ปัจจุบันคอมพิวเตอร์ได้เข้ามามีส่วนในการติดต่อสื่อสาร อันถือว่าเป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ แต่ในทางกลับกันก็มีการนำเทคโนโลยีคอมพิวเตอร์ไปใช้ในทางมิชอบ ก่อให้เกิดรูปแบบการกระทำความผิดที่แตกต่างจากการกระทำความผิดอาญาแบบดั้งเดิม ส่งผลกระทบให้เกิดความเสียหายทางเศรษฐกิจ สังคม และความมั่นคงของประเทศเป็นอย่างมาก จึงได้มีการบัญญัติกฎหมายขึ้นมาเพื่อปราบปรามการกระทำความผิด คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกำหนดให้มี "พนักงานเจ้าหน้าที่" ผู้มีความรู้ความเชี่ยวชาญเกี่ยวกับระบบคอมพิวเตอร์ เข้ามามีอำนาจพิเศษในการรวบรวมพยานหลักฐาน โดยเฉพาะซึ่งวิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์สำคัญในการศึกษาถึงอำนาจของพนักงานเจ้าหน้าที่ โดยมุ่งเน้นถึงการบังคับใช้กฎหมาย และผลลัพธ์ของการใช้อำนาจในทางปฏิบัติ

ผลของการศึกษาพบว่า กฎหมายที่มีอยู่บางส่วน สามารถปรับใช้ในการปราบปรามการกระทำความผิดที่เกิดขึ้นได้ แต่ไม่ครอบคลุมทั้งหมดทุกกรณี โดยในส่วนของกฎหมายวิธีสบัญญัติที่ให้อำนาจพนักงานเจ้าหน้าที่ยังขาดความเหมาะสม เนื่องจากผู้กระทำผิดสามารถลงมือกระทำได้จากทุกที่ทั่วโลกไม่ว่าจะอยู่ ณ ที่ใดก็ตาม ที่มีคอมพิวเตอร์เชื่อมต่อเข้ากับระบบเครือข่ายทำให้ยากที่จะติดตามและพยานหลักฐานส่วนใหญ่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ที่ไม่มีรูปร่างสามารถแก้ไข เปลี่ยนแปลงหรือทำลายได้โดยง่าย แต่กฎหมายกลับมิได้ให้อำนาจในกรณีเร่งด่วนไว้โดยเฉพาะและบทบัญญัติที่ให้อำนาจยังขาดความชัดเจนคลุมเครือ จึงเกิดปัญหาต่อมาว่าทำอย่างไรพนักงานเจ้าหน้าที่จึงจะสามารถเข้าถึงพยานหลักฐานได้อย่างรวดเร็ว และเก็บรวบรวมข้อมูลสำคัญที่จะใช้ในการพิสูจน์ความผิดได้อย่างครบถ้วนสมบูรณ์ เพียงพอที่จะนำสืบให้ศาลรับฟังลงโทษผู้กระทำความผิดได้

ข้อเสนอแนะในการศึกษาครั้งนี้ จึงอยู่ที่การสร้างระบบและมาตรการในการใช้อำนาจของพนักงานเจ้าหน้าที่ให้สามารถรวบรวมพยานหลักฐานได้อย่างทันท่วงที พร้อมทั้งกำหนดให้คดีความผิดเกี่ยวกับคอมพิวเตอร์อยู่ในอำนาจของกรมสอบสวนคดีพิเศษ เพื่อจะได้ใช้อำนาจตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ในการปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งมากกว่าอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา ตลอดจนการตั้งผู้เชี่ยวชาญและประสานงานระหว่างหน่วยงานที่เกี่ยวข้องให้มาร่วมสอบสวนในคดีความผิดเกี่ยวกับคอมพิวเตอร์ได้ อันจะก่อให้เกิดประโยชน์และประสิทธิภาพสูงสุดในการรับมือและรองรับต่ออาชญากรรมหรือการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ต่อไป

At present, computers are significantly and legitimately used in communications, business, and daily life. Conversely, computer technology can be wrongfully used, and can be used to commit offences which differ from traditional criminal offences. This state of affairs brings about economic and social damages and even derogates from national security.

Subsequently, a law was framed that was designed to suppress such offences, viz., the Act on Offences Regarding Computers B.E. 2550 (2007). In this law, it is stated that a "competent authority" is one who has knowledge and expertise regarding computer systems. Accordingly, such a competent authority would be able to collect specific, special, and particular kinds of evidence.

With this background in mind, the researcher thereupon decided to investigate the authority exercised by such competent authorities, especially in regard to how the law designed to regulate their activities should be enforced and how such authority could be exercised in practice.

Findings are as follows:

Although some existing laws could be altered allowing them to be used in suppressing computer offenses, it remains the case that coverage would still be insufficient. Furthermore, the existing law granting authority to competent authority is not entirely appropriate. This is because the offenders can commit computer offences anywhere in the world where they have access to computers that can be connected to a network. It is therefore difficult to detect such crimes. Moreover, the evidence of having committed a computer-related crime is normally electronic in nature and hence easily corrected, changed or deleted.

The law fails to take account of urgent situations and the provisions concerning authority to investigate putative computer crimes are unclear. As a consequence, legal problems arise in regard to the need to access evidence quickly in order to prove guilt in a complete fashion such that courts can appropriately respond and offenders found guilty and subsequently punished.

In this light, then, the researcher would like to offer the following suggestions:

It is necessary to revamp the existing laws regarding the authority of competent authority in computer crimes. Measures must be

adopted which would allow evidence to be gathered with alacrity. In addition, the investigation of purported computer offences should be placed under the authority of the Department of Special Investigation (DSI), whose authority is exercised in accordance with the Act of Special Investigation B.E. 2547 (2004). In suppressing computer offences, more authority should be vested in the DSI than hitherto has been the case under the Code of Criminal Procedure. The DSI would be accordingly authorized to appoint experts and those who could coordinate investigatory efforts on the part of concerned agencies. These reform measures would yield maximum benefits and foster the highest degree of efficiency in confronting and handling computer-related criminal offences in the future.