



บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันสภาพสังคมได้เข้าสู่ยุคของการใช้เทคโนโลยีขั้นสูง ทำให้หน่วยงานต่างๆ ทั้งภาครัฐและเอกชนซึ่งจำเป็นต้องใช้ข้อมูลจำนวนมากเพื่อนำมาประกอบการตัดสินใจ ทำให้เกิดความจำเป็นที่จะต้องนำคอมพิวเตอร์เข้ามาเป็นเครื่องมือในการช่วยเหลือในการรวบรวมข้อมูล ตลอดจนการประมวลผล วิเคราะห์ข้อมูลที่สำคัญแก่การบริหารและตัดสินใจ คอมพิวเตอร์จึงเป็นสิ่งที่หลีกเลี่ยงได้ยากทั้งในปัจจุบันและในอนาคต

ในฐานะที่ข่ายงานคอมพิวเตอร์เป็นสิ่งที่จำเป็นและใช้กันอยู่ทั่วไป ไม่ว่าจะเป็นเครื่องคอมพิวเตอร์ขนาดเล็กซึ่งสามารถที่จะติดตั้งบนโต๊ะทำงานได้ ตลอดจนได้มีการพัฒนาความสามารถหลาย ๆ ด้านของคอมพิวเตอร์ เพื่อความสะดวกและเหมาะสมตรงต่อวัตถุประสงค์ของผู้ใช้ เช่นเดียวกับอาชญากรรมซึ่งมักจะมีการพัฒนารูปแบบของการกระทำความผิดไปตามสภาวะเศรษฐกิจ สังคม ความก้าวหน้าด้านเทคโนโลยี และเช่นเดียวกัน การกระทำความผิดอาญาเกี่ยวกับคอมพิวเตอร์ได้เกิดขึ้นโดยถูกพบครั้งแรกในสหรัฐอเมริกา และพบว่าได้ขยายตัวไปยังประเทศต่าง ๆ ที่มีการนำเครื่องคอมพิวเตอร์ไปใช้

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นปัญหาที่ก่อตัวเพิ่มขึ้นอย่างมากและได้ก่อให้เกิดความเสียหายเป็นมูลค่ามหาศาลในแต่ละครั้งของการกระทำความผิด ประกอบกับมีโอกาสที่จะเกิดขึ้นกับสถาบันการเงิน ส่วนราชการ หรือรัฐวิสาหกิจที่สำคัญของประเทศได้ ซึ่งย่อมจะเป็นผลให้เกิดความเสียหายต่อส่วนรวมมีสูงมากขึ้นตามไปด้วย อย่างไรก็ตามในสหรัฐอเมริกา แม้ว่าจะรูปแบบการ

กระทำความผิดในความผิดประเภทนี้ อาจนากฎหมายที่มีอยู่มาปรับใช้ได้บ้างก็ตาม แต่ก็มีข้อผิดพลาดแตกต่างออกไปในสาระสำคัญของ การกระทำและองค์ประกอบของกฎหมาย ซึ่งอาจก่อให้เกิดปัญหาการบังคับใช้ได้ดั่งนั้นทั้งระดับมลรัฐและรัฐบาลกลาง ต่างก็ได้ออกกฎหมายเพื่อนำมาปรับใช้กับอาชญากรรมคอมพิวเตอร์โดยเฉพาะ ซึ่งในส่วนของรัฐบาลกลางได้ออกกฎหมายเฉพาะฉบับหนึ่งเพื่อมีจุดประสงค์ในการปราบปรามอาชญากรรมเกี่ยวกับคอมพิวเตอร์โดยตรงคือ The Computer Fraud And Abuse Act 1986 โดยได้สร้างบทบัญญัติความผิดใหม่ขึ้นมาคือ

1. ความผิดฐานเข้าถึง (access) หมายถึงการเข้าไปสู่ สิ่ง สื่อสารกับ าสข้อมูล เข้าไปเก็บไว้ ล้วงข้อมูลมาจาก หรืออีกนัยหนึ่ง เป็นการเอาประโยชน์ใดๆ ของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์มาใช้

2. ความผิดฐานแก้ไขเปลี่ยนแปลง (alteration) การแก้ไขเปลี่ยนแปลงทางคอมพิวเตอร์หมายถึง การแก้ไขเปลี่ยนแปลงเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ คอมพิวเตอร์ซอฟต์แวร์ โปรแกรมหรือข้อมูลใดๆ ที่ได้บรรจุอยู่ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์

3. ความผิดฐานทำให้เสียหายหรือทำลาย (damage or destruction) การทำให้เสียหายหรือทำลายทางคอมพิวเตอร์ในที่นี้หมายถึง การทำให้เสียหายหรือทำลายเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ คอมพิวเตอร์ซอฟต์แวร์ โปรแกรมหรือข้อมูลใดๆ ที่ได้บรรจุอยู่ในเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์

นอกจากความผิด 3 ประการที่ได้กำหนดขึ้นมาใหม่ตาม The Computer Fraud And Abuse Act 1986 ซึ่งได้บัญญัติออกมาเพื่อแก้ไขปัญหาการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งไม่อาจลงโทษผู้กระทำความผิดภายใต้กฎหมายที่มีอยู่นี้ เพราะการกระทำใดเป็นความผิดอาญาจะต้องมีกฎหมายกำหนดไว้โดยชัดแจ้งว่าการกระทำนั้นเป็นความผิดและได้กำหนดโทษไว้ ซึ่งรายละเอียดของกฎหมายดังกล่าวจะกล่าวถึงโดยละเอียดต่อไป

อย่างไรก็ตามนอกเหนือจากกฎหมายเฉพาะฉบับนี้แล้ว ยังมีกฎหมายอื่น ๆ อีกที่ผู้
กระทำความผิดเกี่ยวกับคอมพิวเตอร์อาจถูกฟ้องร้องตามกฎหมายอื่นได้อีก คือ¹

มาตรา 1029 - Fraud and Related Activity in Connection with
Access Devices

มาตรา 1343 - Fraud by Wire , Radio or Television

มาตรา 1346 - Scheme or Artifice to Defraud

มาตรา 1362 - Malicious Mischief with Government Property

มาตรา 2510 - The Electronic Privacy Act

มาตรา 2710 - Unlawful Access to Stored Communication

ภายหลังจากที่กฎหมาย The Computer Fraud and Abuse Act 1986 ได้
บังคับใช้แล้ว ปรากฏว่าได้มีความผิดรูปแบบใหม่เกิดขึ้นอีก ในรูปแบบของ"โปรแกรมไวรัสคอมพิวเตอร์"
ซึ่งเป็นชุดคำสั่งที่ถูกเขียนขึ้นโดยนักคอมพิวเตอร์อันมีผลในทางลบต่อการทำงานเกี่ยวกับ
คอมพิวเตอร์ โดยเฉพาะเป็นที่กล่าวขานกันมากในหลาย ๆ ชื่อเช่น"ไวรัสคอมพิวเตอร์"(Computer
Viruses)"เวิร์ม"(Worm) ,"ม้าโทรจัน"(Trojan Horse) , โลจิกบอมบ์ (Logic Bomb)

ประสิทธิภาพของโปรแกรมอันตรายเหล่านี้ ได้นำไปสู่ความเสียหายหรือการทำลายระบบ
คอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ เป็นที่หวั่นวิตกกังเป็นอย่างมาก
เพราะได้ก่อให้เกิดความเสียหายอย่างกว้างขวางและเป็นจำนวนมากอย่างที่สุดที่จะประมาณได้
อีกทั้งยังไม่สามารถควบคุมหรือป้องกันได้อย่างมีประสิทธิภาพ โดยเปรียบเสมือนกับโรคมะเร็งหรือ
โรคเอดส์ที่คร่าชีวิตคนไปเสียมากต่อมากแต่แพทย์ก็ยังไม่สามารถหาวิธีการหรือตัวยาใด ๆ ที่จะ

1. Lance J. Hoffman, ROGUE PROGRAMME viruses, worm and trojan horse
(USA: Van Nostrand Reinhold Ltd.), 1990, p.73

นามารักษาคนไข้ให้ได้ผลอย่างเด็ดขาด การทำให้เกิดความเสียหายหรือทำลายดังกล่าว ซึ่งก็คือชุดคำสั่งที่ถูกเขียนขึ้นมาเพื่อมีวัตถุประสงค์เพื่อการทำลายข้อมูล โดยสามารถติดจากแผ่นดิสก์หนึ่งไปยังอีกแผ่นดิสก์หนึ่ง หรือระบบหรือข่ายงานคอมพิวเตอร์หนึ่งไปสู่ระบบหรือข่ายงานคอมพิวเตอร์อื่น ๆ ต่อไปได้เรื่อย ๆ เสมือนการติดเชื้อของมนุษย์ โดยที่ตัวโปรแกรมดังกล่าวจะไปแอบซ่อนอยู่ในแผ่นดิสก์หรือในระบบของคอมพิวเตอร์ แล้วจะค่อย ๆ ทำลายข้อมูลและรบกวนการทำงานของดิสก์ใดใคร่ และระบบคอมพิวเตอร์ เหมือนเช่นคนที่ติดเชื้อซึ่งจะมีอาการผิดปกติจากเดิมและทำงานได้ไม่เหมือนเดิม² หรืออาจเป็นชุดคำสั่งที่กำหนดให้โปรแกรมเหล่านี้สามารถที่จะเดินทางไปยังข่ายงานต่าง ๆ ที่เชื่อมต่อกัน และสามารถที่จะสร้างความเสียหายให้แก่ข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์ได้

เมื่อวันที่ 5 พฤศจิกายน ค.ศ. 1988 สหรัฐอเมริกาได้เผยแพร่ข่าวสารทางโทรทัศน์ออกไปทั่วโลกว่า สหรัฐอเมริกาประสบกับปัญหาอย่างใหญ่หลวงเกี่ยวกับการทำงานของคอมพิวเตอร์ โดยได้ปรากฏเหตุการณ์แพร่ระบาดไปทั่วสหรัฐซึ่งเรียกกันว่า "ไวรัสคอมพิวเตอร์" (computer viruses) ลักษณะที่เกิดขึ้นเปรียบได้กับไวรัสที่เข้าสู่ร่างกายมนุษย์ โดยได้เข้าไปทำลายระบบการทำงานต่าง ๆ ทำให้ผลที่เกิดขึ้นจากการทำงานของคอมพิวเตอร์แปรปรวนไปหมด แผนภูมิข้อมูล ฯลฯ ต่าง ๆ ล้วนเกิดอาการผิดรูปร่างขึ้น ทำให้หน่วยงานต่าง ๆ ไม่สามารถจะใช้คอมพิวเตอร์ในกิจการของตนได้ บางแห่งถึงกับต้องปิดกิจการลง สหรัฐอเมริกาารู้สึกวิตกกังวลเป็นอย่างมากและยังไม่สามารถหาทางแก้ไขได้ แม้ในปัจจุบันจะมีการสร้างโปรแกรมบางชนิดขึ้นมาเพื่อที่จะตรวจและทำลายไวรัสในเครื่องคอมพิวเตอร์ ทั้งนี้เพื่อป้องกันการทำให้เกิดความเสียหายหรือทำลายของไวรัสดังกล่าว (แม้แต่ประเทศไทยก็ได้มีการสร้างโปรแกรมชื่อ "ศิริราช" เป็นต้น) แต่ก็เพียงแก้ไขไวรัสได้บางชนิดเท่านั้น

และในอนาคตอันใกล้นี้หากไม่มีมาตรการใด ๆ ที่จะมาควบคุมการกระทำผิดเช่นนี้ให้เด็ดขาดแล้ว คาดว่าอาจทำให้เกิดผลเสียหายอย่างใหญ่หลวงต่อกิจการสำคัญ ๆ ของชาติ เช่นองค์

2. ชาลซีย์ และ สุเมธ สัจจอิสริยาวุฒิ, "โรคไวรัสในแผ่นดิสก์ (IBM)", วารสาร
ไมโครคอมพิวเตอร์ 43: 165

การนำ หน่วยข่าวกรองของสหรัฐและหน่วยงานอื่น ๆ อีกจำนวนมาก เนื่องจากระบบที่ต่อเชื่อม (link) กันของระบบคอมพิวเตอร์ ซึ่งจะทำให้มีผลกระทบกระเทือนออกไปอย่างกว้างขวาง ต่อมาวันที่ 6 พฤศจิกายน ค.ศ. 1988 ก็ให้ข่าวต่อเนื่องมาว่า ผลของการสืบสวนผู้เป็นต้นเหตุของไวรัส ที่เกิดขึ้นในครั้งนี้ ปรากฏว่าเป็นบุตรชายของเจ้าหน้าที่ระดับสูงทางคอมพิวเตอร์ ที่ทำงานอยู่ในหน่วยงานที่เกี่ยวกับความปลอดภัยของรัฐและได้จับกุมบุตรชายของเจ้าหน้าที่ผู้นั้นไว้ได้แล้ว แต่การจับกุมรายนี้เป็นเพียงรายเดียว ซึ่งยังมีความเสียหายทางอ้อมเดียวกันนี้อีกมากทั่วสหรัฐอเมริกา

และเมื่อวันที่ 3 ธันวาคม ค.ศ. 1988 หนังสือพิมพ์ได้แพร่ข่าวจากกรุงวอชิงตันว่ากระทรวงกลาโหมสหรัฐอเมริกาตัดสินใจตัดการติดต่อกับคอมพิวเตอร์ที่เชื่อมระหว่างหน่วยงานของฝ่ายศึกษาทั่วประเทศและเครือข่ายประสานงานเมื่อหลายวันก่อน หลังจากที่ข้อมูลต่างๆ ได้รับความเสียหายจากผลของไวรัสคอมพิวเตอร์ที่มีผู้ใส่เข้าไป ซึ่งขณะที่ผู้ทำการใส่เข้าไปกำลังได้รับการพิจารณาจากศาลที่ ซีราคิวส์ นิตยสาร Time ฉบับวันที่ 26 กันยายน ค.ศ. 1988 ถึงกับนำเรื่องราวของไวรัสคอมพิวเตอร์ขึ้นปก และอธิบายว่าในสหรัฐอเมริกาเวลานี้ ได้เกิดการแพร่ระบาดของไวรัสคอมพิวเตอร์อย่างมาก จนถึงกับการกล่าวกันว่า ในหมู่ผู้ใช้คอมพิวเตอร์ในสหรัฐฯ นั้น หัวข่าวไวรัสคอมพิวเตอร์ได้กลายเป็นเรื่องฮิตตกเตียงกันในช่วงตีหมาแพ มีผู้กล่าวอีกว่า การแพร่ระบาดของไวรัสคอมพิวเตอร์นี้ยังเชคคีที่จាក់คอยู่เพียงวงในมหาวิทยาลัย บริษัทห้างร้านบางแห่งองค์การนำ บริษัทโบอิงและสภาผู้แทนราษฎรเท่านั้น ยังไม่เข้าไปเล่นงานการทำงานของธนาคารชาติ ที่เป็นศูนย์กลางการควบคุมระบบถ่ายโอนเงินต่าง ๆ หรือเครื่องมือของตลาดหุ้น ซึ่งหากเกิดขึ้นคงจะสร้างความเสียหายอย่างมากมายมหาศาลจนไม่อาจคิดออกมาเป็นตัวเงินได้

อย่างไรก็ตามผู้เชี่ยวชาญด้านคอมพิวเตอร์ได้เตือนด้วยว่า สภาพการแพร่ระบาดของไวรัสคอมพิวเตอร์จะรุนแรงและร้ายแรงขึ้นเป็นลำดับกว่าที่เป็นอยู่ อันเนื่องมาจากการใช้คอมพิวเตอร์เข้ามามีบทบาทในชีวิตประจำวันของคนเรามากขึ้น และที่วิตกเป็นอย่างยิ่งคือมีการพบไวรัสที่อยู่ในระบบคอมพิวเตอร์ หรือข่ายงานคอมพิวเตอร์แล้วกว่า 1,000 ชนิด เช่น ไวรัสปากีสถานี (Pakistani) ไวรัสแมคอินทอช (Macintosh) ไวรัสสกอร์ส (Scores) หรือไวรัสพิช

(Peace) เป็นต้น³

สำหรับวิธีการป้องกันมิให้ตนเองต้องตกเป็นเหยื่อของไวรัสคอมพิวเตอร์ โดยอาจใช้โปรแกรมคอมพิวเตอร์เองในการค้นหา กำจัด และป้องกันไวรัสคอมพิวเตอร์ ซึ่งอาศัยอยู่ในหน่วยความจำและไวรัสคอมพิวเตอร์ในแผ่นดิสก์ โปรแกรมดังกล่าวได้มีผู้คิดค้นขึ้นเป็นจำนวนมาก เช่น SCAN , CLEAN , PROSCAN , VIRUSBUSTER 4.0 , ANTIVIRUS , VICTOR CHALIE , LASER เป็นต้น โดยโปรแกรมไม่ว่าจะอยู่ในรูปของฮาร์ดแวร์หรือซอฟต์แวร์ก็ตามต้องมีคุณสมบัติหลักที่สำคัญคือ สามารถค้นหา กำจัดและป้องกันไวรัสคอมพิวเตอร์ได้⁴ หรืออาจใช้วิธีป้องกันโดยการควบคุมการใช้เครื่อง เช่น โดยมีการใช้รหัส และเลขที่บัญชี จัดวางนโยบายและแนวทางการการใช้ซอฟต์แวร์ที่ไม่ได้มาตรฐาน จัดวางนโยบายเกี่ยวกับการคัดลอกซอฟต์แวร์ บังคับการตรวจสอบซอฟต์แวร์ทุกชนิดก่อนแจกจ่ายให้พนักงานหรือเจ้าหน้าที่ ตลอดจนการจัดประชาสัมพันธ์ให้พนักงานเจ้าหน้าที่และผู้ที่เกี่ยวข้องทุกคนได้เห็นถึงความสำคัญของการป้องกันไวรัสคอมพิวเตอร์และร่วมมือร่วมใจกันปฏิบัติตามกฎระเบียบโดยเคร่งครัด⁵

ไวรัสคอมพิวเตอร์ (computer viruses) เป็นปรากฏการณ์ใหม่ที่เกิดขึ้นในวงการคอมพิวเตอร์โดยโปรแกรมเหล่านี้ สามารถที่จะทำความเข้าใจได้โดยใช้เวลาศึกษาเพียง 2-3 ชั่วโมง และใช้วิธีการนำเข้าสู่ระบบในเวลาไม่กี่วินาที และสามารถขยายได้อย่างรวดเร็วในเวลาไม่กี่วันหรือนาที แต่เป็นสาเหตุที่ทำให้เกิดความเสียหายและความสูญเสียอย่างมากของข้อมูลทรัพย์สิน ดังนั้นจึงจำเป็นที่เรานักกฎหมายจะต้องเรียนรู้ถึงสภาพความเป็นมาของไวรัสคอมพิวเตอร์ และหาทางป้องกันและปราบปรามการกระทำความผิด มิให้ผู้กระทำความผิดหลุดพ้น

3. ภพเนตร , "บทกวีต่างแดน : ไวรัสคอมพิวเตอร์," ไทยรัฐ (19 พฤศจิกายน 2531): 2.

4. สุเมธ สัจจอิสริยาภรณ์ , "อนาคตโปรแกรมกำจัดไวรัส," คอมพิวเตอร์รีวิว ฉบับที่ 84 (สิงหาคม 2534) : 167.

5. ศรีศักดิ์ จามรมาน , "ความเห็นเกี่ยวกับไวรัสคอมพิวเตอร์," คอมพิวเตอร์รีวิว ฉบับที่ 84 (สิงหาคม 2534) : 127.

จากการถูกโทษ โดยอาศัยช่องว่างของกฎหมาย

แม้สหรัฐอเมริกาจะมีการออกกฎหมายเพื่อใช้ในการปราบปรามอาชญากรรมคอมพิวเตอร์ขึ้นมาโดยเฉพาะและยังมีกฎหมายอื่น ๆ ที่สามารถที่จะปรับบังคับใช้ได้กับการกระทำผิดเกี่ยวกับคอมพิวเตอร์หลายประเภทแล้วก็ตาม แต่กฎหมายดังกล่าวยังมีปัญหาถึงความไม่ชัดเจนถึงการที่จะนำผู้กระทำความผิดเกี่ยวกับซอฟต์แวร์อันตรายมาลงโทษ

นักกฎหมายและผู้เชี่ยวชาญด้านคอมพิวเตอร์ของสหรัฐอเมริกาเอง ได้มีการวิเคราะห์ถึงอันตรายของซอฟต์แวร์อันตราย และการกระทำผิดอันสามารถที่จะนำมาลงโทษกับการกระทำที่ผู้กระทำผิดได้ทำไป และทั้งเจ้าหน้าที่ฝ่ายปราบปรามเองยังได้สงสัยว่าจะสามารถที่จะจับกุมและลงโทษผู้กระทำความผิดเช่นนั้นได้อย่างไร ในเมื่อกฎหมายที่มีอยู่แล้วนั้นล่าช้าเกินไปสำหรับการกระทำซึ่งใช้เทคโนโลยีขั้นสูง แม้ว่าระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ เป็นสิ่งที่น่าหวงใยและควรระวังอย่างยิ่งอยู่ในภาวะวิกฤตในปัจจุบัน⁶

การแพร่ขยายของไวรัสคอมพิวเตอร์ การสร้างความเสียหายของตัวคอมพิวเตอร์ ต่อระบบคอมพิวเตอร์หรือข่ายงานคอมพิวเตอร์ทั่วประเทศ รวมทั้งต่างประเทศที่มีการเชื่อมต่อกัน มิได้เป็นสิ่งที่เป็นไปได้หรือเพื่อฝันในปัจจุบัน แต่การกระทำเช่นนั้นจะถือว่าผู้นั้นต้องรับโทษทางอาญาหรือไม่ ทั้งนี้เพราะการกระทำความผิดอาญาคือการกระทำซึ่งสังครวมทั้งกฎหมาย เห็นว่าเป็นการกระทำที่คุกคามอย่างร้ายแรงต่อระเบียบสาธารณะและความปลอดภัยของสังคม จึงจะลงโทษทุกคนที่กระทำการเช่นนั้น และการกระทำที่จะถือว่าเป็นการกระทำความผิดอาญานั้น จะต้องมีความหมายบัญญัติว่าการกระทำเช่นนั้นเป็นความผิดอาญา กฎหมายจะต้องกำหนดถึงโทษที่จะลงสำหรับการกระทำผิดเช่นนั้นด้วย

องค์ประกอบของกฎหมายอาญาก็จะต้องอธิบายไว้ในกฎหมายเพื่อการฟ้องผู้กระทำความผิด จำเลยจะต้องมีการกระทำที่แสดงออกว่า ได้กระทำในสิ่งซึ่งเป็นองค์ประกอบของกฎหมายอาญาทั้งหมด ดังนั้นถ้ากฎหมายกำหนดว่า ผู้ใดทำลายข้อมูลเป็นความผิดอาญา แต่หากการกระทำนั้นมิ

6. Lance J. Hoffman , ROGUE PROGRAMS virus, worm, and trojan horses
(USA: Van Nostrand Reinhold Co. Ltd. , 1990), p. 61.

ได้เป็นการทำลายข้อมูลย่อมไม่ถือว่าเป็นอาชญากรรม เช่น ถ้าการกระทำที่ทำลายเป็นเพียงการบันทึกการศึกษาของมหาวิทยาลัยย่อมไม่อยู่ในวัตถุประสงค์ของกฎหมายที่ประสงค์จะลงโทษ⁷

และเนื่องจากความไม่แน่ชัดของกฎหมายของสหรัฐอเมริกา จึงได้มีปัญหากับซอฟต์แวร์อันตรายขึ้น เมื่อนาย Robert Morrish ได้ถูกฟ้องในความผิดเกี่ยวกับ"เวิร์ม" (Worm) หรือนักคอมพิวเตอร์บางท่านเรียกอีกชื่อหนึ่งว่า "ไวรัสคอมพิวเตอร์เครือข่าย" (internet computer viruses) ในเดือนพฤศจิกายน ค.ศ.1988 โดยใส่เข้าไปในข่ายงานคอมพิวเตอร์ซึ่งข่ายงานดังกล่าวได้ใช้เพื่อสนับสนุนงานของรัฐบาล โดยเชื่อมกันระหว่างรัฐบาลและมหาวิทยาลัยอื่น ๆ แม้ว่านายมอริส เองจะเชื่อว่าสิ่งที่เขาทำนั้นน่าจะทำได้ในฐานะที่เขาได้กระทำไปเพื่อการทดลอง และแม้ว่าจะมีคนจำนวนมากไม่เห็นด้วยและยังยืนยันว่าการกระทำของเขานั้นเป็นความผิดและไร้จริยธรรม⁸

นายมอริส อายุ 23 ปี นักศึกษาปริญญาตรีของมหาวิทยาลัยเคอเนล บุตรชายของผู้เชี่ยวชาญด้านความมั่นคงแห่งชาติด้านความปลอดภัยเกี่ยวกับข้อมูลคอมพิวเตอร์ ซึ่งผลของการกระทำของเขาเป็นเหตุให้ เครื่องคอมพิวเตอร์หลายพันเครื่องรวมทั้งของกองทัพ และมหาวิทยาลัยต่างๆ ใช้การไม่ได้และยังได้แพร่เข้าสู่ ARPANET (Advanced Research Projects Agency Network) ของกระทรวงกลาโหมและ MILNET (ข่ายงานของกองทัพ) ซึ่งได้เชื่อมโยงกันและได้สร้างความเสียหายมากกว่าระบบคอมพิวเตอร์ 60,000 แห่งทั่วประเทศที่เชื่อมต่อกัน

อย่างไรก็ตามคณะลูกขุน (ในเดือนมกราคม ค.ศ.1989) เชื่อว่าการกระทำของนายมอริส เป็นความผิดและพิพากษาว่าเขาได้กระทำความผิดโดยฝ่าฝืน The Computer Fraud and Abuse Act of 1986 ตามกฎหมายนี้ถือว่าเป็นความผิดร้ายแรง (felony) ในความผิดฐานเข้าถึงระบบโดยไม่ชอบ (abuse the access) ด้วยจุดประสงค์ที่จะทำลายหรือทำให้เสียหาย ซึ่งตามกฎหมาย

7. Peter J. Denning , Computer Under Attack intruders, worm, and viruses. p. 489

8. Ibid, p. 479

ดังกล่าวมีโทษจำคุก 5 ปี หรือปรับ 250,000 เหรียญ และแม้ว่านายมอริส จะถูกพิพากษาว่ากระทำผิดแล้วก็ตาม แต่ยังมีปัญหาทางกฎหมายที่ยังค้างคั่งอยู่ว่า ภายใต้กฎหมายซึ่งตัดสินว่าเขากระทำผิดนั้น ครอบคลุมถึงการกระทำเช่นนี้ด้วยหรือไม่ และด้วยความไม่แน่ชัดนี้เองจึงได้มีการเสนอกฎหมายใหม่เพื่อที่จะแก้ไขปัญหาข้อพิพาทอันตรายนี้อันนี้ขึ้นมาโดยเฉพาะ⁹

นอกเหนือจากปัญหาเกี่ยวกับการขาดกฎหมายที่ทันสมัย อันจะนำมาปรับใช้กับกรณีโปรแกรมคอมพิวเตอร์นี้แล้ว ปัญหาขั้นสอบสวน การฟ้องร้อง และการพิจารณาหลักฐาน ก็เป็นปัญหาที่สำคัญอีกประการหนึ่ง เพราะแม้การกระทำของผู้กระทำผิดจะครบองค์ประกอบของการกระทำ ความผิด และครบเงื่อนไขที่สามารถถูกฟ้องได้แล้วก็ตาม แต่ยังคงอยู่ภายใต้ดุลพินิจในการฟ้องและหลักพยานหลักฐาน อัยการมีดุลพินิจเด็ดขาดเกี่ยวกับว่าจะไรเป็นอาชญากรรมที่เขาจะฟ้อง อัยการสามารถที่จะปฏิเสธการฟ้องบุคคลใดในความผิดอาญา แม้ว่าบุคคลนั้นจะได้กระทำต่อผู้อื่นก็ตาม

มีเหตุผลมากมายว่าทำไมอัยการถึงไม่ฟ้อง เหตุผลหนึ่งคือสำนักงานอัยการมีคดีเป็นจำนวนมากที่เป็นคดีรุนแรง และอัยการจะต้องเลือกอาชญากรผู้ซึ่งก่อให้เกิดอันตรายสูงสุดต่อสังคม เพราะอาชญากรรมเกี่ยวกับคอมพิวเตอร์ บ่อยครั้งที่เป็นการกระทำโดยตรงต่อวงการธุรกิจมากกว่ากระทำต่อบุคคลและปกติก็มีได้ เป็นการคุกคามต่อเนื้อตัวร่างกาย คดีประเภทนี้บ่อยครั้งที่ดูเหมือนว่าจะเป็นคดีที่มีความสำคัญลำดับต่ำที่จะถูกฟ้อง แม้แต่ผู้เชี่ยวชาญด้านคอมพิวเตอร์เองก็ดูเหมือนจะไม่คิดว่าอาชญากรรมคอมพิวเตอร์มีความร้ายแรงอะไร ในปี ค.ศ.1948 จากการสำรวจของ American Bar Association พบว่าลำดับชั้นของอาชญากรรมคอมพิวเตอร์นั้น มีความสำคัญน้อยที่สุดเป็นลำดับ 3 ในประเภทของความผิดที่เกิดขึ้นทั้งหมด ซึ่งมีเพียงการขโมยของในร้านและการลักลอบเข้าเมืองโดยผิดกฎหมายเท่านั้นที่อยู่ในระดับที่ต่ำกว่า ดังนั้นด้วยทัศนคติท่ามกลางความรับผิดชอบในความปลอดภัยเกี่ยวกับคอมพิวเตอร์ ของผู้ซึ่งสามารถที่จะฟ้องเอาตัวผู้กระทำผิดมาลงโทษเพื่อที่จะเปลี่ยนความสนใจของเขาในอันที่จะมาให้ความสำคัญต่ออาชญากรรมคอมพิวเตอร์

9. Peter J. Denning ,Ibid., p. 479

ซึ่งย่อมจะเป็นประโยชน์ต่อการปราบปรามการกระทำความผิดประเภทนี้¹⁰

งานการประเมินเกี่ยวกับความเข้าใจเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ในหมู่ผู้ัยการพบว่าผู้ัยการจะต้องใช้เวลาจำนวนมากในอันที่จะต้องใช้เวลาเพื่อเตรียมคดี ในความผิดที่เกี่ยวกับคอมพิวเตอร์ ซึ่งจำเป็นต้องทำความเข้าใจให้ดีขึ้น ถึงรูปแบบของอาชญากรรมที่มีความซับซ้อนทางเทคโนโลยี อย่างไรก็ตามผู้ัยการที่มีความรู้เกี่ยวกับเรื่องนี้มีน้อย เช่นเดียวกับศาลและคณะลูกขุน ก็มีจำนวนน้อยที่มีความรู้เกี่ยวกับเรื่องนี้ อันเป็นผลให้การพิจารณาคดีจะเป็นไปโดยยากมากและต้องใช้เวลา และสิ่งที่จะปรากฏออกมาในภายหลังยากที่จะทำนายได้ มีคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์คดีหนึ่งผู้ฟ้องได้ใช้เวลาหลายร้อยชั่วโมงที่จะเตรียม และสรุปว่าการกระทำนั้นเป็นความผิด แต่เมื่อศาลได้พิพากษาว่าเป็นการกระทำความผิด ศาลได้กำหนดโทษน้อยมากโดยให้จำคุกเพียงเล็กน้อยเท่านั้น และให้รอการลงโทษไว้ 2 ปีด้วยเหตุนี้ใครก็ตามย่อมไม่แปลกใจเลยว่าการที่ผู้ัยการไม่ให้ความสนใจกับอาชญากรรมคอมพิวเตอร์ ในเมื่อมีอาชญากรรมชนิดอื่นที่ร้ายแรงอีกมาก ซึ่งศาลได้พิจารณาไว้อย่างเห็นได้ชัดว่ามีความสำคัญมากในขณะนั้น

พยานหลักฐานที่จะผูกมัดผู้กระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ มีความจำเป็นที่จะต้องใช้เวลาอย่างมาก อันเนื่องจากขาดคำให้การของประจักษ์พยาน แต่พยานที่ได้รับนั้นโดยแท้จริงแล้วก็เป็นเพียงเหตุผลที่สามารถที่จะเชื่อได้อย่างมีเหตุผลตามที่กล่าวอ้าง ซึ่งผู้ัยการจะต้องพิสูจน์ให้ลูกขุนเชื่อโดยปราศจากเหตุอันสงสัยว่า ผู้นั้นได้กระทำความผิดครบองค์ประกอบของการกระทำความผิดอาญา ตามที่กฎหมายเฉพาะระบุไว้ การที่จะโยงให้การกระทำนั้นเข้ากับการกระทำซึ่งเป็นความผิดอาญาอาจจะยาก ถ้าหากไม่ใช้ความระมัดระวังในสิ่งที่ผิดสังเกตที่เกิดขึ้นกับอาชญากรรมคอมพิวเตอร์ ที่สามารถกระทำได้โดยไม่จำเป็นต้องใช้อุปกรณ์เครื่องมือใดประกอบ การกระทำความผิดสามารถกระทำได้โดยเพียงปลายนิ้วสัมผัสและกระทำได้โดยเงียบเชียบ น้อยคนที่จะรู้ว่า เขากำลังทำอะไรอยู่ ในทางตรงกันข้ามกับความผิดอื่น มือปืนและอาวุธของผู้กระทำความผิด จะต้องมีการแสดงออกทางกายภาพ ผู้พบเห็นอาจจะเห็นได้โดยทางหน้าต่างในการปล้นธนาคาร ซึ่งพยานอาจจะมองเห็นได้ นักย่องเบาเข้าไปในบ้านจะต้องเข้าไปโดยร่างกาย

10. Peter J. Denning ,Ibid., p. 492

เพื่อที่จะเอาสิ่งของในบ้านที่มีคานเวลากลางคืน ซึ่งทั้งหมดนี้ย่อมต่างไปจากอาชญากรรมคอมพิวเตอร์ ที่ผู้กระทำความผิดอาจจะอยู่ห่างกันหลายพันไมล์จากเครื่องคอมพิวเตอร์ที่ถูกกระทำ¹¹

และอาจมีผู้สนใจถามว่าทำไมจึงมีการฟ้องร้องกันทางศาลน้อย ทั้งนี้เนื่องจากเป็นเรื่องที่ซับซ้อนและเริ่มด้วยเหยื่อของซอฟต์แวร์อันตรายในกรณีไวรัสคอมพิวเตอร์ มีปัจจัยหลายอย่างที่ส่งผลกระทบต่อความสามารถของผู้เสียหายในการที่จะเริ่มต้นฟ้อง ปัญหาประการหนึ่งคือความซับซ้อนของไวรัสคอมพิวเตอร์ ซึ่งปัจจุบันยังคงเป็นเรื่องใหม่และมีบรรทัดฐานทางกฎหมายน้อย นอกจากนี้เป็นการยากยิ่งขึ้นถึงการที่ผู้เสียหายจะรู้ว่าผู้กระทำความผิดเป็นใคร และบ่อยครั้งที่ผู้เสียหายสามารถที่จะทราบเพียงความเสียหายโดยพิจารณาจากเวลาและจำนวนเงิน ผู้เสียหายอาจจะยากในการหาพยานหลักฐานการกระทำผิดที่ได้กระทำ เพื่อนำไปสู่ผู้กระทำความผิด ยิ่งกว่านั้นเหยื่อบางคนยังไม่เต็มใจที่จะเปิดเผยความเสียหาย ในกิจการของตนอันเกี่ยวกับไวรัสคอมพิวเตอร์ บริษัทใหญ่บางแห่งโดยเฉพาะอย่างยิ่ง สถาบันการเงิน บรรณานาที่จะให้ลูกค้าของตนเห็นว่าระบบคอมพิวเตอร์ของตนนั้น เชื่อถือได้และมีความปลอดภัย

PC MAGAZINE ได้รายงานถึงการติดต่อไวรัสคอมพิวเตอร์ของ EDS¹² ซึ่งเป็นสาขาหนึ่งของ GENERAL MORTOR ระบุว่าปัจจัยหนึ่งที่ไม่มีการเปิดเผยข้อมูลเกี่ยวกับการติดต่อไวรัสคอมพิวเตอร์ว่า "ส่วนหนึ่งที่เราขายให้แก่ลูกค้าคือความสามารถของเราที่จะดูแลข้อมูลของลูกค้า ดังนั้นเราจึงต้องระมัดระวังอย่างมากเกี่ยวกับสิ่งนั้น" ทศนะเหล่านี้เป็นสิ่งที่ไม่ได้อันที่จะเก็บปัญหาเหล่านี้เป็นความลับ ถ้าบริษัทต่าง ๆ ไม่ใช้วิธีการดำเนินการทางกฎหมายอาญาหรือให้ชดเชยค่าเสียหายทางแพ่งแล้ว ก็ย่อมจะเป็นอุปสรรคอย่างหนึ่งในการที่จะปราบปรามการกระทำความผิดนี้

ปัญหาเกี่ยวกับมาตรการทางกฎหมายนี้ สหรัฐอเมริกาได้มีการเสนอร่างกฎหมายเข้าสู่สภาองเกรสเพื่อที่จะออกเป็นกฎหมายของรัฐบาลกลาง ในอันที่จะปราบปรามการกระทำความผิด

11. Peter J. Denning ,Ibid., p. 492

12. Philip E. Fites , The Computer Virus Crisis (USA :

Van Nostrand Reinhold LTD. ,1992), p 135.

เกี่ยวกับไวรัสคอมพิวเตอร์ อันเป็นมาตรการอย่างหนึ่งที่จะตอบโต้การกระทำความผิด เมื่อสังคม
อยู่ในสถานการณ์ที่ต้องเผชิญกับปัญหาที่มีการเรียกร้องว่า "ควรที่จะมีกฎหมาย"¹³ ซึ่งเห็นว่ามี
เพียงกฎหมายเท่านั้นที่จะก่อตั้งขึ้นเพื่อควบคุมและลงโทษ ในอันจะช่วยแก้ปัญหาการสร้างไวรัส
และการสร้างความเสียหายต่อสังคมอย่างกว้างขวางอยู่ในขณะนี้ แม้ว่าการบัญญัติกฎหมายขึ้นมา
และกำหนดโทษจะเป็นเพียงทางหนึ่งที่จะช่วยแก้ปัญหา แต่ปัญหาอย่างหนึ่งในการออกกฎหมายนั้นคือ
กฎหมายต้องใช้เวลาในการที่จะออกบังคับใช้ ผู้มีอำนาจในการออกกฎหมายไม่ได้มีความรู้ถึงสาระ
สำคัญของไวรัสคอมพิวเตอร์มาก่อน ดังนั้นการที่จะเรียนรู้ถึงการทำงานและเทคนิคต่าง ๆ ของ
คอมพิวเตอร์ ระบบคอมพิวเตอร์ ข่ายงานคอมพิวเตอร์ซอฟต์แวร์อันตรายต่าง ๆ ย่อมเป็นสิ่งสำคัญ
ก่อนที่มีการร่างและออกกฎหมายมาใช้บังคับ มันอาจจะต้องใช้เวลาหลายเดือนหรือหลายปี ในการ
ร่างและผ่านกฎหมาย นอกจากนี้ยังความจำเป็นที่จะต้องให้ผู้ที่เกี่ยวข้องกับกฎหมาย ไม่ว่าจะเป็นผู้
พิพากษา อัยการ ทนายความ ได้มีความรู้และเข้าใจในปรากฏการณ์เช่นนี้

สำหรับประเทศไทยการนำเครื่องคอมพิวเตอร์มาใช้ ได้มีการเพิ่มขึ้นอย่างรวดเร็ว เพราะ
ต่างก็เห็นถึงความสำคัญและความจำเป็นที่จะต้องมีการนำเครื่องคอมพิวเตอร์มาใช้ และสิ่งที่หลีกเลี่ยงไม่
พ้นเช่นเดียวกับสหรัฐอเมริกาเมื่อปรากฏพบว่า ได้มีไวรัสคอมพิวเตอร์เป็นจำนวนมากได้สร้างความ
ความเสียหายต่อระบบคอมพิวเตอร์ ตลอดจนข้อมูลที่ได้บันทึกไว้ในเครื่องคอมพิวเตอร์ และแผ่น
ดิสก์ ไวรัสที่ได้เข้ามาแพร่ระบาดอยู่ในขณะนี้ส่วนหนึ่งจะติดมาจากต่างประเทศ เช่น เจริซาเล็ม
(Jerusalem) คีย์เพรส (Keypress) ดราก อเวนเจอร์ (Drak Avenger) สโตนด์ (stoned)
เป็นต้น นอกจากนี้ยังได้พบไวรัสซึ่งเชื่อว่าเป็นของคนไทยเอง¹⁴ และปัจจุบันมีการติดเข้าสู่ระบบ
คอมพิวเตอร์เป็นจำนวนมากซึ่งมีชื่อว่า "ลาวดวงเดือน" อีกด้วย ดังนั้นจากการที่พบไวรัสคอมพิวเตอร์
ดังกล่าวย่อมแสดงให้เห็นได้โดยชัดแล้วว่า ขณะนี้ประเทศไทยก็ตกอยู่ภายใต้สถานการณ์ที่
น่าเป็นห่วงยิ่งถึงความเสียหายที่จะเกิดขึ้น อันเนื่องมาจากไวรัสคอมพิวเตอร์

13. Philip ,Ibid. , p.144

14. ธนัย อนันต์วัฒนาวิทย์, "ไวรัสยอดนิยม," คอมพิวเตอร์รีวิว ฉบับที่ 87

เมื่อวันที่ 23 กุมภาพันธ์ 2536 หนังสือพิมพ์ผู้จัดการรายวัน ได้ออกข่าวถึงการที่บริษัท ซิปร่า คอมพิวเตอร์ จำกัด ได้ประกาศเตือนไวรัส "สวีตบอยส์" (Swedish Boys) หรือเด็กผู้ชายเชื้อสายสวีเดน ที่จะเริ่มปฏิบัติการสร้างความเสียหายแก่แผ่นดิสก์และข้อมูล ในวันที่ 23-25 กุมภาพันธ์ 2536 นี้ โดยพฤติกรรมของไวรัสชนิดนี้จะเกาะติดอยู่กับข้อมูลทั้งหมดที่บันทึกอยู่ในแผ่นดิสก์เลยก็ได้ ทั้งนี้นอกเหนือจากไวรัสคอมพิวเตอร์สวีตบอยส์ ที่จะระบาดแก่ผู้ใช้คอมพิวเตอร์ในวันที่ 23-25 กุมภาพันธ์แล้ว ไวรัสไมเคิลแองเจโลก็เป็นไวรัสอีกชนิดหนึ่งที่ถูกกำหนดโปรแกรมให้ระบาดในวันที่ 6 มีนาคมของทุกปีเช่นกัน¹⁵

เมื่ออาชญากรรมคอมพิวเตอร์ในกรณีของไวรัสคอมพิวเตอร์ต่าง ๆ ได้เข้ามาสร้างความเสียหาย จึงจำเป็นต้องมีการวิเคราะห์ถึงกฎหมายอาญาที่จะนำมาปรับใช้ว่าได้ครอบคลุมถึงกรณี "ไวรัสคอมพิวเตอร์" แล้วหรือไม่ หากไม่เพียงพอและจะได้วางแนวทางการพิจารณาหาหนทางบัญญัติกฎหมายใหม่ ที่จะนำมาใช้วางระเบียบปฏิบัติ หรือห้ามการกระทำบางอย่างซึ่งเกี่ยวข้องกับหรือมุ่งโดยตรงต่อเครื่องคอมพิวเตอร์ อย่างไรก็ตามในการเขียนวิทยานิพนธ์ฉบับนี้ นอกจากจะวิเคราะห์ในเรื่องการกระทำที่เป็นความผิดทางอาญาแล้ว ก็จะแสดงให้เห็นถึงลักษณะการดำเนินการของเครื่องคอมพิวเตอร์ สิ่งประดิษฐ์ใหม่ทางวิทยาศาสตร์ซึ่งกฎหมายอาญาปัจจุบันของไทยยังล่าหลัง ทั้งนี้ เพื่อที่จะอำนวยความสะดวกแก่การทำความเข้าใจในเรื่องของการกระทำแต่ละชนิดที่เกิดขึ้นจากซอฟต์แวร์อันตราย และความเสียหายที่จะเกิดขึ้น

นอกเหนือจากโทษทางอาญาที่ผู้กระทำผิดเกี่ยวกับไวรัสคอมพิวเตอร์สมควรที่จะได้รับแล้ว ความเสียหายในทางแพ่ง ผู้กระทำก็ต้องรับผิดชอบในทางแพ่งชดเชยค่าเสียหายที่เกิดขึ้น แต่อย่างไรก็ตามไม่มีกฎหมายแพ่ง กำหนดลักษณะความรับผิดที่เกิดขึ้นจากไวรัสคอมพิวเตอร์ขึ้นโดยเฉพาะ โดยอาจจะปรับใช้ได้กับกฎหมายลักษณะ "ละเมิด" สำหรับการกระทำทั้งที่เจตนาและไม่เจตนา ที่ก่อให้เกิดความเสียหายแก่ร่างกาย ทรัพย์สิน หรือการสูญเสียทางเศรษฐกิจ แต่ปัญหาอาจจะเกิดขึ้นตามมาว่าใครบ้างที่จะต้องเป็นผู้รับผิดชอบชดเชยค่าเสียหายที่เกิดขึ้น จากการกระทำเกี่ยวกับไวรัสคอมพิวเตอร์

15. " เตือนผู้ใช้คอมพิวเตอร์ "ไวรัส" ระบาดวันนี้, " ผู้จัดการรายวัน (23 กุมภาพันธ์ 2536) , หน้า 1.

ซึ่งนอกจากผู้กระทำผิดโดยตรงซึ่งโดยปกติก็เป็นสิ่งที่ยากมาก ในการพิสูจน์ความเสียหายที่เกิดขึ้น รวมถึงผู้เขียนโปรแกรมคอมพิวเตอร์ บริษัทผู้ผลิต ผู้ขายส่ง และผู้ขายปลีก จะต้องรับผิดชอบความเสียหายที่เกิดขึ้นจากการที่มีไวรัสคอมพิวเตอร์ติดอยู่เพียงใดหรือไม่ ซึ่งปัญหาความรับผิดชอบทางแพ่งอันเกิดจากไวรัสคอมพิวเตอร์ จึงเป็นปัญหาที่สำคัญอีกปัญหาหนึ่งที่ผู้สนใจสามารถนำไปศึกษาต่อไปได้ ว่าบุคคลใดบ้างเป็นผู้มีหน้าที่และความรับผิดชอบทางแพ่ง

วัตถุประสงค์และขอบเขตของการวิจัย

ความเสียหายที่เกิดจากการการกระทำของไวรัสคอมพิวเตอร์ เป็นการกระทำที่เกิดขึ้นต่อข้อมูล โปรแกรม และระบบคอมพิวเตอร์ ซึ่งความเสียหายที่เกิดขึ้นจะเป็นไปตาม ที่ผู้เขียนโปรแกรมหรือคำสั่งไวรัสคอมพิวเตอร์กำหนด

ความเสียหายที่จะเกิดขึ้นอาจป้องกันได้โดยการป้องกัน ซึ่งแนวทางการป้องกันนี้สามารถแบ่งได้ออกเป็น 3 วิธี คือ

1. การป้องกันโดยอาศัยบุคคลากร คือการวางระเบียบปฏิบัติการทำงานเกี่ยวกับเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ เช่น การควบคุมการใช้เครื่อง เป็นต้น
 2. การป้องกันโดยอาศัยโปรแกรมคอมพิวเตอร์ โดยโปรแกรมนี้จะทำหน้าที่เป็นยามที่รู้จักไวรัสทั้งหลาย มาคอยตรวจสอบก่อนการใช้งาน เท่าที่พบโดยมากโปรแกรมการตรวจหาเหล่านี้ จะรู้จักไวรัสเฉพาะเจาะจงเป็นตัว ๆ เท่านั้น ไม่มีโปรแกรมใดที่รู้จักแบบครอบจักรวาล
 3. การป้องกันโดยกำหนดสภาพบังคับทางกฎหมายต่อไวรัสคอมพิวเตอร์อย่างชัดเจน เพื่อป้องกันมิให้ไวรัสคอมพิวเตอร์ สร้างความเสียหายต่อคอมพิวเตอร์ได้มากยิ่งขึ้น
- แต่เนื่องจากปัญหาในทางป้องกันการกระทำความผิดนี้ จำเป็นที่จะต้องอาศัยความรู้ใน

ทางวิศวกรรม เพื่อที่จะทำความเข้าใจวิธีการป้องกันได้อย่างละเอียดและมีประสิทธิภาพ ดังนั้น ในการวิจัยฉบับนี้ ผู้เขียนจะไม่กล่าวลงไปถึงในส่วนนี้

นอกจากนี้ การสืบสวนสอบสวนและพยานหลักฐาน เป็นเรื่องที่ยากซึ่งละเอียดอ่อนยิ่ง อันเนื่องจากอาชญากรรมคอมพิวเตอร์ประเภทนี้ มีลักษณะการกระทำความผิดที่แตกต่างไปจากการกระทำความผิดโดยทั่วไป และมักจะรู้ตัวผู้กระทำความผิดได้ยาก ตลอดจนผู้เสียหายมีแนวโน้มที่จะไม่เต็มใจที่จะบอกถึงรายละเอียดของคดี ตลอดจนความเสียหายที่เกิดขึ้น เพราะเกรงว่าจะมีผลกระทบต่อธุรกิจของตน นอกจากนี้พนักงานสืบสวนสอบสวน รวมทั้งอัยการจะต้องได้รับการฝึกฝนให้รู้ถึงเทคนิคต่าง ๆ เพื่อการสืบสวนสอบสวน จะได้รับความสำเร็จอย่างสมบูรณ์ รวมทั้งเทคนิคการรวบรวมพยานหลักฐาน อันอื่นที่จะเชื่อมโยงไปถึงผู้กระทำความผิดเกี่ยวกับซอฟต์แวร์อันตราย ทั้งนี้ล้วนแต่ต้องอาศัยความรู้และทักษะในการสืบสวนและการรวบรวม ซึ่งผู้เขียนก็จะไม่กล่าวถึงในส่วนนี้ เพราะเป็นเรื่องที่สำคัญและสมควรที่จะให้ผู้มีความรู้ความสามารถด้านการสืบสวนสอบสวนได้ทำการวิจัยในส่วนนี้

ซึ่งวัตถุประสงค์และขอบเขตของวิทยานิพนธ์ฉบับนี้ ต้องการที่จะวิเคราะห์เฉพาะปัญหาทางกฎหมายอาญาต่อกรณีไวรัสคอมพิวเตอร์เท่านั้น เพื่อให้ทราบถึงประวัติความเป็นมาของไวรัสคอมพิวเตอร์ ความเสียหายที่เกิดขึ้นจากโปรแกรมหรือคำสั่งไวรัสคอมพิวเตอร์ ตลอดจนแนวทางกฎหมายอาญาของต่างประเทศ และศึกษาถึงกฎหมายอาญาของไทยที่มีอยู่ ซึ่งจะนำมาปรับใช้กับการกระทำความผิดเกี่ยวกับไวรัสคอมพิวเตอร์ อันจะนำไปสู่แนวทางการบัญญัติกฎหมายควบคุมไวรัสคอมพิวเตอร์ ให้ได้อย่างมีประสิทธิภาพ

จุฬาลงกรณ์มหาวิทยาลัย

สมมติฐานในการวิจัย

สมมติฐานในการวิจัยฉบับนี้ก็คือ กฎหมายซึ่งมีโทษทางอาญาของไทยในปัจจุบันไม่อาจนำมาบังคับใช้กับการกระทำความผิดเกี่ยวกับโปรแกรมหรือคำสั่งไวรัสคอมพิวเตอร์ ดังนั้นจึงก่อให้เกิดปัญหาทางด้านกฎหมาย และมีความจำเป็นที่จะต้องบัญญัติกฎหมายใหม่เพิ่มเติมขึ้น เพื่อให้ครอบคลุมความผิดในเรื่องนี้ได้อย่างเหมาะสม

ประโยชน์ที่คาดว่าจะได้รับ

1. เพื่อให้ทราบถึงลักษณะและประวัติของไวรัสคอมพิวเตอร์
2. เพื่อให้ทราบถึงลักษณะความเสียหายที่เกิดขึ้นจากไวรัสคอมพิวเตอร์
3. เพื่อแสดงให้เห็นถึงแนวความคิดเกี่ยวกับการนำกฎหมายอาญามาใช้บังคับกับไวรัสคอมพิวเตอร์
4. เพื่อให้ทราบถึงจุดบกพร่องของกฎหมายอาญาต่างประเทศ ตลอดจนแนวทางการแก้ปัญหาเกี่ยวกับไวรัสคอมพิวเตอร์
5. เพื่อที่จะให้ทราบถึงกฎหมายอาญาของไทย ว่ามีหลักเกี่ยวกับการบังคับใช้ต่อกรณีไวรัสคอมพิวเตอร์นี้อย่างไร อันจะนำไปสู่แนวทางการปรับปรุงแก้ไขกฎหมายต่อไป
6. เพื่อลดปัญหาของไวรัสคอมพิวเตอร์ ในระบบคอมพิวเตอร์