นักรบไซเบอร์: กำลังอำนาจแห่งชาติที่จำเป็นต่อการรบในสงครามแห่งอนาคต

Cyber Warrior: Nation Power That Needed For Future War

Received : October 11, 2021
Revised : June11, 2022
Accepted : June 13, 2022

ดนัย ปฏิยุทธ
กองวิชาวิศวกรรมศาสตร์ ฝ่ายศึกษา โรงเรียนนายเรือ
Danai Patiyoot
Faculty of Engineering, Education department, Royal Thai Naval Academy
danaipatiyoot@gmail.com

บทคัดย่อ

บทความวิชาการนี้เป็นการกล่าวถึงวิธีการในการพัฒนานักรบไซเบอร์ของกองทัพไทย เพื่อการต่อกรกับอริราชศัตรูในสงครามที่จะเกิดขึ้นในอนาคต โดยในเบื้องต้นเป็นการกล่าวถึงเรื่องของการโจมตีทางไซเบอร์ที่เกิดขึ้นทั้งในและต่างประเทศ ต่อมาคือ การกล่าวถึงการผลิตนักรบไซเบอร์ที่กองทัพต่าง ๆ ได้กระทำอยู่ และท้ายสุดของบทความวิชาการนี้ได้เสนอการใช้ NICE Cybersecurity Workforce Framework ของกองทัพสหรัฐฯ มาเป็นกรอบความคิดและกรอบการดำเนินงานในการผลิตนักรบไซเบอร์อย่างเป็นรูปแบบที่เป็นมาตรฐาน

คำสำคัญ: ไซเบอร์, กำลังอำนาจแห่งชาติ, สงครามแห่งอนาคต

Abstract

This article is to find the way to produce “Cyber Warrior” for Royal Thai Armed Forces in order to fend off enemies in the future war. Cyber attacks both in the country and around the world are mentioned in the first part. The second part is the detail of how the Royal Thai Armed Forces are doing their parts in producing the cyber warriors. The last part is the recommendation to Royal Thai Armed Forces the proper way to produce Cyber Warriors by adopting the “NICE Cybersecurity Workforce Framework” of US Armed forces.

Keywords: Cyber, National Power, Future war

1. บทนำ

ปัจจุบันมิติไซเบอร์ หรือไซเบอร์โดเมน หรือมิติที่ห้า (Fifth Domain) ของการทำสงครามทางทหารเป็นมิติการรบที่เพิ่มความสำคัญขึ้นเรื่อย ๆ นอกจากเหนือจากมิติทั้งสี่ของพื้นดิน พื้นน้ำ อากาศ และอวกาศ ที่มนุษย์คุ้นเคยกันเป็นอย่างดี ประเทศมหาอำนาจ เช่น สหรัฐอเมริกา จีน จึงได้เร่งผลิตนักรบไซเบอร์อย่างจริงจัง เพื่อทำการรบในมิติการทำสงครามใหม่นี้ ประเทศไทยนับเป็นอีกประเทศหนึ่งที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์ที่เกิดขึ้นบ่อยครั้ง จึงมีความจำเป็นอย่างยิ่งที่ต้องผลิตนักรบไซเบอร์ (Cyber Warriors) ของตนเอง เพื่อตอบโต้ต่อภัยคุกคามดังกล่าว อย่างไรก็ตาม เทคโนโลยีทางไซเบอร์

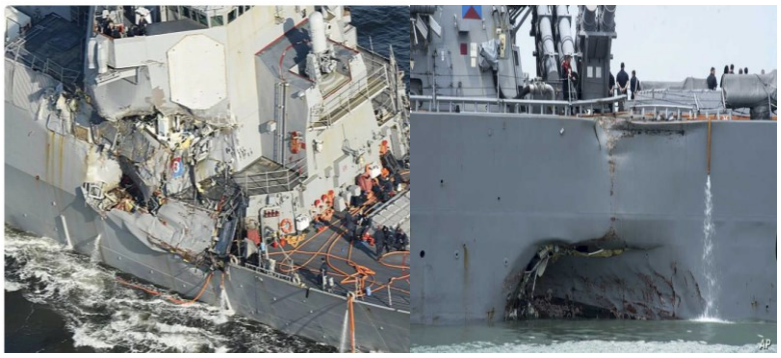
จะมีความก้าวหน้าหรือทันสมัยมากเพียงใด แต่หากไม่สามารถป้องกันระบบจากการโจมตี ก็อาจจะส่งผลกระทบโดยตรงต่อการควบคุมสั่งการ และการวิเคราะห์ฉากทัศน์การรบได้อย่างมีประสิทธิภาพ

2. การโจมตีทางไซเบอร์

การทำสงครามไซเบอร์นั้นประกอบด้วยการโจมตีทางรุกต่อระบบคอมพิวเตอร์ของศัตรู และการตั้งรับในที่ตั้งต่อการถูกโจมตีจากศัตรู โดยการโจมตีทางไซเบอร์อาจกระทำได้ต่อโครงสร้างพื้นฐานที่สำคัญ อาทิเช่น โรงไฟฟ้า เขื่อน สนามบิน โรงพยาบาล หรือการเข้าถึงข้อมูลอาทิเช่นหมายเลขบัตรเครดิต หมายเลขบัญชีธนาคาร รหัสผ่าน โดยผู้ไม่หวังดีที่แอบแฝงวัตถุประสงค์ที่มุ่งร้ายต่อผู้ใช้งาน หรือการเข้าถึงเครือข่ายคอมพิวเตอร์ของศัตรู โดยการทำให้เครือข่ายคอมพิวเตอร์ไม่ทำงาน หรือผู้มีสิทธิเข้าถึงระบบไม่สามารถเข้าถึงได้ ส่วนการโจมตีทางทหารนั้นก็เพื่อจุดประสงค์อาทิเช่น การรู้อาวุธยุทโธปกรณ์ของกองทัพข้าศึก แผนการรบ ฯ

การโจมตีรอบโลกที่สำคัญ ๆ ที่เกิดขึ้น เช่นในปี พ.ศ.2555 กลุ่มแฮคเกอร์ชาวอิหร่านที่เรียกตนเองว่า “Cutting Sword of Justice” ได้ทำการโจมตีบริษัทน้ำมันแห่งชาติของซาอุดีอาระเบีย และทำให้คอมพิวเตอร์ประมาณ 30,000 เครื่องไม่สามารถใช้งาน ในเดือนพฤษภาคม พ.ศ.2556 คณะกรรมการวิทยาศาสตร์ทหารของสหรัฐอเมริกา ได้เปิดเผยว่าจีนได้แฮกข้อมูลเพื่อเข้าถึงโรงการอาวุธของกระทรวงกลาโหมถึง 37 ระบบด้วยกัน เช่น ระบบป้องกันขีปนาวุธเพดานบินสูง (Terminal High Altitude Area Defence) เครื่องบินรบแบบ F-35, F-22, Raptor, V-22 Osprey และ เฮลิคอปเตอร์แบล็คฮอว์ค เป็นต้น โดยในปี 2556 สหรัฐฯ ได้อ้างว่า เขื่อนขนาดเล็กใกล้รัฐนิวยอร์คได้ถูกอิหร่านแฮกเข้าไปในระบบ ทำให้ไม่สามารถปล่อยน้ำออกจากเขื่อนได้ การโจมตีโรงไฟฟ้าของประเทศยูเครน ต่อมาเดือน ธ.ค. ปี 2559 ทำให้มีไฟดับบางพื้นที่เป็นเวลา 1 ชม. และเมื่อเดือน ก.พ.ปี 2560 แฮกเกอร์ปากีสถานได้ทำการเปลี่ยนหน้าเว็ปไซต์ของเลขาธิการสภาความมั่นคงแห่งชาติอินเดียเพื่อเรียกร้องเอกราชของแคว้นแคชเมียร์ จากนั้นเดือน มิ.ย. ปี 2562 สหรัฐฯ ได้โจมตีทางไซเบอร์ต่อระบบควบคุมขีปนาวุธของอิหร่านจนไม่สามารถใช้งานได้ (ดังแสดงในรูปที่ 1) นอกจากนี้ในเดือน ธ.ค. ปี 2563 แฮกเกอร์สัญชาติเกาหลีเหนือซึ่งมีชื่อกลุ่มว่า “Zinc and Cerium” ได้เข้าถึงข้อมูลของวัคซีน COVID-19 ที่ผลิตโดย Pfizer โดยหลายแหล่งข้อมูลระบุว่าแฮกเกอร์ในเกาหลีเหนือมีอยู่ประมาณ 1,000 - 3,000 คน โดยในช่วงปลายเดือน มิ.ย. ปี 2563 อาชญากรรมไซเบอร์ได้ใช้มัลแวร์เรียกค่าไถ่ (Ransomware) เพื่อเข้าถึงโครงข่ายภายในของมหาวิทยาลัยแคลิฟอร์เนีย ที่ซานฟรานซิสโก ณ ศูนย์ควบคุมและป้องกันโรคที่ทำงานเกี่ยวข้องกับการวิจัย โควิด -19 และท้ายที่สุดมหาวิทยาลัยจำเป็นต้องจ่ายเงินให้แฮกเกอร์ถึง 1.14 ล้านเหรียญสหรัฐฯ เพื่อให้ทำการปลดข้อมูลที่ถูกเข้ารหัส นอกจากนี้ยังมีเหตุการณ์ที่เรือรบสหรัฐฯ (USS Fitzgerald, USS John S. McCain) ประสบอุบัติเหตุถูกชน 4 ครั้งในน่านน้ำเอเชีย ในช่วงปี พ.ศ.2560 - 2563 ถูกสงสัยว่าเป็นการโจมตีทางไซเบอร์ (ดังแสดงในรูปที่ 2)

รูปที่ 1 ระบบขีปนาวุธของอิหร่านที่ถูกสหรัฐฯ แฮก ทำให้ระบบใช้งานไม่ได้
ที่มา: https://www.bbc.com/thai/international-48736849

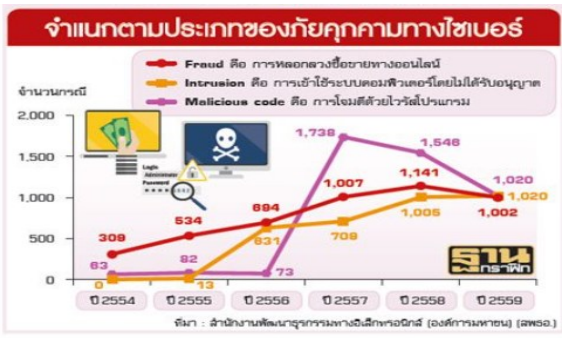


รูปที่ 2 เรือรบสหรัฐฯ USS Fitzgerald และ USS John S. McCain ถูกชนโดยมีข้อสงสัยว่าอาจถูกแฮคเข้าไปในระบบการเดินเรือ
ที่มา: https://pantip.com/topic/36574764

ในปี พ.ศ.2563 สหรัฐฯ ได้แจ้งข้อหานายทหาร 4 นายของจีนในข้อหาแฮคเข้าไปในระบบ Equifax และขโมยข้อมูลส่วนตัวของพลเมืองสหรัฐฯ เป็นจำนวนถึง 14.7 ล้านคน (ดังแสดงในรูปที่ 3)

รูปที่ 3 นายทหารจีน 4 นายที่ถูกกล่าวหาว่าแฮคข้อมูลของบริษัท Equifax
ที่มา: https://www.matichon.co.th/foreign/news_1963847

ส่วนในประเทศไทย จากการสำรวจของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้จำแนกภัยคุกคามทางไซเบอร์ตั้งแต่ พ.ศ.2554 - 2559 เป็น 3 แบบ คือ Fraud, Intrusion และ Malicious code (ดังแสดงในรูปที่ 4)



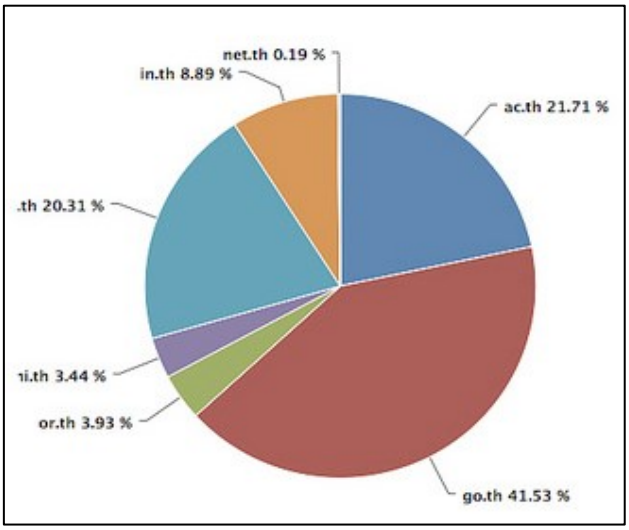
รูปที่ 4 ภัยคุกคามทางไซเบอร์แยกตามประเภท
ที่มา: https://www.thansettakij.com/business/136878

ผลสำรวจจากไซแมนเทค (Symantec) ในปี พ.ศ.2560 พบว่า ประเทศไทยตกเป็นเป้าโจมตีอันดับที่ 21 จากแรนซั่มแวร์ อันดับ 11 จากเน็ตเวิร์ก และอันดับที่ 12 จากสแปม จากทุกประเทศทั่วโลก (ดังแสดงในรูปที่ 5)

รูปที่ 5 การโจมตีเครือข่ายประเทศไทยด้วยวิธีต่าง ๆ

ที่มา: https://www.posttoday.com/economy/news/546511

SRAN Technology ได้ทำการสำรวจภัยคุกคามทางอินเทอร์เน็ตและได้ค้นพบว่า เว็ปไซต์ในประเทศไทยที่ถูกโจมตีประเภทโดเมนมากที่สุดคือ go.th ตามด้วย co.th (ดังแสดงในรูปที่ 6)



รูปที่ 6 การโจมตีโดเมนเนมของเครือข่ายประเทศไทย

ที่มา: https://www.gbtech.co.th/sran-จัดทำระบบสถิติภัยคุกคาม

ตัวอย่างการโจมตีในประเทศไทยที่เกิดขึ้น อาทิเช่น เมื่อเดือนมิถุนายน พ.ศ. 2563 การไฟฟ้าส่วนภูมิภาคได้ถูกโจมตีโดยมัลแวร์ เพื่อเรียกค่าไถ่ หรือในเดือนกันยายน พ.ศ.2563 โรงพยาบาลสระบุรีได้ถูกโจมตีด้วย Ramsonware ทำให้ไม่สามารถเข้าถึงข้อมูลของคนไข้ย้อนหลังในช่วง 5 ปีได้ ซึ่งเหตุการณ์ในครั้งนั้น แฮกเกอร์ได้เรียกเงินค่าไถ่สูงถึง 200,000 บิตคอยน์ หรือ 6.3 หมื่นล้านบาท (ดังแสดงในรูปที่ 7)

รูปที่ 7 ระบบเครือข่ายของโรงพยาบาลสระบุรีขัดข้องอันเนื่องมาจาก Ransomware
ที่มา: https://bitcoinaddict.org/2020/09/09/saraburi-hospital-attacked-by-ransomware/

ความเสียหายจากภัยคุกคามทางไซเบอร์นั้นเป็นที่ประจักษ์อย่างชัดเจน ดังนั้นการต่อต้านภัยคุกคามนี้ด้วยการใช้บุคลากรที่มีความรู้ความสามารถในศาสตร์ด้านนี้หรือที่เรียกว่านักรบไซเบอร์ จึงมีความสำคัญ

3. การผลิตนักรบไซเบอร์

ในส่วนของประเทศไทยนั้น การผลิตนักรบไซเบอร์ได้เริ่มดำเนินการบ้างแล้ว เช่น การตั้งหน่วยงานไซเบอร์ของกองทัพ การรับพนักงานราชการตำแหน่ง “นักตรวจสอบความมั่นคงปลอดภัยไซเบอร์ชั้นสูง” โดยมีอัตราค่าตอบแทนสูงเดือนละ 68,350 บาท ของกองทัพบก หรือการแข่งขันทักษะทางไซเบอร์ (Cyber Contest) ของเหล่าทัพต่าง ๆ (ดังแสดงในรูปที่ 8) แต่การพัฒนาบุคลากรทางไซเบอร์ เพื่อตอบสนองต่อความต้องการของหน่วยงาน หรือองค์กรยังอยู่ในวงจำกัดและผลิตไม่ได้เท่าที่ควร รัฐบาลไทยจึงวางแผนในการใช้งบประมาณ 350 ล้านบาท เพื่อผลิตนักรบไซเบอร์จำนวน 200 คน ภายในห้วงเวลา 3 ปี อย่างไรก็ตามนักรบไซเบอร์อาจจะยังไม่เพียงพอต่อความต้องการที่แท้จริง โดยภาครัฐได้ตั้งเป้าหมายการผลิตนักรบไซเบอร์จำนวน 1,000 คนภายในปี พ.ศ.2563 และ 4,500 - 5,000 คน ภายในปี พ.ศ.2564 โดยให้เป็นไปตามวิสัยทัศน์ของชาติในเรื่องความมั่นคง มั่งคั่ง ยั่งยืน และกระทรวงดิจิทอลเพื่อเศรษฐกิจและสังคมตั้งเป้าหมายในการยกระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ให้ติดในอันดับที่ 20 ของประเทศที่มีความพร้อมจากเดิมที่ประเทศไทยอยู่ในอันดับที่ 22

ผศ.ดร.สุระสิทธิ์ ทรงม้า อาจารย์ มหาวิทยาลัยสวนดุสิต ได้ให้ความเห็นเกี่ยวกับการพัฒนาบุคลากรทางไซเบอร์ดังนี้

“ส่วนใหญ่ที่ผมเห็นทางการก็จะใช้วิธีเอาคนที่มีอยู่แล้วไปอบรมเพิ่ม แต่ความชำนาญที่ได้ก็จะต่างกันเมื่อเทียบกับการที่เขารับคนที่ตรงสายงาน ผมเชื่อว่าคนที่จะทำหน้าที่เป็นนักรบไซเบอร์ที่ดี ควรจะต้องมีความรู้มากกว่าในระดับพื้นฐานที่สอนกันในมหาวิทยาลัยหลักสูตรเทคโนโลยีสารสนเทศเด็ก ๆ ที่เรียนทางไอทีก็จะมีพื้นฐานทาง Security ป้องกันตนเองได้ แต่ถ้าไปทำงาน

เป็นนักรบไซเบอร์จริง ถ้าไม่ได้เรียน และมีประสบการณ์โดยตรงก็จะไม่มีความชำนาญ และการดูแลระบบคอมพิวเตอร์ปกติกับการดูแลความปลอดภัยไซเบอร์นั้นต่างกัน”

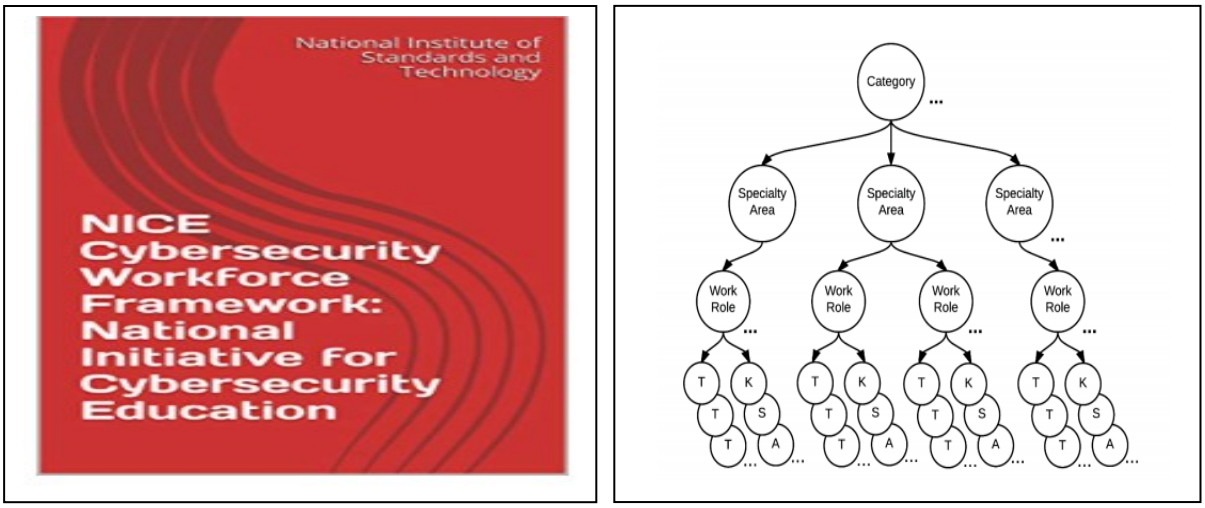
รูปที่ 8 การแข่งขัน Cyber Contest ของแหล่าทัพต่าง ๆ และการรับพนักงานไซเบอร์ของกองทัพบก
ที่มา: https://www.youtube.com/watch?v=th_lGmAjoSs

ในส่วนของประเทศสหรัฐอเมริกานั้น กองทัพสหรัฐฯ ได้มีการจัดตั้งหน่วยงานที่ฝึกอบรมในเรื่องสงครามไซเบอร์ทั้ง 3 เหล่าทัพ โดยกองทัพบกได้ตั้งหน่วยงานที่ชื่อว่า “The Army Cyber Center of Excellence ” กองทัพเรือตั้งหน่วยงานที่เรียกว่า “The Navy Center for Information Dominance ” และกองทัพอากาศได้ตั้งกองบินที่ 24 เป็นกองบินไซเบอร์

กระทรวงกลาโหมสหรัฐอเมริกาได้มีการกระตุ้นให้บุคลากรเข้ามาเป็นนักรบไซเบอร์ โดยนายลีออน พาเนตตา รัฐมนตรีกลาโหมของสหรัฐฯ ได้ประกาศออกมาว่าสหรัฐฯ เตรียมมอบเหรียญกล้าหาญให้กับทหารที่มีผลงานโดดเด่นในการต่อสู้ในสงครามบนโลกออนไลน์ และปฏิบัติการต่อต้านภัยคุกคามทางคอมพิวเตอร์ แม้ทหารเหล่านั้นไม่ต้องเสี่ยงชีวิตในการออกไปต่อสู้กับข้าศึกในแนวหน้า โดยเหรียญกล้าหาญใหม่นี้เรียกว่า “Distinguished Warfare Medal” ดังแสดงในรูปที่ 9

รูปที่ 9 เหรียญกล้าหาญ “Distinguished Warfare Medal”
ที่มา: https://pantip.com/topic/30178709

จากความต้องการนักรบไซเบอร์ของสหรัฐฯ ที่มีจำนวนถึง 30,000 คน ดังนั้นรัฐบาลจึงได้ออกโปรแกรมพิเศษที่เรียกว่า National Initiative for Cybersecurity Education (NICE) ในปี พ.ศ. 2553 โดยให้ NICE รับผิดชอบโครงการสร้างศักยภาพให้บุคลากรผู้เชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่ง NICE ได้ออกเอกสาร NICE Cybersecurity Workforce Framework มาเป็นกรอบความคิด และกรอบการดำเนินงานในการพัฒนาบุคลากรด้าน Cybersecurity ดังรูปที่ 10



รูปที่ 10 ความสัมพันธ์ระหว่างองค์ประกอบต่างๆตามกรอบแนวคิดของ NICE Cybersecurity Workforce framework
ที่มา: https://www.cybertronium.com/Trainings/Nice-Framework

NICE Cybersecurity Workforce Framework ตามรูปที่ 10 มีการแบ่งกรอบการดำเนินงานเป็น 7 ประเภทหลัก(Category) ได้แก่ Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate และ Investigate และภายใต้ 1 ประเภทหลักจะประกอบด้วยความเชี่ยวชาญในแต่ละด้าน (Specialty Area) หลายๆ ด้านของความชำนาญจะประกอบด้วยบทบาทในการทำงาน (Work Role) จำนวนหนึ่ง ถัดมาจะเป็นการอธิบายถึงบทบาทในการทำงานแต่ละด้านต้องปฏิบัติงานอย่างไร เช่น ทางด้านความเสี่ยง (Task) ทางด้านความรู้ (Knowledge) ด้านทักษะ (Skill)

และด้านความสามารถ (Ability) ทำให้ผู้ที่นำ NICE Cybersecurity Workforce Framework สามารถใช้เป็นตัวบ่งบอกได้ว่าองค์กรต้องการบุคลากรประเภทใด มีความรู้ ความสามารถ ทักษะอะไร ถ้ามีความจำเป็นต้องทำสงครามไซเบอร์ ตัวอย่างเช่น บทบาทของครูสอนวิชาไซเบอร์ จะมีรายละเอียดต่าง ๆ ตามกรอบความคิดแบบ NICE จะปรากฏตามตารางที่ 1

ตารางที่ 1 รายละเอียดของบทบาทในการทำงานของ “ครูสอนวิชาไซเบอร์”

ประเภท (Category)	**การบริหารงาน**
พื้นที่ของความเชี่ยวชาญ(Specialty Area)	การฝึกหัด, การศึกษา, การตระหนัก
ชื่อของบทบาทในการทำงาน (Work role name)	ครูสอนวิชาไซเบอร์ (Cyber Instructor)
หมายเลขของบทบาทในการทำงาน (Work role ID)	OV-TEA-002
คำอธิบายของบทบาทในการทำงาน (Work role description)	พัฒนาและดำเนินการฝึกหัดหรือให้การศึกษาบุคลากรที่อยู่ภายในองค์กร
การปฏิบัติงาน (Task)	แนะนำการอัปเดตหลักสูตร, ออกแบบหลักสูตร, ออกแบบคอร์สการสอน, พัฒนาแบบฝึกหัดของหลักสูตรฯ
ความรู้ (Knowledge)	ความรู้ในเรื่องเครือข่ายคอมพิวเตอร์, ความรู้ในเรื่องความปลอดภัยด้านไซเบอร์, ความรู้ในเรื่องระบบปฏิบัติการ ฯ
ทักษะ (Skills)	ทักษะในการวิเคราะห์เครือข่าย, ทักษะในการสแกนเครือข่าย, ทักษะในการทำการเจาะเครือข่าย, ทักษะในการใช้เครื่องมือในการวิเคราะห์เครือข่าย ฯ
ความสามารถ (Abilities)	สามารถทำให้ผู้ใช้งานตระหนักถึงนโยบายและกระบวนการของการรักษาความปลอดภัยได้, สามารถวิเคราะห์มัลแวร์ได้, สามารถตอบคำถามได้อย่างกระทัดสั้นและชัดเจน, สามารถทำการสอนแบบการถกปัญหาแบบกลุ่มได้ ฯ

4. สรุป

หนทางที่จะนำประเทศไทยไปสู่วิสัยทัศน์ที่ตั้งไว้คือ “ประเทศมีความ มั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้วด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” โดยหนึ่งในวิสัยทัศน์ด้านความมั่นคงที่ต้องการให้ประเทศไทยนั้น มั่นคงปลอดภัยจากภัยภายนอกประเทศ โดยเฉพาะอย่างยิ่งจากภัยทางสงครามไซเบอร์นั้น จึงต้องอาศัยกำลังอำนาจแห่งชาติโดยเฉพาะด้านการทหารเป็นสำคัญ ซึ่งกำลังพลของกองทัพผู้เชี่ยวชาญด้านสงครามไซเบอร์หรือนักรบไซเบอร์เป็นสิ่งที่จำเป็นอย่างยิ่งยวด การผลิตบุคลากรนั้นสามารถดูกรอบความคิดจากประเทศต่าง ๆ ที่ได้เสนอไว้แล้ว อาทิเช่น NICE Cybersecurity Workforce Framework ของสหรัฐฯ และมาประยุกต์ให้เข้ากับบริบทของประเทศไทยก็จะเป็นประโยชน์อย่างมาก

การพัฒนานักรบไซเบอร์เป็นการลงทุนที่ใช้ทรัพยากรไม่มาก แต่สามารถทำหน้าที่รักษาความมั่นคงแห่งชาติได้มีประสิทธิภาพไม่แพ้อาวุธยุทโธปกรณ์อื่น ๆ ในบางกรณีนักรบไซเบอร์เพียงหนึ่งนายสามารถที่จะหยุดกองทัพศัตรูได้ทั้งกองทัพ

5. เอกสารอ้างอิง

[1] NIST, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

[2] นักรบไซเบอร์. (2563). สืบค้น 12 มกราคม 2563 จาก https://web.facebook.com/ pp1169/posts/ 2655057897941012/?rdc=1&_rdr

[3] Reuters. (2013). Are there enough cyber warriors to fight against crime? . Retrieved on October 14, 2013 from https://businesstech.co.za/news/internet/47559/are-there-enough-cyber-warriors-to-fight-against-crime/

[4] C.J.Heatherly. (2019). Every Soldier a Cyber Warrior: The Case for Cyber Education in the United States Army. Retrieved on April 30, 2019 from https://cyberdefensereview.army.mil/Portals/ 6/HEATHERLYMELENDEZ_CDR_V4N1.pdf?ver=105206-983

[5] M.A.DeMuth. (2020). Creating Cyber Warriors. Retrieved on April 30, 2010 from https://www.georgiatrend.com/2020/04/30/creating-cyber-warriors/

[6] BBC News. (2562). สื่อหลายแห่งเผย สหรัฐฯ “โจมตีไซเบอร์” รบกวนการทำงานของเครื่องยิงขีปนาวุธอิหร่าน. สืบค้น 23 มิถุนายน 2562 จาก https://www.bbc.com/thai/international-48736849

[7] Pantip. (2560). เรือรบอเมริกาเกิดไรขึ้นที่ญี่ปุ่นครับ. สืบค้น 17 มิถุนายน 2560 จาก https://pantip.com/ topic/36574764

[8] Matichon online. (2565). จีน ปฏิเสธข้อกล่าวหาหลังมะกันตั้งข้อหา 4 จีน แฮกข้อมูลชาวอเมริกัน. สืบค้น 11 มิถุนายน 2565 จาก https://www.matichon.co.th/foreign/news_1963847

[9] ฐานเศรษฐกิจ. (2560). อาชญากรรมไซเบอร์พุ่ง เหรียญอีกด้านยุคดิจิตอล. สืบค้น 28 มีนาคม 2560 จาก https://www.thansettakij.com/ business/136878

[10] Post Today. (2561). 5 เทรนด์ใหม่บนไซเบอร์. สืบค้น 3 เมษายน 2561 จาก https://www.posttoday. com/economy/ news/546511

[11] Global Tech. (2562). SRAN จัดทำระบบสถิติภัยคุกคามทางอินเทอร์เน็ตในประเทศไทย. สืบค้น 8 มีนาคม 2562 จาก https://www.gbtech.co.th/sran-จัดทำระบบสถิติภัยคุกคาม

[12] BitcoinAddict Thailand. (2563). โรงพยาบาลถูก Ransomware หรือไวรัสเรียกค่าไถ่เป็น Bitcoin โจมตี ทำให้ระบบคอมพิวเตอร์ล่มจนไม่สามารถใช้งานได้. สืบค้น 9 กันยายน 2563 จากhttps://bitcoinaddict.org/2020/09/09/saraburi-

[13] Youtube. (2563). มอบรางวัล Army Cyber Contest 2020. สืบค้น 23 ธันวาคม 2563 จาก https://www.youtube.com/watch?v=th_lGmAjoSs

[14] Pantip. (2556). อเมริกา เตรียมออกเหรียญกล้าหาญใหม่สำหรับผู้ปฏิบัติการด้านไซด์เบอร์/UAV Operator. สืบค้น 24 กุ มภาพันธ์ 2556 จาก https://pantip.com/topic/30178709

[15] Cybertronium. NIST National Initiative for Cybersecurity Education (NICE). สืบค้นจาก https://www.cybertronium.com/Trainings/Nice-Framework