การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพและวิจัยสนาม สำหรับการวิจัยเอกสารนั้นจะเป็นการศึกษาค้นคว้าจากรายงานการวิจัย รายงานการสำรวจ เอกสารตำรา เอกสารประกอบการสัมมนาทางวิชาการ หรือรายงานของส่วนราชการต่างๆ บทความ วารสาร รวมถึงข้อมูลข่าวสารเกี่ยวกับอาชญากรรมบนอินเทอร์เน็ต จากเว็บไซต์และหนังสือพิมพ์ตั้งแต่ปี 2543 จนถึงปัจจุบัน ส่วนการวิจัยสนาม มุ่งเน้นการสัมภาษณ์ในเชิงลึกจากผู้ที่เกี่ยวข้องและมีบทบาทสำคัญด้านการป้องกันปราบปรามอาชญากรรมบนอินเทอร์เน็ตของสำนักงานตำรวจแห่งชาติ ซึ่งล้วนแล้วแต่เป็นผู้ที่มีความรู้ ความเชี่ยวชาญ และทำหน้าที่เป็นวิทยากรถ่ายทอดความรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์ให้กับเจ้าหน้าที่ตำรวจและนักศึกษาในสถาบันการศึกษาต่างๆ จำนวน 10 ท่าน โดยมีจุดมุ่งหมายเพื่อสำรวจความคิดเห็นเกี่ยวกับรูปแบบและวิธีการของอาชญากรรมอินเทอร์เน็ต ปัญหาและอุปสรรคด้านการป้องกันปราบปรามอาชญากรรมบนอินเทอร์เน็ต แนวทางแก้ไขปัญหาอาชญากรรมบนอินเทอร์เน็ต และประโยชน์ต่อการปฏิบัติงาน ถ้าหากมีการสนับสนุนให้ใช้อินเทอร์เน็ตในองค์กรตำรวจ

ผลการศึกษาวิจัย มีดังนี้

1. รูปแบบและวิธีการของอาชญากรรมบนอินเทอร์เน็ต จำแนกออกเป็น 3 ลักษณะ ดังนี้

1.1 อาชญากรรมต่อระบบคอมพิวเตอร์ ได้แก่ 1) การก่อวินาศกรรมระบบ 2) การก่อวินาศกรรมและทำลายข้อมูล 3) ไวรัสคอมพิวเตอร์

1.2 อาชญากรรมเพื่อก่ออาชญากรรม ได้แก่ 1) การจารกรรมข้อมูล 2) การ "ตก" รหัสผ่านหรือ "นักสูดกลิ่น" รหัสผ่าน

1.3 อาชญากรรมทั่วไป ได้แก่ 1) การเผยแพร่สิ่งลามกอนาจารและเพศพาณิชย์ 2) การพนัน 3) การฉ้อโกง 4) การฟอกเงิน 5) การหมิ่นประมาทบนอินเทอร์เน็ต 6) การละเมิดทรัพย์สินทางปัญญา 7) การล่อลวงบนอินเทอร์เน็ต 8) การโฆษณาเนื้อหาเกี่ยวกับสิ่งผิดกฎหมายหรือขัดต่อศีลธรรมอันดีของประชาชน

2. ปัญหาและอุปสรรคในการป้องกันปราบปรามอาชญากรรมบนอินเทอร์เน็ตของตำรวจ จำแนกเป็นด้านต่างๆ ดังนี้

2.1 ด้านกฎหมาย ได้แก่ 1) เขตอำนาจศาล 2) ความร่วมมือระหว่างประเทศในการดำเนินคดี 3) ความต่างกันของกฎหมายแต่ละประเทศ 4) ความล้าสมัยของกฎหมาย 5) การตีความโดยเคร่งครัดของกฎหมายอาญา 6) การค้นและยึดพยานหลักฐาน 7) การรับฟังพยานหลักฐานของศาล

2.2 ปัญหาด้านเจ้าหน้าที่ผู้ปฏิบัติ ได้แก่ 1) การขาดความรู้ความเข้าใจเกี่ยวกับอาชญากรรมบนอินเทอร์เน็ต 2) การขาดความรู้เทคนิคการสืบสวนสอบสวนอาชญากรรมบนอินเทอร์เน็ต 3) การขาดความรู้ความชำนาญในการตรวจค้น การยึด และการเก็บรักษาหลักฐาน 4) การขาดความรู้ความเข้าใจในกฎหมายที่ใช้หรือปรับใช้บังคับ 5) การขาดเครื่องมือและอุปกรณ์ที่ทันสมัย 6) การขาดการสนับสนุนค่าตอบแทนในการปฏิบัติงาน

2.3 ปัญหาด้านบริหารและจัดการ ได้แก่ 1) การขาดหน่วยงานที่รับผิดชอบโดยเฉพาะ 2) การขาดบุคลากรที่มีความชำนาญเฉพาะด้าน 3) การขาดการกำหนดวิธีปฏิบัติที่ชัดเจน 4) การขาดการทำงานเชิงบูรณาการหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและ

เอกชน 5) การขาดการส่งเสริมสนับสนุนการฝึกอบรมพัฒนาความรู้ความสามารถ 6) การขาดการให้ความสำคัญหรือสนใจของผู้บังคับบัญชาในหน่วยงาน

2.4 ปัญหาด้านความร่วมมือ ได้แก่ 1) คดีไม่ได้รับความสนใจจากประชาชน 2) คดีไม่ได้รับความร่วมมือจากผู้ต้องหา 3) คดีไม่ได้รับความร่วมมือจากผู้เสียหาย 4) การไม่ได้รับความร่วมมือจากประชาชนแจ้งเบาะแส 5) การไม่ได้รับความร่วมมือจากผู้ให้บริการอินเทอร์เน็ต (ISP)

3. แนวทางแก้ไขปัญหาอาชญากรรมบนอินเทอร์เน็ต จำแนกเป็น 2 ระยะ ดังนี้

3.1 แนวทางแก้ไขปัญหาในระยะสั้น ได้แก่ 1) จัดฝึกอบรมเจ้าหน้าที่ผู้ปฏิบัติให้มีความรู้ความเข้าใจในการสอบสวนดำเนินคดีเกี่ยวกับอาชญากรรมบนอินเทอร์เน็ต 2) ปรับกลยุทธ์วิธีการสืบสวนสอบสวนที่มีอยู่เพื่อใช้กับอาชญากรรมบนอินเทอร์เน็ต 3) ปรับใช้กฎหมายที่มีอยู่เพื่อให้เกิดประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมบนอินเทอร์เน็ต 4) มอบหมายหน่วยงานให้รับผิดชอบในการตรวจสอบ กลั่นกรองเนื้อหาเกี่ยวกับอาชญากรรมบนอินเทอร์เน็ต 5) สร้างแนวร่วมภาคประชาชนโดยร่วมมือกับตำรวจในการป้องกันและปราบปรามอาชญากรรมบนอินเทอร์เน็ต 6) รณรงค์ประชาสัมพันธ์แจ้งเตือนประชาชนในข้อควรปฏิบัติและข้อควรระมัดระวังเกี่ยวกับอาชญากรรมบนอินเทอร์เน็ต

3.2 แนวทางแก้ไขปัญหาในระยะยาว ได้แก่ 1) กำหนดแนวนโยบายการป้องกันและปราบปรามที่ชัดเจนและสอดคล้องกับปัญหาอาชญากรรมบนอินเทอร์เน็ต 2) จัดตั้งหน่วยงานให้มีอำนาจหน้าที่รับผิดชอบเกี่ยวกับอาชญากรรมบนอินเทอร์เน็ตโดยเฉพาะ 3) บรรจุและแต่งตั้งเจ้าหน้าที่ผู้ปฏิบัติที่มีความรู้ความชำนาญด้านอาชญากรรมบนอินเทอร์เน็ต 4) พัฒนาทางวิชาการ ขั้นตอนการปฏิบัติ และกฎหมายเกี่ยวกับอาชญากรรมบนอินเทอร์เน็ต 5) พัฒนาขีดความสามารถในการตรวจพิสูจน์ทางคอมพิวเตอร์ เป็นส่วนหนึ่งของการพิสูจน์หลักฐาน 6) กำหนดกลยุทธ์ในการบูรณาการการทำงานกับหน่วยงานที่เกี่ยวข้องกับอาชญากรรมบนอินเทอร์เน็ตทั้งในและต่างประเทศ 7) กำหนดกลยุทธ์ในการแสวงหาความร่วมมือจากประชาชนในการป้องกันและปราบปรามอาชญากรรมบนอินเทอร์เน็ต

4. ประโยชน์ต่อการปฏิบัติงาน ถ้าหากมีการสนับสนุนให้ใช้อินเทอร์เน็ตในองค์กรตำรวจ ดังนี้

4.1 สามารถรับส่งข้อมูลข่าวสารระหว่างหน่วยผ่านทางไปรษณีย์อิเล็กทรอนิกส์เพื่อความรวดเร็วและประหยัดค่าใช้จ่าย

4.2 สามารถประชาสัมพันธ์ข้อมูลข่าวสารที่เกี่ยวกับตำรวจ หรือประชาสัมพันธ์แจ้งเตือนข้อมูลการกระทำความผิดให้แก่ประชาชนผ่านทางเว็บไซต์

4.3 สามารถศึกษาค้นคว้าข้อมูลข่าวสาร และวิทยาการใหม่ๆ เพื่อเป็นการเพิ่มโลกทัศน์และวิสัยทัศน์ให้กับตำรวจ

4.4 สามารถรับเรื่องร้องเรียนปัญหาการกระทำผิดผ่านทางเว็บบอร์ด

4.5 สามารถเฝ้าระวังและตรวจสอบ กลั่นกรองพฤติการณ์การกระทำผิดบนอินเทอร์เน็ต

4.6 สามารถใช้เป็นเครือข่ายการเชื่อมโยงข้อมูลของตำรวจแทนเครือข่ายเดิม (POLIS)

4.7 สร้างวัฒนธรรมการทำงานแบบใหม่ๆ ให้เกิดขึ้นในองค์กรตำรวจ อาทิ ด้านงานธุรการ สามารถลดขั้นตอนการปฏิบัติงาน ลดความสิ้นเปลืองในการปฏิบัติงาน และเพิ่มความรวดเร็ว ความถูกต้องและชัดเจนมากขึ้นในการประสานงานระหว่างหน่วยงาน

This thesis is based on both qualitative and field researches. In terms of the qualitative research, relevant material was accumulated from research findings, survey reports, academic materials, seminar documents, agendas and the minutes of government agencies, articles, journals as well as information on crimenology on the Internet, web sites, and newspapers issued between 2000 and 2004. With regard to field research, interviews in depth were conducted of 10 experts- lecturers from Police Headquarters, who are known for the major role they have played in crime suppression. They constitute a professional elite with extensive knowledge of computer-related crime, individuals who have taught the police officers and students from a number of institutions. The aim of the interviews was to seek out for their opinions

regarding the type of criminal patterns and ploys found on the Internet, problems and obstacles concerning the suppression of such crime, the foiling of Internet crime, guidelines for solving computer crime as well as advantages to the police regarding to the use of the Internet in day-to-day police work.

Findings of the research

1. The patterns and ploys employed in Internet crime may be classified into three categories as follows:

1.1 The crimes against the computer system are 1) sabotage of the whole system, 2) the destruction or deletion of information 3) the spread of computer viruses

1.2 The crimes employed to commit crimes are 1) the conspiracy of information 2) the stealing of passwords

1.3 Common computer crimes include 1) the publishing and circulation of pornography and sex businesses 2) gambling on the Internet 3) fraud in different forms 4) money laundering 5) slander on the Internet 6) the abuse of intellectual property 7) deception on the Internet 8) the advertising of subject matter involving illegal items or offending people's proper morals.

2. The problems and obstacles facing the police in protecting and suppressing crimes on the Internet result from the following:

2.1 The law itself which are 1) the limit of judicial power 2) the lack of international cooperation in prosecuting criminal cases 3) the differences in each country's laws 4) laws that are out of date 5) the strict interpretation of

criminal law 6) difficulty regarding the discovering and seizure of clues and evidence 7) the court's reluctance to recognize evidence

2.2 The police officers themselves are 1) those who lack knowledge and understanding of the crimes convicted on the Internet 2) those who are lacking in the requisite technical knowledge in investigating crimes committed on the Internet 3) those who do not possess the necessary expertise in inspecting, seizing and storing evidence. 4) those who lack sufficient knowledge and insight to apply, adapt and enforce the law 5) the lack of modern equipment to handle crime on the Internet 6) The total lack of financial support for the purposes of crime suppression on the Internet.

2.3 Problems in terms of administration and management arise from the following: 1) the lack of responsible police agencies for Internet crime 2) the lack of specially qualified police personnel 3) the lack of clearly stated parameter with regard to operations 4) the lack of interdisciplinary cooperation, between the work agencies involving in both the government and private sectors 5) the lack of support and campaigning for training and development in terms of upgrading the police's knowledge and capability 6) the top-brass's lack of interest and attention regarding the suppression of Internet crime.

2.4 Problems arising from the lack of cooperation include the following 1) many cases are of no interest to the public at large 2) in many cases, defendants prefer not to cooperate with the police 3) the victims in a lot of cases do not cooperate with the police 4) there is a lack of cooperation in

acquiring tip-offs 5) the lack of cooperation from Internet operators or Internet service providers (ISP).

3. Guidelines for solving the crime on the Internet can be divided into two stages as follows:

3.1 The short-term stage should adhere to the follow the guidelines 1) to train the police officers to accumulate sufficient knowledge and understanding in dealing with the investigation of criminal cases on the Internet 2) to adjust the existing investigative strategies in order to ensure that they conform to the need to combat the type of crime committed on the Internet 3) to adjust and apply the existing laws to ensure the effective protection against the crackdown on the Internet crime 4) to assign responsibility to designated organizations for investigating and screening the content of Internet-related crime 5) to encourage a commonality of interest with the private sector to facilitate cooperating with the police in order to protect against and suppress the Internet crime 6) to launch public relations campaign so as to inform the public of the things they should and should not do regarding crime on the Internet.

3.2 The long-term stage should adhere to the following guidelines: 1) to delineate clear-cut policies with regard to protecting against and suppressing crime that would facilitate the solving of problems on the Internet 2) to set up an organization specially empowered to deal with Internet crime 3) to recruit police officers who have knowledge of and expertise in the suppression of Internet crime 4) to initiate the measure to ensure the requisite academic development, operation of procedures and use of laws related to the

crackdown on Internet crime 5) to enhance the capability of the police in verifying computer crime which involves the use of forensic science 6) to delineate the requisite interdisciplinary strategies for cooperation with other domestic and international agencies that are involved in combatting the crime on the Internet 7) to lay down or create the necessary strategies to seek for the public's cooperation in protecting against and cracking down on crime convicted on the Internet.

4. Following are the expected benefits to the police operations if the use of the Internet in the police force is achieved:

4.1 It will be able to receive and distribute information to various police agencies via the electronic mail both rapidly and economically.

4.2 It will be able to publicize information regarding police operations or alert the public with regard to fraud through police web sites.

4.3 It will enable the police to study and research for the current and up-to-date information in order to enhance their experience and broaden their horizons.

4.4 It will enable the police to be informed about an act and complaints of web-related crime upon the public's requests.

4.5 It will be able to watch for and screen fraudulent behavior committed on the Internet.

4.6 The Police Internet will be used to pool information thereby replacing the former (POLIS).

4.7 It will introduce a new type of creative work within the police force, for example, clerical work, so as to reduce the steps involved in the working process, operational costs as well as to enhance the rapid response, accuracy and clarity in coordinating among other police agencies.