ĐẠI HỌC QUỐC GIA HÀ NỘI
KHOA LUẬT

TRẦN THỊ HỒNG LÊ

CÁC TỘI PHẠM TRONG LĨNH VỰC TIN HỌC THEO LUẬT HÌNH SỰ VIỆT NAM

LUẬN VĂN THẠC SĨ LUẬT HỌC

Hà Nội - 2009

ĐẠI HỌC QUỐC GIA HÀ NỘI
KHOA LUẬT

TRẦN THỊ HỒNG LÊ

CÁC TỘI PHẠM TRONG LĨNH VỰC TIN HỌC THEO LUẬT HÌNH SỰ VIỆT NAM

Chuyên ngành : Luật Hình sự

Mã số : 60 38 40

LUẬN VĂN THẠC SĨ LUẬT HỌC

Người hướng dẫn khoa học **: TSKH.PGS. LÊ VĂN CẢM**

Hà Nội - 2009

MỤC LỤC

BẢNG KÝ HIỆU VIẾT TẮT

BLHS	: Bộ luật Hình sự
TNHS	: Trách nhiệm hình sự
CNTT	: Công nghệ thông tin

ĐẶT VẤN ĐỀ

1. Tính cấp thiết của đề tài

Công nghệ thông tin (CNTT) - Thuật ngữ đã trở nên quen thuộc với loài người dù nó mới chỉ ra đời từ cuối thế kỷ XX. Ngành công nghệ đã này đưa chúng ta đến với một thời đại mới nơi mà trí tuệ máy móc được tạo ra để phục vụ con người. Những chiếc máy tính nhỏ bé thay cho bộ nhớ con người lưu trữ khối lượng thông tin, tri thức khổng lồ của nhân loại. Chúng có thể xử lý những phép toán, những công thức vô cùng phức tạp để thực hiện mục đích của chúng ta. Mạng máy tính liên kết con người ở khắp nơi trên thế giới, trợ giúp cho những giao lưu kinh tế, văn hóa, khoa học... bỏ qua mọi khoảng cách địa lý. Những ứng dụng của khoa học CNTT không dừng lại ở đó mà được phát triển, mở rộng từng ngày với tốc độ như vũ bão.

Sự ra đời, phát triển của CNTT với những thành tựu siêu việt của nó kéo theo sự xuất hiện một loại tội phạm mới - Tội phạm trong lĩnh vực tin học, còn được gọi là "tội phạm công nghệ cao", "tội phạm trong lĩnh vực CNTT" hay "tội phạm phi truyền thống". Đây là một loại tội phạm vô cùng nguy hiểm vì hậu quả của nó không chỉ dừng lại ở tác động tới một cá nhân, một tổ chức hay một ngành kinh tế, khoa học mà nó có khả năng gây hậu quả trực tiếp trên phạm vi toàn cầu. Trên các phương tiện thông tin hiện nay đang nóng bỏng lên đề tài về một vấn nạn: "Tin tặc". Các hệ thống máy tính, các trang web, mạng máy tính hiện nay thường xuyên bị xâm nhập, hủy hoại, gây rối loạn, đánh cắp thông tin...Việc khắc phục hậu quả của nó để lại những tổn thất chưa thể tính hết được. Phát hiện, xử lý tội phạm này hiện nay cũng là vấn đề nan giải do tội phạm có trình độ rất cao, thủ đoạn phạm tội là những ứng dụng khoa học công nghệ tinh vi và phức tạp. Hành vi phạm tội này diễn ra trong một môi trường phi vật chất

vì thế việc tìm kiếm dấu vết, chứng cứ phạm tội và bản thân tội phạm đòi hỏi những người làm công tác điều tra phải có trình độ chuyên môn cao trong lĩnh vực tin học.

Trên phương diện lý luận, mặc dù là một loại tội phạm nguy hiểm nhưng do mới xuất hiện nên tội phạm trong lĩnh vực tin học còn ít được quan tâm nghiên cứu dưới góc độ pháp lý. Về mặt khoa học thông tin, trên thế giới các nhà nghiên cứu đã tìm ra một số loại "vũ khí", công cụ tin học để chống lại tội phạm trong lĩnh vực tin học. Tuy nhiên, vấn đề bảo mật thông tin, đảm bảo an toàn, chuẩn xác cho hệ thống thông tin toàn cầu vẫn chưa có giải pháp thật sự hữu hiệu. Yêu cầu bức thiết của việc phòng chống tội phạm được đặt ra nhưng khoa học pháp lý nghiên cứu về lĩnh vực này hầu như còn bỏ ngỏ. Các công trình nghiên cứu có quy mô xứng đáng về tội phạm trong lĩnh vực tin học chưa được các nhà luật học tiến hành. Sự chú ý của các nhà lập pháp tới loại tội phạm nguy hiểm trên cũng còn ở mức độ ít ỏi. Có nhiều quốc gia trên thế giới chưa có luật chống tội phạm CNTT. Vì vậy tình trạng phát hiện người xâm hại các lợi ích của người khác, của cộng đồng trong lĩnh vực này nhưng không thể xử lý được không phải là hiếm. ở những quốc gia mà trình độ lập pháp cao hơn, theo kịp thực tiễn hơn thì tội phạm trong lĩnh vực CNTT đã có các quy phạm pháp luật điều chỉnh. Tuy nhiên, ngay cả ở những quốc gia này thì tình trạng không thể xử lý được tội phạm như ở trên cũng không thể tránh khỏi. Sở dĩ như vậy vì mặc dù đã có những quy định xử lý tội phạm nhưng những định đó chưa đầy đủ do bản chất pháp lý, đặc trưng, các yếu tố cấu thành của loại tội phạm mới này chưa được nghiên cứu một cách toàn diện. Đó là vấn đề cấp thiết đang đặt ra cho các nhà luật học nói chung và người nghiên cứu khoa học luật hình sự nói riêng.

Trên phương diện thực tiễn, tại Việt Nam, Bộ luật Hình sự 1999 là bộ

luật đầu tiên có quy định về tội phạm trong lĩnh vực CNTT nhưng trong 8 năm qua vẫn chưa có vụ xét xử về hình sự nào đối với những tội phạm trong lĩnh vực này dù nó đã, đang và tiếp tục xảy ra. Tình trạng đó xuất phát từ nhiều nguyên nhân nhưng chủ yếu là do các quy định của Bộ luật Hình sự về tội phạm này vẫn chưa được giải thích chính xác và thống nhất. Hơn nữa, những quy định của Bộ luật cũng không đầy đủ và xa rời thực tiễn.

Vì vậy, việc nghiên cứu sâu sắc hơn nữa để làm sáng tỏ về mặt khoa học những vấn đề bản chất pháp lý, đặc trưng, các yếu tố cấu thành của tội phạm trong lĩnh vực tin học và diễn biến, nguyên nhân, điều kiện của tội phạm này trong thực tiễn, đồng thời đưa ra những giải pháp hoàn thiện quy định của pháp luật hình sự trong lĩnh vực này không những có ý nghĩa *lý luận-thực tiễn* quan trọng, mà còn là vấn đề mang tính cấp thiết. Đây chính là lý do luận chứng cho việc tôi quyết định lựa chọn đề tài "*Các tội phạm trong lĩnh vực tin học theo Luật hình sự Việt Nam*" làm đề tài luận văn thạc sĩ luật học của mình.

2. Tình hình nghiên cứu

Tội phạm trong lĩnh vực tin học là loại tội phạm phi truyền thống, ra đời cùng với nền công nghệ cao và có khả năng gây hậu quả nguy hiểm cho xã hội không bị giới hạn về không gian. Vậy nên, các nước có nền khoa học công nghệ tiên tiến hiện nay đã dành sự quan tâm đáng kể đến việc xây dựng quy phạm pháp luật làm cơ sở đấu tranh chống tội phạm này, đặc biệt ở Liên minh châu Âu và Mỹ. Tuy nhiên, những văn bản pháp luật đã được xây dựng hầu như quy định chế tài ít nghiêm khắc đối với tội phạm trong lĩnh vực tin học hoặc điều chỉnh một phạm vi rộng, không phân biệt giữa tội phạm trong lĩnh vực tin học với các tội phạm truyền thống có liên quan đến tin học… Thậm chí, ở rất nhiều nơi trên

thế giới, pháp luật hình sự của nhà nước chưa hề có quy định về tội phạm trong lĩnh vực tin học.

Ở Việt Nam, tội phạm trong lĩnh vực tin học được quy định trong Bộ luật Hình sự 1999 với 3 điều luật (Điều 224, 225, 226) được đặt trong Chương XIX - Chương về các tội xâm phạm trật tự công cộng, an toàn công cộng. Tuy nhiên, đây mới chỉ là những quy định về một số hành vi trực tiếp tấn công dữ liệu máy tính, xâm hại trật tự an ninh CNTT chứ chưa đề cập tới hành vi sử dụng CNTT như công cụ phạm tội.

Cũng giống như phương diện *lập pháp*, trên phương diện *lý luận* tội phạm trong lĩnh vực tin học vẫn chưa được quan tâm một cách đúng mức mặc dù đây là một loại tội phạm nguy hiểm và rất khó đấu tranh. Cho đến nay, chưa có một công trình khoa học nào nghiên cứu một cách công phu và đầy đủ ở cấp độ một *luận văn thạc sĩ* hay một *luận án tiến sĩ* về đề tài này. Thậm chí, trong giới khoa học rất ít nghiên cứu có tính chuyên ngành của khoa học luật hình sự về tội phạm trong lĩnh vực tin học mà chủ yếu là các nghiên cứu ở phương diện kỹ thuật, công nghệ để phòng chống tội phạm này.

Hiện nay, công trình khoa học đáng chú ý nhất trong lĩnh vực này có thể kể đến sách chuyên khảo : *Tội phạm trong lĩnh vực CNTT* do TS Phạm Văn Lợi chủ biên (NXB Tư pháp - 2007).

Ngoài ra, tội phạm trong lĩnh vực tin học còn được đề cập trong một số giáo trình và sách tham khảo như: *1) Giáo trình luật Hình sự Việt Nam phần riêng* - NXB Đại học Quốc gia Hà Nội – 2003, TSKH. Lê Cảm (chủ biên). *2) Hoàn thiện pháp luật Hình sự Việt Nam trong giai đoạn xây dựng nhà nước pháp quyền*, NXB Công an nhân dân năm 1999 của TSKH.Lê Cảm . *3) Tội phạm học Việt Nam hiện đại và phòng ngừa tội phạm* – NXB Công An Nhân Dân –

2001 của PGS.TS Nguyễn Xuân Yêm. Hoặc được đề cập đến trong một số (rất hiếm) bài viết trên các tạp chí chuyên ngành.

Tuy nhiên, tất cả những nghiên cứu trên đây của các tác giả mới ở dưới dạng là các bài viết đăng trên tạp chí khoa học chuyên ngành, một phần, mục trong các giáo trình, sách chuyên khảo hay sách tham khảo, hoặc mới chỉ xem xét vấn đề ở cấp độ một khóa luận tốt nghiệp cử nhân luật học. Có nghĩa là cho đến nay trong khoa học Luật hình sự của Việt Nam chưa có công trình nghiên cứu nào đề cập riêng đến tội phạm trong lĩnh vực tin học một cách chuyên sâu. Đặc biệt, nhiều vấn đề lý luận và các quy đinh pháp luật thực định về tội phạm trong lĩnh vực tin học đòi phải được tiếp tục nghiên cứu một cách toàn diện, chuyên khảo và sâu sắc hơn.

3. Phạm vi nghiên cứu

Tội phạm trong lĩnh vực tin học là tội phạm của thế giới hiện đại, liên quan chặt chẽ đến công nghệ tin học, hành vi phạm tội thường diễn ra trong môi trường ảo, thủ đoạn phạm tội tinh vi, phức tạp, người phạm tội có trình độ cao. Bởi vậy, phạm vi nghiên cứu của luận văn chỉ xem xét và giải quyết một số vấn đề lý luận và thực tiễn cơ bản về tội phạm này, mà cụ thể là:

1) Khái niệm, sự ra đời của tội phạm trong lĩnh vực tin học;

2) Sự khác biệt của tội phạm trong lĩnh vực tin học so với các loại tội phạm truyền thống;

3) Phân loại tội phạm trong lĩnh vực tin học;

4) Phân tích các các dấu hiệu cấu thành của tội phạm trong lĩnh vực tin học;

5) Trách nhiệm pháp lý của tội phạm trong lĩnh vực tin học theo pháp luật Việt Nam

7) Trên cơ sở nghiên cứu trên, đưa ra các giải pháp hoàn thiện các quy

định của pháp luật hình sự Việt Nam về tội phạm trong lĩnh vực tin học.

4. Nhiệm vụ nghiên cứu

Với phạm vi nghiên cứu nêu trên trong luận văn này, tác giả tập trung vào giải quyết những nhiệm vụ chính như sau:

1) Xây dựng định nghĩa khoa học của khái niệm tội phạm trong lĩnh vực tin học

2) Nghiên cứu và phân tích các đặc điểm cơ bản của tội phạm trong lĩnh vực tin học để làm rõ sự khác biệt giữa tội phạm này với các tội phạm truyền thống

3) Phân tích trách nhiệm pháp lý của tội phạm trong lĩnh vực tin học được quy định của Bộ luật hình sự năm 1999 và các văn bản pháp luật khác. Từ đó phân tích một số những bất cập của hệ thống quy định này.

4) Luận chứng cho sự cần thiết phải hoàn thiện các quy định của pháp luật hình sự Việt Nam về tội phạm trong lĩnh vực tin học, đưa ra những phương hướng, giải pháp hoàn thiện quy định về tội phạm trong lĩnh vực tin học trong Bộ luật hình sự năm 1999

5. Cơ sở lý luận và phương pháp nghiên cứu

Để đạt được những mục đích đã đặt ra trên cơ sở lý luận là phép duy vật biện chứng và duy vật lịch sử, luận văn đã sử dụng một số phương pháp nghiên cứu như: phương pháp so sánh, phân tích tài liệu, phương pháp tổng hợp, cũng như những thành tựu của khoa học Luật hình sự, khoa học luật tố tụng hình sự, xã hội học pháp luật; v.v... trong các công trình của các nhà khoa học-luật gia ở trong và ngoài nước.

Ngoài ra, việc nghiên cứu đề tài còn dựa vào thông tin trên mạng Internet và các tạp chí chuyên ngành để phân tích và đánh giá, tổng hợp các tri thức khoa

học Luật hình sự.

6. Ý nghĩa lý luận, thực tiễn và điểm mới về khoa học của luận văn

Ý nghĩa lý luận và thực tiễn quan trọng của luận văn là ở chỗ tác giả đã làm rõ khái niệm, các đặc điểm cơ bản, dấu hiệu pháp lý của tội phạm trong lĩnh vực tin học; phân tích hệ thống quy định của pháp luật hiện hành về trách nhiệm pháp lý của tội phạm trong lĩnh vực tin học, đồng thời đưa ra các kiến nghị hoàn thiện các quy định này ở khía cạnh lập pháp và các giải pháp phối hợp đấu tranh phòng chống tội phạm trong lĩnh vực tin học trong thực tiễn.

Về điểm mới về khoa học của luận văn ở một chừng mực nhất định có thể khẳng định rằng, đây là nghiên cứu chuyên khảo đồng bộ đầu tiên ở cấp độ một luận văn thạc sĩ đề cập riêng đến tội phạm trong lĩnh vực tin học trong khoa học Luật hình sự Việt Nam. Điều đó càng trở nên quan trọng hơn vì đây là một loại tội phạm mới, thực tiễn ở Việt Nam đã diễn ra nhưng chưa xét xử được về hình sự một hành vi phạm tội nào. Ngoài ra, nó còn có ý nghĩa làm tài liệu tham khảo cần thiết cho các cán bộ nghiên cứu khoa học, cán bộ giảng dạy, nghiên cứu sinh, học viên cao học và sinh viên thuộc chuyên ngành Tư pháp hình sự.

7. Bố cục của Luận văn

Ngoài Phần mở đầu, Kết luận, Danh mục tài liệu tham khảo, Luận văn bao gồm ba chương với kết cấu như sau:

Chương 1: Một số vấn đề chung về tội phạm trong lĩnh vực tin học

Chương 2: Trách nhiệm pháp lý của tội phạm trong lĩnh vực tin học và thực tiễn xử lý

Chương 3: Vấn đề hoàn thiện quy định pháp luật hình sự về tội phạm trong lĩnh vực tin học và một số giải pháp phối hợp trong đấu tranh phòng chống tội phạm này

Nghiên cứu về tội phạm tin học đòi hỏi đồng thời kiến thức chuyên môn về CNTT, sự am hiểu khoa học pháp lý nói chung, khoa học luật hình sự nói riêng và khối lượng lớn thời gian, công sức nghiên cứu cả về mặt lý luận lẫn thực tiễn tội phạm. Do chưa thể đáp ứng đầy đủ những đòi hỏi đó nên luận văn không tránh khỏi những thiếu sót. Tác giả rất mong nhận được và xin chân thành cảm ơn các ý kiến phê bình, đóng góp của mọi độc giả quan tâm đến luận văn.

CHƯƠNG 1. MỘT SỐ VẤN ĐỀ CHUNG VỀ TỘI PHẠM TRONG LĨNH VỰC TIN HỌC

1.1. Khái quát về tội phạm trong lĩnh vực tin học

1.1.1. Ngành công nghệ thông tin và sự ra đời của tội phạm trong lĩnh vực tin học

Cuộc cách mạng vi tính hóa toàn cầu cuối thế kỷ XX mà trung tâm của nó là những chiếc máy tính kì diệu là một bước nhảy vọt vĩ đại của toàn thể nhân loại. Chính cuộc cách mạng này đã đưa con người đến với một nền công nghệ vượt trội: CNTT. Do tính siêu việt của nó mà CNTT được gọi tên bằng thuật ngữ "công nghệ cao".

Sau cuộc chiến tranh thế giới thứ hai, những chiếc máy tính sơ khai ra đời với kích thước khổng lồ và ở thời kì này chúng mới chỉ là những cỗ máy phục vụ chiến tranh và mục đích quân sự. Vào cuối những năm 70 của thế kỉ XX, những chiếc máy tính cá nhân (PC) nhỏ hơn và có tốc độ mạnh hơn đã chiếm được vị trí độc tôn. Một số công ty ở Châu Âu và Mỹ bắt đầu bước vào lĩnh vực sản xuất kinh doanh máy tính.

Những chiếc máy tính đã dần trở nên không thể thiếu được trong đời sống nhân loại. Và vi tính hóa – Cuộc cách mạng bùng nổ trên toàn cầu cuối thế kỷ 20 mở ra kỷ nguyên phát triển tột bậc của CNTT với sự ra đời của Internet.

Internet là một phương pháp ghép nối các mạng máy tính hiện hành, phát triển một cách rộng rãi tầm hoạt động của từng hệ thống thành viên. Mạng Internet nguyên thủy được thiết kế nhằm mục đích phục vụ việc cung cấp thông tin cho giới khoa học, nên công nghệ của nó cho phép mọi hệ thống đều có thể liên kết với nó thông qua một cổng điện tử. Theo cách đó, có hàng ngàn hệ máy tính hợp tác, cũng như nhiều hệ thống dịch vụ thư điện tử có thu phí, như MCI

và Compuserver, đã trở thành thành viên của Internet.

Sự ra đời của mạng diện rộng Internet như một công cụ toàn cầu, thư viện lưu trữ và trung tâm mua bán đã khiến các công ty viễn thông phút chốc trở nên vô cùng giàu có và có vai trò cực kỳ quan trọng. Internet đã vẽ nên viễn cảnh huy hoàng về một thế giới không bị chia cắt. Internet làm đảo lộn cuộc sống của nhân loại, cuốn hàng tỷ người sinh hoạt và làm việc theo những thói quen mới. Nó tạo điều kiện cho con người, nhưng cũng bắt con người phụ thuộc vào một thế lực vô hình [29].

Nền công nghệ mới đem lại rất nhiều lợi ích nhưng đi kèm với nó là những nguy cơ không nhỏ: sự xuất hiện một loại tội phạm phi truyền thống: tội phạm trong lĩnh vực tin học. Trước hết là vấn đề an ninh, độ tin cậy của thông tin trên Internet. Do dễ dàng trong thủ tục nối với Internet nên ai cũng có thể phát đi thông tin riêng của mình và cũng dễ dàng thực hiện việc sao chép các dữ liệu rồi lại phát đi dưới một tên khác, hoặc có một sự cải biên không đáng kể. Qua Internet, đã xảy ra nhiều vụ đánh cắp bí mật quốc gia, nhiều hoạt động tội phạm, gian lận, đầu cơ, tuyên truyền tài liệu phản động và văn hóa phẩm đồi trụy. Ví dụ như ở Mỹ, theo thống kê năm 2001 có khoảng 85% trang web của các tổ chức chính phủ, các tập đoàn kinh tế và tổ chức đoàn thể khác đã bị hacker tấn công. Theo báo cáo của Cục Điều tra Liên bang Mỹ (FBI) và ủy ban Bảo mật máy điện toán Mỹ (CSI), thiệt hại do các hacker (tội phạm tin học) này gây ra ít nhất 377 triệu USD. Tuy nhên đó mới chỉ là con số do 35% trong tổng số các tổ chức bị hacker xâm nhập công bố [40].

Việc tạo ra, lan truyền các virus trong hệ thống máy tính là một trong những hoạt động điển hình của tội phạm trong lĩnh vực tin học. Người dùng máy tính chỉ mới biết đến virus trong vài năm trở lại đây, nhưng thật ra, virus đã có từ

những năm 60. Các dạng hình sớm nhất chỉ là những chương trình thử nghiệm trong các cơ sở nghiên cứu. Vào cuối những năm 80, một số virus được "cho ra ràng". Đến nay, chúng ngày càng phát triển và luôn làm cho người sử dụng có cảm giác bị "tấn công" bất cứ lúc nào. Thiệt hại mà chúng mang tới là những con số không thể gọi là nhỏ. Đơn cử một vài vụ như năm 1999, virus Chernobyl xuất hiện, nó được phát tán trên mạng khiến ổ cứng và dữ liệu của các nạn nhân hoàn toàn không thể truy cập. Mặc dù ở Mỹ, nó chỉ tấn công một số ít máy, nhưng ở các nước khác, thành tích phá hoại của nó lại thật đáng nể. Tại Trung Quốc, thiệt hại vì Chernobyl lên tới hơn 291 triệu USD. Thổ Nhĩ Kỳ và Hàn Quốc cũng bị một phen điêu đứng. Năm 2000, virus LoveLetter (Bức thư tình) từ quê hương Phillippines đổ bộ sang châu Âu và Mỹ trong vòng 6 tiếng đồng hồ. Nó phá hoại từ 2,5 đến 3 triệu máy, gây thiệt hại ước tính 8,7 tỷ USD [35].

Mặc dù là một nước mới phát triển ngành CNTT nhưng hacker đã xuất hiện ở Việt Nam và thành lập các tổ chức. Cũng như các hacker trên thế giới, hacker Việt Nam có cả những chuyên gia phá hoại lẫn những người hoạt động vì sự đam mê và chỉ nhằm cảnh báo cho các nhà quản trị thông tin về những lỗ hổng bảo mật. Tất nhiên là một nghiên cứu về lĩnh vực hình sự nên đối tượng được đề cập đến ở đây là những kẻ chuyên xâm nhập bất hợp pháp, hoạt động phá hoại các trang web... Các hacker xuất hiện ở Việt Nam khoảng năm 1997-1998. Lúc đó hacker là những anh chàng chuyên sưu tầm virus trên mạng, đính kèm vào các email và gửi cho người khác. Những hacker này chủ yếu tập trung ở mạng "Trí tuệ Việt Nam" của FPT và một ít ở các mạng khác. Một thời gian sau đó những người thường xuyên lên mạng bắt đầu nắm bắt được một số kỹ thuật cơ bản về "bẻ khóa", virus. Họ bắt đầu nghĩ đến việc tụ hội, lập nhóm. Từ sau khi thành lập tổ chức, hacker Việt Nam đã học hỏi được nhiều kinh nghiệm từ

các hacker trình độ cao của hacker nước ngoài. Các tổ chức này công kích lẫn nhau đồng thời đẩy mạnh hacking để thể hiện mình. Hacker Việt Nam không chỉ gây ra một số vụ tấn công làm đau đầu các nhà quản trị mạng mà một số thành phần tiêu cực đã có những hoạt động ăn cắp thông tin tài khoản cá nhân, tổ chức để lấy tiền, sử dụng account trái phép...v.v [30]

1.1.2. Một số thuật ngữ chuyên ngành liên quan đến tội phạm trong lĩnh vực tin học

Tội phạm trong lĩnh vực tin học - như có tác giả đã nói là loại "tội phạm phi truyền thống"- là loại tội phạm mới xuất hiện với những biểu hiện đặc biệt khác với các loại tội phạm trước đó. Do vậy mà hiện nay vẫn chưa có khái niệm thống nhất về tội phạm này. Nó được gọi bằng nhiều cái tên khác nhau như: tội phạm tin học, tội phạm trong lĩnh vực CNTT, tội phạm công nghệ cao, tội phạm phi truyền thống, tội phạm Internet, tội phạm mạng...v.v.

Thậm chí, nhiều nơi trên thế giới những hành vi gây thiệt hại cho lợi ích của người khác thuộc lĩnh vực tin học vẫn chưa bị coi là tội phạm. Mặt khác, do đặc trưng của ngành công thông tin là công nghệ tri thức nên hành vi phạm tội cũng ở một trình độ khoa học cao, rất tinh vi, phức tạp. Để định nghĩa được thế nào là tội phạm trong lĩnh vực tin học buộc các nhà nghiên cứu phải hiểu được một số khái niệm chuyên môn về tin học có liên quan.

"1) Tin học (Informatics): Là ngành khoa học chuyên nghiên cứu về các vấn đề tổ chức, quản lý và xử lý thông tin bằng các công cụ tính toán hiện đại nhằm tạo ra thông tin có ích phục vụ con người.

2) CNTT (Information Technology): Là tập hợp các phương pháp khoa học, các phương tiện công cụ kỹ thuật hiện đại, chủ yếu là kỹ thuật máy tính và

viễn thông nhằm tổ chức khai thác và sử dụng có hiệu quả các nguồn tài nguyên thông tin phong phú, đầy tiềm năng trong mọi lĩnh vực hoạt động của con người và xã hội.

3) Máy vi tính (Computer): Mọi ứng dụng của ngành CNTT tập trung trên một thiết bị gọi là máy vi tính. Computer trong tiếng Anh có nghĩa là một máy có khả năng tuân theo các chỉ lệnh để thay đổi dữ liệu theo cách tùy theo yêu cầu, và để hoàn thành ít nhất vài ba thao tác trong các thao tác đó mà không cần sự can thiệp của con người. Máy tính được dùng để biểu diễn và xử lý văn bản, đồ họa, các ký hiệu, âm nhạc cũng như các con số.

4) Cơ sở dữ liệu (Database): là tập hợp các thông tin dữ liệu về một đối tượng như hoạt động của một tổ chức, doanh nghiệp... được tổ chức và lưu giữ trên máy tính sao cho dễ dàng truy nhập, khai thác, quản lý và cập nhật.

5) Internet: Bước ngoặt lịch sử của ngành CNTT là sự ra đời của Internet - mạng thông tin toàn cầu. Internet là một hệ thống gồm các mạng máy tính được liên kết với nhau trên phạm vi toàn thế giới, tạo điều kiện thuận lợi cho các dịch vụ truyền thông dữ liệu, như đăng nhập từ xa, truyền các tệp tin, thư tín điện tử, và các nhóm thông tin. Đây là môi trường hoạt động chủ yếu của tội phạm tin học và cũng là nơi tạo điều kiện cho hậu quả của những hành vi đó có khả năng tác động trên một quy mô rất lớn" [26].

6) Trang thông tin điện tử (Website): là trang thông tin hoặc một tập hợp trang thông tin trên môi trường mạng phục vụ cho việc cung cấp, trao đổi thông tin [4].

7. Virus, chương trình virus: Bên cạnh các hành vi xâm nhập, đánh cắp, thay đổi, di chuyển dữ liệu trong hệ thống máy tính thì việc tạo ra các loại virus để phá hoại dữ liệu cũng là một loại hành vi phổ biến và gây hậu quả nghiêm

trọng. Thuật ngữ "virus máy tính" được phát minh năm 1983 trong một công trình nghiên cứu do nhà nghiên cứu virus Fred Dohen tiên hành. Virus là một chương trình máy tính được thiết kế dưới dạng một trò chơi khăm, hoặc một sự phá hoại ngầm, có thể tự lây lan bằng cách gắn vào các chương trình khác và tiến hành các thao tác vô ích, vô nghĩa, đôi khi là thao tác phá hoại. Khi một virus nhiễm vào đĩa, nó tự lây lan bằng cách gắn vào các chương trình khác trong hệ thống, kể cả phần mềm hệ thống. Giống như virus ở người, tác hại của virus máy tính có thể chưa phát hiện được trong thời gian vài ngày hay vài tuần. Trong thời gian đó mọi đĩa đưa vào hệ thống máy tính đều mang theo một bản sao ấn của virus đó – các đĩa này đều bị nhiễm virus.

Virus được định nghĩa như sau: "Virus máy tính là các chương trình máy tính (đoạn mã) rất nhỏ, các chương trình này hoạt động bằng cách tự phân thân, tự sao chép chính nó lên các đĩa, các file khác và cứ thế tiếp tục quá trình nhân rộng này" [22, tr.7].

Hoặc: "Virus là chương trình vốn lây nhiễm các tệp máy tính (thường là những chương trình khả thi khác) bằng cách chèn vào những tệp đó những bản sao của bản thân nó. Điều này được thực hiện theo cách mà các bản sao sẽ được tạo ra khi tệp được nạp vào bộ nhớ cho phép chúng nhiễm thêm vào các tệp khác nữa..." [27, tr.1081].

Luật CNTT năm 2006 của Việt Nam định nghĩa: "Vi rút máy tính là chương trình máy tính có khả năng lây lan, gây ra hoạt động không bình thường cho thiết bị số hoặc sao chép, sửa đổi, xóa bỏ thông tin lưu trữ trong thiết bị số".

Khi virus phát tác, chúng gây ra nhiều hậu quả: từ những thông báo mang thông tin xấu đến những tác động làm lệch lạc khả năng thực hiện của phần mềm hệ thống, hoặc xóa sạch mọi thông tin trên đĩa cứng. Các nhà quản trị mạng,

những người sử dụng máy tính trên thế giới đã từng đau đầu khi phải đối mặt với nhiều loại virus nguy hiểm như: Loves, Nimda, Code Red, Kournicova, Blaster, Slamer, Bugbear, Sobig...

8. Tấn công từ chối dịch vụ (DOS): DOS là từ viết tắt của Deny Of Service attack - Tấn công từ chối dịch vụ. Theo lý thuyết, các dịch vụ web trên Internet đều có một giới hạn về khả năng cung cấp dịch vụ cho người truy cập. Nếu một trang web bị gửi tới số lượng yêu cầu truy cập vượt quá giới hạn có thể đáp ứng, thì dịch vụ web sẽ bị tê liệt, không thể trả lời cho các yêu cầu truy cập hợp lệ của người sử dụng bình thường.

9. Tấn công từ chối dịch vụ phân tán (DDOS): DDOS là từ viết tắt của Distributed Deny Of Service attack - Tấn công từ chối dịch vụ phân tán. Tương tự với tấn công DOS, nhưng nguồn gửi không đến từ một máy tính trên Internet, mà từ một hệ thống nhiều máy tính với vô số địa chỉ IP khác nhau. Việc ngăn chặn DDOS khó khăn hơn nhiều so với DOS [41].

1.2. Khái niệm, đặc điểm và phân loại tội phạm trong lĩnh vực tin học

1.2.1. Khái niệm, đặc điểm của tội phạm trong lĩnh vực tin học

1.2.1.1. Khái niệm tội phạm trong lĩnh vực tin học

Trong khoa học kỹ thuật, tội phạm trong lĩnh vực tin học được nói đến bằng một số thuật ngữ:

- Cracker: Người chủ tâm đánh cắp thông tin mật bằng cách đột nhập vào các hệ thống máy tính. Hành vi bẻ khóa là hành động áp dụng một số thủ đoạn tinh vi hòng phát hiện những lỗ hổng bảo mật trong hệ thống máy tính.

- Data Diddling (Lừa đảo tín dụng): Là hành vi thông thường nhất, dễ

nhất, an toàn nhất liên quan đến việc thay đổi dữ liệu sẽ đưa vào máy tính hoặc có trong máy tính.

- Harker (Tin tặc): Có thể nói nguyên nghĩa của từ hacker không xấu. Điều đó được lý giải thích bởi thuật ngữ hacker ethic. Thuật ngữ này chỉ các nguyên lý đạo đức đã được phổ biến rộng rãi trong cộng đồng hacker thế hệ đầu tiên (giai đoạn 1965 – 1982). Phù hợp với các đạo lý hacker đó, tất cả các thông tin kỹ thuật, về nguyên tắc, sẽ phải được dùng cho mọi người, cho nên không bao giờ được phép làm trái đạo đức cố thâm nhập vào một hệ thống máy tính để thăm dò và tìm hiểu. Tuy vậy, luôn có những kẻ vô đạo đức, họ phá hoại, thay đổi hoặc di chuyển các dữ liệu nhằm gây tổn thất cho người khác. Với nhiều quốc gia, những hành động như vậy là phạm pháp. Và cũng vì vậy mà hacker hay cracker mang một nghĩa mặt trái: tội phạm tin học

Hiện nay, hacker được giới CNTT phân loại thành ba trường phái chính:

+ Hacker "mũ trắng" (white hat hacker) là những hacker có thiện chí - những người giúp xây dựng hệ thống chứ không phải phá hoại. Những hành vi của họ chỉ để nhằm cảnh báo nhà quản trị mạng về an ninh thông tin.

+ Hacker "mũ đen" (black hat hacker hay còn gọi là cracker): là các hacker hành động vì mục đích xấu hay để trục lợi.

+ Hacker "mũ nâu" (hoặc mũ xám) là trung gian giữa hai loại hacker trên. Các hacker này hoại động chủ yếu vì mục đích danh tiếng và... giải trí! [56]

- Phreaker (Kẻ bẻ khóa điện thoại): Người áp dụng các kỹ thuật bẻ khóa các hệ thống điện thoại để gọi đường dài miễn phí qua Internet.

- Script Kiddies (Kẻ đánh cắp chương trình): Là người chỉ biết áp dụng các công cụ, chương trình bẻ khóa do người khác tạo ra để xâm nhập vào các hệ

thống, họ hoàn toàn chưa biết hoặc biết ít về các kỹ thuật này.

- Sneaker (Kẻ lén lút): Là người được thuê làm công việc trắc nghiệm mức độ bảo mật của một hệ thống đã được bảo mật.

Trong số những thuật ngữ này thì Hacker - Tin tặc là thuật ngữ được biết đến một cách rộng rãi nhất. Hầu như tất cả những bản tin, bài viết, nghiên cứu khoa học về tội phạm trong lĩnh vực tin học đều đề cập đến thuật ngữ này. Như đã nêu trên, Hacker, là thuật ngữ chuyên ngành chỉ loại người say mê, yêu thích máy tính, nhưng để đùa nghịch, họ cố phá những hệ thống bảo vệ máy tính bằng cách tìm mọi biện pháp để đột nhập vào những hệ thống đó. Nhiều người trong họ hoạt động chỉ với mục đích phơi bày những vết nứt và những sơ hở trong sự bảo vệ của hệ máy tính mà bọn tội phạm có thể sẽ lợi dụng khai thác.

Như vậy, *trong khoa học kỹ thuật tội phạm trong lĩnh vực tin học được hiểu là loại tội phạm chuyên tấn công vào trật tự, an ninh CNTT. Hay nói cách khác đó là loại tội phạm có khách thể xâm hại là hoạt động CNTT.*

Trong khoa học pháp lý, tuy là một loại tội phạm mới, chưa được quan tâm nghiên cứu nhiều nhưng hiện nay các nhà luật học cũng đã có một số cách hiểu khác nhau về tội phạm trong lĩnh vực tin học. Tình hình đó được phản ánh trong đánh giá của PGS.TS Nguyễn Xuân Yêm: "Tội phạm công nghệ cao (The high - tech offender) là một loại tội phạm mới, đã và đang gây ra những thiệt hại nghiêm trọng cho nền kinh tế, an ninh, quốc phòng ở nhiều nước trên thế giới. Trong lĩnh vực tội phạm sử dụng công nghệ cao, các nhà tội phạm học thế giới đã đưa ra nhiều khái niệm như: tội phạm máy tính, virus máy tính, tội phạm lợi dụng máy tính, tội phạm lợi dụng internet, lạm dụng máy tính, hacker (đột nhập)..." [24, tr.506].

Cũng theo PGS.TS Nguyễn Xuân Yêm, khái niệm sau được thừa nhận bởi đa số các nhà tội phạm học trên thế giới: *"Tội phạm máy tính là các hành vi tác động trực tiếp hoặc gián tiếp vào sự hoạt động của máy tính, mạng máy tính, các thiết bị ngoại vi, các cơ sở dữ liệu, các quá trình điều khiển dựa trên sự hoạt động của các thiết bị tin học nhằm mục đích phá hoại, lừa đảo, che dấu, đánh cắp thông tin; các hành vi lạm dụng máy tính, mạng máy tính để tiến hành những hoạt động gây nguy hại cho xã hội"* [24, tr.507].

Nghiên cứu khái niệm này cho thấy tồn tại hai vấn đề không hợp lý. Thứ nhất, khái niệm trên có tính liệt kê, mô tả các dạng hành vi của tội phạm tin học mà những hành vi phạm tội trong lĩnh vực CNTT vô cùng đa dạng. Vì vậy, một khái niệm mang tính liệt kê sẽ không thể đảm bảo là chứa đựng được toàn bộ những hành vi đó. Hơn nữa việc liệt kê các dạng hành vi sẽ luôn phải bổ sung để theo kịp tình trạng phạm tội trong thực tế.

Vấn đề thứ hai, khái niệm trên cho rằng tội phạm máy tính bao gồm tất cả những tội phạm liên quan đến máy vi tính: "các hành vi lạm dụng máy tính, mạng máy tính để tiến hành những hoạt động gây nguy hại cho xã hội". Mọi loại tội phạm được thực hiện qua máy vi tính đều được gọi là tội phạm máy tính. Nếu nhìn nhận như vậy thì giết người với sự trợ giúp của máy tính cũng coi là tội phạm máy tính.

Như vậy, *khác với quan niệm của khoa học kỹ thuật, các nhà khoa học pháp lý thống nhất với khái niệm được trích dẫn ở đây hiểu về tội phạm trong lĩnh vực tin học rất rộng. Theo đó tội phạm trong lĩnh vực tin học không chỉ là những hành vi trực tiếp tấn công trật tự, an ninh CNTT mà còn bao gồm tất cả những hành vi sử dụng CNTT để phạm tội. Nói cách khác, theo quan điểm này, tội phạm trong lĩnh vực tin học bao gồm cả loại tội phạm có khách thể là hoạt*

động CNTT và loại tội phạm sử dụng CNTT làm môi trường, phương tiện phạm tội.

Cũng tương tự với quan điểm đó, các tác giả của cuốn sách chuyên khảo "Tội phạm trong lĩnh vực CNTT" cho rằng: "*Tội phạm trong lĩnh vực CNTT (hay còn gọi là tội phạm mạng, tội phạm máy tính hay tội phạm liên quan đến máy tính…) có thể xác định là hành vi bị coi là tội phạm có liên quan đến lĩnh vực CNTT"* [23, tr.19].

Quan điểm này xác định khái niệm tội phạm trong lĩnh vực CNTT với một nội hàm rất rộng. Bất kỳ một hành vi phạm tội nào có liên quan đến CNTT đều là tội phạm trong lĩnh vực CNTT. Tức là chỉ cần có yếu tố CNTT xuất hiện trong bất kỳ dấu hiệu nào, giai đoạn nào của tội phạm thì tôi phạm đó là tội phạm trong lĩnh vực CNTT. Ví dụ như gửi thư tống tiền bằng email cũng là tội phạm trong lĩnh vực tin học (vì có liên quan đến CNTT). Hay một băng cướp lên kế hoạch và hẹn thời gian, địa điểm đi cướp bằng cách nhắn tin với nhau qua mạng Internet cũng được coi là tội phạm trong lĩnh vực CNTT…

Trong pháp luật thực định, Bộ luật Hình sự Việt Nam năm 1999 đã quy định một số điều về tội phạm liên quan đến máy vi tính (Điều 224, 225, 226) nhưng không đưa ra định nghĩa pháp lý về loại tội phạm này. Và có thể nói rằng các nhà lập pháp Việt Nam coi đây là một dạng hành vi xâm phạm trật tự công cộng, an toàn công cộng khi đặt ba điều luật này trong Chương XIX – Chương về các tội xâm phạm trật tự công cộng, an toàn công cộng. Tuy nhiên, suy luận từ các tội danh được quy định tại đây cũng có thể thấy quan điểm của các nhà lập pháp hình sự Việt Nam về các tội phạm trong lĩnh vực tin học.

Điều 224, 225, 226 Bộ luật Hình sự năm 1999 quy định về các tội phạm: Tội tạo ra và lan truyền, phát tán các chương trình vi rút tin học; Tội vi phạm các

quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử; Tội sử dụng trái phép thông tin trên mạng và trong máy tính. Các hành vi thuộc mặt khách quan của ba tội phạm này đều là các hành vi trực tiếp xâm hại an ninh CNTT. Ngoài ba Điều luật này, Bộ luật Hình sự năm 1999 không còn bất cứ quy định nào khác về các tội phạm trong lĩnh vực tin học. *Qua đó có thể thấy được là các nhà lập pháp khi xây dựng Bộ luật hình sự năm 1999 đã cho rằng tội phạm trong lĩnh vực tin học chỉ bao gồm các tội phạm có khách thể bị xâm hại là trật tự, an ninh CNTT.*

Những phân tích trên cho thấy hiện nay chưa có một cách hiểu đầy đủ và thống nhất về tội phạm trong lĩnh vực tin học. Mặc dù hầu hết mọi người có thể hiểu một cách đơn giản tội phạm trong lĩnh vực tin học là những hành vi xâm phạm trật tự an ninh thông tin trong máy tính, hệ thống mạng máy tính hoặc lợi dụng CNTT để xâm phạm quyền và lợi ích hợp pháp của cá nhân, tổ chức khác. Tuy nhiên, khi đưa ra một khái niệm chung về loại tội phạm này thì các nhà khoa học có nhiều điểm bất đồng và khiếm khuyết. Có thể khái quát tình hình nhận thức về loại tội phạm này hiện nay là có ba nhóm quan điểm chính:

Quan điểm thứ nhất: Tội phạm trong lĩnh vực tin học chỉ bao gồm các hành vi xâm hại trật tự, an ninh CNTT.

Quan điểm thứ hai: Tội phạm trong lĩnh vực tin học bao gồm các hành vi xâm hại trật tự, an ninh CNTT và các hành vi sử dụng CNTT gây nguy hại cho xã hội.

Quan điểm thứ ba: Tội phạm trong lĩnh vực tin học là bất cứ hành vi phạm tội nào có liên quan đến CNTT.

Nhóm quan điểm thứ nhất đề cập đến những hành vi phạm tội mà giới kỹ thuật vẫn gọi là tin tặc, hacker hay chính xác là tội phạm tin học. Thực chất, tội

phạm tin học chỉ là một dạng của các tội phạm trong lĩnh vực tin học. Hơn nữa, trong thực tế hành vi phạm tội đơn thuần chỉ nhằm tấn công trật tự, an ninh CNTT không nhiều, tính nguy hại nói chung không cao bằng các dạng khác của tội phạm trong lĩnh vực tin học.

Ngược lại, quan điểm thứ ba lại cho khái niệm tội phạm trong lĩnh vực tin học một nội hàm quá rộng. Chỉ cần yếu tố CNTT có mặt trong bất kỳ yếu tố nào của tội phạm thì tội phạm đó được coi là tội phạm trong lĩnh vực tin học. Nếu như vậy, trong thời đại thông tin hóa hiện nay khi mà hoạt động của con người ngày càng phụ thuộc chặt chẽ vào các ứng dụng CNTT thì hầu hết các loại tội phạm đều được coi là tội phạm trong lĩnh vực CNTT. Điều này có lẽ không thể được các chuyên gia luật hình sự chấp nhận.

Quan điểm thứ hai có tính thuyết phục cao nhất tuy nhiên cũng chưa hoàn toàn chính xác. Các hành vi phạm tội xâm hại trật tự, an ninh CNTT tất nhiên là tội phạm trong lĩnh vực tin học. Tuy nhiên, không phải bất kỳ hành vi sử dụng CNTT gây nguy hại cho xã hội nào cũng đều là tội phạm trong lĩnh vực tin học. Có những tội phạm mà yếu tố sử dụng CNTT không phải là yếu tố cơ bản. Ví dụ như trường hợp A gửi email tống tiền B về những thông tin cá nhân mà B không muốn tiết lộ. Đây là một tội phạm truyền thống và để thực hiện được tội phạm trong trường hợp này cũng không nhất thiết phải sử dụng CNTT (mà có thể gửi thư qua đường bưu điện chẳng hạn). Vì vậy, nếu không xác định phạm vi một cách rõ ràng thì quan điểm này cũng rơi vào sự bất cập giống quan điểm thứ ba - Cứ liên quan đến yếu tố CNTT sẽ coi là tội phạm trong lĩnh vực tin học.

Tóm lại, để đưa ra khái niệm tội phạm trong lĩnh vực tin học cần phải hiểu rõ hai vấn đề: Thứ nhất, tội phạm trong lĩnh vực tin học là một loại tội phạm, nó mang đầy đủ các dấu hiệu của tội phạm thông thường. Thứ hai, đặc điểm để

phân biệt nó với các loại tội phạm khác là nó gắn bó chặt chẽ với CNTT. Cho dù CNTT có thể đóng những vai trò khác nhau đối với loại tội phạm này nhưng nếu không có yếu tố CNTT thì nó không thể được thực hiện. Do đó, khái niệm tội phạm trong lĩnh vực tin học cũng phải được xây dựng trên cơ sở khái niệm chung về tội phạm kết hợp với đặc trưng của loại tội phạm này.

Từ định nghĩa tội phạm được quy định tại Điều 8 Bộ luật Hình sự năm 1999 có thể hiểu: Tội phạm là hành vi nguy hiểm cho xã hội được quy định tại Bộ luật Hình sự, do người có năng lực trách nhiệm hình sự thực hiện một cách cố ý hoặc vô ý, xâm phạm các quan hệ xã hội được luật hình sự bảo vệ.

Trên cơ sở đó có thể đưa khái niệm tội phạm trong lĩnh vực tin học như sau như sau: ***Tội phạm trong lĩnh vực tin học là những hành vi nguy hiểm cho xã hội được quy định tại BLHS , do người có năng lực TNHS cố ý hoặc vô ý thực hiện bằng cách sử dụng CNTT nhằm xâm phạm trật tự an ninh thông tin trong máy tính, hệ thống mạng máy tính; xâm phạm các quyền lợi ích hợp pháp của cá nhân, tổ chức.***

1.2.1.2. Đặc điểm của tội phạm trong lĩnh vực tin học

Được gọi là tội phạm phi truyền thống, tội phạm trong lĩnh vực tin học có những đặc điểm rất khác biệt so với những tội phạm đã xuất hiện trong lịch sử:

Thứ nhất, tội phạm trong lĩnh vực tin học gắn bó chặt chẽ với yếu tố CNTT. Tội phạm này chỉ được thực hiện nhờ việc lợi dụng kỹ thuật công nghệ tin học vào mục đích phạm tội. Thủ đoạn phạm tội đặc biệt tinh vi do ứng dụng công nghệ tiên tiến nhất.

Thứ hai, do gắn bó chặt chẽ với CNTT, phương tiện phạm tội là các ứng dụng CNTT nên chủ thể của tội phạm này luôn là những người có trình độ

chuyên môn cao về tin học, kỹ năng về máy tính, mạng máy tính.

Thứ ba, tội phạm trong lĩnh vực tin học không diễn ra trong môi trường vật chất xung quanh con người mà diễn ra trong một môi trường ảo - mạng máy tính. Một tội phạm có thể ngồi trước một chiếc máy tính ở Việt Nam và tấn công vào các mục tiêu trên toàn thế giới. Mọi quốc gia đều phải đối mặt với tội phạm trong lĩnh vực tin học từ bất kỳ một nơi nào trên trái đất. Vì vậy, tội phạm trong lĩnh vực tin học không có biên giới để kiểm soát, điều tra, đấu tranh. Xử lý tội phạm trong lĩnh vực tin học cũng dễ vấp phải khó khăn trong phân định thẩm quyền tài phán.

Thứ tư, tội phạm trong lĩnh vực tin học có thể gây nguy hại đến mọi lĩnh vực của đời sống vì CNTT hiện nay đã được áp dụng vào hầu hết các lĩnh vực đó. Sự phát triển của xã hội ngày càng phụ thuộc nhiều vào sự phát triển của các thế hệ máy tính và phương tiện kỹ thuật thì nguy cơ bị tội phạm trong lĩnh vực tin học đe dọa lại càng lớn hơn.

Thứ năm, do có phạm vi lãnh thổ, lĩnh vực, đối tượng tác động rất lớn như vậy nên tội phạm trong lĩnh vực tin học rất khó phân định với các loại tội phạm khác. Có nhiều trường hợp không thể phân biệt được là tội phạm kinh tế, tội phạm xâm phạm an ninh quốc gia, tội phạm xâm phạm quyền sở hữu...v.v hay tội phạm trong lĩnh vực tin học... Vì vậy, hiện nay trong khoa học tồn tại nhiều cách hiểu khác nhau về tội phạm trong lĩnh vực tin học (như đã phân tích trong phần 1.2.1.1).

1.2.2. Phân loại tội phạm trong lĩnh vực tin học

Phân loại tội phạm là xắp xếp các hành vi phạm tội thành những nhóm khác nhau theo những tiêu chí nhất định. Việc phân loại tội phạm có ý nghĩa rất

quan trọng vì việc phân loại tội phạm được tiến hành theo một tiêu chí phù hợp sẽ giúp cho những nhà lập pháp xây dựng được những chế định pháp luật có tính logic cao. Và quan trọng hơn nữa là ý nghĩa trong việc nhận biết, xây dựng các biện pháp đấu tranh phòng chống hiệu quả với các nhóm hành vi phạm tội khác nhau.

Do còn tồn tại nhiều quan điểm khác nhau về tội phạm trong lĩnh vực tin học nên hiện nay có nhiều cách phân loại tội phạm này. Một cách phân loại được sử dụng phổ biến là cách phân loại của hai nhà Tội phạm học Mỹ Catherine H.Conly và J.Thomas Mc Ewen công bố năm 1990. Theo các nhà khoa học này, "tội phạm máy tính" được chia thành năm dạng:

- Các tội xâm phạm nội tạng máy tính (Internal Computer Crimes):
    + Tác động nội ứng (Trojian horses)
    + Làm biến dạng dữ liệu (Logic bombs)
    + Làm sập cửa (Trap doors)
    + Vi rút máy tính (Virus)
- Các tội phạm viễn thông (Telecommunications Crimes):
    + Lừa đảo trên dịch vụ của hệ thống điện thoại (Phone Phreaking)
    + Đột nhập (Hacking)
    + Hệ thống bảng tin bất hợp pháp (Illegal bulletin board)
    + Sử dụng sai mục đích hệ thống điện thoại (Misuse of telephone systems)
- Các tội phạm tác động lên máy tính (Computer Manipulation Crimes):
    + Tham ô (Embezzlement)
    + Lừa đảo (Frauds)
    + Các tội liên quan tới hỗ trợ kinh doanh bất hợp pháp (Support of

Criminal Enterprises)

+ Các dữ liệu hỗ trợ buôn bán ma túy (Databases to support drug distributions)

+ Các dữ liệu hỗ trợ cho vay nặng lãi (Databases to support loan shorking)

+ Các dữ liệu hỗ trợ cho đánh bạc bất hợp pháp (Databases to support illegal gambling)

+ Các dữ liệu lưu dữ số khách hàng kinh doanh bất hợp pháp (Databases to keep records of illegal client transactions)

+ Tẩy rửa tiền (Money laundring)

- Các tội phạm trộm cắp phần cứng, phần mềm máy tính (Hardware, Software Thefts)

+ Cướp phần mềm (Software piracy)

+ Trộm cắp máy tính (theft of computer)

+ Trộm mã nhị phân vi mạch (Theft of microprocessor chips)

+ Đánh cắp bí mật thương mại (Theft of trade secrets)[14]

Xét về tiêu chí, cách phân loại trên tương đối rành mạch. Tuy nhiên, trong đó có một số loại tội phạm mặc dù có liên quan đến máy tính nhưng không thể hiện bản chất của tội phạm đang được đề cập nên việc đưa vào bảng phân loại là không cần thiết, chẳng hạn như: Tội trộm cắp máy tính, Tội tham ô, Tôi lừa đảo (liên quan đến máy tính)... Những tội này thực chất là những tội có tính chất truyền thống đã được các đạo luật về hình sự quy định. Sự xuất hiện của máy tính với tư cách là khách thể của tội phạm không làm thay đổi bản chất của chúng, chúng vẫn là những tội trộm cắp, tham ô lừa đảo chứ không thể định tội danh khác được. Hơn nữa, trong hệ thống phân loại này còn đề cập đến những

khái niệm không phải là tội danh. Ví dụ như: Các dữ liệu hỗ trợ buôn bán ma túy, các dữ liệu hỗ trợ cho vay nặng lãi, các dữ liệu hỗ trợ cho đánh bạc bất hợp pháp, các dữ liệu lưu dữ số khách hàng kinh doanh bất hợp pháp… Đây là các công cụ, phương tiện dùng để phạm tội chứ không phải tội phạm trong lĩnh vực tin học.

Trong sách tham khảo "Tội phạm học hiện đại và pòng ngừa tội phạm", PGS. TS Nguyễn Xuân Yêm đưa ra một cách phân loại khác về tội phạm trong lĩnh vực tin học. Ông sử dụng khái niệm tội phạm trong lĩnh vực tin học và chia tội phạm trong lĩnh vực tin học thành ba nhóm:

a. Các tội phạm máy tính

b. Các tội liên quan đến ngân hàng dấu vết di truyền

c. Các tội phạm đột nhập máy tính.

Ở nhóm a, tác giả Nguyễn Xuân Yêm đã đưa ra rất nhiều dạng hành vi khác nhau về tội phạm máy tính (như: truy nhập bất hợp pháp, làm biến dạng, sai lệch dữ liệu, lừa đảo trên các hệ thống máy tính…). Còn về nhóm b, tác giả gọi tên là các tội phạm liên quan đến ngân hàng dấu vết di truyền nhưng thực chất lại giải thích một phương pháp điều tra, khám phá tội phạm dựa trên dấu vết di truyền. Nhóm c - nhóm được tác giả gọi là các tội đột nhập máy tính - xét về bản chất có thể đưa vào nhóm a (các tội phạm máy tính) [24, tr.510-513].

Như vậy, mặc dù phân loại dựa trên khái niệm tội phạm công nghệ cao theo nghĩa bao gồm các loại công nghệ hiện đại nhưng thực chất các tội phạm được tác giả Nguyễn Xuân Yêm phân loại chỉ bao gồm tội phạm công nghệ máy tính, công nghệ tin học. Bản thân cách phân loại của tác giả lại không dựa trên tiêu chí thống nhất (nhóm a được xác định trên cơ sở mặt khách quan của tội phạm; nhóm b lại xác định trên cơ sở phương pháp điều tra, khám phá tội phạm;

nhóm c được xác định bằng khách thể của tội phạm)

Như đã đề cập ở trên, phân loại tội phạm là xắp xếp các hành vi phạm tội thành những nhóm khác nhau theo những tiêu chí nhất định. Vậy nên, để có cách phân loại logic cần xác định được tiêu chí phù hợp. *"Tiêu chí là các đặc trưng, dấu hiệu làm cơ sở, căn cứ để nhận biết, sắp xếp các sự vật, các khái niệm"* [25, tr.1580]

Xem xét các dấu hiệu của tội phạm trong lĩnh vực tin học cho thấy: về mặt khách quan, hành vi phạm tội có liên quan chặt chẽ đến việc ứng dụng CNTT và các thiết bị tin học. Đó là đặc điểm chung của loại tội phạm này. Vì thế không thể dùng mặt khách quan làm tiêu chí phân loại các hành vi phạm tội trong lĩnh vực này. Về mặt chủ quan, các tội phạm trong lĩnh vực tin học hầu hết được biểu hiện dưới hình thức lỗi cố ý. Do đó mặt chủ quan không phải là một tiêu chí thích hợp để phàn loại. Chủ thể của các tội phạm trong lĩnh vực tin học là những người có trình độ chuyên môn cao về tin học, tuy nhiên đó cũng là dấu hiệu chung của loại tội phạm này chứ không phải là một đặc trưng của riêng nhóm nào để có thể dùng làm tiêu chí phân loại. Chỉ còn lại dấu hiệu khách thể là có khả năng trở thành một tiêu chí phân loại phù hợp. Cùng bằng hành vi về mặt khách quan liên quan tới các ứng dụng tin học nhưng các tội phạm trong lĩnh vực tin học khác nhau xâm phạm đến các khách thể khác nhau. Hơn nữa, phân loại bằng dấu hiệu khách thể của tội phạm cũng phù hợp với logic chung của cả BLHS hiện hành.

Căn cứ trên khách thể bị tội phạm xâm hại, tội phạm trong lĩnh vực tin học được chia thành hai nhóm:

- **Nhóm I:** Các tội xâm phạm trật tự, an ninh thông tin trong hệ thống máy tính, mạng máy tính.

Nhóm I có thể gọi là các tội phạm máy tính hoặc tội phạm tin học. Khách thể của nhưng tội phạm này là trật tự, an ninh trong lĩnh vực CNTT. Trật tự, an toàn trong lĩnh vực CNTT được coi là điều kiện đảm bảo cho mọi hoạt động trong lĩnh vực này diễn ra bình thường. Xâm phạm vào trật tự, an toàn trong lĩnh vực CNTT là xâm phạm vào các quy định pháp luật, quy tắc xử sự trong ngành, làm đảo lộn, sai lệch, phá hoại các hoạt động về CNTT. Nhóm này bao gồm những hành vi như:

1. Tạo ra, lan truyền và phát tán các virus máy tính

2. Sao chép, lấy cắp, sử dụng trái phép thông tin trên mạng và trong máy vi tính

3. Phá hủy, làm hư hỏng hoặc thay đổi các dữ liệu chứa trong một hệ thống máy tính

4. Làm gián đoạn hoạt động của mạng máy tính hoặc mạng viễn thông cản trở các hoạt động bình thường của các loại dịch vụ đó

5. Truy nhập bất hợp pháp (đột nhập)

6. Tác động nội ứng (làm sai lệch dữ liệu hoặc các quá trình tự động một cách bí mật, người sử dụng máy tính không biết được khi sử dụng các dữ liệu và chương trình sai lệch đó)

7. Ngăn cản bất hợp pháp, thay đổi hoặc xóa những thư điện tử của người khác hoặc các thông tin dữ liệu khác, vi phạm quyền tự do thông tin của người khác

8. Tuyên truyền, phổ biến công cụ, phương thức phạm tội công nghệ cao...v.v

- Nhóm II: Các tội sử dụng CNTT xâm phạm quyền lợi của người khác (tội phạm sử dụng CNTT).

Đây cũng là các tội phạm diễn ra trong môi trường mạng máy tính, sử dụng các ứng dụng CNTT làm phương tiện phạm tội. Mục đích của tội phạm này không chỉ là phá hoại, gây rối loạn, cản trở an ninh CNTT mà còn nhằm những mục đích khác như: thu lợi bất chính, gây mất ổn định các hoạt động xã hội thông qua mạng, gian lận thương mại...v.v. Nhóm này gồm những hành vi tiêu biểu như:

1. Đánh cắp thông tin, mật khẩu nhằm rút tiền từ tài khoản của người khác thông qua hệ thống ngân hàng trực tuyến.

2. Đánh cắp account để truy nhập trái phép hoặc sử dụng các dịch vụ trên mạng máy tính.

3. Đánh cắp thời gian sử dụng các dịch vụ trên mạng máy tính (Tác động vào máy tính hoặc hệ thống máy tính với ý đồ không trả tiền hoặc làm sai lệch hệ thống thanh toán tự động dựa trên bộ đếm thời gian với ý đồ giảm hoặc tăng số tiền phải trả)

4. Rút ruột các hệ thống bán hàng tự động qua mạng (bằng cách sử dụng các phương tiện chứa đựng thông tin thanh toán giả)

5. Sản xuất, sao chép phần mềm bất hợp pháp, không có bản quyền

6. Chiếm đoạt quyền sử dụng tên miền để sử dụng, trao đổi kiếm lời hoặc tống tiền chủ sở hữu.

7. Tạo website giả để lừa đảo (Tội phạm thông thường làm giả website của các ngân hàng có uy tín, các hệ thống bán hàng tự động, các dịch vụ khác để lừa khách hàng khai báo thông tin tài khoản cá nhân hoặc chuyển tiền cho chúng)

8. Đưa lên mạng máy tính các thông tin xấu gây rối loạn trật tự công cộng

9. Phá hủy các website của doanh nghiệp, nhà nước để khủng bố...v.v

1.3. Các dấu hiệu pháp lý của tội phạm trong lĩnh vực tin học

Dấu hiệu pháp lý hay dấu hiệu cấu thành của một loại tội phạm có tính đặc trưng và điển hình cho loại tội phạm ấy; nó phản ánh đầy đủ bản chất và đủ để phân biệt loại tội phạm này với các tội phạm khác.

Tội phạm trong lĩnh vực tin học mới xuất hiện, có nhiều điểm khác biệt so với các tội phạm truyền thống nhưng nó vẫn là một loại tội phạm và vẫn mang các dấu hiệu pháp lý bắt buộc. Đó là: khách thể của tội phạm, mặt khách quan của tội phạm, chủ thể của tội phạm, mặt chủ quan của tội phạm.

1.3.1. Khách thể của tội phạm trong lĩnh vực tin học

Khách thể của tội phạm là những quan hệ xã hội được luật hình sự bảo vệ nhưng bị tội phạm đe dọa bằng cách gây thiệt hại và trực tiếp đe dọa gây thiệt hại ở một chừng mực nhất định. Trong khách thể bao gồm khách thể loại và khách thể trực tiếp. Khách thể loại của tội phạm là nhóm quan hệ xã hội có tính chất, đặc điểm giống nhau bị một nhóm các tội phạm xâm hại. Khách thể trực tiếp là quan hệ xã hội cụ thể bị hành vi phạm tội xâm hại và gây nên thiệt hại ở mức độ nhất định [19, tr.72-73].

Khách thể loại mà tội phạm trong lĩnh vực tin học xâm phạm là trật tự, an toàn trong lĩnh vực CNTT và quyền, lợi ích hợp pháp liên quan đến hoạt động CNTT của cá nhân, tổ chức.

Trật tự, an toàn trong lĩnh vực CNTT được coi là điều kiện đảm bảo cho mọi hoạt động trong lĩnh vực này diễn ra bình thường. Xâm phạm vào trật tự, an toàn trong lĩnh vực CNTT là xâm phạm vào các quy định pháp luật, quy tắc xử sự trong ngành, làm đảo lộn, sai lệch, phá hoại các hoạt động về CNTT.

Khách thể trực tiếp của tội phạm trong lĩnh vực tin học rất đa dạng. Đó có

thể là quyền sở hữu (đối với tài khoản, thông tin, phần mềm, dữ liệu, tên miền...), quyền tự do thông tin, trât tự xã hội, thuần phong mỹ tục...v.v

Khi xã hội ngày càng phát triển, các hoạt động của con người ngày càng gắn bó với môi trường CNTT thì cơ hội tấn công của tội phạm trong lĩnh vực tin học càng nhiều hơn.

1.3.2. Mặt khách quan của tội phạm trong lĩnh vực tin học

Mặt khách quan của tội phạm là những biểu hiện ra bên ngoài của tội phạm. Mặt khách quan gồm những dấu hiệu như:

- Hành vi nguy hiểm cho xã hội;
- Hậu quả nguy hiểm cho xã hội;
- Mối quan hệ giữa hành vi và hậu quả;
- Phương pháp, phương tiện, công cụ, thủ đoạn để thực hiện hành vi nguy hiểm cho xã hội;
- Thời gian, không gian nơi xảy ra hành vi nguy hiểm cho xã hội [19, tr.76].

Hành vi nguy hiểm cho xã hội thuộc mặt khách quan của tội phạm trong lĩnh vực tin học được thể hiện bằng cả hai dạng: hành vi hành động (ví dụ: tạo ra, lan truyền các virus tin học) hoặc hành vi không hành động (ví dụ: không thực hiện đúng các quy định của nhà nước về sử dụng máy tính, mạng máy tính).

Hậu quả của tội phạm trong lĩnh vực tin học thông thường là gây rối loạn, phong tỏa hoạt động thông tin; thay đổi, hủy hoại các dữ liệu máy tính; xâm hại quyền lợi ích của cá nhân, tổ chức sử dụng máy tính, mạng máy tính...Trong một số trường hợp hậu quả là yếu tố bắt buộc để định tội. Ví dụ: nếu chỉ tạo ra virus tin học, đưa vào mạng máy tính nhưng không gây được hậu quả gì thì không coi

là tội phạm.

Thủ đoạn thực hiện tội phạm trong lĩnh vực tin học rất tinh vi vì công cụ phạm tội là những ứng dụng công nghệ tiên tiến. Môi trường phạm tội là môi trường ảo nên rất khó khăn cho việc phát hiện, ngăn chặn tội phạm.

Nghiên cứu tình hình tội phạm trong lĩnh vực tin học cho thấy tội phạm này tấn công vào rất nhiều mục tiêu khác nhau với những thủ đoạn tinh vi và đa dạng. Trong đó, những thủ đoạn cơ bản của chúng là:

- Phổ biến nhất là tạo ra và lan truyền virus tin học. Sự lây lan virus máy tính thường thông qua các con đường: Sử dụng đĩa mềm, qua mạng LAN, mạng diện rộng và mạng Internet. Virus nhiễm vào máy tính sẽ gây ra nhiều hậu quả khác nhau như: lỗi thi hành lệnh, làm lệch lạc hoặc hủy hoại dữ liệu, tê liệt hệ thống... Tội phạm trong lĩnh vực tin học phát tán virus thường nhằm mục đích phá hoại, khủng bố, lấy trộm mật khẩu, thậm chí là để khiêu khích hoặc quảng cáo các phần mền diệt virus.

- Một thủ đoạn khác thường được sử dụng để ăn cắp thông tin và mật khẩu là cài đặt chương trình kiểm soát vào một hệ thống máy tính. Khi có người sử dụng máy tính đó, chương trình kiểm soát sẽ tự động ghi lại các thông tin của người sử dụng, trong đó có cả mật khẩu truy cập Internet, thông tin thẻ tín dụng... là những thông tin mà tội phạm trong lĩnh vực tin học tìm kiếm, lợi dụng.

- Đột nhập là thủ đoạn sử dụng các công cụ phần mềm để truy nhập bất hợp pháp vào hệ thống máy tính hoặc mạng máy tính. Hành vi đột nhập thường diễn ra dưới hai dạng: Trực tiếp đột nhập vào hệ thống dữ liệu của một máy tính cụ thể hoặc gián tiếp thông qua mạng đột nhập vào toàn bộ hay một phần của hệ thống máy tính. Với thủ đoạn này là rất khó xác định vị trí của kẻ đột nhập. Nhóm mục đích chính của những kẻ đột nhập là: gây nhiễu, làm tắc nghẽn quá

trình hoạt động của mạng, phá hủy chương trình hệ thống và dữ liệu, khai thác trộm thông tin.

- Tấn công kiểu từ chối cung cấp dịch vụ (Denial of Service - DOS): hành vi này làm tràn ngập một địa chỉ IP (Internet Protocol Address) bằng dữ liệu khiến máy tính bị sự cố hoặc mất kết nối Internet. Tấn công kiểu này thường nhằm vào những Server Web (trang chủ) lớn với mục đích làm cho người dùng không đến được với các site (địa chỉ trên mạng) cần thiết. (IP - Internet Protocol Address là số danh định của một máy tính hai thiết bị và hai máy tính kết nối trực tiếp vào Internet không thể có cùng địa chỉ IP tại cùng một thời điểm. Máy tính có địa chỉ IP tĩnh (những hệ thống kết nối dùng DSL hoặc modem cáp) luôn có một IP cố định; máy tính có địa chỉ IP động (hệ thống dùng kết nối quay số) thì mỗi lần đăng nhập vào Internet được gán một IP mới).

- Tấn công kiểu từ chối cung cấp dịch vụ phân tán (Distributed Denial of Service - DOS): sử dụng nhiều máy tính để đồng loạt tấn công DOS. Thủ phạm sẽ trưng dụng một số máy tính bên ngoài và sử dụng chúng làm những hệ thống để phat động cuộc tấn công gây ra tình trạng nghẽn kết nối trầm trọng.

- Lừa đảo: Thủ phạm xây dựng những trang web giả tương tự với các trang web của các ngân hàng uy tín hoặc các công ty bán hàng qua mạng gây nhầm lẫn cho người sử dụng. Nạn nhân sẽ khai báo thông tin về tài khoản, thẻ tín dụng hoặc chuyển tiền đến tài khoản của kẻ lừa đảo.

- Giả mạo: sau khi đánh cắp được những thông tin về mật khẩu truy nhập hệ thống máy tính, thông tin về tài khoản ngân hàng... thủ phạm sẽ giả mạo chủ nhân của mật khẩu hoặc tài khoản đó để truy nhập mạng máy tính, sử dụng các dịch vụ Internet, rút tiền, mua hàng qua hệ thống bán hàng trên mạng.

...v.v

1.3.3. Chủ thể của tội phạm trong lĩnh vực tin học

Chủ thể của tội phạm là con người cụ thể, thực hiện hành vi nguy hiểm cho xã hội một cách cố ý hoặc vô ý, có đủ năng lực TNHS và đạt độ tuổi nhất định theo quy định của pháp luật [19, tr.76]. Như vậy, chủ thể của tội phạm luôn phải đáp ứng ba yêu cầu: 1) là con người cụ thể đang tồn tại; 2) có năng lực TNHS; 3) đạt độ tuổi chịu TNHS theo quy định của pháp luật

Cũng như các tội phạm khác, độ tuổi đối với tội phạm trong lĩnh vực tin học tuân thủ quy định chung của luật hình sự về độ tuổi của chủ thể tội phạm. Tuy nhiên, vấn đề độ tuổi trong khi xem xét trách nhiệm hình sự đối với tội phạm trong lĩnh vực tin học hiện nay đang là một khó khăn. Trên thế giới, thực tế đã xảy ra rất nhiều vụ tấn công của các hacker gây hậu quả nghiêm trọng nhưng các hacker đó lại chưa đủ tuổi chịu trách nhiệm hình sự. Trong tầng lớp thanh thiếu niên hiện nay, rất nhiều người có trình độ tin học cao khi còn nhỏ tuổi. Và vì nhỏ tuổi nên họ chưa nhận thức được một cách đầy đủ về hành vi do mình thực hiện cũng như hậu quả của hành vi đó.

Về năng lực trách nhiệm hình sự, hầu hết tội phạm trong lĩnh vực tin học là những người có năng lực trách nhiệm hình sự. Sở dĩ như vậy là vì để thực hiện tội phạm này người phạm tội phải có trình độ hiểu biết cao, kiến thức tin học giỏi, có trí tuệ. Sẽ khó có thể tìm thấy trường hợp người phạm loại tội tinh vi này mà mất năng lực trách nhiệm hình sự.

Như vậy, trách nhiệm hình sự về tội phạm này được đặt ra với bất kỳ chủ thể nào có năng lực trách nhiệm hình sự và đủ tuổi chịu trách nhiệm hình sự theo quy định của Bộ luật Hình sự. Tuy nhiên, trên thực tế thì chủ thể của tội này là những chủ thể rất đặc biệt. Họ là những người có kiến thức chuyên môn cao trong lĩnh vực CNTT.

1.3.4. Mặt chủ quan của tội phạm trong lĩnh vực tin học

Mặt chủ quan của tội phạm là diễn biến bên trong phản ánh trạng thái tâm lý của chủ thể đối với hành vi nguy hiểm cho xã hội và hậu quả của hành vi đó. Nếu mặt khách quan của tội phạm là sự biểu hiện ra bên ngoài của tội phạm thì mặt chủ quan là diễn biến bên trong của người phạm tội. Hai mặt này thông nhất chặt chẽ với nhau. Luật hình sự chỉ xem xét trách nhiệm hình sự khi hành vi khách quan có mối quan hệ với mặt chủ quan của chủ thể thực hiện hành vi. Mặt chủ quan của tội phạm bao gồm các dấu hiệu: lỗi, động cơ và mục đích phạm tội. Lỗi trong luật hình sự gồm hai hình thức: lỗi cố ý và lỗi vô ý.

Yếu tố lỗi trong cấu thành tội phạm trong lĩnh vực tin học có thể là cố ý (ví dụ: phát tán virus, sao chép, đánh cắp thông tin) hoặc vô ý (ví dụ: làm sai các quy định về sử dụng, vận hành hệ thống máy tính).

Động cơ, mục đích phạm tội của tội phạm trong lĩnh vực tin học có thể là thu lợi bất chính, cạnh tranh không làn mạnh, xâm phạm bí mật đời tư, quấy rối trật tự xã hội hoặc đơn giản là để nổi danh, thách thức các nhà quản trị mạng...v.v

CHƯƠNG 2. QUY ĐỊNH PHÁP LUẬT VỀ CÁC TỘI PHẠM TRONG LĨNH VỰC TIN HỌC VÀ THỰC TIỄN XỬ LÝ

2.1. Quy định về các tội phạm trong lĩnh vực tin học theo pháp luật Việt Nam

Các tội phạm trong lĩnh vực tin học là loại tội phạm còn rất mới mẻ so với chiều dài phát triển của luật hình sự thế giới nói chung và Việt Nam nói riêng. Bộ luật Hình sự năm 1999 lần đầu tiên đưa vào các quy định về tội phạm trong lĩnh vực tin học, thậm chí trước đó trong các bản dự thảo cuối cùng của Bộ luật cũng chưa xem xét đưa ra vấn đề này. Nó chỉ được Tổng cục Bưu điện trình lên khi toàn văn Bộ luật Hình sự đã được thông qua.

Pháp luật mỗi nước luôn gắn liền với sự phát triển của kinh tế, chính trị, văn hóa, khoa học công nghệ, phong tục tập quán... của nước đó. Vì vậy, mỗi quốc gia điều chỉnh pháp luật nói chung, pháp luật hình sự và pháp luật về khoa học công nghệ nói riêng theo nhưng nguyên tắc khác nhau phù hợp với giai đoạn lịch sử và tùy theo sự phát triển của kinh tế, chính trị, văn hóa, khoa học công nghệ và phong tục tập quán nước đó.

Ở nước ta, sự chuyển biến nhận thức về vai trò của CNTT từ các cấp lãnh đạo cao nhất đã được cụ thể hóa bằng những chỉ thị, nghị quyết, quyết định, luật... Những văn bản đó đã có tác động tích cực đến sự phát triển của CNTT tại Việt Nam.

Chỉ thị số 58-CT/TW ngày 17 tháng 10 năm 2000 của Ban chấp hành Trung ương Đảng Cộng Sản Việt Nam về đẩy mạnh ứng dụng và phát triển CNTT phục vụ sự nghiệp công nghiệp hoá, hiện đại hoá đã khẳng định: “CNTT là một trong các động lực quan trọng nhất của sự phát triển, cùng với một số ngành công nghệ cao khác đang làm biến đổi sâu sắc đời sống kinh tế, văn hóa

xã hội của thế giới hiện đại".

Còn trong Kế hoạch tổng thể về ứng dụng và phát triển CNTT ở Việt Nam đến năm 2005, CNTT được ưu tiên ứng dụng trong các hệ thống kinh tế huyết mạch của đất nước: hệ thống ngân hàng, tài chính, thuế, hải quan, hàng không, viễn thông, thông tin khoa học và công nghệ, ngoại thương; ứng dụng CNTT trong công nghiệp hóa, hiện đại hóa nông thôn; sử dụng CNTT để nâng cao năng lực cạnh tranh của các doanh nghiệp, mở dụng ứng dụng tiếp thị, giao dịch thương mại trên mạng; sử dụng CNTT trong lĩnh vực an ninh quốc phòng, tăng cường sức mạnh chiến đáu cả các lực lượng vũ trang; chú trọng ứng dụng CNTT trong các dịch vụ hành chính công...

Báo cáo chính trị của BCHTW Đảng khóa WIII trình đại biểu quốc hội lần thứ IX của Đảng ghi nhận: "Khoa học công nghệ là quốc sách hàng đầu, giữ vai trò then chốt trong sự nghiệp xây dựng và bảo vệ tổ quốc, là nền tảng và động lực Công nghiệp hóa, hiện đại hóa, phát triển nhanh, bền vững đất nước"

Nhìn chung, tin học hóa mọi mặt của đời sống xã hội là một chính sách chiến lược của Đảng và Nhà nước. Những nhận thức kịp thời đó đã tích cực thúc đẩy và tạo điều kiện cho CNTT phát triển. Cùng với sự phát triển và những lợi ích mà CNTT đem lại, chúng ta cũng đương nhiên phải chấp nhận những mặt trái, hậu quả tiêu cực của nó đối với xã hội. Một yêu cầu cấp thiết đặt ra là cần phải có hành lang pháp lý đủ mạnh để khuyến khích mặt tích cực và hạn chế mặt tiêu cực của sự phát triển này. Đáp ứng yêu cầu này, Đảng và Nhà nước ta một mặt đã ban hành các văn bản nhằm thúc đẩy sự phát triển của CNTT như đã nêu trên, mặt khác, xây dựng và hoàn thiện hành lang pháp lý nhằm điều tiết và khắc phục những tiêu cực, vi phạm diễn ra trong lĩnh vực này.

Quan điểm của Đảng và Nhà nước ta đối với các vi phạm trong lĩnh vực

tin học được thể hiện trực tiếp qua Bộ luật Hình sự năm 1999 và hệ thống các văn bản hành chính. Việc hình sự hóa các vi phạm này thể hiện thái độ nghiêm khắc, kiên quyết không khoan nhượng của Đảng và Nhà nước ta. Có như vậy mới đảm bảo hạn chế được mặt trái của sự phát triển CNTT.

Luật CNTT được ban hành năm 2006 cũng là cơ sở quan trọng để xác định những vi phạm pháp luật trong lĩnh vực CNTT. Bên cạnh đó, tất cả những hành vi vi phạm trong lĩnh vực CNTT đều bị coi là nghiêm cấm. Luật khoa học và công nghệ năm 2000 và sau đó là Luật khoa học và công nghệ năm 2004 quy định khái quát về các hành vi bị nghiêm cấm trong lĩnh vực khoa học công nghệ, bao gồm cả CNTT. Các hành vi bị nghiêm cấm trong hoạt động khoa học và công nghệ là:

"Lợi dụng hoạt động khoa học công nghệ để xuyên tạc, chống lại đường lối, chính sách của Đảng Cộng sản Việt Nam, pháp luật của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, phá hoại khối đại đoàn kết dân tộc.

Lợi dụng hoạt động khoa học công nghệ để xâm phạm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân; gây thiệt hại đến tài nguyên, môi trường, sức khỏe con người; trái với đạo đức, thuần phong mỹ tục của dân tộc.

Xâm phạm quyền sở hữu trí tuệ; chiếm đoạt, chuyển nhượng, chuyển giao bất hợp pháp kết quả khao học và công nghệ; tiết lộ tư liệu, kết quả khoa học và công nghệ thuộc danh mục bí mật nhà nước; lừa dối, giả mạo trong hoạt động khoa học và công nghệ.

Cản trở hoạt động khoa học và công nghệ hợp pháp của tổ chức, cá nhân".

Những hành vi vi phạm trong lĩnh vực CNTT phải gánh chịu những hậu quả pháp lý nghiêm khắc, có thể là trách nhiệm pháp lý hành chính hoặc trách

nhiệm pháp lý hình sự. Những hình thức trách nhiệm đó sẽ được phân tích cụ thể dưới đây.

2.1.1. Quy định pháp luật hình sự về các tội phạm trong lĩnh vực tin học

Nhận thức nguy cơ và hậu quả của tội phạm trong lĩnh vực tin học trên thế giới, sự xuất hiện tội phạm này tại Việt Nam, khi thông qua Bộ luật Hình sự năm 1999 Quốc Hội Việt Nam đã thông qua ba điều luật quy định về tội phạm trong lĩnh vực tin học. Ba điều này (Điều 224, 225, 226) được đặt trong Chương XIX - Chương về các tội xâm phạm trật tự công cộng, an toàn công cộng. Tuy nhiên, đây mới chỉ là những quy định về một số hành vi trực tiếp tấn công dữ liệu máy tính, xâm hại trật tự an ninh CNTT chứ chưa đề cập tới hành vi sử dụng CNTT như công cụ phạm tội.

a.Tội tạo ra, lan truyền và phát tán các virus tin học (Điều 224)

Khoản 1 Điều 24 Bộ luật Hình sự Việt Nam quy định: Người nào tạo ra và cố ý lan truyền, phát tán các chương trình virus qua mạng máy tính hoặc bằng các phương thức khác gây rối loạn hoạt động, phong tỏa hoặc làm biến dạng các dữ liệu của máy tính hoặc đã bị xử lý kỷ luật, xử phạt về hành vi này mà còn vi phạm thì bị...

Theo quy định này tội tạo ra, lan truyền và phát tán các virus tin học được cấu thành bởi các yếu tố cấu thành sau:

Khách thể của tội phạm này là trật tự, an ninh thông tin trong máy tính, mạng máy tính. Các virus tin học khi lan truyền trong mạng máy tính chúng có khả năng phá hủy, làm rối loạn, biến dạng...cơ sở dữ liệu của các máy tính trong mạng. Do đó hành vi tạo ra và lan truyền các virus tin học xâm phạm vào sự an toàn trong hoạt động của mạng máy tính điện tử.

Mặt khách quan của tội phạm: Mặt khách quan của tội này thể hiện bằng một trong các hành vi:

- Tạo ra và lan truyền, phát tán các chương trình virus qua mạng máy tính gây rối loạn, hủy hoại dữ liệu của máy tính. Tạo ra chương trình virus là làm ra, lập trình các phần mềm chương trình virus có khả năng phá hủy các dữ liệu trong mạng máy tính. Lan truyền, phát tán các chương trình virus là thông qua mạng máy tính hoặc bằng các cách khác đưa chương trình virus vào mạng máy tính. Hành vi này được thể hiện bằng hai hành động kế tiếp nhau: tạo ra và lan truyền, phát tán chương trình virus tin học. Nếu chỉ tạo ra mà không lan truyền, phát tán thì TNHS không đặt ra.

- Bằng các phương thức khác gây rối loạn hoạt động, phong tỏa, hủy hoại, làm biến dạng các dữ liệu của máy tính. Các phương thức khác ở đây có thể là sử dụng chương trình virus của người khác hoặc nhân bản các virus có sẵn trong mạng.

Hậu quả của tội phạm này thể hiện bằng việc gây rối loạn hoạt động, phong tỏa hoặc làm biến dạng, hủy hoại các dữ liệu của máy tính. Hậu quả này phải có mối quan hệ nhân quả với hành vi tạo ra, lan truyền các virus tin học. Thời điểm hoàn thành của tội phạm kể từ khi gây nên hậu quả trên. Nếu chưa gây hậu quả thì người vi phạm chỉ bị truy cứu TNHS khi họ đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm.

Mặt chủ quan của tội phạm: Tội phạm được thực hiện dưới hình thức lỗi cố ý. Người phạm tội biết hành vi của mình là nguy hiểm cho xã hội, biết trước hậu quả có thể xảy ra mà vẫn thực hiện.

Chủ thể của tội phạm: Tội phạm này được thực hiện bởi bất kỳ người nào có năng lực TNHS và đạt độ tuổi theo luật định.

Hình phạt:

Khung 1: Phạt tiền từ 5 triệu đồng đến 100 triệu đồng hoặc từ 6 tháng tù đến 3 năm, áp dụng đối với người phạt tội không có tình tiết tăng nặng.

Khung 2: Phạt tù từ 2 năm đến 7 năm, áp dụng đối với người phạm tội trong trường hợp gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng.

Hình phạt bổ sung: Người phạm tội có thể bị phạt tiền từ 5 triệu đồng đến 50 triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 1 năm đến 5 năm.

b.Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử (Điều 225 BLHS)

Bộ luật Hình Sự quy định về tội danh này như sau: Người nào được sử dụng mạng máy tính mà vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính gây rối loạn hoạt động, phong tỏa hoặc làm biến dạng, làm hủy hoại các dữ liệu của máy tính hoặc đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm thì... (Khoản 1 Điều 225)

Khách thể của tội phạm: Tội phạm này xâm phạm vào những quy định về vận hành, khai thác và sử dụng mạng máy tính, xâm phạm vào sự an toàn trong hoạt động của mạng máy tính điện tử.

Mặt khách quan của tội phạm: Mặt khách quan của tội phạm thể hiện bằng hành vi vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính. Hành vi này có hai dạng: không thực hiện các quy định về vận hành, khai thác và sử dụng mạng máy tính; thực hiện không đúng các quy định về vận hành, khai thác và sử dụng mạng máy tính.

Hậu quả của hành vi vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính cũng giống như hậu quả của tội tạo ra, lan truyền các virus

tin học. Nếu chưa gây hậu quả thì người vi phạm chỉ bị truy cứu TNHS khi họ đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm.

Mặt chủ quan của tội phạm: Tội phạm được thực hiện dưới hình thức lỗi cố ý hoặc vô ý.

Chủ thể của tội phạm: Chủ thể của tội phạm là người được sử dụng mạng máy tính, có năng lực TNHS và đạt độ tuổi theo luật định.

Hình phạt:

Khung 1: Phạt tiền từ 5 triệu đồng đến 50 triệu đồng hoặc tù từ 6 tháng đến 3 năm, áp dụng đối với người phạt tội không có tình tiết tăng nặng.

Khung 2: Phạt tù từ 2 năm đến 7 năm, áp dụng đối với người phạm tội trong trường hợp gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng.

Hình phạt bổ sung: Người phạm tội có thể bị phạt tiền từ 5 triệu đồng đến 50 triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 1 năm đến 5 năm.

c.Tội sử dụng trái phép thông tin trên mạng và trong máy vi tính (Điều 226 BLHS)

Người nào sử dụng trái phép các thông tin trên mạng và trong máy tính, cũng như đưa vào mạng máy tính những thông tin trái với quy định của pháp luật gây hậu quả nghiêm trọng, đã bị xử lý kỷ luật, xử phạt hành chính mà còn vi phạm thì... (Điều 226, khoản 1 BLHS).

Theo quy định của điều luật này thì tội sử dụng trái phép thông tin trên mạng và trong máy vi tính có các dấu hiệu cấu thành sau:

Khách thể của tội phạm: Tội phạm này xâm phạm vào những quy định về sử dụng thông tin trên mạng và trong máy tính; xâm phạm vào sự an toàn trong hoạt động của mạng máy tính điện tử.

Mặt khách quan của tội phạm: Mặt khách quan của tội phạm được thể hiện bằng một trong các hành vi sau:

- Sử dụng trái phép thông tin trên mạng và trong máy tính. Sử dụng trái phép nghĩa là sử dụng thông tin không được chủ sở hữu đồng ý hoặc cơ quan quản lý thông tin cho phép.

- Đưa vào mạng máy tính những thông tin trái với quy định của luật. Đó là những thông tin có nội dung xấu mà pháp luật nghiêm cấm đưa vào mạng máy tính.

Hậu quả của tội phạm này gây nên ở mức độ nghiêm trọng. Chẳng hạn như gây thiệt hại nghiêm trọng đến lợi ích của chủ sở hữu thông tin, gây hoang mang cho xã hội, ảnh hưởng đạo đức xã hội…

Nếu hành vi kể trên chưa gây hậu quả nghiêm trọng thì người có hành vi vi phạm chỉ bị truy cứu TNHS khi họ đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà còn vi phạm.

Mặt chủ quan của tội phạm: Tội phạm được thực hiện dưới hình thức lỗi cố ý.

Chủ thể của tội phạm: Tội phạm được thực hiện bởi bất kỳ người nào có năng lực TNHS và đạt độ tuổi theo luật định.

Hình phạt:

Khung 1: Phạt tiền từ 5 triệu đồng đến 50 triệu đồng, cải tạo không giam giữ đến 3 năm hoặc phạt tù từ 6 tháng đến 3 năm.

Khung 2: Phạt tù từ 2 năm đến 5 năm, khi có một trong các tình tiết sau:

+ Có tổ chức.

+ Gây hậu quả rất nghiêm trọng hoặc đặc biệt nghiêm trọng.

Hình phạt bổ sung: Người phạm tội có thể bị phạt tiền từ 3 triệu đồng đến

30 triệu đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 1 năm đến 5 năm.

2.1.2. Quy định pháp luật phi hình sự – một trong các căn cứ để xác định tội phạm trong lĩnh vực tin học

Các tội phạm trong lĩnh vực tin học là những hành vi vi phạm quy định pháp luật trong lĩnh vực tin học có tính chất nghiêm trọng đến mức phải truy cứu TNHS. Vì vậy, các quy định pháp luật phi hình sự trong lĩnh vực tin học chính là một trong những căn cứ để xác định tội phạm trong lĩnh vực này. Quy định về các hoạt động, trật tự, an ninh trong lĩnh vực tin học là chuẩn mực để xác định các hành vi lệch chuẩn - vi phạm, tội phạm trong lĩnh vực này.

Bên cạnh đó, theo nội dung các quy định của Bộ luật Hình sự 1999 về các tội phạm trong lĩnh vực tin học (đã phân tích ở trên) thì những hành vi vi phạm quy định pháp luật trong lĩnh vực tin học nếu gây hậu quả nghiêm trọng hoặc đã bị xử lý hành chính mà tái phạm thì sẽ bị xử lý về mặt hình sự. Vì thế các quy định pháp luật hành chính đối với hoạt động trong lĩnh vực tin học là căn cứ quan trọng để xác định TNHS đối với loại tội phạm này.

Hệ thống các văn bản pháp luật phi hình sự điều chỉnh vi phạm pháp luật trong lĩnh vực CNTT hiện nay bao gồm: Luật CNTT năm 2006, Nghị định số 55/2001/NĐ-CP ngày 23 tháng 08 năm 2001 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet; Quyết định Số 92/2003/QĐ - BBCVT ngày 26 tháng 5 năm 2003 của Bộ trưởng Bộ Bưu chính, Viễn thông ban hành "Quy định về quản lý và sử dụng tài nguyên Internet"; Thông tư số 04/2001/TT-TCBĐ ngày 20 tháng 11 năm 2001 của Tổng cục Bưu điện hướng dẫn thi hành Nghị định số 55/2001/NĐ-CP của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ

truy nhập Internet, dịch vụ kết nối Internet và dịch vụ ứng dụng Internet trong Bưu chính, Viễn thông; Quyết định số 95/2002/QĐ-TTg ngày 17/7/2002 của Thủ tướng Chính phủ Phê duyệt Kế hoạch tổng thể về ứng dụng và phát triển CNTT ở Việt Nam đến năm 2005; Quyết định số 17/2001/QĐ-TTg ngày 13 tháng 2 năm 2001 của Thủ tướng Chính phủ về việc chuyển giao chức năng điều phối các hoạt động Internet ở Việt Nam; Quyết định số 27/2002/QĐ-BVHTT ngày 10/10/2002 của Bộ Văn hóa Thông tin ban hành Quy chế quản lý và cấp phép cung cấp thông tin, thiết lập trang thông tin điện tử trên Internet; Qui định về biện pháp và trang thiết bị kiểm tra, kiểm soát đảm bảo an ninh quốc gia trong hoạt động Internet ở Việt Nam. (Ban hành kèm theo Quyết định số 848/1997/QĐ-BNV(A11) ngày 23/10/1997 của Bộ trưởng Bộ Nội vụ); Quyết định số 84/2001/QĐ-BTC ngày 5 tháng 9 năm 2001 của Bộ trưởng Bộ Tài chính Ban hành Biểu mức thu phí, lệ phí cấp và quản lý tên miền, địa chỉ Internet ở Việt Nam.

Trong số các văn bản kể trên thì Luật CNTT năm 2006 và Nghị định số 55/2001/NĐ-CP ngày 23 tháng 08 năm 2001 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet được coi là cơ sở trực tiếp để xử lý các vi phạm trong lĩnh vực này.

Luật CNTT quy định về hoạt động ứng dụng và phát triển công nghệ thông tin, quyền và nghĩa vụ của cơ quan, tổ chức, cá nhân tham gia hoạt động ứng dụng và phát triển công nghệ thông tin. Ngoài các quy định chung về hoạt động trong lĩnh vực CNTT, quy định về quyền và nghĩa vụ của cá nhân, tổ chức tham gia hoạt động trong lĩnh vực CNTT, Luật CNTT còn chỉ rõ các hành vi bị cấm trong lĩnh vực này. Điều 12 của Luật quy định các hành vi sau bị nghiêm cấm:

- Cản trở hoạt động hợp pháp hoặc hỗ trợ hoạt động bất hợp pháp về ứng dụng và phát triển công nghệ thông tin; cản trở bất hợp pháp hoạt động của hệ thống máy chủ tên miền quốc gia; phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng.

- Cung cấp, trao đổi, truyền đưa, lưu trữ, sử dụng thông tin số nhằm mục đích sau đây:

+ Chống Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, phá hoại khối đoàn kết toàn dân;

+ Kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, kích động dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong mỹ tục của dân tộc;

+ Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định;

+ Xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự, nhân phẩm, uy tín của công dân;

+ Quảng cáo, tuyên truyền hàng hoá, dịch vụ thuộc danh mục cấm đã được pháp luật quy định.

- Xâm phạm quyền sở hữu trí tuệ trong hoạt động công nghệ thông tin; sản xuất, lưu hành sản phẩm công nghệ thông tin trái pháp luật; giả mạo trang thông tin điện tử của tổ chức, cá nhân khác; tạo đường dẫn trái phép đối với tên miền của tổ chức, cá nhân sử dụng hợp pháp tên miền đó.

Quy định này là cơ sở quan trọng để xác định các hành vi vi phạm pháp luật trong lĩnh vực tin học và tùy theo tính chất, mức độ của hành vi đó để xem xét việc truy cứu TNHS (chẳng hạn như hành vi gây hậu quả nghiêm trọng hoặc người vi phạm đã từng bị xử lý kỷ luật về hành vi đó mà tái phạm).

Nghị định số 55/2001/NĐ-CP ngày 23 tháng 08 năm 2001 của Chính phủ quy định cụ thể về quản lý, cung cấp và sử dụng dịch vụ Internet. Điều 41 Nghị định quy định các hành vi vi phạm trong quản lý, cung cấp, sử dụng Internet như sau:

- Hành vi không khai báo làm thủ tục cấp lại khi giấy phép cung cấp dịch vụ Internet bị mất, hoặc bị hư hỏng.

- Sử dụng mật khẩu, khoá mật mã, thông tin riêng của người khác để truy nhập, sử dụng dịch vụ Internet trái phép.

- Sử dụng các công cụ phần mềm để truy nhập, sử dụng dịch vụ Internet trái phép.

- Vi phạm các quy định của Nhà nước về tiêu chuẩn, chất lượng trong việc sử dụng dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về giá, cước trong việc sử dụng dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về quản lý tài nguyên Internet trong việc sử dụng dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về quản lý truy nhập, kết nối Internet trong việc sử dụng dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về mã hoá và giải mã thông tin trên Internet trong việc sử dụng dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về an toàn, an ninh thông tin trên Internet trong việc sử dụng dịch vụ Internet.

- Ngừng hoặc tạm ngừng cung cấp dịch vụ Internet mà không thông báo cho người sử dụng dịch vụ Internet biết trước, trừ trường hợp bất khả kháng.

- Sửa chữa, tẩy xóa làm thay đổi nội dung giấy phép cung cấp dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về tiêu chuẩn, chất lượng dịch vụ Internet trong việc cung cấp dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về giá, cước dịch vụ Internet trong việc cung cấp dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về quản lý tài nguyên Internet trong việc cung cấp dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về quản lý truy nhập, kết nối Internet trong việc cung cấp dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về mã hoá và giải mã thông tin trên Internet trong việc cung cấp dịch vụ Internet.

- Vi phạm các quy định của Nhà nước về an toàn, an ninh thông tin trên Internet trong việc cung cấp dịch vụ Internet.

- Sử dụng Internet để nhằm mục đích đe dọa, quấy rối, xúc phạm đến danh dự, nhân phẩm người khác mà chưa đến mức truy cứu trách nhiệm hình sự.

- Đưa vào Internet hoặc lợi dụng Internet để truyền bá các thông tin, hình ảnh đồi trụy, hoặc những thông tin khác trái với quy định của pháp luật về nội dung thông tin trên Internet, mà chưa đến mức truy cứu trách nhiệm hình sự.

- Đánh cắp mật khẩu, khoá mật mã, thông tin riêng của tổ chức, cá nhân và phổ biến cho người khác sử dụng.

- Vi phạm các quy định về vận hành, khai thác và sử dụng máy tính gây rối loạn hoạt động, phong toả hoặc làm biến dạng, làm hủy hoại các dữ liệu trên Internet mà chưa đến mức truy cứu trách nhiệm hình sự.

- Sử dụng quá hạn giấy phép cung cấp dịch vụ Internet.

- Thiết lập hệ thống thiết bị và cung cấp dịch vụ Internet không đúng với các quy định ghi trong giấy phép.

- Tạo ra và cố ý lan truyền, phát tán các chương trình vi rút trên Internet mà chưa đến mức truy cứu trách nhiệm hình sự.

- Thiết lập hệ thống thiết bị và cung cấp dịch vụ Internet khi không có giấy phép.

Bên cạnh đó, yêu cầu về nội dung thông tin trên Internet được quy định tại Điều 4 Quy chế quản lý và cấp phép cung cấp thông tin, thiết lập trang thông tin điện tử trên Internet như sau:

"Nội dung thông tin không gây phương hại đến độc lập, chủ quyền và toàn vẹn lãnh thổ của nước Cộng hoà Xã hội Chủ nghĩa Việt Nam; không được kích động nhân dân chống Nhà nước Cộng hoà Xã hội Chủ nghĩa Việt Nam, phá hoại khối đại đoàn kết toàn dân.

Không được kích động bạo lực, tuyên truyền chiến tranh xâm lược gây hận thù giữa các dân tộc và nhân dân các nước, kích động dâm ô, đồi truỵ, tội ác.

Không được tiết lộ bí mật Nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật nước Cộng hoà Xã hội Chủ nghĩa Việt Nam quy định.

Không được cung cấp thông tin trên Internet, thiết lập trang tin điện tử trên Internet khi chưa có giấy phép của Bộ Văn hoá - Thông tin.

Không được cung cấp thông tin trái tôn chỉ, mục đích, phạm vi thông tin đã được Bộ Văn hoá - Thông tin cho phép".

Đối với những hành vi vi phạm kể trên, Nghị định số: 55/2001/NĐ-CP quy định hình phạt có thể là cảnh cáo hoặc phạt tiền từ 50.000 đồng đến

70.000.000 đồng. Ngoài các hình thức xử phạt chính, tùy theo tính chất, mức độ vi phạm mà tổ chức, cá nhân còn có thể bị áp dụng một hay nhiều hình thức xử phạt bổ sung hoặc biện pháp khắc phục hậu quả (chẳng hạn như: Tạm đình chỉ hoặc đình chỉ việc cung cấp và sử dụng dịch vụ Internet; Tước quyền sử dụng giấy phép có thời hạn hoặc không thời hạn; Tịch thu tang vật, phương tiện được sử dụng để vi phạm…).

Các cá nhân có những vi phạm kể trên, đã bị xử phạt vi phạm hành chính mà vẫn tái phạm có thể bị truy cứu TNHS theo quy định của pháp luật hình sự.

Tóm lại, cũng như các loại tội phạm trong lĩnh vực chuyên ngành khác, quy định pháp luật chuyên ngành là cơ sở rất quan trọng để xác định tội phạm trong lĩnh vực tin học. Sở dĩ như vậy là vì phải biết được pháp luật quy định về hoạt động trong lĩnh vực tin học như thế nào thì mới có thể xác định những hành vi vi phạm và tội phạm trong lĩnh vực này. Cụ thể, trên cơ sở những quy định cấm, những yêu cầu của pháp luật chuyên ngành đối với hoạt động trong lĩnh vực tin học, người ta xác định được vi phạm pháp luật trong lĩnh vực này; những vi phạm đó với tính chất, mức độ nhất định sẽ bị tội phạm hóa bởi luật hình sự

2.2. Thực tiễn xử lý tội phạm trong lĩnh vực tin học tại Việt Nam và nguyên nhân hạn chế

2.2.1. Thực tiễn xử lý tội phạm trong lĩnh vực tin học tại Việt Nam

2.2.1.1. Tình hình tội phạm trong lĩnh vực tin học

Mặc dù là một nước mới phát triển ngành CNTT nhưng hacker đã xuất hiện ở Việt Nam gần như đồng thời với việc Việt Nam kết nối vào mạng internet toàn cầu. Cũng như các hacker trên thế giới, hacker Việt Nam có cả những chuyên gia phá hoại, những kẻ mưu lợi bất chính lẫn những người hoạt động vì

sự đam mê và chỉ nhằm cảnh báo cho các nhà quản trị thông tin về những lỗ hổng bảo mật. Nhưng dù vì mục đích gì thì hành vi của họ cũng là trái pháp luật.

Giai đoạn mới xuất hiện (khoảng 1997 - 2001): Hoạt động của tội phạm trong lĩnh vực tin học chủ yếu nhằm mục đích gây rối trật tự an ninh trong lĩnh vực CNTT

Lúc mới xuất hiện, các hacker Việt Nam chủ yếu là những người trẻ tuổi thích quậy phá. Hacker xuất hiện ở Việt Nam khoảng năm 1997-1998. Lúc đó hacker là những anh chàng chuyên sưu tầm virus trên mạng, đính kèm vào các email và gửi cho người khác. Những hacker này chủ yếu tập trung ở mạng "Trí tuệ Việt Nam" của FPT và một ít ở các mạng khác. Một thời gian sau đó những người thường xuyên lên mạng bắt đầu nắm bắt được một số kỹ thuật cơ bản về bẻ khóa, virus. Họ bắt đầu nghĩ đến việc tụ hội, lập nhóm.

Khoảng tháng 5, 6 năm 1999 diễn đàn (forum) hackerVN được đưa lên mạng và lưu trữ tại địa chỉ www.thefreeforum.com/hackervn. Từ sau khi thành lập tổ chức, hacker Việt Nam đã học hỏi được nhiều kinh nghiệm từ các hacker trình độ cao của nước ngoài. Đặc biệt các hacker Việt kiều bắt đầu tham gia vào diễn đàn này. Diễn đàn hoạt động chủ yếu nhằm quảng bá các kiến thức về hacking, lỗ hổng bảo mật...HackerVN lúc này được coi là mạnh hơn hẳn các đối tượng cùng lĩnh vực như CLB mật mã, Vncracking, HKC.

Năm 2000, hackerVN hợp nhất với câu lạc bộ mật mã thành một tổ chức có tên gọi HVA - tổ chức hacking lớn nhất Đông Dương đương thời. Lúc đó tại Việt Nam cũng đã xuất hiện nhiều tổ chức hoạt động trong lĩnh vực hacking, cracking. HVA phát triển rất mạnh, nhiều thành viên của nó đã tiến hành phát tán, tuyên truyền các account "chùa", sex (account là các trương mục mà người dùng được sử dụng để bảo mật các hệ thống thông tin. Hầu hết các hệ điều hành

mạng đều yêu cầu người dùng phải có trương mục của mình để truy cập vào hệ thống hay mạng). Các bommail nhằm mục đích phá hủy được gửi đi một cách điên cuồng. Một số thành viên còn liên tiếp tấn công vào các website Việt Nam bất kể lý do. Những hoạt động này đã gây ra không ít thiệt hại cho các cá nhân, tổ chức.

Sau HVA, Viethacker - một tổ chức hacker khác ở Việt Nam được thành lập ngày 1/11/1999, đến năm 2001 đã tụ hội hơn 10.000 thành viên. Viethacker và HVA công kích lẫn nhau đồng thời đẩy mạnh các hoạt động quấy rối, phá hoại để thể hiện mình.

Tới thời điểm tháng 3/2001 ở Việt Nam con số password bị đánh cắp đã không chỉ dừng lại ở hàng nghìn. Phần lớn các tài khoản bị đánh cắp là của các doanh nghiệp. Loại account này được giới hacker ưa chuộng vì khi bị mất, chủ nhân chậm phát hiện hơn so với các account cá nhân. Mỗi tuần có khoảng 50 account bị tung lên mạng để dùng chung. Khi các hacker truy nhập bằng account đánh cắp được, họ có thể xem toàn bộ các giao dịch qua e-mail của chủ nhân account đó. Như vậy, thông tin riêng tư của cá nhân bị tiết lộ. Đối với doanh nghiệp, thiệt hại còn có thể lớn hơn vì thông tin giao dịch làm ăn bị rò rỉ, thậm chí lọt vào tay đối thủ cạnh tranh.

Trong năm 2001, cứ 2-3 tuần lại có một vụ bom e-mail mạo danh chứa virus. Mỗi e-mail gieo rắc virus có thể gửi đến hàng nghìn người. Mục tiêu của họ chỉ cần lấy được mật khẩu của 1% trong số hàng nghìn hộp thư bị đánh bom, như vậy trong tay các hacker có thể nắm giữ vài chục mật khẩu Internet. Đồng thời, những tay hacker cũng không ngần ngại mạo danh cả các chuyên gia virus và các công ty lớn trong lĩnh vực tin học như BKAV, VDC để gửi virus [42].

Những hoạt động quấy rối của hacker không ngừng gia tăng, nạn nhân

không chỉ là các cá nhân, doanh nghiệp mà còn thậm chí cả các cơ quan nhà nước, ngân hàng lớn.

Riêng tháng 5/2001 các hacker đã tấn công làm tê liệt hàng loạt website lớn như website của trường Đại học Bách Khoa và đại học Khoa học Tự nhiên Thành phố Hồ Chí Minh. Trong cùng ngày 20/5/2001, hai trang web của hai hãng cung cấp thiết bị tin học cùng bị tấn công là www.mekonggreen.com.vn (lúc 1h45') và www.apexdalat.com.vn (lúc 2h09'), với thông điệp đầy khiêu khích: "This site is hacked by HackerVN (Trang này đã bị tấn công bởi HackerVN) [43].

Ngay cả website của cơ quan nhà nước cũng bị các hacker tấn công. Ngày 10/6/2001 trang chủ www.nea.gov.vn của Cục Môi trường, trực thuộc Bộ Khoa học Công nghệ & Môi trường bị hacker "phù phép" biến thành một trang trắng với vài dòng chữ linh tinh [44].

Giai đoạn từ năm 2002 đến nay tội phạm trong lĩnh vực tin học gây hậu quả nghiêm trọng hơn với nhiều mục đích bất chính: ngoài gây rối, phá hoại còn nhằm trục lợi về kinh tế, chiếm đoạt tài sản, bôi nhọ danh dự cá nhân, hạ thấp uy tín của doanh nghiệp trong cạnh tranh, đầu độc về văn hóa…v.v.

- Tội phạm trong lĩnh vực tin học tấn công các ngân hàng, doanh nghiệp trực tuyến, lấy cắp thông tin tài khoản tham gia giao dịch trực tuyến để lấy trộm tiền; rửa tiền qua các website thương mại điện tử

Từ năm 2002 các đơn vị kinh doanh trở thành mục tiêu tấn công nhiều hơn của hacker Việt Nam. Ngày 4/6/2002, trang web của Ngân hàng Ngoại thương Việt Nam www.vietcombank.com.vn đã bị hacker tấn công. Nội dung trang chủ bị thay đổi thành một số dòng chữ tiếng Việt vô nghĩa. Sau đó kẻ xâm nhập đã

đưa ra thông tin thẻ tín dụng của hơn 30 khách hàng của Vietcombank và những tài khoản này đã bị tiêu xài một cách phung phí.

Vụ tấn công đầu tiên vào một cơ sở hạ tầng thông tin của ngân hàng ở Việt Nam là một lời cảnh báo đầu tiên về việc tội phạm trong lĩnh vực tin học ở Việt Nam không chỉ còn là những kẻ phá rối mà đã chuyển hướng với mục tiêu trục lợi bất chính.

Theo chị Lý Kim Anh – một nhân viên Phòng dịch vụ trực tuyến trên mạng của công ty VDC cho biết: "chỉ tính trong vài tháng đầu năm 2004, trong số 42 đơn hàng được thực hiện đã có 29 tài khoản do các hacker ăn cắp". Theo chị Kim Anh đánh giá: "Ăn cắp thẻ tín dụng và mua bán ở Việt Nam quá dễ dàng, trên 80% đơn hàng của chúng tôi bị đánh cắp do các hacker Việt Nam, chi một số nhỏ 20% còn lại là của các hacker nước ngoài" [30, tr.2].

Đúng như nhận xét của GS.TS. Nguyễn Xuân Yêm, trong vòng vài năm gần đây số lượng các vụ tội phạm trong lĩnh vực tin học ngày càng tăng mạnh với phạm vi tác động rộng lớn, đối tượng tấn công dần chuyển sang các hệ thống thương mại điện tử, hệ thống thanh toán tự động với thủ đoạn ngày càng tinh vi, phức tạp [36, tr.6].

Theo thống kê của Trung tâm An ninh mạng Đại học Bách khoa Hà Nội (BKIS), hiện nay Việt Nam có khoảng 4 triệu máy tính, trong đó một năm có tới trên 33 triệu lượt máy tính bị nhiễm virus, trên 6.700 loại virus mới xuất hiện và gây thiệt hại tới 2.400 tỷ đồng. Số virus ngày càng tăng vọt; các vụ tấn công tổ chức bài bản, chuyên nghiệp, quy mô, kín đáo hơn và thiệt hại cũng lớn hơn. Đặc biệt, tỷ lệ những cuộc tấn công nhằm mục đích kiếm tiền trong năm 2007 hơn hẳn một vài năm trước và đã có 224 website Việt bị hacker tấn công, chủ yếu là các website của doanh nghiệp, Bộ, ngành, trong đó có cả những công ty tên tuổi

trong làng CNTT [45].

Vụ án Nguyễn Anh Tuấn (SN 1986, quê Hà Tĩnh, trú tại tập thể Thành Công, Hà Nội) và đồng bọn tấn công website, giả mạo email để lừa đảo, lấy trộm hàng tỉ đồng là một vụ án tiêu biểu của những tội phạm lợi dụng CNTT kiếm tiền bất chính. Là những sinh viên, cựu sinh viên am hiểu về công nghệ thông tin, từ giữa năm 2004, Tuấn và các đối tượng đã bàn nhau tấn công vào một số trang web bán hàng trực tuyến trên mạng internet, lấy trộm địa chỉ thư điện tử của khách hàng. Sau đó, chúng dùng thư điện tử của chính những trang web này gửi đến các khách hàng, yêu cầu họ khai báo các thông tin chủ thẻ. Những thông tin lấy cắp được, Tuấn và đồng bọn đưa vào đầu đọc dữ liệu để in thẻ rút tiền giả từ thẻ trắng.

Cơ quan CSĐT đã chứng minh được từ tháng 10/2005 đến cuối tháng 12/2005, Nguyễn Anh Tuấn đã rút trộm gần 1 tỉ đồng, trong đó chiếm hưởng 444 triệu đồng; Nguyễn Đình Cường (SN 1986, trú tại quận 3, TPHCM) rút được 516 triệu đồng và 17.000 USD…[46].

Vụ án Vũ Ngọc Hà ở Hải Phòng cũng là một điển hình tương tự. Vũ Ngọc Hà (SN 1981 ở số 3 D28 Đồng Quốc Bình, Ngô Quyền, Hải Phòng) là một người có hiểu biết tin học và say mê internet. Nhờ làm quen được với một số hacker nước ngoài trên mạng Hà đã có các thông tin về tài khoản của một số người đăng ký dịch vụ chuyển tiền trực tuyến trên mạng. Hà tung virus (Keylogger) vào các địa chỉ e-mail của họ, kích hoạt virus làm cho các thông tin về tài khoản tín dụng được gửi đến e-mail của Hà. Nhiều khách hàng đăng ký tài khoản tại dịch vụ chuyển tiền trực tuyến trên mạng đã bị lộ thông tin và mật khẩu truy cập. Vũ Ngọc Hà thường sử dụng, thực hiện các lệnh chuyển tiền đến bất kỳ địa chỉ nào theo ý mình. Bằng phương thức đó, từ năm 2004 đến 2006, Vũ

Ngọc Hà đã chiếm đoạt được hơn 400 triệu đồng [47].

Cũng bằng thủ đoạn truy cập trái phép và trộm cắp thông tin về tài khoản tín dụng trực tuyến, Nguyễn Ngọc Lâm, trú tại đường Bắc Nam, thành phố Thái Nguyên và Nguyễn Ngọc Thành, trú tại đường 3/2, phường 14, quận 10, TP.HCM đã thu lợi bất chính gần 300.000 USD và bán lại thông tin về các tài khoản này gây thiệt hại gấp nhiều lần [48].

Các thủ phạm Hà, Tuấn, Lâm, Thành trong những vụ án nói trên chủ yếu sử dụng phương thức mua hàng qua mạng để tiêu thụ số tiền do phạm tội mà có.

Cũng lợi dụng hoạt động giao dịch trực tuyến trên mạng để phạm tội nhưng vụ án Đỗ Giang Nam chiếm đoạt tiền của ngân hàng Nông nghiệp và phát triển nông thôn lại có thủ đoạn khác. Nam là giám đốc một công ty tin học nên có trình độ tin học rất tốt. Nam không đánh cắp thông tin tài khoản khách hàng như các trường hợp trên mà đột nhập trực tiếp vào hệ thống giao dịch điện tử của ngân hàng Nông nghiệp và phát triển nông thôn Việt Nam để ra lệnh chuyển tiền ảo từ chi nhánh ngân hàng này ở Hải Phòng đến các chi nhánh tại Ninh Bình, Thái Bình để chiếm đoạt trên 1,4 tỷ đồng [49].

- Tội phạm trong lĩnh vực tin học ở Việt Nam tấn công các hệ thống thương mại điện tử vì mục đích phá hoại uy tín doanh nghiệp, cạnh tranh không lành mạnh.

Năm 2006 là năm được coi là năm "điêu đứng" của hệ thống thương mại điện tử vốn non kém tại Việt Nam. Vào tháng 3/2006: Website chuyên về thương mại điện tử của công ty Vietco JSC bị tấn công DDoS nặng nề. Tất cả dịch vụ đình trệ suốt một tháng dẫn đến nguy cơ doanh nghiệp có thể bị phá sản hoàn toàn.

Vụ việc chưa lắng xuống, thì tháng 7/2006, hacker liên tục tấn công từ

chối dịch vụ (DDoS) vào hệ thống máy chủ của công ty Nhân Hòa - (Công ty cung cấp dịch vụ Hosting và Domain có trụ sở tại Hà Nội). Vụ tấn công này khiến toàn bộ hệ thống của Nhân Hòa bị quá tải và hơn 300 website của các doanh nghiệp thuê máy chủ của Nhân Hòa ngừng hoạt động. Lượng khách hàng của công ty ngày càng giảm, uy tín của công ty cũng bị ảnh hưởng nghiêm trọng.

Mặc dù sau đó thủ phạm hai vụ tấn công trên đã bị cơ quan chức năng bắt giữ nhanh chóng, nhưng đến tháng 9/2006, vụ tấn công lớn nhất trong giới CNTT Việt Nam cho tới thời điểm đó vẫn xảy ra một cách cố ý. Nạn nhân vụ tấn công này là trang web thương mại trực tuyến chodientu.com của Công ty giải pháp phần mềm Hòa bình PeaceSoft. Vào đêm ngày 22.09.2006, từ một máy tính đặt tại nhà, thủ phạm đã thực hiện kết nối vào máy chủ PeaceSoft.net của công ty PeaceSoft đặt tại một nhà cung cấp dịch vụ Internet. Sau khi kết nối thành công, thủ phạm đã sử dụng chính máy chủ này để tiếp tục thực hiện các hành vi phá hoại. Vụ phá hoại đã làm hàng loạt các tên miền trong hệ thống Chợ điện tử của Cty PeaceSoft là chodientu.com, chodientu.net, chodientu.com.vn, chodientu.vn … bị trỏ về địa chỉ 69.37…80. Các khách hàng khi truy cập một trong các website này của công ty PeaceSoft sẽ bị chuyển hướng đến website tại địa chỉ 69.37….80, tại đây có nội dung bôi nhọ danh dự cá nhân nhằm vào ông Nguyễn Hòa Bình – Giám đốc của Cty PeaceSoft. Ngay sau khi phát hiện, PeaceSoft đã nhanh chóng tiến hành khắc phục sự cố. Tuy nhiên các hoạt động của công ty này đã bị ảnh hưởng nặng nề và còn kéo dài nhiều ngày sau đó. Thậm chí hacker còn phát tán mã độc thông qua tên miền chodientu.com bị cướp, khiến VNCERT phải ra chỉ đạo khẩn yêu cầu ngăn chặn truy cập từ người dùng trong nước đến địa chỉ chứa virus [38].

Các nạn nhân của ba vụ tấn công này là ông Nguyễn Hoà Bình (giám đốc PeaceSoft - chodientu.com), ông Phùng Minh Bảo (giám đốc VietCo JSC) và ông Vũ Trung (giám đốc Nhân Hoà) đều cho rằng đang có một xu hướng lợi dụng không gian mạng để tấn công DDoS hoặc hack vì mục đích cạnh tranh không lành mạnh từ chính các doanh nghiệp thương mại điện tử.

Điều này cũng được nhắc lại trong báo cáo mang tên "Tăng cường phối hợp phòng chống tội phạm thương mại điện tử" của VNCERT tại hội thảo "Các hành vi vi phạm, tội phạm trong thương mại điện tử" ngày 9/11/2006. Báo cáo này khẳng định xu hướng đầu tiên trong bốn xu hướng cạnh tranh không lành mạnh từ phía các doanh nghiệp thương mại điện tử Việt Nam là "Thuê Hacker phá hoại hoạt động thương mại điện tử của đối thủ".

- Tội phạm trong lĩnh vực tin học truyền bá các dạng thông tin đồi trụy, xâm phạm bí mật đời tư, bôi nhọ danh dự người khác tràn lan trên mạng internet.

Khả năng cung cấp và truyền tải thông tin khổng lồ của mạng internet đã tạo điều kiện hết sức thuận lợi cho tội phạm phát tán rộng rãi các thông tin, hình ảnh đồi trụy. Hiện nay có hàng chục website tiếng Việt chứa đầy những đoạn phim, hình ảnh, truyện đọc, truyện tranh đồi trụy, trong đó có những trang có hàng triệu thành viên. Nhưng trang này thông thường là miễn phí và không yêu cầu phải đăng ký thành viên nên việc xem hay tải về những nội dung đồi trụy đó không thể kiểm soát được. Những thông tin đồi trụy, nhảm nhí đó đã đầu độc nghiêm trọng quá trình hoàn thiện nhân cách của thanh niên Việt Nam. Không những có cái nhìn thiếu lành mạnh về vấn đề sinh lý mà có nhiều người trong số họ đã trở thành bệnh hoạn, phạm tội hiếp dâm…

Trong mấy năm gần đây cũng đã có hàng loạt vụ tung lên mạng những

cảnh sinh hoạt phòng the của nhiều cá nhân. Từ những cảnh quay lén, chụp chộp của những người bình thường đến chuyện riêng tư của những ngôi sao nghệ thuật nổi tiếng. Điển hình như các vụ tung lên mạng những đoạn phim sex của ca sĩ Hồng Nhung, các diễn viên Yến Vi, Ngô Thanh Vân, Hoàng Thùy Linh... Hiện tượng này không chỉ xâm phạm đời tư, làm mất danh dự của những nhân vật trong đó mà còn ảnh hưởng nghiêm trọng đến thuần phong, mỹ tục.

- Các hành vi phạm tội trong lĩnh vực tin học với mục đích đơn thuần nhằm gây rối, phá hoại an ninh công nghệ thông tin cũng trở nên táo tợn và để lại hậu quả trên phạm vi rộng hơn.

Theo thống kê của Trung tâm an ninh Mạng BKIS thuộc Đại học Bách khoa Hà Nội, chỉ trong tháng 7/2006 có đến 185.000 máy tính ở Việt Nam bị nhiễm virus Rontokbro. Hai tháng sau con số này đã lên tới trên nửa triệu máy tính [37]. Cũng trong năm 2006, một loại virus có tên là Xrobot được tung lên mạng bởi một học sinh phổ thông ở Hải Phòng đã lây nhiễm cho hơn 10.000 máy tính chỉ trong hai ngày [57] …

Ngoài việc ảnh hưởng trực tiếp đến công việc của những người sử dụng (do máy tính khi bị nhiễm virus này sẽ chạy rất chậm và thỉnh thoảng tự khởi động lại), sự lây lan của các loại virus còn ảnh hưởng nặng nề đến tài nguyên của cả hệ thống mạng, gây tốn băng thông, tắc nghẽn đường truyền… Thậm chí, virus sẽ làm chủ máy tính người dùng, có thể xóa, ăn cắp dữ liệu, mật khẩu....

Các hành vi gây rối trên mạng cũng ngày càng táo tợn. Đối tượng bị tấn công có thể là bất kỳ hộp thư điện tử cá nhân, website của doanh nghiệp hoặc ngay cả website của cơ quan Chính phủ. Đáng chú ý nhất là vụ một học sinh tên là Bùi Minh Trí ở Vĩnh Long đã tấn công làm ngừng hoạt động

website của Bộ GD-ĐT (www.moet.gov.vn) và thay ảnh của Bộ trưởng bằng ảnh một thanh niên cởi trần vào ngày 27.11.2006.

Từ những diễn biến thực tế trên, có thể khái quát về ***đặc điểm tình hình tội phạm trong lĩnh vực tin học ở Việt Nam*** như sau:

Tội phạm trong lĩnh vực tin học mới xuất hiện ở Việt Nam khoảng 10 năm nhưng *tình hình ngày càng diễn biến xấu hơn*. Khi tội phạm này mới xuất hiện mục đích phạm tội chủ yếu là quấy phá an ninh CNTT. Nhưng hiện nay, ngoài mục đích gây rối đơn thuần, tội phạm này đã chuyển hướng sang những mục đích xấu xa hơn như đánh cắp thông tin, trộm cắp tiền từ các tài khoản trực tuyến, lừa đảo, rửa tiền, cạnh tranh không lành mạnh, truyền bá thông tin, phim ảnh có nội dung xấu, phản động… Tuy hiện nay tội phạm trong lĩnh vực tin học ở Việt Nam hầu như chưa hướng tới những mục tiêu chính trị như khủng bố hoặc đánh cắp thông tin bí mật nhà nước nhưng nếu không có biện pháp ngăn chặn kịp thời thì xu hướng này cũng có thể sẽ xuất hiện trong tương lai không xa.

Tình hình *tội phạm ẩn chiếm phần lớn* đối với các tội phạm trong lĩnh vực tin học. Rất nhiều vụ tấn công website, lan truyền virus, lừa đảo, chiếm đoạt tài sản trên mạng diễn ra trót lọt mà thủ phạm không bị phát hiện. Nguyên nhân có thể do bản thân các nạn nhân không tố cáo hoặc cơ quan chức năng không điều tra, phát hiện được bởi tính chất tinh vi, phức tạp của các hành vi phạm tội trên môi trường ảo.

Cũng như trên thế giới, *thủ phạm gây ra các tội phạm trong lĩnh vực tin học ở Việt Nam thường có tuổi đời trẻ*. Để thực hiện được tội phạm trong lĩnh vực này đòi hỏi thủ phạm phải có trình độ chuyên môn CNTT ở mức độ cao. Tin học mới phát triển mạnh ở Việt Nam khoảng 10 năm nên thế hệ được tiếp cận và có khả năng sử dụng những ứng dụng phức tạp của ngành khoa học này chủ yếu

được sinh ra từ những năm 70 của thế kỷ XX trở lại đây.

Thủ đoạn phạm tội của các tội phạm trong lĩnh vực tin học ngày càng tinh vi. Ban đầu tội phạm trong lĩnh vực tin học chỉ đơn thuần là sao chép các loại virus có sẵn trên mạng rồi gửi kèm vào email. Tốc độ lan truyền của các virus này chậm và chỉ có khả năng gây rối loạn, gián đoạn hoạt động thông tin trong phạm vi nhỏ. Tuy nhiên, chỉ mấy năm sau các hacker Việt Nam thậm chí còn học phổ thông đã có khả năng tạo ra những loại virus làm tê liệt được hàng vạn máy tính nối mạng trong một ngày. Với khả năng trao đổi thông tin cực lớn của Internet, tội phạm trong lĩnh vực tin học đã lập nên các nhóm, câu lạc bộ, hội nhập với cộng đồng tội phạm trong lĩnh vực tin học quốc tế để trao đổi về kinh nghiệm, phương tiện cũng như thành quả phạm tội. Hacker Việt Nam ngày nay có thể dễ dàng làm tê liệt website của các cơ quan, doanh nghiệp, ngay cả doanh nghiệp hoạt động trong lĩnh vực tin học. Họ có khả năng giả mạo cả những website uy tín; lừa đảo bằng nhiều phương thức phức tạp; đột nhập, đánh cắp, hủy hoại cơ sở dữ liệu trên máy tính; truyền bá nhanh chóng những thông tin xấu đi toàn thế giới một cách nhanh chóng…

Với những diễn biến xấu như vậy, tội phạm trong lĩnh vực tin học đã gây tổn thất rất lớn cho nhà nước, tổ chức, cá nhân và nếu không có giải pháp ngăn chặn thì khả năng gây thiệt ngày sẽ càng lớn hơn trong quá trình tin học hóa mọi hoạt động kinh tế, xã hội nước ta hiện nay.

2.2.1.2. Thực tiễn xử lý tội phạm trong lĩnh vực tin học

Như đã đề cập ở trên, tình trạng tội phạm ẩn chiếm tỉ lệ lớn đối với các tội phạm trong lĩnh vực tin học ở Việt Nam. Có hai nguyên nhân chủ yếu dẫn tới tình trạng đó: Thứ nhất là do tội phạm này diễn ra trong môi trường ảo với thủ

đoạn tinh vi, phức tạp nên khó điều tra, phát hiện và xử lý. Thứ hai là số lượng nạn nhân của mỗi vụ phạm tội trong lĩnh vực tin học thường rất đông nhưng lại ít khi có cá nhân, tổ chức nào trong số đó tố cáo với cơ quan chức năng trừ khi bị tổn thất nặng nề.

Mặc dù vậy, cũng không thể phủ nhận những thành quả đã đạt được của các cơ quan chức năng trong đấu tranh xử lý tội phạm trong lĩnh vực tin học. Tỉ lệ điều tra ra và xử lý thủ phạm trong những vụ gây rối an ninh CNTT nói chung mà không nhằm tấn công đích xác vào đối tượng nào rất thấp so với thực tế diễn ra. Nhưng ngược lại, những vụ phạm tội có đối tượng xâm hại rõ ràng đã được các cơ quan chức năng phát hiện và xử lý tương đối kịp thời. Ví dụ như các vụ đánh cắp thông tin về tài khoản để rút trộm tiền đã nêu trên, các thủ phạm như Nguyễn Anh Tuấn và 9 đồng bọn, Vũ Ngọc Hà, Nguyễn Ngọc Lâm, Nguyễn Ngọc Thành… đều bị bắt giữ và xử lý. Thủ phạm của các vụ tấn công 3 website thương mại điện tử năm 2006; tập đoàn lừa đảo qua mạng Colony; thủ phạm tung lên mạng phim sex của Yến Vi, Hồng Nhung, Hoàng Thùy Linh; tác giả tạo ra và lan truyền virus Xrobot… đều đã nhanh chóng bị phát hiện, xử lý. Đó là nhờ những nỗ lực không ngừng của các cơ quan bảo vệ pháp luật trong điều kiện còn hạn chế cả về nhân lực, phương tiện đáp ứng cho yêu cầu đấu tranh với tội phạm thời công nghệ hiện đại.

Tuy đã đạt được những thành quả nhất định nhưng không thể phủ nhận một thực tế là công tác đấu tranh, xử lý tội phạm trong lĩnh vực tin học còn nhiều hạn chế, vướng mắc:

Hạn chế trong công tác điều tra, phát hiện tội phạm: Công tác điều tra, phát hiện tội phạm trong lĩnh vực tin học hiện nay kém hiệu quả. Phép so sánh sau có thể cho thấy tính kém hiệu quả đó. Ví dụ như trong vụ tấn công từ chối

dịch vụ hệ thống máy chủ của công ty Nhân Hòa làm cho website của khoảng 300 doanh nghiệp khác ngừng hoạt động. Thiệt hại do gián đoạn hoạt động kinh doanh của Nhân Hòa và hàng trăm công ty chỉ tính từng ngày đã không phải là con số nhỏ. Vậy nhưng tốc độ điều tra của cơ quan chức năng lại tính bằng tháng nên đến khi ngăn chặn được thì hậu quả về kinh tế đã cực lớn. Đó là chưa kể đến rất nhiều vụ phạm tội diễn ra trót lọt mà thủ phạm không bị phát hiện.

Hạn chế trong việc xác định tội danh và khung hình phạt: Các cơ quan tiến hành tố tụng hiện nay thường vướng mắc và không thống nhất quan điểm trong xác định tội danh cũng như mức hình phạt đối với các tội phạm trong lĩnh vực tin học. Các tội phạm trong lĩnh vực tin học diễn ra trong môi trường ảo lại có khách thể tác động rất đa dạng dẫn đến cơ quan chức năng lúng túng trong việc xác định tội danh. Ví dụ hành vi đánh cắp thông tin về tài khoản rồi lại ngang nhiên rút tiền từ tài khoản đó mà định tội danh là "trộm cắp tài sản" – hành vi có tính chất lén lút dường như không đúng hoàn toàn về bản chất. Hoặc có thể đã xác định được tội danh nhưng cơ quan công tố, xét xử cũng không biết đề nghị và phán quyết khung hình phạt nào trong điều luật quy định về tội danh đó bởi vì vấn đề xác định hậu quả của tội phạm trong lĩnh vực tin học rất khó. Ví dụ một virus máy tính được lan truyền tới hàng triệu máy tính nhưng có thể chỉ gây tác hại ở mức độ làm chậm hoạt động của những máy tính này. Ngược lại, có virus lan truyền trong phạm vi hẹp hơn nhưng lại làm mấy toàn bộ cơ sở dữ liệu trong các máy tính bị nhiễm hoặc gây lộ những thông tin bí mật của cá nhân, tổ chức… Trong những tình huống như thế, không ai có thể so sánh hay xác định chính xác được hậu quả.

Hạn chế trong việc áp dụng quy định pháp luật hình sự: Hạn chế này xuất phát từ nguyên nhân chủ yếu là sự thiếu sót của chính các quy định pháp

luật hình sự. Đại đa số các hành vi vi phạm pháp luật trong lĩnh vực tin học hiện nay không xử lý được về hình sự. Sở dĩ như vậy vì cấu thành các tội này yêu cầu yếu tố gây hậu quả nghiêm trọng mà như đã đề cập, hậu quả của tội phạm trong lĩnh vực tin học rất khó xác định. Đa số các cuộc tấn công trên mạng trong năm 2006 đều được làm rõ, nhưng thủ phạm chỉ bị xử lý hành chính với mức tiền phạt 10-20 triệu đồng trong khi hành vi của họ gây thiệt hại, đình đốn hoạt động của hàng trăm doanh nghiệp, cơ quan. Bên cạnh đó, việc áp dụng quy định hiện hành về các tội phạm truyền thống để xử lý tội phạm trong lĩnh vực tin học cũng không thích đáng vì tính chất nguy hiểm và phạm vi tác động của tội phạm này lớn hơn nhiều lần (ví dụ, một vụ lừa đảo truyền thống có đến vài trăm nạn nhân là nhiều nhưng vụ lừa đảo trên mạng của tập đoàn Colony giả có đến hàng chục nghìn nạn nhân.)

2.2.2. Nguyên nhân hạn chế trong xử lý tội phạm tin học tại Việt Nam

Hạn chế trong xử lý tội phạm trong lĩnh vực tin học xuất phát từ nhiều nguyên nhân cả chủ quan và khách quan.

Nguyên nhân thứ nhất xuất phát từ đặc thù của tội phạm trong lĩnh vực tin học. Tội phạm trong lĩnh vực tin học diễn ra trên trong không gian điều khiển, các chứng cứ, dấu vết của tội phạm chỉ được để lại trong môi trường ảo đó. Thủ đoạn phạm tội hết sức tinh vi, phức tạp với những phương tiện đặc biệt hiện đại. Do vậy công tác điều tra, phát hiện tội phạm này rất khó khăn và đòi hỏi trình độ am hiểu về CNTT ở mức độ cao.

Hậu quả do tội phạm trong lĩnh vực tin học gây ra rất đa dạng và khó xác định. Thiệt hại do tội phạm này gây ra có thể về kinh tế, có thể về văn hóa, danh dự, uy tín của cá nhân, tổ chức… Một virus có thể lan truyền tới hàng triệu máy

tính nhưng không ai có thống kê và mức độ thiệt hại đối với mỗi máy tính bị nhiễm cũng không được khai báo. Hay phạm vi ảnh hưởng của việc phát tán phim ảnh đồi trụy qua internet không thể xác định được. Trong khi đó vấn đề xác định hậu quả của tội phạm lại có ảnh hưởng trực tiếp đến việc đưa ra biện pháp xử lý thích hợp.

Khách thể của tội phạm trong lĩnh vực tin học cũng rất đa dạng. Quá trình tin học hóa đang diễn ra trên mọi lĩnh vực kinh tế xã hội nên tội phạm trong lĩnh vực tin học có thể tấn công vào tất cả những lĩnh vực đó. Vậy nên, việc xác định tội danh đối với tội phạm này có nhiều khó khăn. Ví dụ như hành vi tấn công làm tê liệt một website của cơ quan nhà nước rất khó xác định được là hành vi quấy rối thông thường hay hành vi chống phá nhà nước. Tương tự như vậy với một website của doanh nghiệp cũng khó xác định được chỉ là quậy phá hay có tính chất trục lợi kinh tế, cạnh tranh không lành mạnh…

Nguyên nhân thứ hai là do thiếu sót của hệ thống các quy phạm pháp luật đang điều chỉnh tội phạm trong lĩnh vực tin học. Những quy định hiện nay của BLHS cũng như các luật có liên quan còn lạc hậu so với sự phát triển của tội phạm trong lĩnh vực tin học cũng như chưa đầy đủ để làm cơ sở pháp lý cho công tác đấu tranh với tội phạm này. Bản thân những quy định hiện có cũng còn chưa được hiểu thống nhất và khó khăn trong áp dụng (vấn đề này được phân tích cụ thể ở chương 3 luận văn)

Nguyên nhân thứ ba dẫn đến những hạn chế đó là ý thức về đề phòng và đấu tranh chống tội phạm trong lĩnh vực tin học của người dân chưa cao. Hầu hết các cơ quan, tổ chức, cá nhân sử dụng các ứng dụng CNTT hiện nay chưa quan tâm và đầu tư đúng mức cho an ninh, bảo mật thông tin. Bên cạnh đó, tinh thần cảnh giác của của người dùng internet cũng chưa cao. Đáng lẽ phải đề

phòng với các email, tin nhắn, đề nghị đầu tư, lời chào hàng khác thường nhưng mọi người lại thường bị tâm lý tò mò, hám lợi đánh lừa. Khi đã trở thành bị hại, các cá nhân, tổ chức cũng không có ý thức cao trong việc tố giác, đấu tranh với tội phạm. Đại đa số các tin báo, tố giác về phạm trong lĩnh vực tin học mà cơ quan công tố nhận được là từ cơ quan điều tra chứ không phải từ những cá nhân, tổ chức bị tội xâm hại hay quần chúng nhân dân [23, tr.94].

Nguyên nhân thứ tư là điều kiện vật chất và phương tiện trang bị cho công tác đấu tranh chống tội phạm trong lĩnh vực tin học chưa đảm bảo. Do điều kiện kinh tế nên đầu tư vật chất và các phương tiện kỹ thuật cao cho các cơ quan có trách nhiệm đấu tanh, xử lý tội phạm trong lĩnh vực tin học ở nước ta chưa được cao. Trong khi đó lại phải đối mặt với lực lượng tội phạm trong lĩnh vực tin học đông đảo cả trong nước và ngoài nước vốn có trình độ tin học cao lại có điều kiện trao đổi, phổ biến về phương thức, công cụ phạm tội trên quy mô toàn cầu, thậm chí được sự hỗ trợ về mọi mặt của các tổ chức tội phạm, tổ chức phản động chống phá Việt Nam.

Nguyên nhân thứ năm là do trình độ chuyên môn CNTT của đội ngũ cán bộ tiến hành tố tụng chưa đáp ứng được yêu cầu công tác đấu tranh, xử lý tội phạm trong lĩnh vực tin học. Phần lớn đội ngũ này được trang bị kiến thức tin học cơ bản nhưng những kiến thức này chỉ đủ để sử dụng các trang thiết bị phục vụ công việc văn phòng. Kiến thức chuyên sâu về CNTT để có thể thực hiện nhiệm vụ phát hiện, điều tra, truy tố, xét xử tội phạm trong lĩnh vực tin học vẫn rất hạn chế. Đặc biệt là lực lượng cán bộ điều tra chuyên về các tội phạm này còn mỏng, nhiệm vụ điều tra tội phạm được giao cho Phòng chống tội phạm công nghệ cao thuộc Cục cảnh sát điều tra các tội phạm kinh tế Bộ công an. Lực lượng chuyên trách này mới được thành lập, hạn chế cả về cơ sở vật chất, nhân

lực lẫn bề dầy công tác: đội ngũ cán bộ ít, những người có kinh nghiệm điều tra thì chưa được đào tạo căn bản về CNTT, ngược lại những người được đào tạo căn bản về CNTT lại từ các trường đào tạo bên ngoài chuyển vào lực lượng điều tra.

2.3. Quy định pháp luật và kinh nghiệm đấu tranh xử lý tội phạm trong lĩnh vực tin học ở một số nước trên thế giới

2.3.1. Quy định pháp luật về tội phạm trong lĩnh vực tin học của một số nước trên thế giới

Khoảng gần 10 năm trước thế giới đã được chứng kiến nhiều vụ không thể kết tội các hacker do thiếu cơ sở pháp lý .Chẳng hạn như ở Các tiểu vương quốc Ả rập Thống nhất (UAE) ngày 1/7/2001, một người Anh (Lee Ashurst, 22 tuổi) bị kết tội tấn công nhà cung cấp dịch vụ Internet (ISP) duy nhất của Các tiểu vương quốc Ả rập Thống nhất, Etisalat, khiến hệ thống của họ thường bị xung đột trong 2 tháng liền. Lee đã đưa đơn kháng án lên tòa phúc thẩm UAE với lý do tòa sơ thẩm đã khép tội anh khi ở UAE chưa có điều luật nào quy định hacking là một tội lỗi [50].

Hay ở Argentina, ngày 16/4/2002, một quan toà phán quyết rằng hacking là hợp pháp bởi pháp luật Argentina bao trùm mọi tội phạm chống lại con người, sự việc và loài vật, nhưng không hề đề cập đến không gian mạng. Vị thẩm phán đã đưa ra quyết định của mình sau khi xem xét hành vi của một nhóm người đột nhập và thay đổi website của Toà án tối cao. Đây là trường hợp xét xử tội phạm máy tính đầu tiên ở Argentina. Luật pháp Argentina không bảo vệ website, nên việc đột nhập vào website là không phạm pháp, vị thẩm phán giải thích khi tuyên bố những bị cáo kia vô tội [51].

Ở Philippin, Onel de Guzman - tác giả virus Tình Yêu làm náo loạn thế giới năm 2000 đã bị kết tội ăn cắp thẻ tín dụng vì ở nước này không có đạo luật chống virus. Nhưng sau đó nhà cầm quyền phải miễn cưỡng rút lại buộc tội này vì điều luật về tội ăn cắp thẻ tín dụng không thể áp dụng cho trường hợp này khi mà hành vi của Onel de Guzman chỉ là phát tán virus chứ không liên quan gì đến thẻ tín dụng.

Tuy nhiên, đó đã là quá khứ. Ngày nay, trước sự phát triển mạnh mẽ của các ứng dụng CNTT và tình trạng bùng nổ tội phạm trong lĩnh vực tin học, hầu hết các quốc gia đã chú ý tới việc xây dựng quy định pháp luật và các biện pháp khác nhau để phòng chống tội phạm này.

Nhiều nước đã ban hành các đạo luật riêng hoặc một số điều luật cụ thể trong Bộ luật hình sự ghi nhận về các tội phạm liên quan đến tin học để đấu tranh phòng chống. Ví dụ như theo Luật của Australia, hành vi phá hủy, xóa bỏ hoặc làm thay đổi dữ liệu lưu trữ trong máy tính hoặc đưa thêm dữ liệu vào máy vi tính một các bất hợp pháp có thể bị xử phạt đến 10 năm tù hoặc có thể bị phạt đến 48 nghìn USD [31].

Ở Nhật Bản, BLHS nước này đã dành một số điều luật quy định về các hành vi phạm tội liên quan đến lĩnh vực tin học, như: Tội làm giả dữ liệu điện từ và cung cấp dữ liệu ấy; Tội làm hư hại máy tính để cản trở nghiệp vụ; Tội lừa đảo bằng cách sử dụng máy tính... Trong đó, có tội có mức hình phạt nghiêm khắc là tù khổ sai đến 10 năm hoặc phạt tiền với mức tương đối cao [18, tr.48-49; tr.72-73; tr.75-76].

BLHS Liên bang Nga đã dành hẳn một Chương 28 quy định về các tội phạm trong lĩnh vực thông tin máy tính với ba điều luật cụ thể liên quan đến nhóm tội phạm này, như: Điều 268 - Tội sử dụng trái phép thông tin trong máy

vi tính; Điều 269 - Tội xây dựng, sử dụng và lan truyền các chương trình virus; Điều 270 - Tội vi phạm các quy định về vận hành hệ thống hay mạng vi tính [39].

Rumani ban hành một đạo luật riêng về chống tội phạm tin học (được Quốc hội Rumani thông qua năm 2003). Liên minh Châu âu còn xác lập cả Công ước quốc tế của Hội đồng châu Âu về tội phạm mạng năm 2004. Các nước thuộc khối thịnh vượng chung xây dựng cả luật về tội phạm trong lĩnh vực tin học cũng như luật về tố tụng đối với tội phạm này. Đó là Luật mẫu về tội phạm máy tính và liên quan đến máy tính; Luật mẫu về chứng cứ điện tử của các nước thuộc khối thịnh vượng chung [23, tr.204-228]...

2.3.2. Kinh nghiệm đấu tranh, xử lý tội phạm trong lĩnh vực tin học của một số nước trên thế giới.

Bên cạnh việc xây dựng, hoàn thiện quy định pháp luật làm cơ sở đấu tranh chống tội phạm trong lĩnh vực tin học, các nước trên thế giới cũng triển khai nhiều biện pháp khác nhằm nâng cao hiệu quả đấu tranh, xử lý tội phạm này.

Hầu hết các nước đã chú trọng xây dựng lực lượng chuyên đấu tranh chống tội phạm trong lĩnh vực tin học.

Nước Anh đã sớm xây dựng một *đội cảnh sát phòng chống tội phạm riêng trong lĩnh vực công nghệ cao* (NHTCU). Đội đặc nhiệm này có nhiệm vụ đấu tranh chống lại các tội phạm trực tuyến như hacker, lừa đảo, gieo rắc khiêu dâm trẻ em và bất kỳ hành vi phạm tội nào có liên quan đến máy tính [35].

Nhật bản cũng xây dựng một lực lượng cảnh sát đặc nhiệm trong lĩnh vực an ninh CNTT - Cyber Force. Lực lượng này được ví như đơn vị tinh nhuệ nhất

của Cảnh sát Nhật Bản trong đấu tranh và bảo vệ người dân, doanh nghiệp, cơ quan, tổ chức và chính phủ trước tội phạm công nghệ cao hoạt động xuyên biên giới. Cyber Force chính là cánh tay trợ giúp đắc lực cho công tác điều tra tội phạm tin học. Trung tâm xử lý thông tin của Cyber Force có nhiệm vụ thu thập và phân tích dữ liệu. Các thành viên của đội Cyber Force được đào tạo, huấn luyện thường xuyên về nghiệp vụ tin học tại phân viện đào tạo riêng (Cyber Force Training System) nhằm đảm bảo bắt kịp đà gia tăng của tội phạm công nghệ cao cũng như có thể thích ứng với mọi tình huống thực tế. Họ thường xuyên phải luyện tập và thực hành đối phó với tấn công bằng cách chia nhóm: một nhóm đóng giả là tội phạm công nghệ cao - phải cố gắng hết sức để hành động và tránh được cảnh sát và nhóm còn lại cũng hết sức nỗ lực tìm ra chân tướng tội phạm.Cách thực hành này có nhiều ưu điểm. Quan trọng hơn cả là chương trình đã đưa tất cả thành viên của Cyber Force vào tình huống thực tế nên hiểu rõ hơn về nghiệp vụ cũng như tâm lý của tội phạm từ đó tìm ra cách hóa giải tốt nhất [52].

Lực lượng tương tự được thành lập ở Nga với tên gọi Ủy ban bảo mật, ở Trung Quốc là Đội cảnh sát mạng...

Hàn Quốc còn thành lập một hệ thống Cơ quan điều tra tội phạm tin học bao gồm:

a) Trung tâm chỉ huy ứng phó với tội phạm tin học;

b) Ban điều tra tội phạm tin học;

c) Đội điều tra tội phạm tin học [33, tr.49].

Vấn đề hợp tác quốc tế đấu tranh chống tội phạm trong lĩnh vực tin học được đẩy mạnh trên thế giới.

Tổ chức Cảnh sát Quốc tế (Interpol) cũng đã thành lập nhiều *nhóm an ninh mạng*, phối hợp với đội ngũ chuyên gia mạng để chống các hình thức tội ác trong

thế giới mạng. Các nhóm này đã phối hợp theo khu vực Mỹ, Âu, Phi và Châu á-Thái Bình Dương. Mỗi nhóm bao gồm những người đứng đầu *đội đặc nhiệm chống tội ác tin học* (Information Technology Crime Unit-ITCU) của mỗi quốc gia. Mặc dù các đội đặc nhiệm ITCU này ở mỗi quốc gia có nhiều khác biệt, nhưng Interpol vẫn liên tục tổ chức trao đổi thông tin, cập nhật tình hình tội phạm, chia sẻ kinh nghiệm và huấn luyện các kỹ năng tin học cần thiết để các nhóm chiến đấu với tội phạm tin học và chiến thắng thế giới ngầm trên Internet. Trong đó, nhóm phối hợp Châu Á - Thái Bình Dương hình thành năm 1998 và Việt Nam trở thành thành viên từ năm 2002 [53].

Ngoài ra, cảnh sát toàn thế giới đã cùng nhau cam kết tiến hành cuộc đọ sức thực sự chống lại tội phạm mạng. Từ ngày 15 đến ngày 17/9/2004, gần 200 chuyên gia đến từ Châu Âu, Mỹ, Úc, Trung Quốc, Nhật Bản đã họp tại Strasbourg để bàn các giải pháp chống tội phạm mạng. Đặc biệt, Công ước của Châu Âu về tội phạm mạng đã có hiệu lực từ ngày 1/07/2004 nhằm tăng cường hợp tác về vấn đề trên [54].

Riêng đối với các nước ASEAN đã thành lập *nhóm chống tội phạm tin học*. Theo đó, Bộ trưởng viễn thông các quốc gia Đông Nam á đã quyết định thiết lập một hệ thống cảnh báo sớm để theo dõi những kẻ khủng bố sử dụng mạng máy tính để gây bất ổn trong khu vực. Do đó, việc hợp tác an ninh mạng của khối (ASEAN) sẽ được thành lập để làm nhiệm vụ "bảo vệ những thông tin và cơ sở hạ tầng thông tin" trong khu vực.

Biện pháp nâng cao ý thức phòng ngừa tội phạm cũng được sử dụng trong đấu tranh chống tội phạm trong lĩnh vực tin học

Ngày 24/2/2005 Chính phủ Anh đã cho thành lập một website cung cấp miễn phí các cảnh báo về virus giúp những người sử dụng máy tính có thể tránh

các virus nguy hiểm từ internet. Khi người dùng truy cập vào trang web (http://www.itsafe.gov.uk) và đăng ký, họ sẽ nhận được các lời khuyên về việc bảo mật các cơ sở dữ liệu và các cảnh báo virus để có thể phòng tránh. Các cảnh báo sẽ được gửi trực tiếp tới người dùng bằng email với các hướng dẫn cụ thể từng bước để xử lý tất cả các vấn đề. Website sẽ sử dụng các thông tin được cung cấp bởi trung tâm an ninh mạng quốc gia của Anh (NISCC) [55].

Phối hợp nhiều biện pháp cũng là một cách để nâng cao hiệu quả đấu tranh chống tội phạm trong lĩnh vực tin học

Song song với việc hình thành một hệ thống Cơ quan điều tra tội phạm tin học, Hàn Quốc còn áp dụng đồng bộ và có hệ thống một số biện pháp sau để tăng cường công tác điều tra và chất lượng công tác điều tra đối với tội phạm tin học, mà cụ thể là:

a) Tổ chức các khóa đào tạo cho các điều tra viên, công tố viên phụ trách điều tra tội phạm tin học. Hoạt động này do Viện Công tố tối cao và Viện nghiên cứu-đào tạo pháp vụ thuộc Bộ Tư pháp đảm nhiệm việc tổ chức tập huấn hoặc mời các chuyên gia giỏi các nước phát triển trên thế giới về đào tạo.

b) Thành lập Trung tâm quản lý tội phạm trên mạng Internet (ICIC). Nhiệm vụ của tổ chức này là bảo vệ cơ sở hạ tầng quốc gia và các hoạt động tư nhân trên mạng Internet và tiếp nhận, xử lý những lời đe dọa hoặc chống lại các cuộc tấn công vào cơ sở hạ tầng của Nhà nước.

c) Đầu tư trang thiết bị hiện đại nhất để phục vụ việc điều tra tội phạm tin học.

d) Thiết lập và giữ vững mối quan hệ chặt chẽ với cơ quan an ninh thông tin Hàn Quốc, với các cơ sở đào tạo đại học, các Viện nghiên cứu, các nhà cung cấp dịch vụ Internet trên đất nước để có thông tin và kiến thức chuyên ngành cập nhật, giảm bớt các nguy cơ có thể xảy ra trong công tác điều tra tội phạm tin học.

đ) Tăng cường hợp tác quốc tế trong việc phát hiện, phòng ngừa và trấn áp tội phạm tin học. Với sự tham gia của Hàn Quốc vào Hội nghị quốc tế được tổ chức tại Mỹ và là thành viên một cơ quan với tên gọi "*Địa điểm liên lạc quốc tế về tội phạm công nghệ cao 24/24h*" tháng 12/2000 đã góp phần quan trọng như là một phương tiện để hỗ trợ và phối hợp điều tra và xử lý tội phạm tin học [33, tr.50-55]

Những hướng xây dựng pháp luật, giải pháp, kinh nghiệm trong đấu tranh phòng chống tội phạm trong lĩnh vực tin học của các nước trên thế giới được nêu trên có thể là bài học bổ ích cho Việt Nam tham khảo trong công tác đấu tranh, xử lý tội phạm này tại Việt Nam.

CHƯƠNG 3. VẤN ĐỀ HOÀN THIỆN QUY ĐỊNH PHÁP LUẬT HÌNH SỰ VỀ CÁC TỘI PHẠM TRONG LĨNH VỰC TIN HỌC VÀ MỘT SỐ GIẢI PHÁP PHỐI HỢP TRONG ĐẤU TRANH PHÒNG CHỐNG LOẠI TỘI PHẠM NÀY

3.1. Hoàn thiện các quy định của pháp luật hình sự Việt Nam về các tội phạm trong lĩnh vực tin học

3.1.1. Sự cần thiết phải hoàn thiện các quy định của pháp luật hình sự Việt Nam về các tội phạm trong lĩnh vực tin học

Như đã nêu ở phần nguyên nhân hạn chế trong xử lý tội phạm trong lĩnh vực tin học hiện nay, các quy định pháp luật làm cơ sở đấu tranh chống tội phạm này của Việt Nam còn nhiều thiếu sót và lạc hậu so với tình hình tội phạm.

Mặc dù khi soạn thảo BLHS năm 1999 thì tội phạm công nghệ cao ở Việt Nam mới chỉ vừa xuất hiện nhưng các nhà lập pháp Việt Nam đã kịp thời đưa vào bộ luật 3 điều luật về tội phạm trong lĩnh vực tin học. Về mặt lý luận điều đó đã thể hiện được sự nhạy bén của các nhà lập pháp Việt Nam. Tuy nhiên, lần đầu tiên quy định về một loại tội phạm có đặc trưng hoàn toàn khác biệt các loại tội phạm truyền thống nên BLHS năm 1999 không thể tránh khỏi những thiếu sót.

Vấn đề đầu tiên là vị trí của những quy định về tội phạm trong lĩnh vực công nghệ thông tin hiện nay chưa được các nhà lập pháp đánh giá đúng. Trong BLHS 1999, ba điều về tội phạm trong lĩnh vực tin học được đặt chung với các quy định về các tội xâm phạm trật tự công cộng, an toàn công cộng trong chương XIX. Điều đó không hợp lý khi mà tội phạm trong lĩnh vực tin học là những tội phạm rất nguy hiểm, có khả năng gây hậu quả đặc biệt nghiêm trọng cả về quy mô và tính chất, chúng có phạm vi khách thể rất lớn, biểu hiện về mặt khách quan khác với những tội phạm đã từng có trong lịch sử.

Vấn đề thứ hai là các quy định này lạc hậu so với thực tế phát triển của tội phạm trong lĩnh vực tin học. Ba điều luật trong BLHS hiện nay chỉ phản ánh được một phần rất nhỏ trong số những hành vi phạm tội trong lĩnh vực tin học. Điều 224, 225, 226 mới chỉ đề cập đến những tội phạm tấn công trực tiếp vào dữ liệu máy tính, an ninh thông tin trong máy tính, hệ thống máy tính (tức là nhóm I của các tội phạm trong lĩnh vực tin học). Mà theo đánh giá của các nhà tội phạm học thế giới thì loại tội phạm này hiện nay chỉ còn là thiểu số. Tội phạm công nghệ cao không đơn thuần tấn công dữ liệu máy tính, an ninh thông tin trong máy tính, hệ thống máy tính với mục đích quậy phá, đùa nghịch như khi mới xuất hiện. Tội phạm công nghệ cao hiện nay hướng tới những mục tiêu chủ yếu như lợi nhuận, mưu đồ chính trị và các ý đồ phi pháp khác.

Vấn đề thứ ba các quy định hiện hành có tính chất chung chung gây khó áp dụng. Ví dụ như Điều 225 Bộ luật Hình sự quy định về tội vi phạm các quy định về vận hành, khai thác, sử dụng mạng máy tính điện tử. Những hành vi vi phạm các quy định về vận hành, khai thác, sử dụng mạng máy tính điện tử ở đây bao gồm rất nhiều hành vi khác nhau. Thậm chí, còn bao gồm cả những hành vi được quy định tại điều 224 và 226. Đó là một quy định mang tính tổng hợp dễ gây ra một hình dung là nó giống như một chiếc túi để người ta gói vào mọi hành vi phạm tội chưa được định danh trong lĩnh vực này.

Vấn đề thứ tư là yêu cầu về cấu thành của tội phạm trong các quy định này dẫn đến khó xử lý tội phạm trong lĩnh vực tin học. Cả ba Điều 224, 225 và 226 đều quy định nếu hành vi chưa gây hậu quả nghiêm trọng thì người có hành vi đó chỉ bị truy cứu TNHS khi đã bị xử lý kỷ luật hoặc xử phạt vi phạm hành chính về hành vi này. Tại cuộc hội thảo về các hành vi vi phạm, tội phạm trong thương mại điện tử do Bộ Thương mại tổ chức ngày 10/11/2006 ở Hà Nội, đại

diện đơn vị chống tội phạm công nghệ cao của C15 (Bộ Công an) ông Trần Ngọc Hoà cho rằng "Quy định hiện hành rất khó truy cứu trách nhiệm hình sự đối với tin tặc. Luật quy định việc phá hoại gây 'hậu quả nghiêm trọng', hoặc từng bị kỷ luật, xử lý hành chính rồi mà tái phạm mới bị truy cứu trách nhiệm hình sự. Nhưng trên môi trường Internet yếu tố này rất khó xác định vì sự quan trọng của thông tin chứa trong máy tính hoặc mạng máy tính khó có thể đo đếm được. Nhiều nước quy định nếu truy cập trái phép vào máy tính người khác là đã có thể bị xử lý hình sự, bất kể việc đó đã gây ra thiệt hại gì cho chủ nhân hay chưa". Như đã phân tích ở trên, khả năng gây hậu quả của tội phạm trong lĩnh vực tin học rất lớn nhưng hậu quả thực tế lại khó xác định. Bản thân việc sử dụng CNTT để phạm tội đã là sử dụng phương tiện có khả năng gây nguy hại ở mức độ rất nghiêm trọng nên có lẽ không cần thiết phải quy định hậu quả nghiêm trọng là yếu tố bắt buộc của cấu thành cơ bản.

Bên cạnh đó, theo quy định hiện nay, một người có thể vi phạm lần đầu với hành vi của tội quy định ở điều 224 và bị xử phạt hành chính. Lần sau người này lại vi phạm vào tội được quy định ở điều 225 (không gây hậu quả nghiêm trọng) nhưng vẫn không bị xử lý về mặt hình sự được vì người này chưa từng bị xử phạt hành chính về hành vi ở Điều 225. Có nghĩa là một người có thể vi phạm nhiều lần với những tội danh khác nhau của tội phạm trong lĩnh vực tin học nhưng không phải chịu chế tài hình sự khi không gây hậu quả nghiêm trọng.

Ngoài ra, các quy định pháp luật trong các ngành luật phi hình sự có liên quan và là cơ sở cho việc xác định tội phạm trong lĩnh vực tin học vẫn chưa đáp ứng được yêu cầu này. Ví dụ như các quy định về vận hành, khai thác, sử dụng mạng máy tính điện tử hiện nay nằm trong rất nhiều văn bản khác nhau từ luật đến thông tư, nghị định. Đó là hàng chục các văn bản như: Luật

CNTT năm 2006, Nghị định số 55/2001/NĐ-CP ngày 23 tháng 08 năm 2001 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet; Quyết định Số 92/2003/QĐ - BBCVT ngày 26 tháng 5 năm 2003 của Bộ trưởng Bộ Bưu chính, Viễn thông ban hành "Quy định về quản lý và sử dụng tài nguyên Internet"; Thông tư số 04/2001/TT-TCBĐ ngày 20 tháng 11 năm 2001 của Tổng cục Bưu điện hướng dẫn thi hành Nghị định số 55/2001/NĐ-CP của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ truy nhập Internet, dịch vụ kết nối Internet và dịch vụ ứng dụng Internet trong Bưu chính, Viễn thông; Quyết định số 95/2002/QĐ-TTg ngày 17/7/2002 của Thủ tướng Chính phủ Phê duyệt Kế hoạch tổng thể về ứng dụng và phát triển CNTT ở Việt Nam đến năm 2005; Quyết định số 17/2001/QĐ-TTg ngày 13 tháng 2 năm 2001 của Thủ tướng Chính phủ về việc chuyển giao chức năng điều phối các hoạt động Internet ở Việt Nam; Quyết định số 27/2002/QĐ-BVHTT ngày 10/10/2002 của Bộ Văn hóa Thông tin ban hành Quy chế quản lý và cấp phép cung cấp thông tin, thiết lập trang thông tin điện tử trên Internet; Qui định về biện pháp và trang thiết bị kiểm tra, kiểm soát đảm bảo an ninh quốc gia trong hoạt động Internet ở Việt Nam. (Ban hành kèm theo Quyết định số 848/1997/QĐ-BNV(A11) ngày 23/10/1997 của Bộ trưởng Bộ Nội vụ); Quyết định số 84/2001/QĐ-BTC ngày 5 tháng 9 năm 2001 của Bộ trưởng Bộ Tài chính Ban hành Biểu mức thu phí, lệ phí cấp và quản lý tên miền, địa chỉ Internet ở Việt Nam. Điều này gây khó khăn cho việc viện dẫn, áp dụng khi xử lý các tội phạm trong lĩnh vực tin học.

Ngoài ra, quy định của các ngành luật dân sự, kinh tế cũng có thể ảnh hưởng đến việc áp dụng các quy định của luật hình sự. Ví dụ như quy định về tài sản trong Bộ luật Dân sự chưa thừa nhận những loại tài sản ảo hình thành từ kinh doanh, tham gia các trò chơi trên mạng trong khi loại tài sản này có thể đổi ra

tiền mặt hoặt rất có giá trị trao đổi…

Tóm lại, với nhiều hạn chế, bất cập như vậy, các quy định pháp luật hiện hành về tội phạm trong lĩnh vực tin học cần thiết phải được sửa đổi, hoàn thiện kịp thời để phục vụ công tác đấu tranh phòng chống tội phạm trước diễn biến đang ngày một trầm trọng của tội phạm này.

3.1.2. Phương hướng hoàn thiện các quy định của pháp luật hình sự Việt Nam về các tội phạm trong lĩnh vực tin học

Trên cơ sở phân tích những khiếm khuyết của pháp luật thực về tội phạm trong lĩnh vực tin học tác giả luận văn xin được đưa ra một số kiến nghị nhằm hoàn thiện các quy định pháp luật nhằm đáp ứng yêu cầu làm cơ sở đấu tranh phòng, chống tội phạm này.

Như đã phân loại ở chương 1, các tội phạm trong lĩnh vực tin học gồm hai nhóm: Nhóm I: Các tội xâm phạm trật tự, an ninh thông tin trong hệ thống máy tính, mạng máy tính; nhóm II: Các tội sử dụng CNTT xâm phạm quyền lợi của người khác (tội phạm sử dụng CNTT). Các tội phạm thuộc hai nhóm này có một số đặc điểm khác nhau vậy nên phương hướng hoàn thiện quy định pháp luật đối với các tội phạm thuộc hai nhóm cũng khác nhau.

Đối với nhóm I - Các tội xâm phạm trật tự, an ninh thông tin trong hệ thống máy tính, mạng máy tính

1) Các tội phạm thuộc nhóm này nên được đưa thành một chương riêng là Các tội xâm phạm trật tự, an ninh CNTT tách khỏi Chương các tội xâm phạm trật tự công cộng, an toàn công cộng như hiện nay. Sở dĩ như vậy là vì các tội xâm phạm trật tự, an ninh thông tin trong hệ thống máy tính, mạng máy tính có khách thể xâm hại khác hẳn những tội phạm xâm phạm trật tự an ninh công cộng và mức độ nguy hiểm của chúng đặc biệt lớn. Việc đưa thành một chế định như

vậy vừa thể hiện được sự logic của một đạo luật vừa khiến cho cơ quan tư pháp, các cơ quan, tổ chức có liên quan thấy được vai trò của việc phòng chống tội phạm trong lĩnh vực tin học trong công cuộc phát triển đất nước hiện nay cũng như bảo vệ hệ thống thông tin và các hoạt động kinh tế, chính trị văn hóa đang diễn ra trong môi trường CNTT.

2) Chương các tội xâm phạm trật tự, an CNTT mới được xây dựng trên cơ sở cụ thể hóa và bổ sung các quy định hiện nay trong BLHS năm 1999. Chương này có thể được xây dựng theo mô hình dưới đây:

Chương...: Các tội xâm phạm trật tự, an ninh CNTT

Điều...: Tội tạo ra, lan truyền và phát tán các virus máy tính

Điều...:Tội sao chép, lấy cắp, sử dụng trái phép thông tin trên mạng và trong máy vi tính

Điều...: Tội phá hủy, làm hư hỏng hoặc thay đổi các dữ liệu chứa trong một hệ thống máy tính

Điều...: Tội làm gián đoạn hoạt động của mạng máy tính hoặc mạng viễn thông cản trở các hoạt động bình thường của các loại dịch vụ đó

Điều...: Tội truy nhập bất hợp pháp

Điều...: Tội ngăn cản bất hợp pháp, thay đổi hoặc xóa những thư điện tử của người khác hoặc các thông tin dữ liệu khác

Điều...: Tội tuyên truyền, phổ biến công cụ, phương thức phạm tội trong lĩnh vực tin học

Điều...: Tội sử dụng trái phép các dịch vụ trên mạng máy tính.

Điều...: Tội sản xuất, sao chép phần mềm bất hợp pháp, không có bản quyền

Điều...: Tội chiếm đoạt quyền sử dụng tên miền để sử dụng, trao đổi kiếm

lời hoặc tống tiền chủ sở hữu.

Điều...: Tội tạo giả mạo website.

Điều...: Tội phá hủy website.

3) Cấu thành cơ bản của các tội xâm phạm trật tự, an ninh CNTT nên bỏ quy định bắt buộc về yếu tố gây hậu quả nghiêm trọng bởi vì hậu quả của các tội phạm này rất khó xác định. Yếu tố gây hậu quả nghiêm trọng nên chuyển thành tình tiết tăng nặng TNHS đối với tội phạm này.

4) Quy định về yếu tố đã "từng bị xử lý kỷ luật, xử phạt vi phạm hành chính" cũng cần được sửa đổi. Hiện nay, trong các quy định của BLHS thì các tội phạm trong lĩnh vực tin học đều yêu cầu cấu thành cơ bản phải có yếu tố "đã bị xử lý kỷ luật, xử phạt hành chính về hành vi này mà vẫn vi phạm" (hoặc gây hậu quả nghiêm trọng). Quy định này dẫn đến khả năng một người thực hiện nhiều hành vi xâm phạm trật tự, an ninh CNTT, mỗi lần đều bị xử lý kỷ luật hoặc xử phạt hành chính nhưng hành vi lần sau không trùng với hành vi trước nên không bị coi là đã bị xử lý kỷ luật, xử phạt hành chính về hành vi đó và không bị xử lý về hình sự. Vậy nên cần phải quy định là: "Đã bị xử phạt hành chính về một trong các hành vi xâm phạm trật tự, an ninh CNTT"

Đối với nhóm II - Các tội sử dụng CNTT xâm phạm quyền lợi của người khác (tội phạm sử dụng CNTT)

Về cơ bản những tội phạm thuộc nhóm này có thể trùng bản chất với các tội phạm truyền thống đã có chỉ có công cụ, phương tiện phạm tội là mới. Ví dụ như hành vi tấn công website để tống tiền có thể xác định là tội cưỡng đoạt tài sản; hành vi đánh cắp thông tin về tài khoản trực tuyến và rút trộm tiền cũng trùng với tội trộm cắp tài sản; hành vi sao chép bất hợp pháp phần mềm máy tính cũng giống như tội xâm phạm quyền tác giả; đưa lên mạng phim ảnh đồi trụy

chính là tội truyền bá văn hóa phẩm đồi trụy; giả mạo website để lừa đảo chính là lạm dụng tín nhiệm chiếm đoạt tài sản...v.v. Mặc dù như vậy nhưng cơ quan chức năng lúng túng trong xác định tội danh đối những hành vi này do môi trường điễn ra tội phạm đặc biệt, phương tiện phạm tội hiện đại, phạm vi gây tác động rộng lớn... Do đó, cần phải nhanh chóng ban hành văn bản hướng dẫn áp dụng thống nhất, chính xác các quy định pháp luật hiện hành để xử lý tội phạm trong lĩnh vực tin học.

Tuy nhiên, áp dụng nguyên xi quy định pháp luật về các tội phạm truyền thống để xử lý các tội phạm trong lĩnh vực tin học cũng không hoàn toàn hợp lý. Sở dĩ như vậy là bởi vì tuy có cùng bản chất nhưng các tội phạm sử dụng tin học, diễn ra trên môi trường ảo có khả năng gây hậu quả nghiêm trọng trên phạm vi rộng lớn hơn gấp nhiều lần so với phạm tội bằng các phương tiện thông thường, trên môi trường vật chất bình thường. Do đó, để có chế tài phù hợp với tội phạm sử dụng CNTT cần bổ sung một tình tiết tăng nặng TNHS vào điều 48 BLHS hiện hành. Đó là tình tiết tăng nặng TNHS do sử dụng CNTT (hay sử dụng công nghệ cao) để phạm tội.

Bên cạnh việc hoàn thiện quy định của luật hình sự về các tội phạm trong lĩnh vực tin học cũng đồng thời phải hoàn thiện các quy định pháp luật phi hình sự liên quan đến tội phạm này. Ví dụ như phải xây dựng một văn bản thống nhất, đầy đủ quy định về vận hành, khai thác, sử dụng máy tính, mạng máy tính điện tử. Có thể điều chỉnh quan niệm pháp luật truyền thống về những vấn đề như tài sản, giao dịch…v.v.

3.2. Một số giải pháp phối hợp trong đấu tranh phòng chống các tội phạm trong lĩnh vực tin học ở Việt Nam

Ngoài vấn đề hoàn thiện pháp luật, công tác đấu tranh phòng, chống tội phạm trong lĩnh vực tin học còn cần có sự phối hợp đồng bộ nhiều giải pháp và sự tham gia tích cực cả từ phía nhà nước, các tổ chức và công dân.

Phát hiện, xử lý tội phạm trong lĩnh vực tin học đòi hỏi ở những người tiến hành tố tụng không chỉ trình độ chuyên môn, nghiệp vụ mà còn cả kiến thức sâu về CNTT. Do đó, cần phải nhanh chóng bồi dưỡng, nâng cao trình độ CNTT cho các cán bộ bảo vệ pháp luật để kịp thời đáp ứng yêu cầu của công tác đấu tranh, xử lý loại tội phạm này. Vấn đề nâng cao trình độ chuyên môn CNTT đặc biệt quan trọng đối với các điều tra viên vì việc điều tra, phát hiện, chứng minh tội phạm trong lĩnh vực này đòi hỏi trình độ CNTT của điều tra viên phải cao hơn cả giới tội phạm. Về nhân lực của lực lượng này nên tuyển chọn đồng thời những cử nhân giỏi về CNTT từ các trường đại học và cơ sở đào tạo, có nguyện vọng đấu tranh chống tội phạm mạng và bên cạnh đó là những nhân viên trong ngành điều tra có năng lực, kinh nghiệm sẽ được đào tạo sâu về CNTT.

Tổng kết kinh nghiệm điều tra, xét xử tội phạm trong lĩnh vực tin học cũng rất có ý trong việc nâng cao hiệu quả đấu tranh phòng, chống tội phạm này. Tội phạm trong lĩnh vực tin học là loại tội phạm phi truyền thống nên chúng ta hầu như chưa có kinh nghiệm điều tra, xét xử tội phạm trong lĩnh vực này. Vì thế, sẽ rất hữu ích nếu chúng ta đồng thời tổng kết, rút kinh nghiệm từ quá trình đấu tranh với các tội phạm trong lĩnh vực tin học trong nước cũng như học tập kinh nghiệm từ các nước đi trước trong lĩnh vực này.

Đẩy mạnh nghiên cứu, phát minh ra các biện pháp phòng chống, vũ khí tin học chống lại tội phạm trong lĩnh vực tin học cũng là một giải pháp hết sức quan trọng. Thực tiễn cho thấy, các công trình nghiên cứu của các chuyên gia pháp lý cũng như các chuyên gia tin học, các giải pháp bảo mật, vũ khí tin học đã đóng

góp rất lớn trong phòng ngừa và chống tội phạm trong lĩnh vực tin học. Tuy nhiên, đây là một quá trình tốn kém, đòi hỏi nhiều thời gian, kinh phí, trí tuệ mà Nhà nước cần ưu tiên đầu tư.

Tội phạm trong lĩnh vực tin học hiện nay rất phổ biến và có thể tấn công bất kì một cá nhân, tổ chức nào có sử dụng mạng Internet. Vì vậy, việc giáo dục ý thức tự phòng vệ của người sử dụng mạng máy tính là vô cùng cần thiết. Các kỹ thuật bảo mật thông tin, các công cụ ngăn chặn harker cần phải được phổ biến rộng rãi. Trách nhiệm của các nhà quản trị thông tin cũng phải được nâng cao hơn.

Biện pháp giáo dục pháp luật cũng được đưa ra ở đây vì thực tế cho thấy rằng một số lượng lớn harker đang ở lứa tuổi thanh thiếu niên. Họ lại là những người có trí tuệ và óc sáng tạo. Nếu có thể giáo dục và hướng nghiệp tốt cho những người này thì đây sẽ là nguồn nhân lực mạnh cho phát triển kinh tế đất nước. ở lứa tuổi này đa số có những hành vi vi phạm pháp luật là do thiếu hiểu biết đầy đủ, hiếu kỳ và thích tự chứng minh. Vậy đối với những đối tượng là thanh thiếu niên khi truy cứu TNHS về tội phạm tin học cũng nên xem xét kỹ động cơ phạm tội để quyết định hình phạt.

Vấn đề tăng cường hợp tác quốc tế để trao đổi kinh nghiệm đấu tranh chống tội phạm trong lĩnh vực tin học và cần phải có những cam kết quốc tế nhằm hợp tác đấu tranh với tội phạm này hết sức quan trọng đặc trưng của tội phạm trong lĩnh vực tin học là không biên giới.

KẾT LUẬN

Tội phạm trong lĩnh vực tin học là những hành vi nguy hiểm cho xã hội được quy định tại BLHS , do người có năng lực TNHS cố ý hoặc vô ý thực hiện bằng cách sử dụng CNTT nhằm xâm phạm trật tự an ninh thông tin trong máy tính, hệ thống mạng máy tính; xâm phạm các quyền lợi ích hợp pháp của cá nhân, tổ chức.

Các tội phạm trong lĩnh vực tin học gồm hai nhóm khác nhau. Nhóm 1 - Các tội xâm phạm trật tự, an ninh CNTT. Khách thể của nhưng tội phạm này là trật tự, an ninh trong lĩnh vực CNTT. Trật tự, an toàn trong lĩnh vực CNTT được coi là điều kiện đảm bảo cho mọi hoạt động trong lĩnh vực này diễn ra bình thường. Xâm phạm vào trật tự, an toàn trong lĩnh vực CNTT là xâm phạm vào các quy định pháp luật, quy tắc xử sự trong ngành, làm đảo lộn, sai lệch, phá hoại các hoạt động về CNTT. Nhóm II - Các tội sử dụng CNTT xâm phạm quyền lợi của người khác (tội phạm sử dụng CNTT). Đây cũng là các tội phạm diễn ra trong môi trường mạng máy tính, sử dụng các ứng dụng CNTT làm phương tiện phạm tội. Mục đích của tội phạm này không chỉ là phá hoại, gây rối loạn, cản trở an ninh CNTT mà còn nhằm những mục đích khác như: thu lợi bất chính, gây mất ổn định các hoạt động xã hội thông qua mạng, gian lận thương mại...v.v.

Tội phạm trong lĩnh vực tin học gắn bó chặt chẽ với các ứng dụng CNTT và có khả năng gây nguy hại nghiêm trọng đến mọi lĩnh vực của đời sống vì CNTT hiện nay đã được áp dụng vào hầu hết các lĩnh vực đó.

Tội phạm trong lĩnh vực tin học ở Việt Nam tuy mới xuất hiện nhưng cũng đã gây nhiều hậu quả nghiêm trọng và tình trạng tội phạm ngày càng trầm trọng. Vậy nhưng, thực tiễn đấu tranh, xử lý các tội phạm này hiện nay gặp phải rất

nhiều khó khăn, bất cập. Nguyên nhân có thể xuất phát từ nhiều yếu tố như: thiếu sót của hệ thống pháp luật, hạn chế về trình độ CNTT của cán bộ bảo vệ pháp luật, đặc thù của tội phạm trong lĩnh vực tin học …

Để khắc phục tình trạng đó và nâng cao hiệu quả công tác đấu tranh phòng, chống tội phạm trong lĩnh vực tin học cần phải nhanh chóng hoàn thiện quy định pháp luật hình sự về các tội phạm này cũng như tiến hành đồng bộ một số giải pháp khác như: nâng cao trình độ chuyên môn CNTT cho cán bộ các cơ quan bảo vệ pháp luật; giáo dục ý thức tuân thủ pháp luật cho công dân khi tham gia các hoạt động CNTT; nâng cao tinh thần cảnh giác của cá nhân, tổ chức tham gia hoạt động CNTT; đầu tư nghiên cứu các giải pháp khoa học về bảo mật và phòng chống tội phạm trong lĩnh vực tin học …

Những nội dung trên là một số kết quả nghiên cứu tội phạm trong lĩnh vực tin học của luận văn. Bằng việc mạnh dạn đưa ra một số kiến nghị như vậy, tác giả hy vọng rằng có thể góp phần tích cực vào công tác đấu tranh phòng, chống tội phạm này.

Do điều kiện nghiên cứu và khả năng bản thân còn hạn chế nên chắc chắn luận không thể tránh khỏi những sai sót. Rất mong nhận được sự phê bình, đóng góp từ thầy cô và các độc giả quan tâm để tác giả tiếp tục hoàn thiện công trình nghiên cứu này.

Xin chân thành cảm ơn!

DANH MỤC TÀI LIỆU THAM KHẢO

A. Các văn bản pháp luật:

1. Luật Khoa học và Công nghệ năm 2004.
2. Bộ luật Hình sự Việt Nam năm 1999.
3. Luật Công nghệ thông tin năm 2006.
4. Nghị định số: 55/2001/NĐ-CP ngày 23 tháng 08 năm 2001 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet;
5. Quy chế tạm thời về quản lý, thiết lập, sử dụng mạng Internet ở Việt Nam (Ban hành kèm theo Nghị định 21/CP ngày 5/3/1997)
6. Quy định về biện pháp và trang thiết bị kiểm tra, kiểm soát đảm bảo an ninh quốc gia trong hoạt động Internet ở Việt Nam. (Ban hành kèm theo Quyết định số 848/1997/QĐ-BNV(A11) ngày 23/10/1997 của Bộ trưởng Bộ Nội vụ).
7. Quyết định Số 92/2003/QĐ - BBCVT ngày 26 tháng 5 năm 2003 của Bộ trưởng Bộ Bưu chính, Viễn thông ban hành "Quy định về quản lý và sử dụng tài nguyên Internet";
8. Quyết định số 95/2002/QĐ-TTg ngày 17/7/2002 của Thủ tướng Chính phủ Phê duyệt Kế hoạch tổng thể về ứng dụng và phát triển công nghệ thông tin ở Việt Nam đến năm 2005.
9. Quyết định số 17/2001/QĐ-TTg ngày 13 tháng 2 năm 2001 của Thủ tướng Chính phủ về việc chuyển giao chức năng điều phối các hoạt động Internet ở Việt Nam.

10. Quyết định số 27/2002/QĐ-BVHTT ngày 10/10/2002 của Bộ Văn hóa Thông tin ban hành Quy chế quản lý và cấp phép cung cấp thông tin, thiết lập trang thông tin điện tử trên Internet.

11. Quyết định số 84/2001/QĐ-BTC ngày 5 tháng 9 năm 2001 của Bộ trưởng Bộ Tài chính Ban hành Biểu mức thu phí, lệ phí cấp và quản lý tên miền, địa chỉ Internet ở Việt Nam.

12. Thông tư liên tịch số 08/TTLT của Tổng cục bưu điện, Bộ nội vụ, Bộ văn hóa - thông tin - hướng dẫn cấp phép việc kết nối, cung cấp và sử dụng internet ở Việt Nam

13. Thông tư số 04/2001/TT-TCBĐ ngày 20 tháng 11 năm 2001 của Tổng cục Bưu điện hướng dẫn thi hành Nghị định số 55/2001/NĐ-CP của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ truy nhập Internet, dịch vụ kết nối Internet và dịch vụ ứng dụng Internet trong Bưu chính, Viễn thông.

B. Sách giáo khoa, giáo trình, sách tham khảo:

- Tiếng Anh:

14. Catherine H.Conly and J. Thomas McEwen, (1990), *Computer Crime*, NIJ Reports.

15. Dorothy E. Denning; William E. Baugh Jr, (1999), *Hiding crimes in cyberspace*, Published in: Information - Communication & Society, Volume 2, Issue 3, Routledge Publisher, USA.

16. P.N. Grabosky and Russell G. Smith, (1997), *Telecommunications and Crime: Regulatory dilemmas*, Law & Policy, Vol 19, No 3, Blackwell Publisher, Oxford, UK.

17. P.N. Grabosky and Russell G. Smith, (1999), *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Transaction Publishers.

18. Fukio Nakane, (2002), The Penal Code of Japan, Printed by Heibunsha Printing Co.

- Tiếng Việt:

19. TSKH Lê Cảm (chủ biên), (2001), *GT Luật hình sự phần chung*, NXB Đại học Quốc gia Hà Nội.

20. TSKH. Lê Cảm (chủ biên), (2003), *Giáo trình luật Hình sự Việt Nam phần riêng*, NXB Đại học Quốc gia Hà Nội.

21. TSKH.Lê Cảm, (1999), *Hoàn thiện pháp luật Hình sự Việt Nam trong giai đoạn xây dựng nhà nước pháp quyền*, NXB Công an nhân dân.

22. Vũ Ngọc Cừ, Virus máy tính, (1997), *Bản chất, hiện tượng, phòng nhiễm và tiêu diệt*, NXB Khoa học & Kỹ thuật.

23. TS. Phạm Văn Lợi (chủ biên), (2007), Tội phạm trong lĩnh vực Công nghệ thông tin, NXB Tư pháp.

24. PGS.TS Nguyễn Xuân Yêm, (2001), Tội phạm học Việt Nam hiện đại và phòng ngừa tội phạm – NXB Công An Nhân Dân.

25. Nguyễn Như Ý (chủ biên), (2008), Đại từ điển tiếng Việt, NXB Đại học Quốc gia TP Hồ Chí Minh.

26. *Từ điển tin học*, Từ điển điện tử Lạc Việt MTD, (2002), Công ty cổ phần Tin học Lạc Việt.

27. *Từ điển Điện tử - Tin học - Truyền thông Anh Việt*, (1997), Ban từ điển, Nxb Khoa học & Kỹ thuật.

C. Bài báo, phóng sự:

28. Đinh Tiến Dũng, "Nhận thức về tội phạm công nghệ cao và một số giải pháp nâng cao hiệu quả phòng ngừa, ngăn chặn loại tội phạm này", *Tạp chí Dân chủ và Pháp luật*, số chuyên đề sửa đổi, bổ sung BLHS năm 1999, năm 2008.

29. Nguyễn Hữu Hùng, "Internet", *Tạp chí Thông tin Khoa học Công nghệ*, số 1, năm 1998.

30. Đỗ Thanh Hương, "Hacker mũ đen" những tên tội phạm ảo trên màn hình vi tính, *An ninh Thế giới*, số ra ngày 15/4/2004.

31. Dương Tuyết Miên & Nguyễn Ngọc Khanh, "Tội phạm vi tính", *Tạp chí Tòa án nhân dân*, số 5, năm 2000.

32. Nguyễn Mạnh Toàn, "Tìm hiểu về tội phạm tin học", *Tạp chí Kiểm sát*, số 1, năm 2002.

33. Nông Xuân Trường, "Tội phạm tin học và các biện pháp đấu tranh chống tội phạm tin học tại Hàn Quốc", *Tạp chí Kiểm sát*, số 10, năm 2003.

34. Nguyễn Văn Thuyết, "Đấu tranh với các tội phạm có liên quan đến sử dụng máy tính tại Australia", *Tạp chí Kiểm sát*, số 8, năm 2002.

35. Trịnh Tiến Việt, "Tình hình tội phạm tin học trên thế giới, kinh nghiệm đấu tranh phòng chống và vấn đề tiếp thu vào Việt Nam", *Tạp chí Tòa án nhân dân*, số 7, năm 2006.

36. GS.TS Nguyễn Xuân Yêm, "Phòng chống tội phạm sử dụng công nghệ cao trong thời kỳ hội nhập quốc tế", *Báo An ninh*, số ra ngày 16/5/2007.

37. Thế Phong, "Bức tranh toàn cảnh an ninh mạng năm 2006 - phần I", *Báo điện tử vietnamnet* thuộc Bộ Bưu chính Viễn thông, ngày 28/3/2006. Xem tại: http://www.vnn.vn/cntt/2007/01/651849/

38. Thế Phong, "Bức tranh toàn cảnh an ninh mạng năm 2006 - phần II", *Báo điện tử vietnamnet* thuộc Bộ Bưu chính Viễn thông, ngày 28/3/2006. Xem tại: http://vietnamnet.vn/cntt/2007/01/654104/

39. Số Chuyên đề về Luật hình sự của một số nước trên thế giới. Tạp chí Dân chủ và Pháp luật (Bộ Tư pháp), Hà Nội, 1998

40. 85% trang web của Mỹ bị hacker tấn công, trên VnExpress.net ngày 20/01/2002.

41. Thế Phong và Hoàng Hùng, Tấn công DOS: hiểm họa khôn lường, báo điện tử Vietnamnet thuộc Bộ Bưu chính Viễn thông, ngày 28/3/2006. Xem tại: http://vietnamnet.vn/cntt/vienthong/2006/03/554662/

42. Hàng nghìn password internet bị đánh cắp, trên vnexpress.net ngày 13/3/2001 (Xem tại địa chỉ: http://www.vnexpress.net/GL/Vi-tinh/Hacker-Virus/2001/03/3B9AE9DE/)

43. T.Tú và V. Bình, Tin tặc tiếp tục gây nhiễu các website nội địa, trên trang vnexpress.net ngày 21/5/2001 (Xem tại địa chỉ: http://www.vnexpress.net/GL/Vi-tinh/2001/05/3B9B09EB/)

44. Văn Bình, HackerVN tấn công vào website cơ quan nhà nước, trên trang vnexpress.net ngày 11/6/2001 (Xem tại địa chỉ: http://www.vnexpress.net/GL/Vi-tinh/Hacker-Virus/2001/06/3B9B14BA)

45. Hoàng Mai, Các website Việt – Nguy cơ bị tin tặc tấn công, Báo Công an nhân dân điện tử, ngày 30/6/2008, nguồn: http://ca.cand.com.vn/

46. Trần Khôi, Đề nghị truy tố 10 bị can làm giả thẻ tín dụng, báo Tiền phong, số ra ngày 4/12/2006.

47. Hacker trộm hơn 400 triệu đồng qua mạng, báo Lao động, số ra ngày 24/8/2007

48. Hai hacker Việt Nam tiếp tay cho tội phạm quốc tế, trên báo Công an nhân dân điện tử ngày 25/3/2007 nguồn: http://ca.cand.com.vn/

49. Kẻ âm mưu chiếm đoạt tiền ngân hàng qua mạng internet sa lưới, báo Công an nhân dân điện tử ngày 11/8/2005. Xem tại: http://ca.cand.com.vn/vivn/anninhkinhte/phongsudieutra/2007/1/60097.cand

50. Hacker Anh khiếu nại vì bị kết án khi chưa có luật, trên vnexpress.net ngày 4/9/2001. Xem tại: http://www.vnexpress.net/GL/Vitinh/HackerVirus/2001/09/3B9B41FB/

51. Hacker được tha bổng tại Argentina, trên vnexpress.net ngày 16/4/2002. Xem tại: http://www.vnexpress.net/GL/Vitinh/HackerVirus/2002/04/3B9BB28A/

52. Lực lượng đặc nhiệm Cyber Force của Cảnh sát Nhật Bản, báo Công an nhân dân điện tử, ngày 23/7/2008. Xem tại: http://antg.cand.com.vn/News/PrintView.aspx?ID=66921

53. Thảo Phu, Tuyên chiến với tội phạm máy tính, Báo Echip số 50/2003.

54. Cảnh sát mạng chống tội phạm mạng: Chạy đua với thời gian, Báo điện tử Vietnamnet thuộc Bộ Bưu chính Viễn thông, ngày 22/09/2004, xem tại: http://vietnamnet.vn/cntt/virus-hacker/2004/09/261508/

55. Thanh Tú, Chính phủ Anh lập website cảnh báo virus, Báo Thanh niên online ngày 26/2/2005. Xem tại: http://www.thanhnien.com.vn/CNTT/2005/4/4/82870.tno

56. Lịch sử hacker Việt Nam - website http://www.hackervn.net/

57. Virus Xrobot phát tán mạnh qua Yahoo Messenger, Báo lao động điện tử ngày 10/4/2006. Xem tại: http://www1.laodong.com.vn/pls/bld/display$.htnoidung(42,153699)