งลงเครื่องคอมพิวเตอร์ตามที่แฮกเกอร์ต้องการแล้วนำไปใช้ประโยชน์ เป็นต้น แต่ภัยคุกคามนั้นก็สามารถเกิดจากภายในได้และป้องกันได้ยาก อย่างไรก็ตาม Hacker สามารถโจมตีไปยังเครือข่ายต่าง ๆ ได้โดยตรง หรือแฝงเข้ามาโจมตีระบบที่มีความสำคัญ (Highly Sensitive) หรือที่เป็นความลับได้

อิสราเอลใช้สงครามไซเบอร์โจมตีซีเรีย

ที่มา http://monsoonphotonews.blogspot.com/2013/09/un.html

สหรัฐอเมริกาและมหาอำนาจทางนิวเคลียร์ กำหนดว่าจะยุติการขายองค์ความรู้ ด้านอาวุธนิวเคลียร์ และไม่ให้ประเทศอื่นๆ มีอาวุธนิวเคลียร์ จุดเริ่มต้น คือ ซีเรีย ประเทศที่มีชายแดนติดกับอิสราเอล เคยเปิดการเจรจากับอิสราเอลผ่านทางตุรกี และได้มีความพยายามอย่างจริงจังแบบลับๆ ในอันที่จะครอบครองอาวุธนิวเคลียร์ ต่อมามีประเทศที่เป็นผู้เชี่ยวชาญได้เริ่มตั้งข้อสงสัยว่า ซีเรียกำลังสร้างระเบิดนิวเคลียร์ขึ้นมา จึงได้เกิดการวางแผนโจมตีอาคาร ที่ถูกสงสัยว่าเป็นสถานที่ผลิตนิวเคลียร์ แต่ยังไม่เป็นที่แน่ชัดว่า อาคารที่ถูกทำลายนั้นเป็นสถานที่ผลิตนิวเคลียร์จริงหรือไม่ ซึ่งมีผู้วิเคราะห์ว่า ซีเรียอาจไม่ใช่เป้าหมายที่แท้จริง แต่อิสราเอลกำลังส่งสัญญานเตือนไปยังอิหร่าน ให้เห็นว่าอิสราเอลสามารถโจมตีทำนองเดียวกันกับอาคารสถานที่ทางนิวเคลียร์ของอิหร่านได้ หากทางอิหร่านไม่ยุติโครงการพัฒนานิวเคลียร์

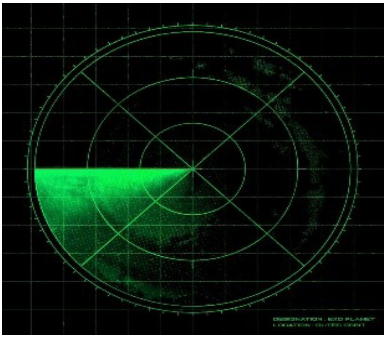
เมื่อเดือนกันยายน ปี ค.ศ.๒๐๐๗ กลุ่มอาคารแห่งหนึ่งทางตะวันออกของซีเรีย ซึ่งเป็นอาคารที่กำลังก่อสร้างโดยใช้คนงานเกาหลีเหนือ ถูกฝูงบินอิสราเอลโจมตี โดยแหล่งข่าวของอิสราเอลระบุว่า สถานที่ซึ่งถูกโจมตีเป็นโรงงานผลิตอาวุธนิวเคลียร์ที่ออกแบบโดยเกาหลีเหนือ

ที่มา https://mgronline.com/around/detail/9610000028253

อย่างไรก็ตาม เบื้องหลังความลึกลับทั้งหมดนี้ ยังมีเรื่องให้แปลกใจอยู่อีกอย่าง ที่ผ่านมาซีเรียใช้เงินหลายพันล้านดอลลาร์เพื่อระบบป้องกันภัยทางอากาศ ในค่ำคืนของเดือนกันยายนนั้น เจ้าหน้าที่ของกองทัพซีเรียก็จับตามองเรดาร์ของตนอย่างใกล้ชิดตลอดเวลา หลังจากที่ช่วงเช้าในวันนั้นอิสราเอลสั่งการให้ทหารของตนที่ประจำการอยู่บนที่ราบสูงโกลัน เตรียมพร้อมเต็มพิกัดจากที่มั่นของกองทหารดังกล่าวซึ่งเป็นพื้นที่ยึดครองอยู่ในดินแดนของซีเรีย และอิสราเอล ได้เข้าโจมตีอาคารที่ต้องสงสัยเมื่อเวลาเที่ยงคืน โดยส่งฝูงบินที่ประกอบด้วย F-15 อีเกิล และ F-16 ฟัลคอล โดยบินผ่านมาทางตุรกี ซึ่งเครื่องบินเหล่านี้ ยังอยู่ห่างไกลจากความสามารถในการล่องหน หลีกเร้นจากเรดาร์ ในขณะนั้นกองทัพซีเรียมีการเตรียมพร้อมอย่างสูงสุดระบบป้องกันภัยทางอากาศของซีเรียควรตรวจจับฝูงบินที่เข้ามาโจมตีได้ ควรมีสัญญานเตือน และควรเกิดจุดสว่างบนจอเรดาร์ของซีเรีย แต่ปรากฏว่าไม่มีสัญญานเตือน ไม่มีจุดสว่างบนจอเรดาร์ของซีเรียแม้แต่น้อยบนจอเรดาร์

ไม่มีอะไรผิดปกติปรากฏให้เห็น แสดงผลให้เห็นว่าน่านฟ้าของซีเรียนั้น ปลอดภัย

ที่มา : https://www.tnews.co.th/social/354249



ที่มา : https://twitter.com/siraxkyungsoo/status/1396119751777083399/photo/1

หลังเหตุการณ์ ซีเรียได้สรุปผลว่า ก่อนที่จะถูกโจมตีเครือข่ายระบบป้องกันภัยทางอากาศของซีเรียถูกครอบครองโดยอิสราเอล โดยเข้าไปควบคุมระบบป้องกันภัยทางอากาศไม่ให้ตรวจจับฝูงบินได้ ทำให้ไม่มีการแสดงภาพปรากฏบนจอเรดาร์ ภาพที่กองทัพซีเรียเห็นบนจอเรดาร์นั้นว่างเปล่า

น่านฟ้าไม่ถูกบุกรุกและมีความปลอดภัย แต่ในความเป็นจริงน่านฟ้าทางตะวันออกของซีเรีย ถูกบุกรุกและตกอยู่ภายใต้การโจมตีของฝูงบินทิ้งระเบิดอิสราเอล โดยระบบป้องกันภัยทางอากาศของซีเรียนั้นไม่สามารถระดมยิงได้ เพราะถูกควบคุมโดยอิสราเอล ซึ่งระบบป้องกันภัยทางอากาศของซีเรียนั้นสร้างโดยรัสเซีย ซีเรียจึงได้สอบถามไปที่รัสเซีย ให้ตรวจสอบว่าระบบนี้ผิดพลาดได้อย่างไร แต่บรรดาเหล่านักรบไซเบอร์กลับไม่ประหลาดใจกับเรื่องนี้ เพราะนักรบไซเบอร์อิสราเอลใช้วิธีการส่งไวรัสเข้าไปควบคุมเรดาร์ของซีเรีย ไม่ให้ซีเรียตรวจพบฝูงบินของอิสราเอลที่บุกเข้าโจมตี แทนที่จะใช้วิธีเข้าไปโจมตีทิ้งระเบิดเรดาร์ของซีเรีย ซึ่งอาจจะทำให้เกิดการสูญเสีย หรือภารกิจการทำลายเป้าหมายไม่สำเร็จได้ จะเห็นได้ว่าอิสราเอลวางแผนการโจมตีซีเรียในสงครามไซเบอร์ได้อย่างไร้ที่ติ เหลือเพียงประเด็นที่ว่า อิสราเอลทำได้อย่างไร ซึ่งมีความเป็นไปได้ ๓ วิธี ที่อิสราเอลสามารถครอบครองระบบการป้องกันภัยทางอากาศของซีเรียได้

วิธีแรก มีความเป็นไปได้ว่า ก่อนการโจมตีของอิสราเอลมีการส่ง (UAV) บินลักลอบเข้าไปในน่านฟ้าซีเรีย โดยจงใจบินเข้าไปอยู่ในแนวสัญญาณของระบบเรดาร์ป้องกันภัยทางอากาศของซีเรีย ตามหลักแล้วระบบเรดาร์จะส่งสัญญาณออกไปในทิศทางต่างๆ เมื่อสัญญาณที่ส่งไปกระทบกับวัตถุใดจะสะท้อนกลับมายังเครื่องรับ หลังจากนั้นระบบจะประมวลข้อมูลและแสดงผลออกมาว่า วัตถุที่สัญญาณกระทบนั้นอยู่ที่ใด บินอยู่ในระดับความสูงเท่าใด มีความเร็วเท่าไร และมีขนาดเล็กใหญ่เพียงใด ตรงนี้มีข้อเท็จจริงสำคัญประการหนึ่งอยู่ นั่นก็คือ สัญญาณเรดาร์ที่ส่งสัญญาณอิเล็กทรอนิกส์ออกไปในอากาศนั้นจะต้องอนุญาตให้รับสัญญาณที่สะท้อนกลับเข้ามายังระบบคอมพิวเตอร์ที่ติดตั้งไว้บนภาคพื้นดิน ดังนั้นเรดาร์จึงเป็นเสมือนประตูที่เปิดกว้างที่คอยรับสัญญาณอิเล็กทรอนิกส์ที่ส่งออกไปค้นหาอะไรก็ตามที่อยู่บนท้องฟ้ากลับเข้ามาในระบบ UAV ของอิสราเอลอาจไม่ถูกพบเห็นจากเรดาร์ระบบป้องกันภัยทางอากาศของซีเรีย เพราะอาจถูกเคลือบด้วย

วัสดุที่ดูดซับหรือหักเหทิศทางของสัญญานเรดาร์ไปทางอื่น แทนที่จะสะท้อนกลับไปยังแหล่งที่มา อย่างไรก็ตาม ยูเอวีนี้อาจตรวจจับสัญญาณเรดาร์ที่ถูกส่งออกมาจากภาคพื้นดินได้ หลังจากนั้นก็ใช้คลื่นความถี่เดียวกันส่ง “packet data”กลับไปยังคอมพิวเตอร์ของเรดาร์ และเครือข่ายระบบป้องกันภัยทางอากาศของซีเรียโดย “packet data” หรือชุดข้อมูลคอมพิวเตอร์ดังกล่าวทำให้ระบบทำงานผิดพลาด และควบคุมระบบแสดงผลให้เห็นภาพน่านฟ้าที่ว่างเปล่า แม้ว่าในขณะนั้นได้มีฝูงเครื่องบินรบของอิสราเอลบินเข้ามาโจมตีก็ตาม

วิธีที่สอง มีความเป็นไปได้ว่า รหัสคอมพิวเตอร์ของรัสเซียที่ใช้ในการควบคุมเครือข่ายระบบป้องกันภัยทางอากาศของซีเรียรั่วไหลโดยฝีมือของสายลับอิสราเอล ณ ที่ใดที่หนึ่ง อาจเป็นที่ห้องปฏิบัติงานของรัสเซียหรือสถานที่ทางด้านการทหารของซีเรียเอง หรืออาจมีผู้อื่นทำให้กับอิสราเอลโดยลักลอบติดตั้ง “Trapdoor” ซึ่งเป็นคำสั่งที่แฝงไว้ในระบบปฏิบัติการหรือแอพพลิเคชั่น มีหน้าที่ควบคุมการทำงานของโปรแกรมระบบป้องกันภัยทางอากาศ (การตรวจสอบการทำงานของซอฟแวร์ แม้กระทั่งผู้เชี่ยวชาญก็ยังไม่สามารถค้นหาความบกพร่องที่ถูกแทรกใส่ไว้ในซอฟต์แวร์ได้) โดย“Trapdoor” ที่ถูกใส่แฝงเอาไว้อาจถูกกำหนดให้รับคำสั่งหรือตอบสนองต่อสัญญาณโดยเฉพาะ เช่น เมื่อระบบประมวลผลของเรดาร์ตรวจพบสัญญาณอิเล็กทรอนิกส์พิเศษชุดหนึ่งแล้วตอบสนองโดยการควบคุมระบบให้แสดงผลว่าไม่มีเป้าหมายบนท้องฟ้าในช่วงเวลาที่กำหนดไว้ โดยต้องควบคุมเครื่อง UAV ให้ส่งชุดสัญญาณอิเล็กทรอนิกส์ ชุดหนึ่งสะท้อนกลับไปยังระบบคอมพิวเตอร์ภาคพื้นโดย “Trapdoor” อาจเป็นจุดเชื่อมต่อลับ ๆ ที่เปิดเป็นช่องทางไว้ให้สามารถเข้าถึงเครือข่ายระบบป้องกันภัยทางอากาศ โดยข้ามระบบตรวจสอบการล่วงล้ำและไฟร์วอลล์ ผ่านระบบการเข้ารหัสความปลอดภัยแล้วเข้าไปควบคุมทั้งเครือข่ายโดยมีสิทธิและอำนาจเทียบเท่ากับผู้ดูแลระบบ

วิธีที่สาม อิสราเอลส่งสายลับ “Hacker”เข้าไปในซีเรียและสามารถค้นพบเคเบิลไฟเบอร์ออพติกของเครือข่ายระบบป้องกันภัยทางอากาศในซีเรีย โดยได้เชื่อมต่อและ “Hack” เข้าไปในระบบผ่านเคเบิลฯ โดยควบคุมสั่งให้ “Trapdoor” เปิดช่องทาง แม้เป็นเรื่องที่เสี่ยงมากสำหรับสายลับอิสราเอลที่จะเข้าไปอยู่ในซีเรียเพื่อดำเนินการเชื่อมต่อเข้ากับเคเบิลฯ ก็ตาม แต่ก็ไม่ใช่เรื่องที่เป็นไปไม่ได้ มีรายงานออกมาว่า อิสราเอลได้ส่งสายลับ “Hacker” เข้าไปอยู่ที่ซีเรียมานานหลายสิบปีมาแล้ว เครือข่ายไฟเบอร์ออฟติกที่ใช้เพื่อรองรับระบบป้องกันภัยทางอากาศของซีเรียนั้นมีการเชื่อมต่อไปทั่วประเทศ ไม่จำกัดอยู่เฉพาะภายในที่ตั้งทางทหารเท่านั้น จึงทำให้สายลับสามารถปฏิบัติการในพื้นที่อื่นที่ไม่ใช่ที่ตั้งทางทหารเพื่อ “Hack” เข้าไปในเครือข่ายได้สะดวกขึ้น ทำให้การปฏิบัติการนั้นไม่ได้ขึ้นอยู่กับความสำเร็จของ UAV ที่จะต้องส่ง “packet data” สะท้อนกลับมาเพื่อแทรกเข้าสู่เน็ตเวิร์คภาคพื้นเพียงอย่างเดียว ที่สำคัญคือสายลับนั้นสามารถเชื่อมต่อสื่อสารผ่านสายเคเบิลไฟเบอร์ออพติกในพื้นที่กลับไปยังฐานบัญชาการของกองทัพอากาศอิสราเอลได้ โดยใช้วิธีการสื่อสารที่เรียกว่า “LPI” (Low-probability-of-intercept) ซึ่งเป็นการสื่อสารที่มีความเป็นไปได้ต่ำที่จะถูกดักจับสัญญาณได้ สายลับอิสราเอลอาจสามารถจัดตั้งช่องทางการสื่อสารลับ “Covert Communications Network (CCN)” แม้จะอยู่ในย่านธุรกิจในกลางกรุงดามัสกัส โดยเสี่ยงต่อการที่จะถูกตรวจพบในซีเรียได้น้อยมาก

ไม่ว่าจะเลือกใช้วิธีการใดเล่นงานเครือข่ายของระบบป้องกันภัยทางอากาศของซีเรีย มีความเป็นไปได้ว่ามันอาจจะมาจากตำรายุทธวิธีที่หยิบยืมมาจากสหรัฐอเมริกา

การเรียนรู้จากบทเรียนของสหรัฐอเมริกา

อิสราเอลได้เรียนรู้จากโปรแกรมการฝึกร่วมที่ดำเนินการมานาน

กว่าสองทศวรรษ ในปี ๑๙๙๐ ขณะที่สหรัฐอเมริกาเตรียมเข้าสู่สงครามกับอิรักเป็นครั้งแรก ขุนศึกไซเบอร์ยุคบุกเบิกของสหรัฐอเมริกาต้องทำงานร่วมกับหน่วยปฏิบัติการพิเศษ เพื่อหาวิธีการทำลายเรดาร์ และเครือข่ายระบบจรวดต่อต้านอากาศยานในระบบป้องกันภัยทางอากาศที่ครอบคลุมประเทศอิรักได้อย่างไร ก่อนที่ฝูงบินโจมตีของอเมริกาและพันธมิตรจะบินเข้าสู่น่านฟ้ากรุงแบกแดด ครั้งแรกมีแผนที่จะส่งสายลับ “Hacker”ร่วมไปกับหน่วยปฏิบัติการพิเศษเข้าไปในอิรักก่อนที่จะส่งฝูงบินเข้าไปโจมตี โดยให้สายลับ “Hacker”เข้าไปควบคุมระบบเรดาร์ทางด้านใต้ของอิรัก เพื่อทำหน้าที่ “Hack” เข้าไปในระบบเครือข่ายของอิรักจากภายในฐาน และจัดการส่งโปรแกรมไวรัสที่จะทำให้คอมพิวเตอร์ทุกตัวที่อยู่ในเน็ตเวิร์คล่มไปพร้อม ๆ กัน และไม่สามารถรีบูทใหม่ได้ แต่ นายพล ชวาร์ซคอรฟ์ ในขณะนั้นคิดว่าแผนดังกล่าวเสี่ยงและไม่มีความแน่นอน เขาไม่มั่นใจในการปฏิบัติของหน่วยปฏิบัติการพิเศษของสหรัฐอเมริกามากนัก และกลัวว่าหน่วยคอมมานโดที่ส่งเข้าไปจะตกเป็นเชลยศึกก่อนที่สงครามจะเปิดฉากด้วยซ้ำไป และชวาร์ซคอรฟ์ กลัวว่าฝ่ายอิรักจะสามารถรีบูทคอมพิวเตอร์ขึ้นมาใหม่ได้ ทำให้ระบบป้องกันภัยทางอากาศสามารถระดมยิงฝูงบินโจมตีที่ส่งเข้าไปโจมตี โดยแผนบินจะใช้มากกว่าสองพันเที่ยวในวันแรกของการโจมตีทางอากาศ “มีแนวความคิดว่า ถ้าคุณต้องการให้แน่ใจว่าเรดาร์และขีปนาวุธระบบป้องกันภัยทางอากาศของพวกนั้นจะทำงานไม่ได้ ต้องระเบิดมันทิ้งเสียก่อนเป็นสิ่งแรก แล้วถึงเข้าไปถล่มเป้าหมายด้านใน” ด้วยเหตุนี้ เที่ยวบินโจมตีเริ่มแรกของสหรัฐอเมริกาและพันธมิตรจึงถูกส่งเข้าไปโจมตีทิ้งระเบิดเข้าใส่เป้าหมายเป็นฐานที่ตั้งเรดาร์ และระบบจรวดต่อต้านอากาศยาน จึงทำให้เครื่องบินรบของสหรัฐและพันธมิตรบางส่วนถูกทำลายในการเข้าโจมตีเป้าหมายดังกล่าว และมีทหารบางส่วนถูกจับเป็นเชลยศึก ซึ่งเป็นบทเรียนที่สำคัญของอเมริกา

ผลจากบทเรียนของสหรัฐอเมริกา

ในอีก ๑๓ ปีต่อมา เมื่อสหรัฐอเมริกาเข้าสู่สงครามกับอิรักเป็นครั้งที่สอง ก่อนหน้าที่เครื่องบินโจมตี ของอเมริการะลอกแรกจะทะยานเข้าไป อเมริกาได้ทำสงครามไซเบอร์ก่อน โดยกองทัพอิรัก ได้รับรู้ล่วงหน้าว่าเครือข่ายคอมพิวเตอร์ของกองทัพที่เป็นเครือข่ายระบบปิด แยกเป็นเอกเทศและมั่นคงอย่างยิ่งนั้น ถูกทอนอานุภาพทั้งหมดลงแล้ว ซึ่งฝ่ายอเมริกาแจ้งให้พวกเขาได้รับรู้อย่างนั้น ทหารอิรักจำนวนมากได้รับอีเมล จากระบบอีเมลของกระทรวงกลาโหมอิรักเองก่อนหน้าที่สงครามจะเริ่มต้น และมีแหล่งข่าวที่เชื่อถือได้หลายคนเปิดเผยเนื้อความโดยสรุป เป็นไปในทำนองดังต่อไปนี้

“นี่คือสารจากศูนย์บัญชาการกองทัพสหรัฐอเมริกา ตามที่พวกท่านรับทราบกันอยู่แล้วกองทัพฯ อาจได้รับมอบหมายให้รุกเข้าไปในอิรักในอนาคตอันใกล้นี้ หากเป็นเช่นนั้น กองทัพฯจะทุ่มกำลังเข้าไปให้เหนือกว่ากำลังใดๆ ที่อาจใช้ต่อต้านเหมือนเช่นที่กองทัพฯ เคยใช้เมื่อหลายปีก่อนหน้านี้ ทางกองทัพฯ ไม่ต้องการให้เกิดอันตรายกับท่านหรือหน่วยทหารของท่าน เป้าหมายของกองทัพฯที่ได้รับมอบหมายมีเพียงประการเดียวนั่นคือการโค่นล้ม ซัดดัม ฮุสเซน และลูกชายทั้งสอง หากท่านไม่ต้องการให้เกิดอันตรายใด ๆ ขึ้น กรุณาสั่งการให้รถถังหรือยานยนต์หุ้มเกราะอื่นใดให้อยู่แต่ในที่ตั้งและทิ้งไว้อย่างนั้น ท่านและทหารของท่านควรกลับบ้าน ท่านและกองกำลังอื่น ๆ ของอิรักจะได้รับสถานภาพกลับคืนหลังการเปลี่ยนแปลงรัฐบาลในแบกแดดสิ้นสุดลงแล้ว”

ปรากฏว่าทหารอิรักจำนวนมากเชื่อข้อความในอีเมลของกองทัพอเมริกา ที่แพร่ไปผ่านเน็ตเวิร์คลับของกองทัพอิรัก ผู้บัญชาการฐานทัพอิรักบางราย อนุญาตให้ทหารลาพักกลับได้ก่อนสงครามเกิดขึ้นไม่กี่ชั่วโมง ทหารจำนวนมากเดินทางกลับบ้าน เมื่อกองกำลังของสหรัฐอเมริกาเข้าโจมตีได้พบว่ามีหลายหน่วยที่จอดรถถังเรียงแถวอย่างเป็นระเบียบภายในฐานส่งผลให้เครื่องบินรบของสหรัฐอเมริกาสามารถโจมตีทิ้งระเบิดทำลายได้อย่างง่ายดาย นี่คือการแฮกเข้าไปในระบบเครือข่ายสื่อสารทางทหารของอิรักเพื่อใช้ปฏิบัติการจิตวิทยาก่อนหน้าที่จะมีการโจมตีในรูปแบบปกติ

สงครามสหรัฐอเมริกา-อิรัก รอบที่สอง และเหตุการณ์ที่อิสราเอลโจมตีซีเรียถัดมาหลังจากนั้น แสดงให้เห็นการใช้ประโยชน์จากสงครามไซเบอร์ (Cyber War) เพื่อให้การโจมตีทางทหารตามรูปแบบเดิมง่ายขึ้น ด้วยการทำลายศักยภาพในการป้องกันตัวเองของฝ่ายศัตรู การปฏิบัติการจิตวิทยาโดยใช้การแจกจ่ายอีเมลหรือเครื่องมืออื่นใดในการสื่อสารผ่านอินเตอร์เน็ต แทนการโปรยใบปลิวที่ใช้กันก่อนหน้านี้ (คงจำกันได้ถึงใบปลิวจำนวนมาก ที่มีข้อความและภาพวาดแสดงวิธีการดำเนินการที่โปรยลงใส่กองกำลังของอิรักในปี ๑๙๙๑ บอกวิธีการต่อทหารเหล่านั้นว่าจะยอมจำนนต่อกองกำลังสหรัฐอเมริกาได้อย่างไร ทหารอิรักจำนวนไม่น้อยที่เก็บใบปลิวที่ว่านี้ติดมากับตัวเมื่อตอนที่ยอมแพ้ต่อกองทัพอเมริกา)

การโจมตีสถานที่ตั้งทางนิวเคลียร์ของซีเรียและปฏิบัติการในโลกไซเบอร์ของสหรัฐอเมริกาก่อนหน้าที่จะมีการส่งกำลังบุกเข้าไปในอิรัก คือตัวอย่างของการที่กองทัพ ใช้ “Hacker”เป็นเครื่องมือช่วยเหลือในการทำสงครามในรูปแบบที่เราคุ้นเคยกันมากกว่า อย่างไรก็ตาม การใช้ไซเบอร์สเปซเพื่อเป้าหมายทางการเมือง การทูต และการทหารของชาติใดชาติหนึ่งอาจไม่จำเป็นต้องลงเอยด้วยการส่งฝูงบินทิ้งระเบิดโจมตีหรือส่งกำลังทหารบุกเข้าไปโจมตีแต่อย่างใด

การโจมตีเอสโตเนียด้วย DDoS (Web War One)

เอสโตเนีย เป็นประเทศล้ำหน้าที่สุดด้านดิจิทัล แม้จะเป็นประเทศเล็ก ๆ โดยมีเมือง ทัลลินน์ (Tallinn) เป็นเมืองหลวงของประเทศ (มีประชากรราว ๔๐๐,๐๐๐ คน) ที่ได้แยกตัวออกมาเป็นอิสระภายหลังจากการล่มสลายของโซเวียต

ช่วงปี ค.ศ.๑๙๔๑ - ๑๙๔๔ เอสโตเนียถูกยึดครองโดยนาซีเยอรมัน และเมื่อสิ้นสงครามโลกครั้งที่ ๒ สหภาพโซเวียตมีชัยเหนือกองทัพนาซี เอสโตเนียจึงถูกยึดครองและผนวกเข้าเป็นส่วนหนึ่งของสหภาพโซเวียตและได้สร้างอนุสาวรีย์รูปปั้นสำริดทหารกองทัพแดง (Red Army) แห่งพรรคคอมมิวนิสต์โซเวียตไว้ เพื่อไม่ให้ชาวเอสโตเนียลืมความเสียสละ ของเหล่าทหารกองทัพแดงโซเวียต ที่ปลดปล่อยเอสโตเนียจากนาซี อนุสาวรีย์รูปปั้นสำริดทหารกองทัพแดง (Bronze Soldier of Tallinn) ตั้งอยู่ที่สุสานทหารแห่งทัลลินน์ (Defense Forces Cemetery of Tallinn)

เมื่อเอสโตเนีย ประกาศตัวเป็นอิสระอีกครั้ง ความขัดแย้งระหว่างชาวเอสโตเนีย กับชาวรัสเซียที่มาอาศัยอยู่ในเอสโตเนียก็เริ่มขึ้น เมื่อคนส่วนใหญ่ในเอสโตเนียพยายามลบล้างสัญลักษณ์ใดๆ ที่บ่งบอกถึงการตกเป็นเมืองขึ้นรัสเซียออกไป ต่อมารัฐบาลเอสโตเนีย ออกกฎหมายการอนุรักษ์หลุมฝังศพของทหารจากสงคราม เนื่องจากต้องการปกป้องหลุมฝังศพวีรบุรุษของชาติ และมรดกทางประวัติศาสตร์ จึงส่งผลให้สิ่งปลูกสร้างที่มีลักษณะต้องห้าม เช่น รูปปั้นสำริดทหารกองทัพแดงโซเวียตจะต้องถูกรื้อถอน และศพทหารโซเวียตจะต้องถูกเคลื่อนย้ายออกจากสุสานทหารเอสโตเนีย

ค่ำวันที่ ๒๗ เมษายน ค.ศ.๒๕๕๐ สื่อทั่วโลกเรียกว่า “Bronze Night” เกิดจลาจลระหว่างฝ่ายคัดค้านการย้ายรูปปั้นสำริดทหารกองทัพแดง (กลุ่มคนเชื้อสายรัสเซีย) และฝ่ายสนับสนุนการย้าย (กลุ่มชาตินิยมเอสโตเนีย) เกิดการตะลุมบอนกันจนทำให้มีผู้เสียชีวิต รัฐบาลเอสโตเนีย จึงได้เคลื่อนย้ายรูปปั้นสำริดทหารกองทัพแดง ออกจากสุสานทหารเอสโตเนียไปที่ใหม่

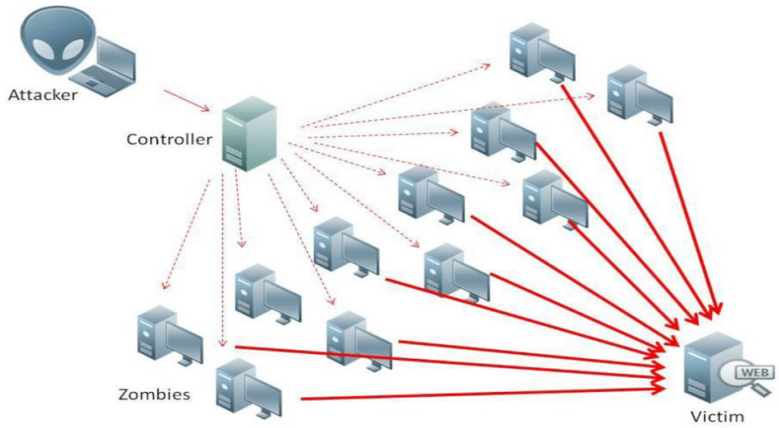
และได้ส่งทหารมาอารักขารูปปั้น ทำให้เหตุการณ์ต่อสู้กันบนถนนได้สงบลง แต่ความขัดแย้งบนโลกความเป็นจริงได้ย้ายการต่อสู้กันมาบนโลกไซเบอร์สเปซแทน

(The Bronze Soldier monument at the Defense Forces Cemetery of Tallinn)
ที่มา https://www.atlasobscura.com/places/the-bronze-soldier-of-tallinn-tallinn-estonia

เอสโตเนียได้รับเอกราชเพียง ๒๕ ปี แต่ได้รับการยกย่องว่าเป็นสังคมเศรษฐกิจดิจิทัลที่ก้าวหน้าที่สุดแห่งหนึ่งของโลก ความสำเร็จต่าง ๆ ถูกกล่าวขานถึงทั้ง e-Society e-Government e-Residency e-Voting etc. บริการออนไลน์ของภาครัฐ และภาคเอกชน ครอบคลุมแทบทุกมิติของประชากรชาวเอสโตเนีย การจ่ายภาษีออนไลน์ การทำธุรกรรมธนาคารออนไลน์ บัตรประชาชนอิเล็กทรอนิกส์ ข้อมูลด้านสุขภาพของประชาชนถูกจัดเก็บไว้อย่างเป็นระบบ บนคลาวด์ ฯลฯ

ไม่กี่วันหลังจากเหตุการณ์ “Bronze Night” บรรดา Server ที่ให้บริการต่างๆ ในเอสโตเนียถูกโจมตีโดยมีการส่งคำขอเข้าสู่หน้าเว็บ (Request to send) จำนวนมหาศาลจนทำให้ Server Down การบริการต่าง ๆ ปิดตัวลง และบาง Server ได้รับคำสั่ง Ping เข้ามาจำนวนมหาศาลจนเว็บค้าง ไม่สามารถให้บริการได้ รวมทั้งระบบรัฐบาลอิเล็กทรอนิกส์ไม่สามารถให้บริการได้ โดนการโจมตีที่เรียกว่า DDoS Attack

DDoS “Dustributed-Denial-of-service” Attack เป็นการโจมตีทางไซเบอร์ด้วยวิธีการส่ง “packet data” ปริมาณมหาศาลโจมตีไปยัง Server เป้าหมาย เมื่อ Server เป้าหมายได้รับข้อมูลจำนวนมหาศาลจนปริมาณ Traffic data ในการรับส่งใช้เวลาการทำงานหนักมากจนไม่สามารถให้บริการได้ เช่น ได้รับ E-mail ขยะจำนวนมหาศาลนับล้านๆ ฉบับมายัง Server เป้าหมาย หรือการส่ง TCP SYN Flood DOS Attack (การส่ง Packet TCP/SYN โดยใช้ IP ที่ไม่มีอยู่จริง) ทำให้ Server ที่ถูกโจมตีต้องใช้หน่วยความจำในการประมวลผลจำนวนมาก เป็นผลให้การทำงานไม่ปกติ หรือการส่ง Ping of Death คือการส่งแพ็คเกจขนาดใหญ่มากกว่าปกติเข้ามาเรื่อย ๆ จน Server รองรับไม่ไหว นอกจากนั้นการโจมตีทางไซเบอร์ “Hacker” ยังสามารถยืมมือคนอื่นช่วยโจมตีได้ด้วยการ “Hack” คอมพิวเตอร์จำนวนมาก อาจถึงล้านเครื่องช่วยโจมตีโดยใช้ Malware ส่งไปฝังไว้ที่คอมพิวเตอร์ ของคนอื่น ๆ หรือองค์กรอื่น ๆ ซึ่งเรียกบรรดาเครื่องคอมพิวเตอร์ที่ถูกฝัง Malware ไว้เพื่อควบคุมช่วยในการโจมตี เหล่านั้นว่า Zombie หรือ Botnet



การโจมตีแบบ DDOS Attack

ที่มา https://www.atlasobscura.com/places/the-bronze-soldier-of-tallinn-tallinn-estonia

DDoS Attack ดูเหมือนเป็นแค่เรื่องก่อกวนเล็กน้อย ไม่ใช่อาวุธหนักสำหรับการทำสงครามไซเบอร์ แต่ในครั้งนั้นรัฐบาลเอสโตเนียถูกโจมตีด้วย DDoS Attack โดยควบคุมเครื่องคอมพิวเตอร์ที่ถูกฝัง Malware ไว้ให้เป็น Zombie และ Botnet ซึ่งมีเป็นจำนวนนับหมื่นนับแสนเครื่องให้ส่ง “packet data” ปริมาณมหาศาลโจมตีต่อเนื่องยาวนานนับสัปดาห์ ซึ่งเจ้าของเครื่องคอมพิวเตอร์ ไม่มีทางทราบได้เลยว่า ตนตกเป็นเหยื่อที่เครื่องคอมพิวเตอร์ถูกทำให้ กลายเป็น Zombie หรือ Botnet ที่นำไปเข้าร่วมการโจมตีด้วย

เอสโตเนียถูกโจมตีด้วย DDoS ครั้งใหญ่ที่สุดในประวัติศาสตร์โดย Server เว็บไซต์ต่าง ๆ รวมถึง Server ของระบบเครือข่ายโทรศัพท์เคลื่อนที่ ระบบการสื่อสาร หนังสือพิมพ์ ธนาคารออนไลน์ และระบบพาณิชย์อิเล็กทรอนิกส์ของรัฐบาลถูกโจมตี จนทำให้ Server Down ลงทั้งหมด และเอสโตเนียได้ร้องขอความช่วยเหลือไปที่สภาความร่วมมือแอตแลนติกเหนือ (North Atlantic Cooperation Council) องค์กรของกลุ่มประเทศพันธมิตรทางทหารนาโต้ และได้ส่งผู้เชี่ยวชาญด้าน Cyber security จากยุโรป และอเมริกา เดินทางไปช่วยเหลือทันที ซึ่งผู้เชี่ยวชาญได้ทำการแกะรอย Track back ย้อนรอยคำสั่ง Ping ไปยังเครื่องคอมพิวเตอร์ Zombie จำนวนหนึ่ง เมื่อเครื่องคอมพิวเตอร์ Zombie เหล่านั้น เรียกกลับ ไปยังผู้ควบคุมมันอยู่ สุดท้ายผู้เชี่ยวชาญได้อ้างจากผลการตรวจสอบ พบว่าเครื่องคอมพิวเตอร์ลำดับสุดท้ายที่ใช้ในการควบคุมการโจมตีนั้นมาจากรัสเซีย แต่รัสเซียแถลงปฏิเสธว่า มิได้อยู่เบื้องหลังการโจมตีทางไซเบอร์กับเอสโตเนีย และ ยังปฏิเสธคำร้องขอทางการทูตอย่างเป็นทางการในการให้ความช่วยเหลือแกะรอยผู้ควบคุมการโจมตีครั้งนี้ ถึงแม้จะมีความตกลงทวิภาคีที่ระบุว่ารัสเซียต้องให้ความร่วมมืออยู่ก็ตาม

ริชาร์ด และ โรเบิร์ต (Richard and Robert, 2012) เชื่อว่าเป็น “กลุ่มรัสเซียรักชาติ” กลุ่มชาตินิยมรัสเซียรุ่นใหม่กลุ่มวัยรุ่นคลั่งชาติ และเป็นกลุ่มแฮกเกอร์ที่ชำนาญที่สุดในรัสเซีย ส่วนใหญ่คนเหล่านี้ทำงานให้องค์กรอาชญากรรม

อาชญากรรมแห่งความเกลียดชัง (Hate crime) เป็นภัยคุกคามชาติอย่างรุนแรง และยากที่คนทั่วไปจะรู้เท่าทัน เพราะเป็นทฤษฎีทางอาชญาวิทยา หากแบ่งคนในชาติเป็นสองฝ่าย และนำเรื่องความเชื่อ เคารพ ศรัทธาที่แตกต่างกันมาทำเป็นประเด็นสร้างความแตกแยก และเมื่อความชิงชังขยายวงกว้างเมื่อไรจะทำให้คนชาติเดียวกันลุกขึ้นมาทำลายล้างกันเอง อันที่จริงเหตุการณ์ Bronze night มีการใช้ Fake news สร้างความแตกแยก สร้างข่าวปลอม ให้เกิดความเกลียดชังผ่านโลกออนไลน์ เป็นปรากฏการณ์ที่คล้าย ๆ จะเกิดขึ้นในหลาย ๆ ประเทศในปัจจุบัน เพียงแต่บทความนี้เน้นเรื่อง DDoS เป็นสำคัญ และคงไม่ยากนักที่ประเทศต่าง ๆ จะเตรียมการรับมือภัยคุกคามรูปแบบใหม่ ๆ เหล่านี้ในอนาคต

หลังจากเอสโตเนียถูกโจมตีทางไซเบอร์ หลังจากเหตุการณ์ “Bronze Night” นาโต้ได้เตรียมการป้องกันภัยทางไซเบอร์ โดยนาโตได้จัดตั้งศูนย์ป้องกันภัยทางไซเบอร์ “Cooperative Cyber Defence Centre of Excellence” ขึ้นมา และเปิดดำเนินการอย่างเป็นทางการเมื่อปี ๒๐๐๘ ตั้งอยู่ที่ทัลลินน์ประเทศเอสโตเนีย

การโจมตีโรงงานนิวเคลียร์ของอิหร่านโดยหนอนไวรัส Stuxnet

ที่มา : https://www.zdnet.com/pictures/the-worlds-most-famous-and-dangerous-apt-state-developed-malware/

Stuxnet Worm ถูกค้นพบในปี ๒๐๑๐ ซึ่งเป็นตัวอย่างของการใช้กลยุทธ์แบบ (Multiple Layers) ในการโจมตี ที่นำมาใช้จนประสบความสำเร็จ เนื่องจากมีเจ้าหน้าที่ ที่ทำงานในโครงการพลังงานนิวเคลียร์ของอิหร่าน อาจตั้งใจหรือไม่ได้ตั้งใจก็ไม่ทราบได้ ได้ทำการเสียบอุปกรณ์ USB ที่ติดไวรัส Stuxnet Worm ทำให้ไวรัสแพร่เข้าสู่ระบบ Air-gapped หลังจากนั้น มัลแวร์ (Malware) ได้เข้าโจมตีแบบ (Zero-Day Exploits) “การโจมตีช่องโหว่ที่ไม่เคยถูกค้นพบมาก่อน” ในทันทีโดยที่ไม่ทันตั้งตัว โดยมีเป้าหมายค้นหาซอฟต์แวร์เฉพาะสำหรับการควบคุมเครื่องหมุนเหวี่ยง จากนั้นไวรัสจะดำเนินการตั้งโปรแกรมใหม่ เพื่อควบคุมให้เครื่องหมุนเหวี่ยงหมุนรอบตัวเองอย่างรวดเร็วมากผิดปกติ แล้วก็กลับมาหมุนช้า ๆ แบบที่ไม่สามารถตรวจจับได้ ทำงานแบบนี้อยู่หลายเดือน จนในที่สุดเครื่องหมุนเหวี่ยงเกิดการแตกเสียหาย เครื่องมากกว่า ๑,๐๐๐ เครื่องถูกทำลายแม้ว่าจะไม่มีใครออกมารับผิดชอบเรื่องการโจมตี แต่ก็เป็นที่รู้ว่าถูกโจมตีด้วยไวรัสซึ่งเป็นอาวุธทางไซเบอร์ (Cyber Weapon) ที่ถูกสร้างขึ้น โดยเป็นความพยายามที่เกิดจากความร่วมมือกันระหว่างกองทัพอิสราเอล และสหรัฐฯ แต่ทั้งสองประเทศได้ปฏิเสธในเรื่องนี้

ย้อนกลับไปเมื่อช่วงปี ค.ศ.๑๙๕๐ ที่สหรัฐฯ ได้พัฒนาโครงการปรมาณูเพื่อสันติและมองหาประเทศพันธมิตร เพื่อทดลองสร้างโรงไฟฟ้านิวเคลียร์สำหรับการผลิตไฟฟ้าให้พลเรือน ซึ่งอิหร่านได้รับอนุญาตให้พัฒนาได้ ซึ่งขณะนั้นยังเป็นพันธมิตรกันอยู่ เมื่อปี ค.ศ.๑๙๗๙ เกิดการปฏิวัติในอิหร่าน ผู้นำในเวลานั้นได้สั่งหยุดโครงการนิวเคลียร์ทั้งหมด แต่หลังจากการปฏิวัติ ๕ ปี ผู้นำของอิหร่านได้รื้อฟื้นโครงการโรงไฟฟ้านิวเคลียร์สำหรับการผลิตไฟฟ้าให้พลเรือนขึ้นมาใหม่ แต่หลายฝ่ายเชื่อว่าโครงการที่แท้จริงคือการผลิตอาวุธนิวเคลียร์

ภาพถ่ายดาวเทียมที่ไม่ระบุวันที่ล่าสุดนี้จัดทำโดย Space Imaging/Inta SpaceTurk แสดงศูนย์นิวเคลียร์ Natanz ที่ครั้งหนึ่งเคยเป็นความลับในเมือง Natanz ประเทศอิหร่าน ห่างจากกรุงเตหะรานไปทางใต้ประมาณ ๑๕๐ ไมล์

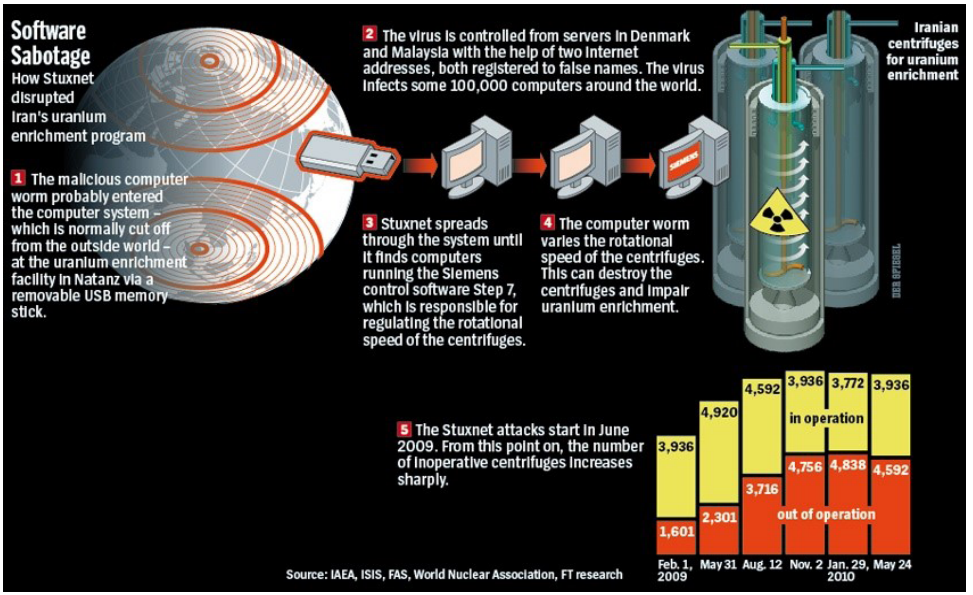
ที่มา:https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

ในปี ๒๐๐๖ สหรัฐฯ และอิสราเอลได้หารือกับเจ้าหน้าที่หลายฝ่ายในการยับยั้งการพัฒนานิวเคลียร์ของอิหร่าน โดยป้องกันไม่ให้เกิดสงครามระหว่างประเทศขึ้น ซึ่งมีทางเลือกอยู่สองทางคือ ให้อิหร่านพัฒนานิวเคลียร์ต่อไป หรือเข้าไปทำสงคราม

ต่อมาหน่วยงาน US Strategic Command ซึ่งดูแลหัวรบนิวเคลียร์เสนอให้ใช้กลยุทธ์ซื้อเวลา เพื่อให้สามารถเข้าไปเจรจาทางการทูต และให้สหประชาชาติคว่ำบาตร และเรียกร้องให้อิหร่านลงนามใน Joint Comprehensive Plan of Action เพื่อป้องกันไม่ให้อิหร่านสร้างหัวรบนิวเคลียร์ขึ้น ซึ่งกลยุทธ์ซื้อเวลาคือการส่งไวรัส Stuxnet Worm เข้าไปโจมตีโรงงานนิวเคลียร์ของอิหร่าน โดยแพร่กระจายผ่านระบบเน็ตเวิร์คโดย Stuxnet Worm มีหน้าที่ทำให้เตาปั่น (Centrifuge) ที่ใช้แยกไอโซโทปของยูเรเนียม ปั่นเร็วขึ้นกว่าปกติหลังจากนั้นให้ปั่นเร็วปกติ ต่อมาให้ปั่นช้าลงกว่าปกติ ๕๐ นาที แล้วให้ปั่นเร็วปกติ วนลูปซ้ำไปเรื่อย ๆ นานหลายเดือน แต่ที่สำคัญคือ Stuxnet Worm จะส่งข้อความกลับมาแสดงผลว่าเตาปั่นทำงานปกติ ดังนั้นเจ้าหน้าที่จะไม่รู้เลยว่าโรงงานนิวเคลียร์กำลังตกอยู่ในความเสี่ยงที่จะเกิดความเสียหายร้ายแรง

Stuxnet Worm ถูกค้นพบมาก่อนแล้วแต่ยังไม่มีใครรู้เป้าหมายการทำงานที่แท้จริง นักถอดรหัสพบว่าการทำงานของ Stuxnet นั้นแปลกมาก แม้เขาจะทำให้เครื่องคอมพิวเตอร์ของตนเองติดไวรัสตัวนี้ แต่มันกลับไม่ทำอะไร ได้แต่เพิ่มจำนวน “Stuxnet Worm ได้ถูกกำหนดเป้าหมายเฉพาะในการโจมตีไว้คือระบบ Windows และติดตั้งโปรแกรม Siemens Step7 ซึ่งเป็นโปรแกรมที่ใช้ควบคุมอุปกรณ์ในโรงงานอุตสาหกรรม” เนื่องจากเน็ตเวิร์คของโรงงานนิวเคลียร์ในเมืองนาทานซ์ของอิหร่าน เป็นระบบปิด ไม่มีการเชื่อมต่อกับอินเทอร์เน็ตภายนอก จึงเป็นไปไม่ได้ที่สหรัฐฯ หรืออิสราเอลจะส่งไวรัสพวกนี้ผ่านอินเทอร์เน็ตเข้ามาในโรงงาน

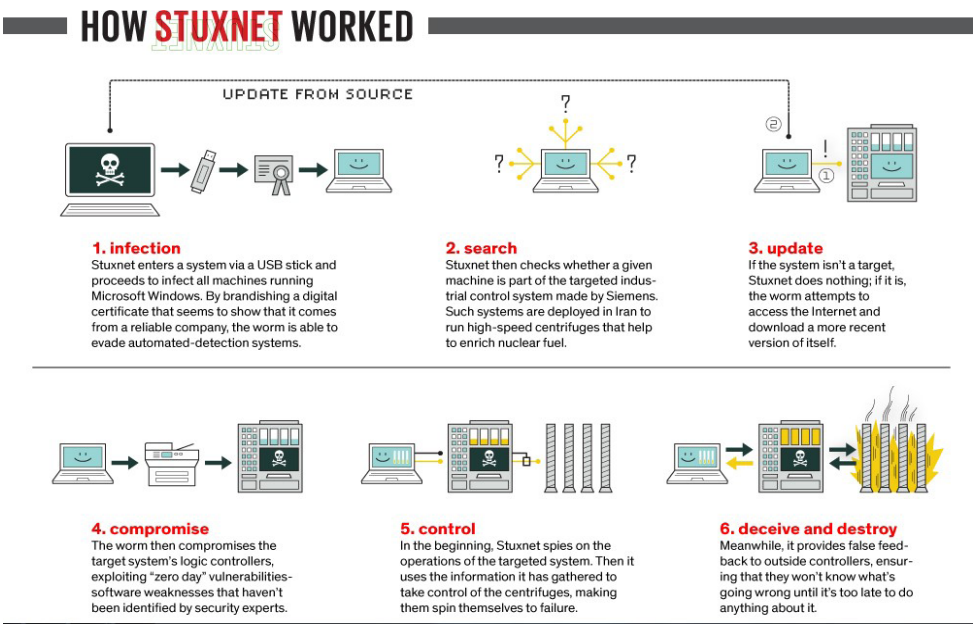
Stuxnet Worm เข้าสู่ระบบปิดได้อย่างไร



กราฟิกนี้แสดงให้เห็นว่าเวิร์ม Stuxnet ทำงานอย่างไร เวิร์มตัวนี้เพียงพอที่จะสร้างความเสียหายอย่างมีนัยสำคัญต่อโครงการอาวุธนิวเคลียร์ของอิหร่าน

ที่มา : https://www.armadainternational.com/2017/10/a-fatal-error-has-occurred/

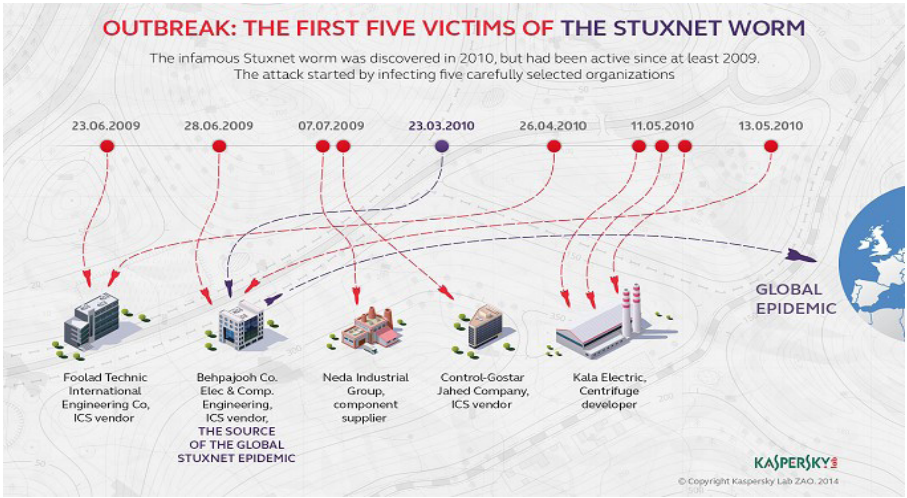
มีหลายทฤษฎีเกิดขึ้นเกี่ยวกับวิธีการส่งไวรัสเข้าสู่ระบบปิดของโรงงานนิวเคลียร์ อย่างแรก คืออิสราเอล ได้รวบรวมรายชื่อเจ้าหน้าที่ที่ทำงานเกี่ยวข้องกับเตาปั่นในโรงงาน เมื่อได้รายชื่อแล้วจึงปล่อยไวรัสให้แพร่เข้าไปที่คอมพิวเตอร์ของเจ้าหน้าที่เหล่านั้นผ่านเครือข่ายอินเทอร์เน็ต ในขณะที่พวกเขาทำงานอยู่ที่บ้าน ซึ่งเมื่อที่เจ้าหน้าที่เสียบไดรฟ์ USB เข้าโน้ตบุ๊กของตัวเองจึงทำให้ USB ของเจ้าหน้าที่ติดไวรัสเข้าไปด้วย และเมื่อเจ้าหน้าที่ได้เสียบไดรฟ์ USB ที่ติดไวรัสเข้าไปในคอมพิวเตอร์ของโรงงาน Stuxnet Worm จะเข้าสู่คอมพิวเตอร์ของโรงงาน พร้อมเข้าโจมตีคอมพิวเตอร์ที่กำหนดไว้ ซึ่งทฤษฎีแรกนี้มีผู้เชื่อว่าเจ้าหน้าที่ นำไวรัสเข้าไปจริง ๆ



ภาพที่แสดงถึงกระบวนการที่อยู่เบื้องหลังการโจมตีอย่างดี (ได้รับความอนุเคราะห์จาก IEEE)

ที่มา : https://gemserv.com/our-thoughts/stuxnet-the-first-cyber-weapon/

อีกทฤษฎีหนึ่งเชื่อว่า ได้มีการแพร่ไวรัสเข้าไปยังคอมพิวเตอร์หรืออุปกรณ์ ที่เป็นซัพพลายเออร์ของโรงงานนิวเคลียร์ในเมืองนาทานซ์ โดยจากการตรวจสอบแล้วพบว่ามีบริษัทซัพพลายเออร์ ๕ แห่ง ที่ส่งอุปกรณ์อิเล็กทรอนิกส์ให้กับโรงงานฯ ในเมืองนาทานซ์นั้น มีไวรัส Stuxnet Worm อยู่ด้วย ดังนั้น จึงเป็นไปได้ว่าไวรัสอาจถูกแพร่ผ่านจากซัพพลายเออร์เหล่านี้ โดยมีข้อสนับสนุนที่ค้นพบในช่วงหลังว่า ไวรัส Stuxnet Worm ถูกสร้างมาตั้งแต่ปี ค.ศ.๒๐๐๕ แล้ว



Stuxnet Zero Victims ตัวตนของบริษัทที่ตกเป็นเป้าหมายของอาวุธไซเบอร์ตัวแรก

ที่มา: https://www.kaspersky.com/blog/stuxnet-victims-zero/6775/

Stuxnet Worm ทำงานสำเร็จ

Stuxnet Worm สามารถทำงานได้อย่างดีเยี่ยม คือ Stuxnet Worm ถูกค้นพบหลังจากที่ทำความเสียหายต่อเตาปฏิกรณ์ของโรงงานนิวเคลียร์ ส่วนการค้นพบนั้น เริ่มจากที่นักถอดรหัสได้ศึกษาพฤติกรรม Stuxnet Worm ไว้ก่อนหน้า พบว่าได้ถูกแพร่ไปที่อิหร่านเป็นจำนวนมาก

รวมถึงเกิดการผิดพลาดของไวรัสเองที่แสดงโค้ดของตัวเองออกมาบนอินเทอร์เน็ต (ขณะที่พวกมันแฝงตัวอยู่ในโน้ตบุ๊กของเจ้าหน้าที่) ทำให้นักถอดรหัสตรวจสอบพบและแจ้งไปยังอิหร่าน

Stuxnet Worm สามารถยื้อเวลาให้อิหร่านหยุดพัฒนาหัวรบนิวเคลียร์ได้ชั่วคราว และนำไปสู่การเจรจาพร้อมลงนามในสัญญา Joint Comprehensive Plan of Action ได้ในที่สุด นับว่า Stuxnet Worm เป็นหนอนไวรัสที่ถูกใช้เป็นอาวุธไซเบอร์ครั้งแรก

สหรัฐอเมริกาเริ่มปฏิบัติการซ้อมรบในสงครามไซเบอร์

สหรัฐอเมริกาเริ่มปฏิบัติการซ้อมรบในสงครามไซเบอร์ ที่รู้จักกันในชื่อ “Cyber Storm” เพื่อทดสอบการป้องกันระบบเครือข่ายคอมพิวเตอร์ โดยการซ้อมรบในปี ค.ศ.๒๐๐๙ มีชาติต่าง ๆ เข้าร่วมคือ ญี่ปุ่น เกาหลีใต้ แต่สื่อมวลชนในเกาหลีเหนือได้ตอบโต้การซ้อมรบดังกล่าว เนื่องจากเห็นว่าการซ้อมรบที่จะมีขึ้นนั้นเป็นฉากบังหน้าเพื่อเตรียมการรุกรานเกาหลีเหนือ ซึ่งเป็นปกติที่เกาหลีเหนือดำเนินการมาตลอด

ในวันที่ ๔ กรกฎาคม อเมริกาตรวจพบการยิงจรวดจากเกาหลีเหนือ ซึ่งเป็นจรวดพิสัยใกล้ และมีเป้าหมายยิงใส่ทะเล โดยมีการยิงทั้งหมด ๗ ลูก แต่เหตุการณ์ไม่ได้หยุดลงเพียงเท่านั้น ได้มีการโจมตีทาง ไซเบอร์สเปซด้วย โดยก่อนหน้าที่จะถึงวันชาติอเมริกา แฮกเกอร์ ได้แพร่ไวรัสไปยังคอมพิวเตอร์ประมาณ ๔๐,๐๐๐ เครื่องทั่วโลก ทำให้คอมพิวเตอร์ติดเชื้อไวรัสกลายเป็น Zombie และ Botnet โดยควบคุมสั่งการให้คอมพิวเตอร์เหล่านั้นส่งคำสั่ง “Ping” ไปยังเว็บไซต์ที่เป็นของรัฐบาลเกาหลีใต้และสหรัฐอเมริกา รวมถึงบรรดาบริษัทต่าง ๆ เมื่อคอมพิวเตอร์ที่ติดไวรัสถูกเปิดขึ้นใช้งาน จะถูกควบคุมเข้าร่วมการโจมตี ซึ่งเป็นการโจมตีด้วย DDoS โดยเครื่องคอมพิวเตอร์ในเครือข่ายที่ติดไวรัส กลายเป็น Zombie และ Botnet ได้ถูกควบคุมให้ส่งคำสั่งร้องขอเข้าเว็บไซต์เป็นจำนวนมหาศาลพร้อม ๆ กัน ซึ่งเว็บไซต์ของ

ทางการอเมริกา ถูกโจมตีด้วยคำขอมากถึง ๑ ล้านครั้งต่อวินาที ทำให้ server เว็บไซต์หน่วยงานต่าง ๆ ถูกโจมตีจนระบบ server down ในช่วงใดช่วงหนึ่งระหว่างวันที่ ๔ จนถึงวันที่ ๙ กรกฎาคม เช่น เว็บไซต์ของกระทรวงการคลัง หน่วยสืบราชการลับ กระทรวงการขนส่ง เว็บไซต์ของแนสแดค ตลาดซื้อขายโภคภัณฑ์ล่วงหน้าที่นิวยอร์ก ตลาดหลักทรัพย์นิวยอร์ก วอชิงตันโพสต์ เป็นต้น

ข้อสังเกต การโจมตีทำเนียบขาวนั้นล้มเหลว เนื่องจากมีการป้องกันการโจมตีด้วย DDoS หลังจากที่เกิดขึ้นครั้งแรกเมื่อปี ค.ศ.๑๙๙๙ โดยทำการแยก packet data ที่พยายามเข้าถึงเว็บไซต์ของทำเนียบขาวไปยัง server ที่กระจายอยู่ทั่วโลก มากกว่า ๒๐,๐๐๐ server เมื่อใดก็ตามที่มีการร้องขอเข้าถึงเว็บไซต์ทำเนียบขาว packet data นั้นจะถูกส่งไปยังเซิร์ฟเวอร์ที่ใกล้ผู้ที่ออกคำสั่งมากที่สุด ดังนั้น เมื่อแฮกเกอร์ส่ง packet data โจมตีเว็บไซต์ทำเนียบขาว packet data ที่ส่งมาจะถูกส่งไปยังเซิร์ฟเวอร์ที่อยู่ใกล้กับผู้ออกคำสั่งโจมตีมากที่สุด ดังนั้นจึงมีเพียงสถานที่ต่างๆในเอเชีย ที่ทำหน้าที่รองรับการโจมตี เว็บไซต์ของทำเนียบขาว คือ server ในเอเชียที่เจอปัญหายุ่งยากในการถูกโจมตีด้วย DDoS แทนสหรัฐอเมริกา หลังจากนั้น สหรัฐอเมริกาก็ออกมาแถลงขออภัยต่อบรรดาผู้ใช้งานเว็บไซต์ในเอเชีย ซึ่งมีข้อสงสัยว่าที่อเมริกาทำนั้นถูกต้องหรือไม่

หลังจากนั้นการโจมตีที่เกิดขึ้นต่อมาคือ คอมพิวเตอร์ประมาณ ๓๐,๐๐๐ ถึง ๖๐,๐๐๐ เครื่องทั่วโลก ที่ติดเชื้อไวรัสกลายเป็น Zombie และ Botnet ถูกควบคุมให้โจมตีเว็บไซต์ของเกาหลีใต้ ทั้งที่เป็นเว็บไซต์ของรัฐบาล ธนาคาร บริษัทต่างๆ ที่ให้บริการบนอินเตอร์เน็ต ตั้งแต่วันที่ ๙ กรกฎาคม จนถึงวันที่ ๑๐ กรกฎาคม การโจมตีระลอกสุดท้ายนั้นมีเครื่องคอมพิวเตอร์ที่โจมตีเข้ามาเพิ่มจำนวนมากขึ้นถึง ๑๖๖,๐๐๐ เครื่อง

อเมริกาไม่ได้มีความเห็นว่าการโจมตีครั้งนี้เป็นเกาหลีเหนือ แต่เกาหลีใต้มีความเห็นว่า เกาหลีเหนือ คือผู้ต้องสงสัยลำดับแรก จากการ

ตรวจสอบการโจมตีนั้นใช้ ๘ server เป็น Host ทำหน้าที่ควบคุม คอมพิวเตอร์อื่นๆ ในเครือข่ายทั้งหมดในการโจมตี โดย server นั้นอยู่ใน เกาหลีใต้, สหรัฐอเมริกา, เยอรมนี, ออสเตรีย และ จอร์เจีย โดยทั้ง ๘ server นั้นถูกควบคุมโดย server อีกแห่งซึ่งตั้งอยู่ในเมืองไบรตัน ประเทศอังกฤษ (บริษัท Bach Khoa Internetwork Security “BKIS” ระบุในบล็อกบริษัทว่าสามารถตรวจพบเซิร์ฟเวอร์ ๒ ตัว ที่เป็นเครื่องสั่งการในการโจมตีครั้งนี้ พบว่าเซิร์ฟเวอร์ดังกล่าวมีหมายเลขไอพีแอดเดรสในช่วง 195.90.118.x ซึ่งเป็นแอดเดรสที่ถูกลงทะเบียนไว้ในศูนย์ Global Digital Broadcast ที่ตั้งอยู่ใน สหราชอาณาจักร เป็นเครื่องควบคุมคอมพิวเตอร์ที่มีมัลแวร์ฝังอยู่ ๑๖๖,๙๐๘ เครื่องใน ๗๔ ประเทศ)

สำนักงานข่าวกรองแห่งชาติเกาหลีใต้ “NIS” ยืนยันว่า หน่วยแฮกเกอร์เกาหลีเหนือ ที่ชื่อ “Lab 110” (โดยมีกลุ่มที่ชื่อ Lazarus หรือเป็นที่รู้จักกันในชื่อ Hidden Cobra นั้นเป็นขบวนการแฮกเกอร์ของเกาหลีเหนือ ซึ่งเคยโจมตีหน่วยงานรัฐบาลของประเทศต่าง ๆ หรือองค์กรต่าง ๆ ทั่วโลกตั้งแต่ปี ค.ศ.๒๐๐๙ และเชื่อว่ากลุ่ม Lazarus นี้ทำงานภายใต้องค์กรที่ดูแลการเจาะระบบ ที่ขึ้นตรงกับรัฐบาลเกาหลีเหนืออย่าง Reconnaissance General Bureau โดยกลุ่มนี้ได้ใช้เทคนิคการโจมตีหลากหลายแบบเช่น Zero-day, Phishing, Malware, Backdoor, เผยแพร่ข้อมูลปลอม หรือฝังตัว Download Malware เพิ่มเติมอีกทอดหนึ่ง โดยจะใช้มัลแวร์โจมตีอย่างต่อเนื่อง และเจาะระบบจนเข้าถึงเครือข่ายได้ เพื่อวัตถุประสงค์ต่าง ๆ ที่ต้องการ) โดย Reconnaissance ได้รับคำสั่งให้เตรียมการโจมตีทางไซเบอร์เกาหลีใต้ทันทีหลังจากเข้าร่วมการซ้อมรบ “Cyber Storm” ซึ่งเกาหลีเหนือนั้นมีหน่วยปฏิบัติการทางทหารทางสงครามไซเบอร์ ประกอบด้วย หน่วย ๑๑๐ หน่วย ๒๐๔ หน่วย ๑๒๑ และหน่วย ๓๕ ซึ่งเป็นหน่วยปฏิบัติการทางสงครามไซเบอร์ที่มีศักยภาพสูงมาก

ในปัจจุบันนี้เกาหลีใต้มีความพร้อมที่จะทำสงครามไซเบอร์เต็มรูปแบบกับเกาหลีเหนือ โดยเกาหลีใต้ประกาศแผนการจัดตั้งหน่วยบัญชาการสงครามไซเบอร์ในปี ค.ศ.๒๐๑๒ แต่หลังการโจมตี เกาหลีใต้ได้จัดตั้งหน่วยดังกล่าวขึ้นในปี ค.ศ.๒๐๑๐ โดยหน่วยบัญชาการสงครามไซเบอร์ของเกาหลีใต้นี้ จะดำเนินการป้องกันและตอบโต้ในกรณีที่มีการโจมตีทางไซเบอร์

บรรดานักรบบนโลกไซเบอร์จำนวนมาก ยกให้เหตุการณ์หลายๆ กรณีดังกล่าวมานี้เป็นการโจมตีกันระหว่างประเทศ บนไซเบอร์สเปซเป็นครั้งแรกๆ ที่ล่วงรู้ถึงสาธารณชน ยังมีอีกหลายเหตุการณ์ รวมทั้งที่เกี่ยวเนื่องกับปฏิบัติการ ของจีน ไต้หวัน อิสราเอล และอื่นๆ แสดงให้เห็นว่าการทำสงครามไซเบอร์นั้นได้เริ่มขึ้นแล้ว โดยสงครามไซเบอร์เป็นเรื่องจริง เท่าที่เราได้เห็นมานั้นยังห่างไกลจากการเป็นดัชนีชี้วัดว่าอะไรสามารถเกิดขึ้นได้บ้างในสงครามจริงๆ เกือบทั้งหมดของเหตุการณ์โจมตีในไซเบอร์สเปซเหล่านี้นั้นใช้เพียงแค่การโจมตีขั้นพื้นฐานเท่านั้น จะมีที่แตกต่างออกไปชัดเจนในกรณีปฏิบัติการของ อิสราเอลเท่านั้น โดยมีสมมติฐานว่า บรรดาผู้ลงมือโจมตียังไม่ต้องการเปิดเผยขีดความสามารถที่มีศักยภาพมากกว่านี้ออกมาให้เห็น ซึ่งอาจมีขีดความสามารถในการทำสงครามไซเบอร์นั้นอาจสามารถทำลายชาติใดชาติหนึ่งได้

สงครามไซเบอร์โจมตีกันด้วยความเร็วระดับของความเร็วแสง การโจมตีทางไซเบอร์นั้น จะส่งแพ็คเกจจำนวนมากผ่านสายเคเบิลใยแก้วนำแสงไปนั้น จะมีระยะเวลาระหว่างการเริ่มต้นโจมตีกับเมื่อเกิดผลกระทบขึ้นแทบจะเป็นเวลาเดียวกัน ดังนั้นจึงเป็นความเสี่ยงสูงมาก สำหรับผู้ทำหน้าที่ตัดสินใจสั่งการ

สงครามไซเบอร์อาจนำไปสู่สงครามโลกได้ ในความขัดแย้งใด ๆ เมื่อมีการทำสงครามไซเบอร์ อาจสามารถขยายเป็นสงครามโลกได้อย่าง

รวดเร็วยิ่ง เมื่อเซิร์ฟเวอร์ และคอมพิวเตอร์ที่ถูกแฮก หรือถูกครอบงำอย่างลับ ๆ ทั่วทั้งโลกถูกควบคุมสั่งการให้เริ่มปฏิบัติการโจมตี หลายต่อหลายชาติย่อมถูกดึงเข้าสู่สงครามได้อย่างรวดเร็วยิ่ง เนื่องจากประเทศหรือเจ้าของ Server หรือเครื่องคอมพิวเตอร์ ถูกแฮกทำให้ติดไวรัสกลายเป็น Zombie หรือ Botnet จะถูกควบคุมจากแฮกเกอร์ นำไปโจมตีประเทศเป้าหมายที่ต้องการทำสงครามไซเบอร์ โดยสงครามไซเบอร์สามารถก้าวข้ามสมรภูมิรบ ระบบซึ่งผู้คนทั้งหลายต้องพึ่งพา ไม่ว่าจะเป็นธนาคาร การบริการทางอินเตอร์เน็ตต่าง ๆ หรือเรดาร์ป้องกันภัยทางอากาศ สามารถถูกแฮกและเข้าถึงได้จากไซเบอร์สเปซ และสามารถ ถูกยึดครองหรือถูกปิดระบบได้ โดยไม่จำเป็นต้องทำสงครามอย่างเช่นที่เคยเป็นมาในอดีต

สงครามไซเบอร์เริ่มขึ้นแล้ว เนื่องจากมีการทำสงครามไซเบอร์ตามที่ได้กล่าวมาแล้ว ทำให้หลายประเทศได้เริ่มเตรียมการเพื่อทำสงครามไซเบอร์ โดยอาจมีการแฮกเจาะระบบเข้าสู่เครือข่ายคอมพิวเตอร์และโครงสร้างสาธารณูปโภคซึ่งกันและกัน อาจมีการจัดวาง “Logic Bomb” (ซอฟต์แวร์ หรือชุดคำสั่งที่ปิดระบบหรือเครือข่าย และ/หรือลบข้อมูลหรือซอฟต์แวร์ในเครือข่าย) และ “Trapdoor” (ซอฟต์แวร์ประสงค์ร้าย ที่ถูกเพิ่มในระบบโดยไม่ได้รับอนุญาต เป็นตัวที่จะเปิดการเข้าถึงเครือข่าย หรือโปรแกรมนั้นโดยไม่ได้รับอนุญาตในภายหลัง) เอาไว้เรียบร้อยแล้วตั้งแต่เวลาสันติอย่างเช่นตอนนี้ เพื่อดำเนินการทำสงครามไซเบอร์ในอนาคต จึงทำให้เกิดมิติใหม่ของการไร้เสถียรภาพทางไซเบอร์ที่อันตรายยิ่งขึ้นอีกมิติหนึ่ง

เอกสารอ้างอิง

- RICHARD A. CLARKE AND ROBERT K. KNAKE. (2012) - CYBER WAR The Next Threat to National Security and what to do about it
- ไพรัตน์ พงศ์พานิชย์ (2555)- CYBER WAR สงครามไซเบอร์
- ACM DL DIGITAL LIBRARY – https://dl.acm.org/doi/book/10.5555/2604876
- GBHackers on Security - https://gbhackers.com/lazarus-apt-hackers-attack-japanese-organization/
- Extreme IT - https://www.extremeit.com/extreme-history-stuxnet/
- https://gemserv.com/our-thoughts/stuxnet-the-first-cyber-weapon/
- https://arstechnica.com/information-technology/2014/11/stuxnet-worm-infected-high-profile-targets-before-hitting-iran-nukes/
- https://arstechnica.com/information-technology/2014/11/stuxnet-worm-infected-high-profile-targets-before-hitting-iran-nukes/