ĐẠI HỌC HUẾ

TRƯỜNG ĐẠI HỌC LUẬT

----- -----

BÁO CÁO TỔNG KẾT
ĐỀ TÀI NGHIÊN CỨU KHOA HỌC SINH VIÊN

Tên đề tài: PHÁP LUẬT QUỐC TẾ VÀ THỰC TIỄN VỀ XỬ LÝ TỘI PHẠM CÔNG NGHỆ CAO – KINH NGHIỆM CHO VIỆT NAM

Mã số:	**ĐHL2019-SV-02**
Chủ nhiệm đề tài:	**Thân Trọng Ngọc Trâm**
Thời gian thực hiện:	**01/201- đến 12/2019**

Huế, 11/2019

ĐẠI HỌC HUẾ

TRƯỜNG ĐẠI HỌC LUẬT

----- 🕮 -----

BÁO CÁO TỔNG KẾT
ĐỀ TÀI NGHIÊN CỨU KHOA HỌC SINH VIÊN

Tên đề tài: PHÁP LUẬT QUỐC TẾ VÀ THỰC TIỄN VỀ XỬ LÝ TỘI PHẠM CÔNG NGHỆ CAO – KINH NGHIỆM CHO VIỆT NAM

Mã số: **ĐHL2019-SV-02**

Chủ nhiệm đề tài: **Thân Trọng Ngọc Trâm**

Thời gian thực hiện: **01/201- đến 12/2019**

Giảng viên hướng dẫn: **ThS. Lê Khắc Đại**

Ký xác nhận đồng ý nghiệm thu:.....

Sinh viên phối hợp nghiên cứu:

Nguyễn Hoàng Hoài Thương

Dương Thị Mỹ Nhi

Huế, 11/2019

Lời Cảm Ơn

Sau thời gian học tập và rèn luyện tại Trường Đại học Luật – Đại học Huế, bằng sự biết ơn và kính trọng, nhóm nghiên cứu xin gửi lời cảm ơn chân thành đến Ban Giám hiệu, các phòng, khoa thuộc Trường và các thầy cô giảng viên đã nhiệt tình hướng dẫn, giảng dạy và tạo mọi điều kiện thuận lợi giúp đỡ trong suốt quá trình nghiên cứu và hoàn thiện đề tài nghiên cứu khoa học này.

Để thực hiện và hoàn thành đề tài nghiên cứu khoa học này, nhóm đã nhận được sự hỗ trợ, giúp đỡ cũng như là quan tâm, động viên từ phía nhà trường và gia đình. Đề tài nghiên cứu khoa học cũng được hoàn thành dựa trên sự tham khảo, học tập kinh nghiệm từ các kết quả nghiên cứu liên quan, các sách, báo chuyên ngành của nhiều tác giả ở các trường Đại học, các tổ chức nghiên cứu, tổ chức chính trị cả trong và ngoài nước. Đặc biệt hơn nữa xin gửi lời cảm ơn sâu sắc đến giảng viên hướng dẫn đề tài Th.s. Lê Khắc Đại, người luôn dành nhiều thời gian, công sức hướng dẫn trong suốt quá trình thực hiện nghiên cứu và hoàn thành đề tài nghiên cứu khoa học.

Tuy có nhiều cố gắng, nhưng trong đề tài nghiên cứu khoa học này không tránh khỏi những thiếu sót. Em kính mong Quý thầy cô, Ban Giám hiệu nhà trường, những người quan tâm đến đề tài, gia đình và bạn bè tiếp tục có những ý kiến đóng góp, giúp đỡ để đề tài được hoàn thiện hơn.

Nhóm nghiên cứu xin chân thành cám ơn!

DANH SÁCH SINH VIÊN THAM GIA THỰC HIỆN ĐỀ TÀI

1. CHỦ NHIỆM ĐỀ TÀI

Họ và tên : Thân Trọng Ngọc Trâm

MSSV : 16A5011409

Lớp : Luật K40A

Khoa : Luật quốc tế

2. SINH VIÊN PHỐI HỢP THỰC HIỆN

STT	HỌ VÀ TÊN	MSSV	LỚP	KHOA
1	Nguyễn Hoàng Hoài Thương	16A5011377	Luật K40A	Luật hành chính
2	Dương Thị Mỹ Nhi	17A5011481	Luật K41M	Luật quốc tế

DANH MỤC CÁC TỪ VIẾT TẮT

BLTTHS	:	Bộ luật tố tụng hình sự
BLHS	:	Bộ luật hình sự
TNHS	:	Trách nhiệm hình sự
TPCNC	:	Tội phạm công nghệ cao
CNTT	:	Công nghệ thông tin
TPM	:	Tội phạm mạng
PCTP	:	Phòng chống tội phạm
BCA	:	Bộ công an

MỤC LỤC

LỜI MỞ ĐẦU

Các thiết bị công nghệ cao và đặc biệt là Internet là một phần không thể thiếu trong cuộc sống là minh chứng cho sự bùng nổ của thời đại công nghệ thông tin, đồng thời tạo nên những thay đổi lớn trong đời sống xã hội. Bên cạnh những lợi ích mang tính vượt trội thì thực trạng này cũng ẩn chứa những nguy hiểm đáng báo động về loại tội phạm mới hình thành-Tội phạm công nghệ cao. Nhận thấy tính chất nguy hiểm và phức tạp của loại tội phạm mới này, các quốc gia phát triển thế giới đã sớm thiết lập hành lang pháp lý chặt chẽ nhằm xử lý và ngăn chặn tội phạm. Các quy định pháp luật về xử lý tội phạm công nghệ cao được xây dựng tương đối toàn diện nhằm ngăn chặn, giảm thiểu và xử lý tác động của tội phạm công nghệ cao đến đời sống con người. Tại Việt Nam, trải qua từng thời kỳ có thể thấy rằng pháp luật Việt Nam đã có những bước phát triển đáp ứng với nhu cầu đấu tranh phòng chóng tội phạm trong lĩnh vực Tội phạm công nghệ cao. Tuy bước đầu đã có những quy định pháp luật cơ bản quy định về loại tội phạm nguy hiểm này, nhưng thực chất nếu so sánh với thực tiễn phát triển nhanh chóng của Tội phạm công nghệ cao và pháp luật của các quốc gia khác trên thế giới thì vẫn còn tồn tại các mặt hạn chế.

Nhận thấy điều này, nhóm nghiên cứu đã tiến hành hệ thống hóa các vấn đề về lí luận pháp luật và thực tiễn xử lí tội phạm công nghệ cao ở quốc tế. Trên cơ sở đó rút ra bài học kinh nghiệm trong thực tiễn xây dựng pháp luật và xử lý tội phạm công nghệ cao ở Việt Nam.

1. Mục tiêu đề tài

- Hệ thống hóa các vấn đề về lí luận pháp luật và thực tiễn xử lí tội phạm công nghệ cao ở quốc tế. Trên cơ sở đó rút ra bài học kinh nghiệm trong thực tiễn xét xử tội phạm công nghệ cao ở Việt Nam.

Để đạt được mục tiêu trên, thì cần phải tập trung vào các nhiệm vụ nghiên cứu sau đây:

- Nghiên cứu các quy định về xử lí tội phạm công nghệ cao trong pháp luật quốc tế và pháp luật Việt Nam. Từ đó tiến hành phân tích , so sánh để tìm ra những hạn chế của pháp luật nước nhà. Giúp định hướng xây dựng một hành lang pháp lý về xử lí tội phạm công nghệ cao hiệu quả hơn ở Việt Nam.

- Nghiên cứu thực tiễn áp dụng pháp luật vào xử lí tội phạm công nghệ cao ở quốc tế và Việt Nam bao gồm: nghiên cứu và đánh giá hiệu quả

của của chế tài xử lí tội phạm công nghệ cao. Từ đó tiến hành so sánh, phân tích nhằm tìm ra những hạn chế của thực tiễn xử lí tội phạm ở Việt Nam. Trên cơ sở đó tiến hành xây dựng các phương pháp áp dụng chế tài xử lí tội phạm công nghệ cao một cách hiệu quả đảo bảo đảm tính tương thích mà không xâm phạm quyền công dân.

- Nghiên cứu kết hợp giữa pháp luật thực định và thực tiễn xử lí tội phạm công nghệ cao ở quốc tế nhằm tìm ra những hạn chế của thực tiễn áp dụng pháp luật xử lí tội phạm công nghệ cao ở Việt Nam. Trên cơ sở đó tiến hành rút ra bài học kinh nghiệm và đề xuất những định hướng và giải pháp hoàn thiện quy định pháp luật, đồng thời nâng cao hiệu quả xử lí về tội phạm công nghệ cao trong thực tiễn Việt Nam.

2. Đối tượng, phạm vi nghiên cứu

2.1. Đối tượng nghiên cứu

- Pháp luật thực định và thực tiễn xử lí tội phạm công nghệ cao nhóm hệ lợi dụng mạng máy tính, viễn thông để hoạt động bất hợp pháp ở quốc tế

- Pháp luật thực định và thực tiễn xử lí tội phạm công nghệ cao nhóm hệ lợi dụng mạng máy tính, viễn thông để hoạt động bất hợp pháp ở Việt Nam.

2.2. Phạm vi nghiên cứu

- Phạm vi về không gian: Pháp luật và thực tiễn xử lí tội phạm công nghệ cao quốc tế và Việt Nam.

- Phạm vi về thời gian: Khoảng thời gian những năm từ 2010 đến 2019.

3. Cách tiếp cận, phương pháp nghiên cứu

3.1. Cách tiếp cận

Đề tài tiếp cận các vấn đề nghiên cứu ở các góc độ sau:

- Từ cơ sở lý luận: nghiên cứu hệ thống văn bản quy phạm pháp luật của Việt Nam quy định về xử lý tội phạm công nghệ cao. Quan tâm xem xét đến pháp luật quốc tế cũng như các cam kết quốc tế liên quan đến đề tài nghiên cứu. Nhằm đánh giá sự hoàn thiện của hệ thống pháp luật Việt Nam về việc xử lý tội phạm công nghệ cao, từ đó kiến nghị những điểm hạn chế cần sửa đổi, tránh hiện tượng chồng chéo, tạo điều kiện thuận lợi cho việc áp dụng pháp luật xử lý tội phạm công nghệ cao.

- Từ cơ sở thực tiễn: Tập trung nghiên cứu thực tiễn áp dụng pháp luật đồng thời đánh giá, để tìm ra cơ chế hiệu quả trong xử lí tội phạm công nghệ cao của pháp luật quốc tế. Nhằm rút ra bài học kinh nghiệm, đề ra các phương pháp xây dựng, thực thi pháp luật xử lý tội phạm công nghệ cao ở

Việt Nam có tính hiệu quả hơn, sao cho không để lọt lưới tội phạm đồng thời vẫn đảm bảo các quyền cơ bản của công dân.

- Kết hợp song song giữa lý luận và thực tiễn: nghiên cứu để đưa ra những kiến nghị nhằm xây dựng một cơ chế pháp luật xử lý tội phạm công nghệ cao hiệu quả tại Việt Nam trong tương lai.

3.2. Phương pháp nghiên cứu

Các phương pháp được sử dụng trong đề tài nghiên cứu bao gồm: phương pháp phân tích tổng hợp, phương pháp so sánh, phương pháp quy nạp, … Đồng thời đề tài nghiên cứu còn dựa vào những số liệu thống kê về thực tiễn áp dụng pháp luật tội phạm công nghệ cao trong phạm vi trên toàn thế giới nói chung và Việt Nam nói riêng cũng như những thông tin trên mạng Internet...cụ thể:

- Phương pháp phân tích - tổng hợp được nhóm sử dụng khi tiến hành đánh giá, phân tích các quan điểm, các quy định pháp luật, các tình huống thực tiễn làm cơ sở cho những kết luận khoa học về việc xử lý tội phạm công nghệ cao nhằm hoàn thiện khung pháp luật về xử lý tội phạm công nghệ cao tại Việt Nam hiện nay.

- Phương pháp đánh giá, nhận định được nhóm sử dụng nhằm đánh giá diễn biến tội phạm, hậu quả mà tội phạm công nghệ cao tác động tới xã hội và thực tiễn áp dụng pháp luật xử lí tội phạm công nghệ cao, đồng thời xác định tính hiệu quả trong thực tiễn xử lý tội phạm công nghệ cao ở Việt Nam và quốc tế.

- Phương pháp so sánh được nhóm sử dụng để nhìn thấy những tiến bộ trong quy định pháp luật cũng như thực tiễn xử lí tội phạm công nghệ cao quốc tế. Từ đó rút ra bài học kinh nghiệm để xây dựng, hoàn thiện pháp luật Việt Nam. Đồng thời đánh giá tính tương thích giữa pháp luật quốc tế và Việt Nam. Nhằm phát triển các quy định về xử lí tội phạm công nghệ cao có tính hiệu quả trong ngăn chặn tội phạm mà vẫn bảo đảm quyền công dân.

4. Bố cục đề tài

Ngoài lời nói đầu, đề tài được bố cục gồm ba chương như sau:

Chương 1: Lý luận về pháp luật sử lý tội phạm công nghệ cao

Chương 2: thực tiễn của hoạt động xử lý tội phạm công nghệ cao hiện nay

Chương 3: kinh nghiệm quốc tế và bài học cho Việt Nam trong hoạt động xử lý tội phạm công nghệ cao

CHƯƠNG 1: LÝ LUẬN VỀ PHÁP LUẬT XỬ LÝ TỘI PHẠM CÔNG NGHỆ CAO

Cuộc cách mạng khoa học công nghệ thông tin bùng phát từ những thập kỷ 70, 80 của thế kỷ XX, với việc phát minh ra máy tính điện tử (Computer) và phổ biến mạng thông tin toàn cầu (Internet). Theo thống kê vào năm 2011, có ít nhất 2,3 tỷ người, tương đương với hơn một phần ba tổng dân số thế giới đã truy cập Internet; Có 60% người dùng Internet là ở các quốc gia đang phát triển, với 45% người dùng Internet ở độ tuổi dưới 25 tuổi. Ước tính vào năm 2017 số thuê bao di động sẽ đạt 70% trên tổng dân số thế giới. Dự đoán vào năm 2020, số lượng các thiết bị được kết nối mạng "Internet of thing" sẽ đông gấp sáu lần dân số thế giới.[1] Sự bùng nổ công nghệ cao này đã tạo nên những thay đổi lớn trong đời sống xã hội. Bên cạnh những lợi ích mang tính vượt trội thì thực trạng này cũng ẩn chứa những nguy hiểm đáng báo động về loại tội phạm mới hình thành-Tội phạm công nghệ cao.

1.1. Khái niệm tội phạm công nghệ cao.

Lợi dụng sự phổ biến và tiện lợi của công nghệ cao, một số đối tượng đã thực hiện hành vi phạm tội, gây nên những hậu quả nghiêm trọng cho đời sống con người. Từ đó, thuật ngữ TPCNC được ra đời. Tuy nhiên, cho đến nay vẫn chưa có một khái niệm thống nhất về TPCNC, ngay về tên gọi, hiện nay đã có rất nhiều thuật ngữ khác nhau như: TPCNC, tội phạm sử dụng công nghệ cao, tội phạm lợi dụng công nghệ cao, tội phạm Internet. Có thể thấy đây là khái niệm mới lạ không chỉ đối với Việt Nam mà cả với nhiều nước trên thế giới. Do đó, ngay từ việc sử dụng thuật ngữ đến việc đưa ra khái niệm, đặc điểm hay xác định hành vi nào là nguy hiểm cho xã hội cũng còn có nhiều ý kiến chưa thống nhất.

[1] Thống kê của UNODC Văn phòng Liên Hiệp Quốc về chống Ma túy và Tội phạm tại sách Comprehensive Study on Cybercrime.

1.1.1. Khái niệm tội phạm công nghệ cao theo pháp luật quốc tế.

Vào những năm cuối thế kỉ XX, công nghệ cao đã xuất hiện ở các nước có nền khoa học công nghệ phát triển, dẫn đến loại tội phạm này cũng hình thành và diễn biến từ rất sớm. Các quốc gia trên thế giới đã có những công trình nghiên cứu ở những phạm vi nhất định, khía cạnh và phương diện khác nhau về loại tội phạm này. Tuy nhiên vì tính chất phức tạp, và thay đổi nhanh chóng nên vẫn còn nhiều quan điểm chưa thống nhất về TPCNC.

Theo nghiên cứu của Philip N. Ndubueze Đại học Liên bang Dutse, bang Jigawa, Nigeria "TPCNC là một thuật ngữ được sử dụng để mô tả các hành vi phạm tội được thực hiện thông qua các phương tiện điện tử và công nghệ dựa trên kỹ thuật số như Internet hoặc máy tính."[2] Khái niệm này xác định TPCNC trong phạm vi rất rộng, tức là tất cả hành vi phạm tội thông qua việc sử dụng các thiết bị công nghệ tiên tiến đều được xem là TPCNC.

Tuy nhiên, thiết bị công nghệ cao bị tội phạm sử dụng phổ biến nhất hiện nay đó là máy tính và mạng Internet. Có thể nói đây là môi trường phạm tội phổ biến nhất của loại tội phạm này. Do đó các nhà nghiên cứu đã thu hẹp phạm vi và đưa ra định nghĩa mang tính chi tiết dành cho TPCNC. Ví dụ theo Từ điển luật học Black's Law, tội phạm máy tính (computer crime) được định nghĩa là: "tội phạm đòi hỏi về kiến thức công nghệ máy tính chẳng hạn như phá hoại hoặc ăn cắp dữ liệu máy tính hay sử dụng máy tính để thực hiện một số tội phạm khác."[3] Ngoài ra, pháp luật nhiều nước trên thế giới cũng đã đưa ra những khái niệm khác nhau về TPCNC, chẳng hạn trong luật hình sự năm 1995 của Australia và phần 10.7 của luật Thịnh vượng chung (Commonwealth legislation - Part 10.7: Computer Offences), TPCNC (hi- tech crime) được định nghĩa là sự xâm nhập máy tính một cách trái phép; sự sửa đổi trái phép dữ liệu bao gồm việc phá hủy dữ liệu;

[2] Philip N. Ndubueze, High-tech crimes, boundaryless policing and cyber security policy in digital nigeria: a periscope.
[3] Từ điển Luật học Black Law.

tấn công từ chối dịch vụ (DoS); tấn công từ chối dịch vụ phân tán (DdoS) có sử dụng botnets; tạo ra và phân phối phần mềm độc hại.[4]

Sự khác nhau về định nghĩa cũng dẫn đến những cách phân loại khác nhau về TPCNC trong pháp luật quốc tế. Việc phân loại TPCNC có ý nghĩa rất quan trọng bởi vì sẽ tạo điều kiện xác định, khoanh vùng tội phạm tốt hơn, giúp đưa ra các biện pháp phòng chống tội phạm một cách hiệu quả, chính xác.

Theo Công ước của Hội đồng Châu Âu về TPM 2001, gọi tắt là Công ước Budapest, đã phân loại TPM như sau: (1) vi phạm về bảo mật, tính toàn vẹn và tính sẵn có của dữ liệu và hệ thống máy tính; (2) tội liên quan đến máy tính; (3) các tội liên quan đến nội dung; (4) các tội vi phạm liên quan đến bản quyền.[5] Hay tại nghiên cứu của giáo sư Murughendra Tubake, trường Đại học Luật Navanagar, Ấn Độ [6] dựa trên cơ sở đối tượng nạn nhân bị ảnh hưởng bởi những tội ác này ông đã chia thành 4 nhóm tội phạm: (1) Nhóm tội phạm chống lại cá nhân: Những tên tội phạm tấn công từng nạn nhân thông qua máy tính của họ với mục đích ác ý bằng những hành vi khác nhau như gửi email giả mạo, phỉ báng qua mạng, lừa đảo hay rình rập đe dọa. (2) Nhóm tội phạm với mục đích tài sản: Thông qua máy tính, tội phạm này có thể làm ảnh hưởng tiêu cực đến tài sản của một cá nhân hay tổ chức. (3) Nhóm tội phạm chống lại các tổ chức: Mục tiêu tội phạm hướng tới là các cơ quan chính phủ, các công ty doanh nghiệp lớn, ngân hàng hay các hiệp hội. (4) Nhóm tội phạm chống lại xã hội: Bao gồm các hành vi như tạo lập các trang web bất hợp pháp và tiến hành các hoạt động khủng bố diễn ra bằng cách sử dụng máy tính hoặc mạng Internet.

Việc chưa thể thống nhất được định nghĩa và cách phân loại TPCNC phần nào chứng tỏ tội phạm này đang diễn ra hết sức phức tạp, đa dạng về

[4] Hoàng Việt Quỳnh, Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định pháp luật Việt Nam**,** Tạp chí KHGD CSND số 79 (tháng 8/2016).
[5] Understanding cybercrime: Phenomena, challenges and legal response by ITU, pages 13.
[6] Murughendra Tubake, Cyber Crime: An Overview.

mọi mặt. Chúng ngày càng phát triển và được xác định là mối đe dọa, thách thức đối với sự ổn định và phát triển của các quốc gia trên thế giới. Tuy nhiên, pháp luật Việt Nam cũng có thể dựa vào những kinh nghiệm của pháp luật quốc tế để vận dụng vào hoạt động nghiên cứu bản chất cũng như cách thức xử lý về TPCNC.

1.1.2. Khái niệm tội phạm công nghệ cao theo pháp luật Việt Nam.

Cuộc cách mạng công nghệ không chỉ ngày càng bùng nổ ở các nước trên thế giới mà hiện đang phát triển mạnh mẽ ở Việt Nam. Chính vì vậy mà TPCNC ở Việt Nam đang có xu hướng gia tăng nhanh chóng. Chúng đã gây ra những hậu quả nặng nề cho các cá nhân, tổ chức và toàn xã hội. Cho đến nay, ở Việt Nam qua từng thời kỳ lại có những cách hiểu khác nhau về định nghĩa loại tội phạm này.

Pháp luật Việt Nam đã đưa ra định nghĩa về TPM tại Luật An ninh mạng 2018 "TPM là hành vi sử dụng không gian mạng, CNTT hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại BLHS."[7] Bên cạnh đó, tại những nghiên cứu cũng đã đưa ra các khái niệm khác về TPCNC như tại Giáo trình "Những vấn đề cơ bản về phòng, chống tội phạm sử dụng công nghệ cao" cũng có đề cập đến khái niệm về tội phạm sử dụng công nghệ cao như sau: "Tội phạm được thực hiện bằng việc cố ý sử dụng tri thức, kỹ năng, công cụ, phương tiện CNTT ở trình độ cao tác động trái pháp luật đến thông tin số được lưu trữ, xử lý, truyền tải trong hệ thống máy tính, xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức, cá nhân."[8] Ngoài ra, trong bài nghiên cứu của mình, thạc sĩ Trần Thị Hồng Lê cho rằng: "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

[7] Khoản 7 Điều 2 Luật An ninh mạng Việt Nam 2018.
[8] Giáo trình "Những vấn đề cơ bản về phòng, chống tội phạm sử dụng công nghệ cao" của Học viện Cảnh sát nhân dân.

tin trong máy tính, hệ thống mạng máy tính; xâm phạm các quyền lợi ích hợp pháp của cá nhân, tổ chức."[9] Theo định nghĩa này, thạc sĩ cũng căn cứ trên khách thể bị tội phạm xâm hại để phân loại tội phạm thành 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). Hay trong quá trình đấu tranh với TPCNC, pháp luật nước ta cũng dựa vào cách thức và mục tiêu để phân loại tội phạm. Cụ thể, theo hướng dẫn 16/HD-BCA-C41 ngày 31/12/2013 của Bộ Công an[10] đã tiến hành việc phân chia các nhóm đối tượng phạm tội có sử dụng công nghệ cao thành 2 hệ đó là: Hệ xâm phạm hoạt động của mạng máy tính, viễn thông và Hệ lợi dụng mạng máy tính, viễn thông để hoạt động bất hợp pháp.

Chúng ta đang gặp khó khăn trong việc thống nhất định nghĩa và các phân loại về TPCNC nhưng từ những khái niệm và cách phân loại trên ta có thể thấy điểm chung trong nội hàm của các khái niệm này đều chỉ các hành vi liên quan đến việc sử dụng máy tính, thiết bị số, khai thác mạng máy tính, mạng viễn thông để gây tổn hại cho lợi ích của các tổ chức, cá nhân và toàn xã hội.

Từ việc tham khảo và phân tích các quy định pháp luật kết hợp với các công trình nghiên cứu của trong và ngoài nước, có thế thấy dù khái niệm công nghệ cao là rất rộng bao quát trên nhiều lĩnh vực. Tuy nhiên, có thể thấy điểm chung trong nội hàm của các khái niệm này đều chỉ các hành vi liên quan đến việc sử dụng máy tính, thiết bị số, khai thác mạng máy tính, mạng viễn thông để gây tổn hại cho lợi ích của các tổ chức, cá nhân và toàn xã hội. Từ đó, nhóm nghiên cứu rút ra định nghĩa về TPCNC như sau: " *tội phạm công nghệ cao là loại tội phạm thực hiện các hành vi trái pháp luật*

[9] Trần Thị Hồng Lê, Các tội phạm trong lĩnh vực tin học theo Luật Hình sự Việt Nam, 2009.
[10] Theo hướng dẫn 16/HD-BCA-C41 ngày 31/12/2013 của Bộ Công an hướng dẫn thực hiện một số quy định trong các Thông tư 18, 19, 20, 21, 22 ngày 1/4/2013 của Bộ trưởng Bộ Công an quy định về công tác nghiệp vụ cơ bản của lực lượng Cảnh sát nhân dân.

một cách trực tiếp hoặc gián tiếp bằng những công nghệ hiện đại liên quan đến mạng viễn thông như Internet và điện thoại nhằm mục đích xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức, cá nhân". Và đồng thời nhóm nghiên cứu tiến hành phân loại TPCNC làm hai nhóm chính là: Thứ nhất, nhóm tội phạm sử dụng công nghệ cao là công cụ để thực hiện hành vi trái pháp luật. Thứ hai, nhóm tội phạm chọn công nghệ cao là đối tượng để tấn công, phá hoại.

1.2. Đặc điểm của tội phạm công nghệ cao

Sự tăng trưởng nhanh chóng của Internet và máy tính công nghệ cao đã giúp phát triển kinh tế và xã hội. Tuy nhiên sự phụ thuộc vào Internet đã tạo ra nhiều rủi ro, các lỗ hổng, và mở ra những khả năng mới cho hoạt động TPM. Đi kèm với tốc độ phát triển chóng mặt của Internet là sự thay đổi không ngừng về đặc điểm của TPCNC. Do tính chất kết nối của Internet và hoạt động chia sẻ thông tin dữ liệu giữa các quốc gia dẫn đến sự tương đồng về mặt đặc điểm của TPCNC. Theo đó, nhóm nghiên cứu nhận thấy rằng TPCNC trên thế giới nói chung và Việt Nam nói riêng đều có những đặc điểm chung. Nắm rõ đặc điểm TPCNC sẽ giúp hoạt động nhận diện, ngăn chặn, xử lý tội phạm được dễ dàng, chính xác.

Thứ nhất, đặc điểm về mặt khách thể TPCNC là thông qua công nghệ hiện đại, điển hình là sử dụng mạng Internet và các thiết bị CNTT để thực hiện hành vi xâm phạm "trực tự an toàn thông tin" gây tổn hại cho lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức cá nhân. Trong đó, có thể xác định trật tự an toàn thông tin gồm 3 loại thuộc tính đó là: Tính bảo mật, tính toàn vẹn và tính khả dụng. Một tội phạm sử dụng công nghệ cao cụ thể có thể tác động đến một hoặc cả hai khía cạnh của trật tự an toàn thông tin.[11]

Thứ hai, xét về mặt khách quan TPCNC. Mặt khách quan của tội phạm là những biểu hiện ra bên ngoài của tội phạm; bao gồm những dấu

[11] Hoàng Việt Quỳnh, Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định pháp luật Việt Nam**,** Tạp chí KHGD CSND số 79 (tháng 8/2016).

hiệu như: Hành vi, hậu quả nguy hiểm cho xã hội, mối quan hệ giữa hành vi và hậu quả, phương pháp, phương tiện, công cụ, thủ đoạn, thời gian, không gian nơi xảy ra hành vi nguy hiểm cho xã hội.

Đối với hành vi: TPCNC xâm phạm đến trật tự an toàn thông tin, gây tổn hại cho xã hội được pháp luật các quốc gia điều chỉnh. Tội phạm thực hiện các hành vi có liên quan là mạng Internet và các thiết bị CNTT khác quan tới công nghệ cao. Thứ nhất, công nghệ cao có thể là mục tiêu của hoạt động tội phạm, ví dụ như: chiếm quyền điều khiển trang mạng, hệ thống máy tính: bằng các thủ đoạn lợi dụng lỗ hổng bảo mật của các trang mạng, hệ thống máy tính để đột nhập cổng hậu (backdoor); hoặc bẻ khóa, đánh cắp mật khẩu (password) để đột nhập vào các trang mạng. Thứ hai, máy tính có thể hoạt động như một phương tiện trung gian, nhằm phục vụ cho hành vi phạm tội phương tiện cho tội phạm chống lại một doanh nghiệp hoặc cá nhân, ví dụ như: tấn công trái phép vào Website để lấy đi những thông tin bí mật, lấy cắp thông tin tài khoản cá nhân, tổ chức, làm thẻ ATM giả. Đồng thời các hành vi sử dụng công nghệ cao để thực hiện hành vi cần được pháp luật quốc gia quy định và điều chỉnh. Ví dụ: tại Điều 44 luật An ninh mạng Trung Quốc đã quy định rằng: Các cá nhân hoặc tổ chức không được ăn cắp hoặc sử dụng các phương pháp bất hợp pháp khác để có được thông tin cá nhân và không được bán bất hợp pháp hoặc cung cấp bất hợp pháp cho người khác thông tin cá nhân. Hay tại Điều 287 BLHS Việt Nam năm 2015 quy định hành vi thể hiện là cố ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu điện tử hoặc ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc có hành vi khác cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử. 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.

Về thủ đoạn: Trong lĩnh vực sử dụng CNTT, viễn thông đều thực hiện với thủ đoạn gian dối, lợi dụng các lỗ hổng của hệ thống mạng và sự thiếu hiểu biết về bảo mật an toàn thông tin mạng của người dùng.

Về thời gian và không gian: Sự kết nối toàn cầu của Internet và tiện lợi của các thiết bị điện tử công nghệ cao đã tạo nên bản chất xuyên quốc gia cho TPCNC. Người phạm tội không nhất thiết phải ở nơi diễn ra hành vi phạm tội như các loại tội phạm khác mà có thể ở bất kỳ nơi nào, thời điểm nào. Việc thực hiện hành vi phạm tội chỉ cần thông qua các thao tác máy tính và thời gian hoàn thành được tính bằng giây.

Về công cụ, phương tiện: Công cụ, phương tiện phạm tội là điểm căn bản tạo ra sự khác biệt giữa TPCNC và tội phạm truyền thống. Tội phạm thường sử dụng sự tiến bộ của CNTT coi CNTT là một công cụ, phương tiện và phương thức nhằm mục đích tư lợi, chiếm đóng trái phép tài sản của người khác hoặc tội phạm coi CNTT chính là mục đích phạm tội của mình nhằm xâm phạm trật tự an ninh để. Sự khác biệt về công cụ, phương tiện phạm tội đã khiến cho TPCNC thực hiện được những hành vi phạm tội mà tội phạm truyền thống không thể làm được. Có thể nói, CNTT là một công cụ hữu hiệu giúp cho tội phạm tiến hành hoạt động của mình một cách nhanh chóng mà ít bỏ lại dấu vết.

Thứ ba, mặt chủ thể, TPCNC có thể được thực hiện bằng bất kỳ ai có đủ năng lực TNHS. Xuất phát từ tính chất của hành vi phạm tội của tội phạm mỗi quốc gia, chủ thể trực tiếp thực hiện tội phạm sử dụng công nghệ cao phải là những người có tri thức và kỹ năng cần thiết để trực tiếp khai thác, sử dụng thiết bị, công cụ, phương tiện công nghệ hoặc trực tiếp phát triển, ứng dụng công nghệ.[12] Một TPCNC không thể không có trình độ tin học nhất định, phần lớn chủ thể phạm tội đều có trình độ tri thức và có thể là lập thành tổ chức có quy mô.

[12] Hoàng Việt Quỳnh, Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định pháp luật Việt Nam**,** Tạp chí KHGD CSND số 79 (tháng 8/2016).

Thứ tư, xét về mặt chủ quan thì TPCNC được thực hiện bởi lỗi cố ý. Do tính chất của tội phạm nên khi thực hiện tội phạm sử dụng công nghệ cao, người phạm tội buộc phải ý thức rõ hành vi của mình là trái quy định pháp luật, có thể gây hậu quả xấu cho các tổ chức, cá nhân có liên quan nhưng vẫn thực hiện, mong muốn hoặc để mặc cho những hậu quả xấu xảy ra. Động cơ, mục đích phạm tội sử dụng công nghệ cao không phải là yếu tố bắt buộc trong cấu thành tội phạm ở mỗi quốc gia. Tuy nhiên, trong thực tế, tội phạm sử dụng công nghệ cao có thể được thực hiện do vụ lợi hoặc vi lợi ích trong cạnh tranh hay giải quyết mâu thuẫn, trả thù cá nhân... hoặc cũng có thể là sự tò mò, thử nghiệm, muốn chứng tỏ khả năng của bản thân.[13] Động cơ, mục đích phạm tội rất đa dạng: chính trị, kinh tế, phá hoại, đe dọa, khủng bố tinh thần. Nếu như trước đây, TPCNC chủ yếu mang tính phá hoại để khẳng định tài năng cá nhân do một số đối tượng có trình độ cao về CNTT, thì nay tội phạm đang có xu hướng chuyển sang mục đích chính trị, kinh tế rõ rệt.

Dù cho pháp luật và phương pháp nghiên cứu của các quốc gia trên thế giới và Việt Nam về TPCNC vẫn tồn tại các khác biệt. Tuy nhiên, những đặc điểm mà nhóm nghiên cứu tiến hành phân tích ở trên có thể coi là những đặc điểm cơ bản nhất của TPCNC.

1.3. Quy định của pháp luật về xử lý tội phạm công nghệ cao

Theo thống kê của IC3, vào năm 2018 đã có 351,937 vụ khiếu nại về TPCNC trên toàn thế giới với tổng số thiệt hại lên đến 2,7 tỷ đô.[14] Từ thực tế trên có thể thấy rằng, TPCNC được xem là loại tội phạm nguy hiểm và những thiệt hại mà chúng gây ra cho toàn xã hội là vô cùng lớn. Đòi hỏi các quốc gia cần hành động ngay nhằm xây dựng các hành lang pháp lý để ngăn chặn và xử lý loại tội phạm này. Bên cạnh đó với tính chất xuyên biên giới của TPCNC thì đây không chỉ là vấn đề của mỗi một quốc gia mà còn và mối nguy hiểm toàn cầu cần có sự hợp tác quốc tế.

[13] Hoàng Việt Quỳnh, Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định pháp luật Việt Nam**,** Tạp chí KHGD CSND số 79 (tháng 8/2016).
[14] IC3: Internet Crime Report 2018.

1.3.1. Quy định của pháp luật quốc tế về xử lý tội phạm công nghệ cao

Tội phạm máy tính, có thể đã bắt đầu hình thành kể từ khi máy tính được phát minh, nhưng tại thời điểm đó, nó không trở thành một vấn đề quan trọng và cũng không gây ra mối quan tâm lớn. Khi thời đại CNTT thực sự bùng nổ, TPM phát triển gần như đồng bộ với công nghệ và để lại những hậu quả nặng nề và lúc đó thế giới mới nhận thức được mối nguy hiểm của loại tội phạm này.

Máy tính lần đầu tiên ra đời vào năm 1946, việc lắp đặt máy tính lúc này còn rất phức tạp và tốn nhiều thời gian và số lượng máy tính còn rất hạn chế, tội phạm máy tính đã bắt đầu xuất hiện với sự phát triển của máy tính nhưng chúng chưa gây ra hậu quả đáng kể nào. Hơn nữa, không gian mạng là một phạm trù còn rất mới và chưa được ứng dụng nhiều vào đời sống dẫn đến chưa có một khung pháp lý nào để kiểm soát không gian mạng lúc bấy giờ và các cơ quan thực thi pháp luật sử dụng khung pháp luật truyền thống để đối phó với hiện tượng này. Bởi vì không có luật TPM, không có định khung hình phạt cũng như thống kê hậu quả tội mạng phải gây ra, dưới hoàn cảnh như vậy, xác suất kết án gần như bằng không. Do đó tội phạm sẽ tăng lên nhanh chóng.

Cho đến những năm 1970, khi công nghệ bắt đầu phát triển, TPM có xu hướng tăng nhanh cùng với nhiều phương thức khác nhau, khung pháp lý đầu tiên cho TPM bắt đầu xuất hiện. Trong những năm này, TPM bắt đầu các hành vi như trộm cắp thông tin, trộm cắp tài sản hay gian lận và hậu quả mà TPM để lại là lớn hơn rất nhiều so với tội phạm truyền thống. Chính vì vậy, một số nước đã hình sự hóa pháp luật tội phạm máy tính. Nhiều luật và quy định đã được thực hiện trong nhiều hơn các nước trong những năm 1980. Trong thời kì này, tất cả các quốc gia Bắc Âu bắt đầu đưa ra nhiều hơn các chế định nhằm kiểm soát tốt hơn không gian mạng. Các quốc gia đã nỗ lực để loại bỏ khoảng cách pháp lý để đối phó với TPM. Làn sóng cải cách luật đầu tiên trong hầu hết các hệ thống pháp luật

phương Tây nổi lên trong lĩnh vực bảo vệ quyền riêng tư trong những năm 1970 và 1980. Đây là một phản ứng đối với những thách thức về việc xâm phạm quyền riêng tư được gây ra bởi khả năng mở rộng thu thập, lưu trữ và truyền dữ liệu bằng các công nghệ mới. "Luật bảo vệ dữ liệu" đã được ban hành và liên tục được sửa đổi và cập nhật, bảo vệ quyền riêng tư của công dân với các quy định hành chính, dân sự và hình sự năm 1973 tại Thụy Điển, 1974 tại Hoa Kỳ, 1977 tại Cộng hòa Liên bang Đức, 1978 ở Áo, Đan Mạch, Pháp và Na Uy, 1979 và 1982 ở Luxembourg, 1981 ở Iceland và Israel, 1982 ở Úc và Canada, 1984 ở Anh, 1987 ở Phần Lan, 1988 ở Ireland.[15] Tuy nhiên, các biện pháp pháp lý này còn rời rạc, sơ sài; pháp luật chỉ mới xuất hiện ở các nước phát triển và các quy định này không đủ hiệu lực cũng như thiếu các hình phạt răn đe cho tội phạm và chỉ mới dừng lại ở việc bảo vệ và ngăn chặn việc dữ liệu máy tính bị xâm nhập và những quy định đó chưa thể kiểm soát hết những hành vi diễn ra trên không gian mạng. Trong giai đoạn này, Mỹ đã thông qua Đạo luật lạm dụng và gian lận máy tính vào năm 1984, đạo luật đã kiểm soát hầu như toàn bộ các vấn đề an ninh mạng trong vấn đề an ninh quốc gia tuy nhiên chưa đề cao đến quyền riêng tư cá nhân. Đạo luật này bước đầu tạo nên tiền đề cho cho sự phát triển khung pháp lý mới, cụ thể hơn dành cho TPCNC.

Các quy định trong pháp luật hình sự về TPCNC chưa thể điều chỉnh hết được trong phạm vi không gian mạng dẫn đến tỷ lệ tội phạm ngày càng tăng. Kể từ những năm 1990, TPM đã bước vào một quá trình toàn cầu hóa nhanh chóng. Với phát minh của WWW, truy cập Internet trở nên dễ dàng và phổ biến hơn cho mọi người. Từ đó trở đi, các máy tính toàn cầu được kết nối và Internet đã phải đối mặt với các mối đe dọa từ một không gian mạng toàn cầu hóa. Song song với sự phát triển Internet, TPM đã phát triển thành các hình thức phức tạp hơn. Các không gian mạng nơi thủ phạm hoạt động, chúng được liên kết, và với kiến thức mà chúng có được, các công cụ

[15] Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society,1998

mà chúng phát minh ra làm cho tội phạm trở nên tinh vi và nguy hiểm hơn. Chính vì vậy, ảnh hưởng của Internet về TPM bắt đầu được xem xét nhiều hơn trong pháp luật, nội dung được quy định cụ thể hơn và phạm vi của nó đã được mở rộng. Việc hình thành sự hợp tác quốc tế ảnh hưởng đến một số luật pháp quốc gia. Tội phạm máy tính và pháp luật liên quan được toàn cầu hóa, mở rộng từ các nước phát triển sang các nước kém phát triển hơn và các nước đang phát triển. Thực thi pháp luật cũng thực hiện một loạt các biện pháp chống TPM. Hầu hết các quốc gia dù là quốc gia phát triển hay đang phát triển đều đưa những quy định về TPCNC vào BLHS. Ngoài ra, một số nước đã bắt đầu ban hành Luật an ninh mạng riêng như tại Anh Đạo luật lạm dụng máy tính 1990, Đạo luật tội phạm máy tính 1997 tại Malaysia, Luật máy tính Israel 1995,… Chính sự phát triển nhanh chóng của pháp luật đã làm cho tội phạm có tốc độ tăng trưởng giảm xuống. "Để đạt đến giai đoạn này, nhiều loại TPM đều được phát hiện và bị hình sự hóa, xác suất phát hiện hành vi phạm tội đã đạt đến cấp độ cao hơn, mức độ răn đe của hình phạt đã nghiêm khắc hơn, chỉ để lại không gian nhỏ cho các loại TPM."[16]

Và từ những năm 2000 đến nay, nhân loại chứng kiến sự bùng nổ của thời đại CNTT và đây là điều kiện cho sự phát triển nhanh chóng của TPCNC, khi mà tội phạm đang trở nên phổ biến thì các khoảng cách pháp lý đang dần được lấp đầy. Theo thống kê của Hội nghị Liên Hiệp Quốc về Thương mại và Phát triển, tính đến năm 2017, có 72% quốc gia tức gồm 138 nước đã có luật về an ninh mạng, 9% quốc gia đang dự thảo luật, 18% quốc gia không có pháp luật và 1% quốc gia không có dữ liệu về pháp luật TPCNC. [17] Từ thống kê, hầu hết các quốc gia phát triển và đang phát triển đều đưa ra những quy định nhằm phòng chống TPCNC và hầu hết là các nước thuộc khu vực Châu Âu, Châu Mỹ, và Châu Á, những quốc gia đang

[16] Johannes Xingan Li, Cyber crime and Legal countermeasures: A history Analysis.
[17]https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

dự thảo luật và chưa có luật về an ninh mạng đều là những quốc gia thuộc khu vực Châu Phi. Châu lục này là khu vực có nhiều nước kém phát triển vì vậy nhiều quốc gia chưa tiếp xúc nhiều máy tính và Internet dẫn đến TPCNC ở khu vực này chưa phổ biến.

Để làm rõ khía cạnh này nhóm nghiên cứu tiến hành phân tích pháp luật về xử lý TPCNC tại một số quốc gia trên thế giới cụ thể như sau:

Trung Quốc

Là quốc gia lớn và đông dân nhất thế giới, Trung Quốc vào năm 2018 đã có số lượng người sử dụng máy tính đạt mức 802 triệu người, giúp củng cố vị trí của nước này là cộng đồng trực tuyến lớn nhất thế giới.[18] Theo báo cáo của Symantec-nhà cung cấp phần mềm bảo mật máy tính như công cụ chống vi-rút thì Trung Quốc là nước có các hoạt động tấn công mạng bằng phần mềm độc hại phát triển mạnh nhất trong khu vực. Đồng thời quốc gia này cũng là nơi tồn tại nhiều hình thức tấn công do TPM gây ra. Với thực tế hoạt động mạnh mẽ và gây nên thiệt hại lớn cho xã hội của TPCNC, chính phủ Trung Quốc đã tiến hành những hành động thực tế nhằm ngăn chặn và xử lý loại tội phạm nguy hiểm này.

Vào ngày 7 tháng 11 năm 2016, Ủy ban thường vụ Đại hội Đại biểu Nhân dân Toàn quốc Cộng hòa Nhân dân Trung Hoa đã ban hành Luật An ninh mạng Trung Quốc và được thực hiện vào ngày 1 tháng 6 năm 2017.[19] Bộ luật gồm 79 điều, được chia làm 7 chương. Mục đích mà chính phủ Trung Quốc hướng đến khi xây dựng bộ luật này là để đảm bảo an ninh mạng; bảo vệ chủ quyền không gian mạng an ninh quốc gia, và lợi ích xã hội và công cộng; bảo vệ quyền và lợi ích hợp pháp của công dân, pháp nhân và các tổ chức khác; đồng thời thúc đẩy sự phát triển lành mạnh của thông tin hóa nền kinh tế và xã hội.[20] Các mục đích trên được cụ thể hóa

[18] Báo cáo của Trung tâm Thông tin Internet Trung Quốc (CNNIC).
[19]https://vi.wikipedia.org/wiki/Lu%E1%BA%ADt_An_ninh_m%E1%BA%A1ng_Trung_Qu%E1%BB%91c
[20] Điều 1 Luật an ninh mạng Trung Quốc.

bằng các hành động như sau: (1) Bảo vệ chủ quyền không gian mạng; (2) Xác định nghĩa vụ bảo mật của các nhà cung cấp sản phẩm và dịch vụ Internet; (3) Hoàn thiện các quy tắc bảo vệ thông tin cá nhân; (4) Thiết lập hệ thống bảo mật cho cơ sở hạ tầng thông tin quan trọng; (5) Thiết lập các quy tắc cho việc truyền dữ liệu xuyên quốc gia tại cơ sở hạ tầng thông tin quan trọng.[21] Có thể thấy nội dung của Luật an ninh mạng Trung Quốc đề cao vai trò và sự quản lý của nhà nước trong việc kiểm soát hoạt động của các nhà cung cấp mạng và người sử dụng mạng Internet. Các quy định của luật cũng nêu rõ chính phủ Trung Quốc có quyền ban hành các biện pháp nhằm giám sát, ngăn chặn và xử lý các rủi ro, đe dọa an ninh mạng phát sinh từ trong và ngoài lãnh thổ quốc gia này.[22] Đồng thời có các biện pháp trừng phạt các hoạt động bất hợp pháp và TPM theo quy định của pháp luật. Bên cạnh việc tạo ra quyền lực nhà nước trong hoạt động quản lý mạng, chính phủ Trung Quốc còn tiến hành đặt ra các quy định cho nhà cung cấp mạng yêu cầu các hoạt động kinh doanh và dịch vụ mạng phải tuân thủ luật pháp và các quy định hành chính, tôn trọng đạo đức xã hội, tuân thủ đạo đức thương mại, trung thực và đáng tin cậy, thực hiện nghĩa vụ bảo vệ an ninh mạng, chấp nhận sự giám sát của chính phủ và công chúng; đồng thời chịu trách nhiệm xã hội.[23] Các yêu cầu này được cụ thể hóa như sau: (1) Xây dựng hệ thống quản lý an ninh nội bộ và quy tắc hoạt động, xác định những người chịu trách nhiệm về an ninh mạng và thực hiện trách nhiệm bảo vệ an ninh mạng; (2) Áp dụng các biện pháp kỹ thuật để ngăn chặn virus máy tính, tấn công mạng, xâm nhập mạng và các hành động khác gây nguy hiểm cho an ninh mạng; (3) Áp dụng các biện pháp kỹ thuật để theo dõi và ghi lại trạng thái hoạt động của mạng và sự cố an ninh mạng và tuân theo các quy định để lưu trữ nhật ký mạng trong ít nhất sáu

[21]https://www.computerweekly.com/opinion/Chinas-first-cyber-security-law-what-it-means-for-companies
[22] Điều 5 luật an ninh mạng Trung Quốc.
[23] Điều 9 luật an ninh mạng Trung Quốc.

tháng; (4) Áp dụng các biện pháp như phân loại dữ liệu, sao lưu dữ liệu quan trọng và mã hóa; (5) Các nghĩa vụ khác được cung cấp bởi pháp luật hoặc các quy định hành chính.

Có thể thấy các quy định của Luật An ninh mạng Trung Quốc đã tạo nên một hệ thống các quy định và chế tài chặt chẽ nhằm để phòng và xử lý sự tấn công của TPCNC vào các trang mạng để thực hiện hành vi phạm pháp. Với số lượng người sử dụng mạng Internet đông nhất khu vực Châu Á, thì có thể thấy rằng động thái quan hành các quy định này của chính phủ Trung Quốc là vô cùng hợp lý giúp giảm thiểu một cách rõ rệt số lượng TPCNC lợi dụng mạng để thực hiện hành vi trái pháp luật.

Tuy nhiên, bên cạnh các ưu điểm, thì bộ luật Luật An ninh mạng của Trung Quốc vẫn còn tồn tại những bất cập nhất định. Ví dụ như Internet ở Trung Quốc đang dần mất đi tính lưu trữ thông thông tin và phát triển ứng dụng tự do khi chính phú tiến hành kiểm soát chặt chẽ cả về nội dung, mạng lưới kết nối, ứng dụng và các kênh giao tiếp. Một số quy định đề ra rằng người dùng mạng xã hội khi chia sẻ thông tin và bình luận nhạy cảm có thể bị phạt tù. Các công ty nước ngoài phải lắp đặt máy chủ tại Trung Quốc chứa dữ liệu của người Trung Quốc. Người dùng Internet phải đăng ký các dịch vụ trên mạng với tên thật, và dự kiến gắn liền với nó là hệ thống chấm điểm công dân. Hay các trang web không được chính phủ cấp phép bị cấm không được đăng bất kỳ tin tức gì trên mạng. Tất cả các quy định này vấp phải những phản đối không chỉ từ phía người dân mà còn từ các tập đoàn, doanh nghiệp đa quốc gia có hoạt động kinh doanh tại nội địa Trung Quốc. Họ cho rằng quyền riêng tư về mặt lưu trữ thông tin, liên lạc cá nhận đang có dấu hiệu bị xâm hại.

Hoa Kỳ

Là một nước phát triển Internet từ rất sớm, Hoa Kỳ đồng thời cũng phải đối mặt với hậu quả của TPCNC gây ra. Ngay đầu những năm 1980, các cơ quan thực thi pháp luật đã phải đối mặt với tình trạng số lượng tội

phạm ngày càng tăng về việc luật hình sự không thể chống lại TPCNC và tạo điều kiện cho tội phạm pháp triển. Thống kê của FBI (Cục điều tra liên bang Hoa Kỳ) cho biết năm 2006, tội phạm trên không gian ảo gây thiệt hại cho ngành công nghiệp CNTT nước này vào khoảng 400 tỷ USD.[24] Theo Christopher Painter, Vụ phó vụ TPM và các vấn đề sở hữu trí tuệ của Bộ tư pháp Hoa Kỳ. "Bây giờ chúng ta không còn thấy những hacker 'đơn thương độc mã' nữa mà thay vào đó là những nhóm tội phạm có tổ chức với mục tiêu tấn công được định nghĩa rõ ràng hơn."[25] Điển hình là các nhóm tội phạm chuyên ăn cắp thông tin cá nhân, thẻ tín dụng và những kẻ xây dựng hệ thống mạng botnet. Để bắt kịp với tốc độ phát triển của TPCNC, các nhà lập pháp Hoa Kỳ đã ban hành các đạo luật nhằm ngăn chặn, phòng chống kịp thời những hậu quả mà TPCNC gây ra.

Ba mươi năm trước, các cơ quan thực thi pháp luật Hoa Kỳ phải đối mặt với mối đe dọa mới đó là TPM mà không có sự trợ giúp nào từ các quy định tại BLHS Hoa Kỳ. Cho đến năm 1983, chính phủ nước Mỹ bắt đầu nhận ra tầm quan trọng, cấp thiết của việc xây dựng các đạo luật cụ thể để xử lý tội phạm công nghệ cao và bảo vệ an ninh mạng. Hoa Kỳ bắt đầu ban hành phần 1030 trong đạo luật kiểm soát tội phạm toàn diện năm 1984. Đồng thời, liên tục ban hành các văn bản pháp luật mới và sửa đổi luật cũ sao cho phù hợp với tình trạng diễn biến của TPM. Và tính đến nay Hoa Kỳ đã ban hành các bộ luật, quy định nhằm ngăn chặn và xử lý TPCNC như: Đạo luật tự do thông tin Hoa Kỳ 1996 (FOIA), Đạo luật bảo mật thông tin liên lạc điện tử 1986 (ECPA), Đạo luật chuyển tiền điện tử (EFTA).[26]

Trong số đó, phải kể đến Đạo luật lạm dụng và gian lận máy tính viết tắt là đạo luật CFAA. Đối mặt với tội phạm nguy hiểm mới hình thành, thay

[24]https://vi.wikipedia.org/wiki/T%E1%BB%99i_ph%E1%BA%A1m_c%C3%B4ng_ngh%E1%BB%87_cao
[25]https://vi.wikipedia.org/wiki/T%E1%BB%99i_ph%E1%BA%A1m_c%C3%B4ng_ngh%E1%BB%87_cao
[26] B. Lynn Winmill, David L. Metcalf and Michael E. Band, Cybercrime: Issues and challenges in the United States, pages 24.

vì sửa đổi BLHS để giải thích, quy định thêm về các tội liên quan đến TPCNC, Quốc hội Mỹ đã quyết định ban hành Đạo luật lạm dụng và gian lận máy tính (CFAA).

Đây là một quyết định đúng đắn và nó đã nhanh chóng trở thành một giải pháp rõ ràng, mạnh mẽ hơn trong việc đối phó TPCNC. Đạo luật gian lận và lạm dụng máy tính là một đạo luật an ninh mạng được Hoa Kỳ đã được ban hành vào năm 1986, với mục đích sửa đổi, bổ sung các quy định hiện hành còn thiếu sót trong việc xử lý hành vi gian lận máy tính (18 USC § 1030), vốn đã được quy định trong Đạo luật toàn diện tội phạm kiểm soát năm 1984. Mục đích của CFAA là để bảo vệ thông tin mật, hồ sơ tài chính, thông tin tín dụng về chính phủ và các tổ chức tài chính. Sau nhiều lần sửa đổi, đạo luật đã thêm hình phạt bổ sung cho hành vi gian lận và các hành vi khác liên quan đến kết nối và truy cập máy tính. Đạo luật cũng hình sự hóa các hành vi liên quan đến máy tính khác bao gồm các quy định xử phạt hành vi trộm cắp tài sản thông qua máy tính để xử phạt những người cố ý thay đổi, gây thiệt hại và cố ý thay đổi dữ liệu thông tin của người khác. Các nhà làm luật thông qua Đạo luật CFAA đã cố gắng đạt được sự cân bằng phù hợp những lợi ích của Chính phủ Liên bang trong tội phạm máy tính với lợi ích và khả năng của các bang để cấm và trừng phạt những hành vi phạm tội đã được quy định trong đạo luật.[27]

Đạo luật CFAA được áp dụng cho bất kỳ chủ thể nào trong phạm vi quyền tài phán của lãnh thổ Hoa Kỳ và các phán quyết, hoạt động điều tra sẽ được thi hành bởi bộ Tư pháp (DOJ), Cơ quan Mật vụ Hoa Kỳ (SS) và Cục Điều tra Liên bang (FBI). Trong những năm qua, đạo luật đã được sửa đổi nhiều lần nhằm theo kịp xu hướng phát triển của TPCNC và lần gần đây nhất là vào năm 2008. Theo đó, đạo luật cấm việc truy cập trái phép hoặc truy cập vượt quá ủy quyền để có được thông tin từ các máy tính của tổ chức tài chính,

[27] B. Lynn Winmill, David L. Metcalf and Michael E. Band, Cybercrime, Issues and challenges in the United States, pages 24, 25 26.

máy tính của chính phủ Hoa Kỳ hoặc máy tính được bảo vệ. Cấm các hành động khác với dữ liệu được bảo vệ hoặc hạn chế nhất định ảnh hưởng đến lợi ích quốc gia hoặc tạo lợi thế cho bất kỳ quốc gia nước ngoài nào.[28]

Kể từ khi ra đời, CFAA đã xử lý được rất nhiều vụ án lớn về TPCNC trong nhiều lĩnh vực. Điển hình là vụ án Palpay 14,[29] Palpay 14 là vụ án mà một nhóm tập thể nam nữ ẩn danh đã phạm tội với tội danh âm mưu phá vỡ quyền truy cập vào trang web thanh toán Palpay, 13 người trong số đó đã nhận tội trong một tòa án ở California , Hoa Kỳ vào tháng năm 2013. Trong đó, 11 trong số 13 bị cáo bị buộc tội vào một trọng tội theo Đạo luật Lừa đảo và Lạm dụng Máy tính vì hành vi công khai gây thiệt hại có chủ ý cho một máy tính được bảo vệ. Trong một số trường hợp nhất định, CFAA cho phép một cá nhân bị thiệt hại phải đưa ra một vụ kiện dân sự để bồi thường thiệt hại hoặc giảm nhẹ trách nhiệm đối với người vi phạm.

Bên cạnh đó, CFAA còn có một số bất cập như việc sử dụng các khái niệm công nghệ lỗi thời trong các hoạt động hàng ngày gây ảnh hưởng đến trong quá trình xét xử. Các định nghĩa mơ hồ của CFAA cung cấp một cách thụ động quyết định truy tố rộng rãi có thể biến hàng triệu người dùng Internet hàng ngày thành tội phạm, ngay cả trong các trường hợp vi phạm phổ biến thỏa thuận điều khoản dịch vụ trực tuyến.

Anh quốc

Vương quốc Anh là một trong những nền kinh tế lớn nhất thế giới, nổi tiếng với sức mạnh dịch vụ tài chính, khiến nó trở thành mục tiêu hàng đầu cho các tin tặc tham vọng nhất thế giới. Theo thống kê vào năm 2012-2013 đã có sự gia tăng 60% số lượng báo cáo về TPM, và trong cũng khoảng thời gian này số thiệt hại về tài chính mà TPM và các loại gian lận khác gây thiệt hại cho nền kinh tế Anh 81 tỷ bảng.[30] Hay gần đây vào năm 2018,

[28] Office of Legal Education Executive Office for United States Attorneys : Prosecuting Computer Crimes
[29] https://en.wikipedia.org/wiki/PayPal_14#References
[30] Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter: 12.

54% các vụ lừa đảo tại quốc gia này có liên quan đến mạng Internet.[31] Với mục đích nâng cao hiệu quả trong hoạt động ngăn chặn và xử lý TPCNC thì nước Anh mặc dù là một quốc gia theo hệ thống thông luật chủ yếu sử dụng những án lệ thì nay cũng đã xây dựng cho mình các hành làng pháp luật hoàn thiện và đầy đủ nhất nhằm điều chỉnh loại tội phạm nguy hiểm này.[32]

Đặc biệt phải kể đến Đạo luật lạm dụng máy tính năm 1990 đây là đạo luật đầu tiên quy định rõ nhất các hành vi phạm tội của TPCNC cũng như thực hiện xác định thẩm quyền, phạm vi xét xử với loại tội phạm này. Đạo luật này gồm 18 điều và được chia thành 3 chương. Chương 1 gồm các quy định định nghĩa hành vi bị xem là phạm tội hình sự liên quan đến công nghệ cao. Chương 2 đạo luật xác định thẩm quyền của các cơ quan nhà nước trong hoạt động xử lý TPCNC đồng thời chỉ rõ phạm vi xét xử của các cơ quan tài phán. Cuối cùng, Chương 3 của Đạo luật lạm dụng máy tính năm 1990 đưa ra các quy định hướng dẫn dành cho các quốc gia thành viên phụ thuộc Vương quốc Anh như Scotland, Bắc Ireland trong hoạt động phối hợp nhằm nâng cao chất lượng hoạt động ngăn chặn xử lý TPCNC.

Đạo luật lạm dụng máy tính 1990 ra đời đã góp phần làm giảm sự gia tăng đáng kể của TPCNC ở Anh trong giai đoạn này. Các quy định trong đạo luật bước đầu đã hạn chế được những hành vi phổ biến của TPCNC như truy cập trái phép vào dữ liệu máy tính hay những hành vi gây thiệt hại nghiêm trọng. Đạo luật lạm dụng máy tính năm 1990 tuy chưa phân biệt đầy đủ các loại TPM tuy nhiên các quốc gia khác như Canada và Cộng hòa Ireland đã lấy cơ sở từ đạo luật này để phát triển đạo luật riêng vì đạo luật này được xem là một bộ luật đủ mạnh mẽ và linh hoạt để đối phó với TPM.[33]

[31] https://www.governmenteuropa.eu/cybercrime-in-the-uk/92545/
[32] Phụ lục 1.

[33] Computer Misuse Act 1990: https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990

Đến năm 2015, Đạo luật lạm dụng máy tính năm 1990 đã được sửa đổi và đưa vào Đạo luật tội phạm nghiêm trọng 2015. Dự luật đã được Quốc hội thông qua vào ngày 2 tháng 3 năm 2015 và nhận được sự đồng ý của hoàng gia vào ngày 3 tháng 3 năm 2015. Phần về TPCNC được sửa đổi và đưa vào phần II của đạo luật Đạo luật tội phạm nghiêm trọng 2015. Đạo luật mới đã mở rộng phạm vi xác định hành vi phạm tội của TPCNC bao gồm việc cung cấp công cụ để thực hiện hành vi vi phạm bất kể ý định cung cấp công cụ đó và việc mở rộng hành vi phạm tội hiện có để có thể dễ dàng hơn trong việc bắt giữ cá nhân sử dụng các công cụ để thực hiện hành vi phạm tội lạm dụng máy tính.

Trong lĩnh vực xét xử, Đạo luật tội phạm nghiêm trọng 2015 mở rộng phạm vi lãnh thổ trong việc xét xử bằng cách quy định rõ hơn về "quốc tịch Anh" vào quyền tài phán trong nước. Điều này cung cấp một cơ sở pháp lý để truy tố một công dân Vương quốc Anh thực hiện bất kỳ hành vi phạm tội nào bên ngoài lãnh thổ, nơi không có liên quan đến Vương quốc Anh ngoài quốc tịch của người phạm tội, với điều kiện là hành vi phạm tội cũng là một hành vi phạm tội ở quốc gia nơi nó đã diễn ra.

Nhìn chung, để bắt kịp với xu hướng phát triển của TPM về số lượng và về phương thức thủ đoạn, Vương quốc Anh cũng đã mở rộng đối tượng phạm tội, phạm vi xét xử nhằm kiểm soát tốt hơn không gian mạng, tránh cho tội phạm có cơ hội thoát tội.

Các thỏa thuận song phương, đa phương về xử lý tội phạm công nghệ cao trên thế giới

Rất nhiều quốc gia trên thế giới báo cáo rằng, từ 50% đến 100% hoạt động của TPCNC là có tính chất xuyên quốc gia.[34] Việc mở rộng nhanh chóng của CNTT và kết nối máy tính toàn cầu đã tạo cơ hội cho TPCNC khai thác các lỗ hổng bảo mật trong môi trường trực tuyến tại nhiều quốc gia khác nhau. Tính chất xuyên quốc gia của TPCNC đã đặt ra thách thức

[34] Comprehensive study on cybercrime by United Nations office on drugs and crime, pages 183.

cho các quốc gia trên thế giới về việc xây dựng pháp luật nhằm ngăn chặn và quản lý loại hình tội phạm này không chỉ tại lãnh thổ quốc gia mình mà còn ở các tình huống xuyên biên giới. Thực trạng này đòi hỏi hoạt động truy tố các hành vi của TPCNC xuyên quốc gia phải có được hai loại quyền tài phán cơ bản. Thứ nhất là các quốc gia có quyền tài phán đối với TPCNC ở lãnh thổ đất nước mình. Thứ hai, các quốc gia phải có khả năng thực hiện các hoạt động điều tra liên quan đến TPCNC trên lãnh thổ quốc gia khác.[35] Tuy nhiên những hành vi này rất dễ dẫn đến xâm phạm chủ quyền của quốc gia. Do đó việc tạo ra một thỏa thuận chung giữa các quốc gia với nhau là điều vô cùng cần thiết. Nhận thấy được nhu cầu cấp bách này các quốc gia đã cùng nhau xây dựng những thỏa thuận song phương, đa phương nhằm điều chỉnh, hòa hợp nhiều vấn đề về xử lý TPCNC. Theo báo cáo của Văn phòng Liên Hiệp Quốc về chống Ma túy và Tội phạm, viết tắt tiếng Anh là UNODC, thì từ những năm 2000 trở đi, bắt đầu từ khu vực Châu Âu, thì đến nay trên thế giới đã có thể ghi nhận được 19 công ước điều chỉnh về lĩnh vực TPCNC.[36] Sự ra đời của hàng loạt các hiệp định song phương, đa phương giữa các quốc gia trên thế giới thể hiện nhận thức của con người về sự cấp bách trong hoạt động ngăn chặn, xử lý TPCNC.

Công ước của Hội đồng Châu Âu về tội phạm mạng (Budapest 2001)

Một trong những thỏa thuận đa phương về TPCNC được thiết lập mà có sự gia nhập của nhiều quốc gia nhất chính là Công ước của Hội đồng Châu Âu về TPM, gọi tắt là Công ước Budapest. Đây là công ước quốc tế đầu tiên tìm cách giải quyết vấn đề Internet và tội phạm máy tính (TPM) bằng cách hài hòa pháp luật quốc gia, nâng cao kỹ thuật điều tra, và tăng cường hợp tác giữa các dân tộc. Công ước Budapest được soạn thảo bởi Hội đồng Châu Âu tại Strasbourg, Pháp, ngày 23 tháng 11 năm 2001.[37]

[35] Comprehensive study on cybercrime by United Nations office on drugs and crime, pages IV.
[36] Phụ lục 2.
[37] https://en.wikipedia.org/wiki/Convention_on_Cybercrime

Được soạn thảo và thành lập bởi những quốc gia đi đầu về lĩnh vực công nghệ cũng như lập pháp, sự ra đời của các công ước tạo nên một môi trường nhằm hòa hợp pháp luật của các quốc gia, đồng thời tạo nên cơ chế hợp tác nhằm ngăn chặn, xử lý TPCNC. Tính đến tháng 9 năm 2019, 64 quốc gia đã phê chuẩn công ước, trong khi bốn quốc gia khác đã ký kết công ước nhưng không phê chuẩn. Công ước không chỉ dành riêng cho các quốc gia thành viên của Liên minh Châu Âu mà còn cho phép các quốc gia không phải là thành viên tham gia kí kết. Điển hình là Canada , Nhật Bản , Hoa Kỳ và Nam Phi đã tiến hành kí kết công ước vào ngày 23 tháng 11 năm 2001 tại Budapest . Úc, Canada, Cộng hòa Dominican, Israel, Nhật Bản, Mauritius, Panama, Sri Lanka và Hoa Kỳ tiến hành phê chuẩn công ước Budapest từ tháng 7 năm 2016.[38]

Với 48 điều được chia làm 3 chương, Công ước Budapest đặt ra mục đích tạo nên sự hài hòa giữa các yếu tố pháp luật hình sự trong nước và các điều khoản trong lĩnh vực TPM. Công ước đã tiến hành định nghĩa và phân loại loại TPCNC làm bốn nhóm từ điều 2 tới điều 10: Nhóm 1 gồm các tội phạm chống lại tính bí mật, toàn vẹn và sẵn có của dữ liệu máy tính và hệ thống máy tính; Nhóm 2 các tội phạm liên quan đến máy tính; Nhóm 3 Các tội phạm liên quan đến nội dung; Nhóm 4 Các tội phạm xâm phạm quyền tác giả và quyền liên quan. Tiếp đến Công ước đã nêu các hình thức hợp tác mà các quốc gia thành viên có thể áp dụng cụ thể như sau: Quốc gia thành viên công ước có thể, trong phạm vi giới hạn luật quốc gia mình và không có yêu cầu trước, chuyển cho quốc gia thành viên công ước khác các thông tin thu thập được trong quá trình điều tra của mình nếu như quốc gia này thấy việc tiết lộ thông tin ấy có thể giúp cho quốc gia tiếp nhận thông tin khởi động hoặc tiến hành điều tra hoặc hoạt động tố tụng về tội phạm quy định trong công ước này hoặc có thể dẫn đến việc yêu cầu hợp tác bởi

[38]https://en.wikipedia.org/wiki/Convention_on_Cybercrime#Accession_by_other_non%E2%80%93Council_of_Europe_states.

quốc gia thành viên.[39] Tại chương 3 công ước đã thiết lập được một cơ chế hợp tác quốc tế nhanh chóng và hiệu quả đảm bảo được sự dung hòa pháp luật của các quốc gia. Giúp tạo điều kiện cho việc truy bắt, dẫn độ tội tội phạm và thực hiện các thủ tục tố tụng được dễ dàng dù ở trong hay ngoài lãnh thổ quốc gia. Cụ thể như sau: nếu một quốc gia thành viên công ước quy định việc dẫn độ phải có điều kiện là có hiệp định dẫn độ với quốc gia thành viên công ước khác, mà hiện tại giữa các quốc gia này chưa có hiệp định dẫn độ, thì quốc gia thành viên công ước có thể coi công ước này là cơ sở pháp lý cho việc dẫn độ.[40] Không chỉ dừng lại ở đó, công ước này còn tạo ra những điều kiện thuận lợi để các quốc gia hỗ trợ nhau trong vấn đề tương trợ tư pháp cụ thể như sau: Trường hợp không có hiệp định tương trợ tư pháp hoặc các thoả thuận về việc áp dụng luật thống nhật hoặc về việc áp dụng nguyên tắc có đi có lại điều chỉnh quan hệ giữa bên yêu cầu tương trợ và bên được yêu cầu tương trợ thì các quốc gia có thể căn cứ áp dụng quy định tại Khoản 2 đến Khoản 9 Điều 27 của công ước này.[41]

Có thể khẳng định rằng sự ra đời của công ước Budapest sẽ cung cấp một khung pháp lý chung nhằm loại bỏ các rào cản tài phán để tạo điều kiện cho việc thực thi pháp luật đối với các TPCNC hoạt động xuyên biên giới, tuy nhiên việc tạo lập một cơ chế pháp lý chung trên toàn thế giới vẫn còn gặp nhiều khó khăn. Nguyên nhân chính được xác định là do hoạt động nội luật hóa các điều khoản của Công ước còn nhiều vướng mắc. Các quy định yêu cầu hình sự hóa các hoạt động như hack (bao gồm sản xuất, bán hoặc phân phối các công cụ hack) và các hành vi phạm tội liên quan đến nội dung khiêu dâm trẻ em và mở rộng TNHS đối với các vi phạm sở hữu trí tuệ. Nó cũng yêu cầu mỗi quốc gia ký kết phải thực hiện các cơ chế tố tụng liên quan trong luật pháp của họ. Ví dụ, các cơ quan thực thi pháp luật có quyền buộc nhà cung cấp dịch vụ Internet theo dõi hoạt động của của

[39] Khoản 1, điều 26, công ước về tội phạm mạng Budapest 2001.
[40] Khoản 3, điều 24, công ước về tội phạm mạng Budapest 2001.
[41] Khoản 1, điều 27, công ước về tội phạm mạng Budapest 2001.

người sử dụng nhằm tạo điều kiện cho quá trình điều tra. Ngoài ra Công ước yêu cầu các quốc gia ký kết phải tạo điều kiện hợp tác quốc tế ở mức độ rộng nhất có thể để giúp cho các cuộc điều tra và tố tụng liên quan đến các TPCNC cao hình sự nhằm thu thập bằng chứng dưới dạng điện tử của tội phạm hình sự một cách nhanh chóng và đầy đủ. Các cơ quan thực thi pháp luật sẽ phải hỗ trợ cảnh sát từ các quốc gia tham gia khác hợp tác với các yêu cầu hỗ trợ lẫn nhau của họ. Sự hỗ trợ này đòi hỏi sự chia sẻ thông tin, cũng như quyền truy cập vào mạng lưới Internet giữa các quốc gia. Nhưng thực tế hiện nay thấy rằng, Internet và mạng viễn thông là một trong những giao thức chính của các quốc gia nhằm lưu trữ, trao đổi và quản lý các thông tin công việc nội bộ quan trọng liên quan đến chính trị, quốc phòng, an ninh quốc gia. Đây là lí do chính tạo nên sự khó khăn trong việc hợp tác nhằm chia sẻ thông tin cũng như quyền truy cập dữ liệu giữa các quốc gia với nhau trong hoạt động truy bắt TPCNC. Chính sự khó khăn này đã khiến các quốc gia quan trọng như Brazil và Ấn Độ đã từ chối thông qua Công ước với lý do họ không tham gia soạn thảo. Nga phản đối Công ước, tuyên bố rằng việc áp dụng sẽ vi phạm chủ quyền của Nga và thường từ chối hợp tác trong các cuộc điều tra thực thi pháp luật liên quan đến TPM.

Thực tế áp dụng công ước Budapest có thể còn nhiều khó khăn vướng mắc. Tuy nhiên vẫn phải khẳng định rằng, tính đến thời điểm hiện này thì Công ước Budapest là một trong những công ước cung cấp đầy đủ nhất các các công cụ cần thiết cho việc điều tra và truy tố TPCNC cũng như các hành vi phạm tội khác được thực hiện bằng hệ thống máy tính hoặc bằng chứng liên quan đến hình thức điện tử. Sự chia sẻ thông tin giữa các quốc gia một cách nhanh chóng, kịp thời, chính là phương tiện hữu hiệu nhất giúp xử lý TPCNC. Đặc biệt, Công ước Budapest còn có tầm ảnh hưởng quan trọng trong việc tạo lập nên các công cụ hợp tác tại các châu lục khác.

1.3.2. Quy định của pháp luật Việt Nam về xử lý tội phạm công nghệ cao

Quy định về xử lý tội phạm công nghệ cao trong pháp luật hình sự

Ở thời kỳ đất nước ta đang trong giai đoạn đầu bước vào quá trình đổi mới đất nước sau khi giành độc lập. Năm 1985 BLHS đầu tiên của nước ta ra đời trên cơ sở của nền kinh tế bao cấp và thực tiễn của tình hình tội phạm thời kỳ đó. BLHS năm 1985 với ý nghĩa là nguồn duy nhất trong đó quy định tội phạm và hình phạt. Tại Việt Nam, dịch vụ Internet được chính thức cung cấp vào năm 1997. Giai đoạn này về mặt đời sống xã hội, sự phát triển kinh tế và nhận thức của người dân còn nhiều hạn chế nên TPCNC thời kỳ gần như không xuất hiện do thực tiễn xã hội không tồn tại mối quan hệ này nên các nhà làm luật không thể điều chỉnh.

Bộ luật hình sự năm 1999

Với sự hội nhập quốc tế tương đối nhanh chóng của nước ta, trước sự thay đổi về mọi mặt kinh tế - xã hội trong thời kỳ hội nhập và cùng với nền kinh tế trên đà phát triển kéo theo sự xuất hiện của loại tội phạm công nghệ. Đến năm 1999 giai đoạn mới xuất hiện hoạt động của tội phạm chủ yếu nhằm mục đích gây rối trật tự an ninh. BLHS năm 1999 quy định tại chương XIX các tội xâm phạm an toàn công cộng, trật tự công công trong đó tội phạm sử dụng công nghệ cao với 3 tội danh có liên quan đến máy tính, mạng máy tính tại các (Điều 224) Tội tạo ra và lan truyền, phát tán các chương trình vi - rút tin học; (Điều 225) Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử; (Điều 226) Tội sử dụng trái phép thông tin trên mạng và trong máy tính. Nhìn chung, những quy định về tội danh tội phạm công nghệ thời điểm này cho thấy hành vi của tội phạm là hành vi trực tiếp tấn công dữ liệu máy tính, xâm hại trật tự an ninh CNTT sử dụng công nghệ làm mục đích phạm tội chứ chưa đề cập tới hành vi sử dụng CNTT như công cụ phạm tội. Việc sửa đổi là để phù hợp với sự biến đổi, phát triển của tình hình kinh tế, chính trị, xã hội lúc bấy giờ. Tuy nhiên, những quy định trên đã bộc lộ nhiều điểm hạn chế

và không còn phù hợp để điều chỉnh các quan hệ xã hội. Không thể dậm chân tại chỗ mà phải chủ động bắt kịp xu thế phát triển từ đó tiến hành sửa đổi, bổ sung chiến lược, chính sách pháp luật phù hợp với hoàn cảnh của đất nước. Trước tình hình đó Quốc hội đã tiến hành đã sửa đổi, bổ sung 1999 đề phù hợp với tình hình thực tiễn.

Bộ luật hình sự 1999 (Sửa đổi, bổ sung 2009)

Nhằm đáp ứng và phục vụ công cuộc đấu tranh phòng chống tội phạm nhằm khắc phục tạm thời những hạn chế của BLHS 1999. BLHS năm 1999 (sửa đổi, bổ sung năm 2009) cho rằng TPCNC là các tội phạm mà khách thể của tội phạm xâm hại đến hoạt động bình thường của máy tính và mạng máy tính được quy định chi tiết tại chương XIX các tội xâm phạm an toàn công cộng, trật tự công công trong đó quy định tội phạm sử dụng công nghệ cao quy định tại (Điều 224) Tội phát tán vi rút, chương trình tin học có tính năng gây hại cho hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số; (Điều 225) Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, mạng Internet, thiết bị số; (Điều 226) Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông, mạng Internet; (Điều 226a) Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác; (Điều 226b) Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản.

BLHS 1999 (sửa đổi bổ sung 2009) tiếp cận dưới góc độ TPCNC chỉ là tội phạm được thực hiện và gây hậu quả trên môi trường ảo, thế giới ảo do thành tựu của khoa học công nghệ tin học đem lại và nó hoàn toàn khác với các loại tội phạm truyền thống trước kia. Phương pháp tiếp cận này tuy có ưu điểm là định rõ được tội danh cần xử lý nhưng lại có nhược điểm là rất dễ bỏ sót những hành vi nguy hiểm cho xã hội cần được coi là tội phạm, nhất là trong bối cảnh CNTT đang phát triển mạnh mẽ trong tình hình hiện

nay.[42] BLHS 1999 (sửa đổi, bổ sung 2009) không những có những quy định về một số hành vi trực tiếp tấn công dữ liệu máy tính, xâm hại trật tự an ninh CNTT sử dụng công nghệ làm mục đích phạm tội mà đã đề cập tới hành vi sử dụng CNTT như công cụ, phương tiện phạm tội. Tuy nhiên BLHS năm 1999 (sửa đổi, bổ sung năm 2009) chưa quy định hết các hành vi nguy hiểm cho xã hội có liên quan đến tội phạm máy tính, tội phạm mạng máy tính.

Bộ luật hình sự năm 2015

Tiến bộ mạnh mẽ về khoa học - công nghệ, đặc biệt là cuộc cách mạng công nghiệp 4.0 mở đường cho những bước nhảy vọt trên nhiều lĩnh vực. Tình hình tội phạm sử dụng công nghệ cao xem công nghệ cao làm mục đích tấn công hoặc sử dụng công nghệ cao làm công cụ, phương tiện hữu hiệu để thực hiện hành vi bất hợp pháp của mình cũng gia tăng nhanh chóng. Những mối nguy hiểm như khủng bố và an ninh không gian mạng, an ninh tài chính, diễn biến ngày càng phức tạp, tác động sâu sắc đến nước ta. Tội phạm sử dụng công nghệ cao tập trung chủ yếu tại các thành phố lớn, các đối tượng thường tập hợp, liên kết với nhau thông qua các diễn đàn trên mạng Internet (còn gọi là underground hay thế giới ngầm). Vì vậy thủ đoạn ngày càng tinh vi, kín đáo và liên tục thay đổi phương thức nhằm lẩn tránh sự phát hiện của cơ quan. Trước tình hình tội phạm có những dấu hiệu diễn biến mạnh mẽ, việc sửa đổi, bổ sung BLHS năm 1999 cũng chưa thể bảo đảm quy định hết các hành vi nguy hiểm cho xã hội có liên quan đến tội phạm máy tính, tội phạm mạng máy tính cần được coi là TPCNC. Ví dụ, như hiện nay đang tranh cãi về việc có coi hành vi trộm cắp, lừa đảo tài sản (như kiếm, áo giáp… trong các trò chơi ảo) mà người chơi game có được xem chơi trò chơi trực tuyến hay không. Tuy nhiên, những "tài sản ảo" này có thể quy đổi ra giá trị thực khi người chơi này bán

[42] Nguyễn Ngọc Anh, Một số quy định pháp luật về tội phạm công nghệ cao, Tạp chí CSND tháng 11/2014.

cho người chơi khác như những tài sản vật chất khác nên khi bị xâm hại, người chơi game bị thiệt hại như những tài sản vật chất khác và có nên đặt vấn đề pháp luật cần phải bảo vệ những "tài sản ảo" này như những tài sản thực khác.[43] Điều này cho thấy trong thời đại 4.0 thì tội phạm vẫn là những tội danh truyền thống nhưng cách thức thực hiện hành vi là phi truyền thống. BLHS 2015 ra đời khắc phục hạn chế, bổ sung thêm và cụ thể hóa 5 tội danh mới về tội phạm trong lĩnh vực CNTT và mạng viễn thông, quy định phù hợp để có thể phòng ngừa, đấu tranh một cách có hiệu quả loại tội phạm mới đặc biệt nguy hiểm này.

Tội phạm sử dụng công nghệ cao trong BLHS 2015 được quy định tại Chương XXI Các tội phạm xâm phạm an toàn công cộng, trật tự công cộng. Cụ thể tại Mục 2 các tội phạm trong lĩnh vực CNTT, mạng viễn thông từ Điều 285 – Điều 294. Nhóm tội phạm sử dụng công nghệ cao thuần tuý xâm phạm trật tự an toàn thông tin, các tội phạm sử dụng công nghệ cao thuộc loại này bao gồm : (Điều 285) Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật; (Điều 286) Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; (Điều 287) Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; (Điều 289) Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác.

Nhóm tội phạm sử dụng máy tính, thiết bị số, mạng máy tính, mạng viễn thông làm công cụ, phương tiện phạm tội gồm các tội phạm "truyền thống" nhưng được thực hiện với thủ đoạn mới, tức sử dụng CNTT để thực hiện tội phạm.[44] Tội phạm sử dụng công nghệ cao thuộc nhóm này gồm: (Điều 288) Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng

[43] Nguyễn Ngọc Anh, Một số quy định pháp luật về tội phạm công nghệ cao, Tạp chí CSND tháng 11/2014.

[44] Hoàng Việt Quỳnh, Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định pháp luật Việt Nam**,** Tạp chí KHGD CSND số 79 (tháng 8/2016).

viễn thông; (Điều 290) Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản; (Điều 291) Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng; (Điều 292) Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông; (Điều 293) Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh; (Điều 294) Tội cố ý gây nhiễu có hại.

BLHS 2015 đã nhìn nhận được bối cảnh mất an toàn thông tin, nguy cơ chiến tranh thông tin ngày một hiện hữu. Tội phạm không những sử dụng công nghệ là mục đích mà tội phạm đã lợi dụng nền phát triển kinh tế, sự phát triển của các thiết bị máy tính, mạng viễn thông trong thời đại công nghệ 4.0 đã coi công nghệ như là một công cụ, phương tiện hữu hiệu để thực hiện hành vi bất hợp pháp của mình.

Theo đó BLHS 2015 đã có những điểm mới về nhóm tội phạm CNTT, mạng viễn thông. Thứ nhất, bổ sung thêm và cụ thể hóa 5 tội danh mới về Tội phạm trong lĩnh vực CNTT và mạng viễn thông xuất phát từ thực tiễn công tác đấu tranh, chống và phòng ngừa các tội phạm thời gian qua bao gồm: (Điều 285)Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật; (Điều 291) Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng; (Điều 292) Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông; (Điều 293) Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh; (Điều 294) Tội cố ý gây nhiễu có hại. Những tội danh mới bổ sung này được quy định cụ thể về dấu hiệu hành vi, hậu quả thiệt hại tính toán được cũng như chế tài xử lý tương xứng với tính chất và hậu quả gây thiệt hại của người phạm tội trong tình hình hiện nay.

Thứ hai, sửa đổi, bổ sung lại 5 tội danh về tội phạm trong lĩnh vực CNTT và mạng viễn thông từ Điều 286 đến Điều 290 với việc bỏ dấu hiệu

"gây hậu quả nghiêm trọng, rất nghiêm trọng, đặc biệt nghiêm trọng". Tuy nhiên, thực tế chưa xét xử được vụ nào, một phần là do bế tắc trong công tác giám định. Việc quy định cụ thể dấu hiệu hành vi và tính toán cụ thể hậu quả thiệt hại cụ thể (bằng số phút, số giờ; số tiền cụ thể…) như tại khoản 1 Điều 287 BLHS năm 2015 Người nào tự ý xóa, làm tổn hại hoặc thay đổi phần mềm, dữ liệu điện tử hoặc ngăn chặn trái phép việc truyền tải dữ liệu của mạng máy tính, mạng viễn thông, phương tiện điện tử hoặc có hành vi khác cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; phạt tiền từ 30.000.000 đồng đến 200.000.000 đồng hoặc phạt tù từ 06 tháng đến 03 năm các trường hợp làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử từ 30 phút đến dưới 24 giờ hoặc từ 03 lần đến dưới 10 lần trong thời gian 24 giờ; Làm đình trệ hoạt động của cơ quan, tổ chức từ 24 giờ đến dưới 72 giờ; Quy định giúp cho công tác phát hiện, điều tra, truy tố, xét xử được tiến hành nhanh chóng, kịp thời và chính xác hơn.

Thứ ba, tăng cường, mở rộng áp dụng chế tài phạt tiền là hình phạt chính áp dụng đối với nhóm tội phạm trong lĩnh vực CNTT và mạng viễn thông thuộc trường hợp phạm tội ít nghiêm trọng (khung hình phạt đến 3 năm tù) hoặc nghiêm trọng (khung hình phạt từ trên 03 năm đến 07 năm tù) với mức phạt tiền thấp nhất là từ 20 triệu đồng đến mức cao nhất là 1,5 tỷ đồng.

Bộ Luật cũng đã sửa đổi tăng mức phạt tiền là hình phạt bổ sung tại 8/10 tội danh trong lĩnh vực CNTT và mạng viễn thông; bổ sung thêm quy định "tịch thu một phần hoặc toàn bộ tài sản" do người phạm tội có được so với quy định trước đây.[45]

Thứ tư, cụ thể hóa dấu hiệu hậu quả thiệt hại tại tất cả các tội danh qua các tình tiết tăng nặng TNHS như: thu lợi bất chính, gây thiệt hại (số tiền cụ thể); Làm lây nhiễm phương tiện điện tử hoặc hệ thống thông tin (số

[45] http://tapchitaichinh.vn/nghien-cuu--trao-doi/trao-doi-binh-luan/hoan-thien-khung-kho-phap-ly-xu-phat-toi-pham-cong-nghe-thong-tin-mang-vien-thong-112331.html

lượng người sử dụng cụ thể); Làm tê liệt, gián đoạn, ngưng trệ hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử (theo số phút, giờ hoặc số lần truy cập/24h); Làm đình trệ hoạt động của cơ quan, tổ chức (số giờ). Quy định này giúp cho cơ quan chức năng có thể tiến hành các thủ tục tố tụng, xác minh hậu quả thiệt hại một cách nhanh chóng, chính xác trong các giai đoạn tố tụng.[46]

Thứ năm, sửa đổi, bổ sung một số quy định mới về hậu quả thiệt hại tại khoản 2 liên quan đến "Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông" (Điều 288) xuất phát từ thực tiễn diễn biến phức tạp của loại tội phạm này thời gian qua cũng như hậu quả nguy hiểm do hành vi này mang lại như: Xâm phạm bí mật cá nhân dẫn đến người bị xâm phạm tự sát; Gây ảnh hưởng xấu đến an ninh, trật tự, an toàn xã hội hoặc quan hệ đối ngoại của Việt Nam. Khoản 2 Điều 288 cũng bổ sung mức phạt tiền từ 200 triệu đồng đến 1 tỷ đồng đối với người phạm tội so với quy định cũ nhằm tạo điều kiện cho người phạm tội khắc phục hậu quả thiệt hại do hành vi của mình gây ra.[47]

Thứ sáu, sửa đổi, bổ sung một số quy định mới về "tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản" khi người phạm tội sử dụng mạng máy tính, mạng viễn thông hoặc phương tiện điện tử thực hiện những hành vi: Lừa đảo trong thanh toán điện tử, kinh doanh đa cấp hoặc thiết lập, cung cấp trái phép dịch vụ viễn thông, Internet nhằm chiếm đoạt tài sản nhưng không thuộc trường hợp của tội trộm cắp tài sản và tội lừa đảo chiếm đoạt tài sản.[48]

Năm 2015, Quốc hội Việt Nam thông qua Luật An toàn thông tin mạng, tạo nền tảng pháp lý và nâng cao chất lượng hoạt động bảo vệ các hệ

[46] http://tapchitaichinh.vn/nghien-cuu--trao-doi/trao-doi-binh-luan/hoan-thien-khung-kho-phap-ly-xu-phat-toi-pham-cong-nghe-thong-tin-mang-vien-thong-112331.html
[47] http://tapchitaichinh.vn/nghien-cuu--trao-doi/trao-doi-binh-luan/hoan-thien-khung-kho-phap-ly-xu-phat-toi-pham-cong-nghe-thong-tin-mang-vien-thong-112331.html
[48] http://tapchitaichinh.vn/nghien-cuu--trao-doi/trao-doi-binh-luan/hoan-thien-khung-kho-phap-ly-xu-phat-toi-pham-cong-nghe-thong-tin-mang-vien-thong-112331.html.

thống CNTT và mạng máy tính của Việt Nam trước các cuộc tấn công của TPCNC. Trên cơ sở đó, Chính phủ đã ban hành nhiều văn bản triển khai thực hiện Luật An toàn thông tin mạng vào cuộc sống như: Nghị định 58/2016/NĐ-CP quy định chi tiết về kinh doanh sản phẩm, dịch vụ mật mã dân sự và xuất khẩu, nhập khẩu sản phẩm mật mã dân sự; Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định 108/2016/NĐCP quy định chi tiết điều kiện kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng; Quyết định 05/2017/QĐ-TTg ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia… Năm 2017, Chính phủ đã ban hành một số văn bản hướng dẫn thực thi Luật này, và các quy định hướng dẫn tiếp tục được ban hành trong thời gian tới. Lực lượng tham gia phòng chống TPCNC của Việt Nam hiện có Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông và các Bộ chủ quản hệ thống thông tin. Một số bộ chủ quản, trong đó có Bộ Tài chính, đã thành lập phòng chuyên trách về an toàn an ninh thông tin.

Luật An ninh mạng 2019

Xuất phát từ mục đích không lành mạnh, bất hợp pháp của một số người mà ngày nay tính ưu việt của Internet đã bị lợi dụng nó trở thành miếng mồi màu mỡ cho tội phạm thực hiện hành vi phạm tội của mình, khống chỉ thế Internet cũng là công cụ nguy hiểm gây bất ổn cho xã hội. Nhìn nhận rõ mối đe dọa của TPCNC đối với an ninh mạng quốc gia, các quốc gia phát triển trên thế giới như Mỹ, Anh, Hà Lan, Pháp, Canada, Hàn Quốc,.. đã thiết lập các chủ trương, chính sách, văn bản pháp luật nhằm tạo ra các thiết chế, cơ sở pháp lý chống lại mối đe dọa từ không gian mạng; thành lập các lực lượng chuyên trách về an ninh mạng, tình báo mạng, chiến tranh mạng, phòng chống khủng bố mạng và TPM. Chỉ trong vòng

06 năm trở lại đây, đã có 23 quốc gia trên thế giới ban hành trên 40 văn bản luật về an ninh mạng.[49]

Việt Nam cùng là một trong các quốc gia không nằm ngoài mối đe dọa nguy hiểm của nền công nghệ khoa học tiên tiến đem lại. Hiện nay, ở nước ta đang có sự tranh cãi, thảo luận về việc có nên ban hành Luật an ninh mạng. Diễn biến vấn đề ở trong nước và quốc tế cũng cho thấy, tại Việt Nam yêu cầu ban hành, thực thi Luật An ninh mạng trong hoạt động thực tiễn đã trở nên cấp bách, là tất yếu khách quan trong bối cảnh phát triển trí tuệ nhân tạo đã và đang tạo ra những thành tựu vượt trội nhưng nếu không có sự kiểm soát chặt chẽ sẽ gây nên một mối đe dọa lớn cho xã hội. Vì vậy, việc triển khai, xây dựng pháp luật lĩnh vực an ninh, ban hành thực thi Luật An ninh mạng 2019 của nhà nước Việt Nam là sự hết sức cần thiết.

Ngày 12-6-2018, kỳ họp thứ năm Quốc hội khóa XIV, Quốc hội đã thông qua Luật An ninh mạng với tỷ lệ 86,86% (có hiệu lực từ 1-1-2019) gồm 7 chương, 43 điều quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; xác định trách nhiệm của cơ quan, tổ chức, cá nhân liên quan. Bố cục của Luật cụ thể như sau: Chương I. Những quy định chung, gồm 9 điều, (từ Điều 1 đến Điều 9); Chương II. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, gồm 6 điều (từ Điều 10 đến Điều 15); Chương III. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng, gồm 7 điều (từ Điều 16 đến Điều 22) ;Chương IV. Hoạt động bảo vệ an ninh mạng, gồm 7 điều (từ Điều 23 đến Điều 29); Chương V. Bảo đảm hoạt động bảo vệ an ninh mạng, gồm 6 điều (từ Điều 30 đến Điều 35); Chương VI. Trách nhiệm của cơ quan, tổ chức, cá nhân, gồm 7 điều (từ Điều 36 đến Điều 42); Chương VII. Điều khoản thi hành, gồm 01 điều (Điều 43), quy định về hiệu lực thi hành.

Một trong những nội dung quy định trong Luật an ninh mạng 2019 mà người dân quan tâm, tranh cãi là hành vi nào sẽ bị nghiêm cấm hay nói

[49] http://tuyengiao.vn/ban-can-biet/hieu-ve-luat-an-ninh-mang-113375

cách khác phải sử dụng mạng Internet như thế nào mới không vi phạm pháp luật, đặc biệt là vấn đề sử dụng Facebook, Google, các dịch vụ nước ngoài cung cấp có hay không luật an ninh đã ngăn chặn quyền tự do ngôn luận, bày tỏ ý kiến, triển khai ý tưởng sáng tạo trên không gian mạng. Theo đó, Luật an ninh mạng quy định rõ ràng các hành vi bị nghiêm cấm về an ninh mạng và xử lý vi phạm pháp luật về an ninh mạng (Điều 8, Điều 9). Luật an ninh mạng chỉ nghiêm cấm sử dụng không gian mạng để thực hiện các hành vi vi phạm pháp luật đã được pháp luật (BLHS, Bộ luật dân sự và các văn bản quy phạm pháp luật khác liên quan) quy định. Theo đó, Điều 8 Luật an ninh mạng đã liệt kê cụ thể, rõ ràng các hành vi bị nghiêm cấm về an ninh mạng, góp phần thuận lợi trong việc thực hiện và xử lý hành vi vi phạm điều cấm, bao gồm: (1) Sử dụng không gian mạng để thực hiện hành vi sau đây: Hành vi sử dụng không gian mạng, CNTT, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự an toàn xã hội; Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; Thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; Xúi giục, lôi kéo, kích động người khác phạm tội. (2) Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, TPM; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia. (3) Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn

hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác. (4) Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng. (5) Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi. (6) Hành vi khác vi phạm quy định của Luật này.[50]

Như vậy, Luật an ninh mạng không có quy định cấm Facebook, Google hoặc các nhà cung cấp dịch vụ nước ngoài hoạt động tại Việt Nam; không ngăn cản quyền tự do ngôn luận, quyền bày tỏ quan điểm của công dân; không cấm công dân sử dụng các dịch vụ mạng xã hội như Facebook, Google; không cấm công dân tham gia hoạt động trên không gian mạng hoặc truy cập, sử dụng thông tin trên không gian mạng; cấm công dân khởi nghiệp, sáng tạo hay trao đổi, triển khai ý tưởng sáng tạo của mình trên không gian mạng. Bên cạnh đó, Luật quy định người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu TNHS, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật (Điều 9).[51]

Ban hành luật an ninh mạng đã góp một phần nào đó vào công cuộc phòng chống và bảo vệ trật tự an ninh quốc gia. Qua những lợi ích và tác hại của công nghệ mang lại, ta nhận thấy rằng nếu sử dụng đúng cách, có chọn

[50] Điều 8 Luật an ninh mạng số 24/2018/QH14.
[51] https://www.ctu.edu.vn/images/upload/notice/2019/De-cuong-luat-an-ninh-mang.pdf

lọc và có những biện pháp những chương trình ngăn chặn sự phá hoại của tội phạm sử dụng công nghệ cao thì kết quả phòng chống loại tội phạm này mới thực sự hiệu quả.

Trải qua từng thời kỳ có thể thấy rằng pháp luật Việt Nam đã có những bước phát triển đáp ứng với nhu cầu đấu tranh phòng chóng tội phạm trong lĩnh vực CNTT. Tuy bước đầu đã có những quy định pháp luật cơ bản quy định về loại tội phạm nguy hiểm này, nhưng thực chất nếu so sánh với thực tiễn phát triển nhanh chóng của TPCNC và pháp luật của các quốc gia khác trên thế giới thì nhà nước Việt Nam cần phải chủ động, tích cực và nhanh chóng hoàn thiện hệ thông quy định pháp luật trong lĩnh vực đấu tranh và phòng chống TPCNC. Đồng thới phát triển nguồn nhân lực, người lao động tự nâng cao kiến thức của mình để biết sử dụng Internet và từng bước tương tác với nó một cách hợp pháp mang lại lợi ích cho cá nhân và xã hội theo hướng thúc đẩy môi trường cạnh tranh lành mạnh phục vụ cho tăng trưởng kinh tế xã hội và đời sống nhân dân.

TỔNG KẾT CHƯƠNG 1

Tổng quan những phân tích trên có thể thấy rằng TPCNC là loại tội phạm mới. Do đó, khái niệm về tội phạm là rất rộng, bao quát trên nhiều lĩnh vực với nhiều quan điểm khác nhau. Tội phạm trong lĩnh công nghệ gắn bó với các ứng dụng CNTT và có khả năng gây nguy hại nghiêm trọng đến mọi lĩnh vực trong đời sống vì CNTT hiện nay đã được áp dụng hầu hết trên các lĩnh vực. Trong chương một đề tài nghiên cứu rút ra được khái niệm, phân loại và đặc điểm của TPCNC. Đồng thời làm rõ các quy định pháp luật về TPCNC của Việt Nam và một số quốc gia cụ thể như Trung Quốc, Hoa Kì, Anh Quốc- đây là những đại diện tiêu biểu cho các Châu lục trên thế giới; Cùng các thỏa thuận song phương, đa phương về xử lí tội phạm công nghệ cao. Nhằm tạo ra nhận thức chính xác hơn về TPCNC cũng như là các quy định trong hệ thống pháp luật một số quốc gia trên thế giới nói chung và Việt Nam nói riêng.

CHƯƠNG 2: THỰC TIỄN CỦA HOẠT ĐỘNG XỬ LÝ TỘI PHẠM CÔNG NGHỆ CAO HIỆN NAY.

2.1. Thực trạng hoạt động của tội phạm công nghệ cao hiện nay

2.1.1. Thực trạng hoạt động của tội phạm công nghệ cao theo khu vực địa lý thế giới

Các thiết bị công nghệ cao và đặc biệt là Internet hiện đang là một phần không thể thiếu trong cuộc sống là minh chứng cho sự bùng nổ của thời đại CNTT. Internet mang lại rất nhiều tiện ích cho người dùng như cung cấp một lượng thông tin khổng lồ hay giúp cho mọi người dễ dàng liên kết với nhau. Hiện nay có 4.333 tỷ người dùng Internet, chiếm tỷ lệ 56% dân số trên toàn thế giới.[52]

Toàn cầu

Theo một báo cáo tháng 12 năm 2018, TPCNC hiện nay tiêu tốn của thế giới gần 600 tỷ đô la, tương đương 0,8% GDP toàn cầu[53]. Loại tội phạm này có tác động toàn cầu, và có vị trí thứ ba, chỉ đứng đằng sau tội phạm tham nhũng và ma túy. Theo báo cáo thống kê năm 2018 của IC3, cho biết rằng đã nhận được 4,415,870 khiếu nại về TPCNC và trong các năm gần đây, từ năm 2014 đến năm 2018, IC3 đã nhận được trung bình gần 300,000 khiếu nại mỗi năm.[54] Cụ thể năm 2014, có 269,422 vụ khiếu nại được gửi đến IC3 và đến năm 2018 con số này tăng lên đến 351,937 vụ với tổng số thiệt hại trong năm 2018 là hơn 2,7 tỷ đô. Ngoài ra, qua bảng thống kê chi tiết thì IC3 đã chỉ ra 10 nước có nhiều khiếu nại nhất về TPCNC bao gồm: Ấn Độ, Anh, Canada, Australia, Georgia, Đức, Brazil, Mexico, Greece, Philipines. Trong đó, Ấn Độ là quốc gia có nhiều người khiếu nại nhất về TPCNC với 4,566 vụ khiếu nại và tiếp đến là Anh với 3,970 vụ và thứ ba là Canada với 2880 vụ khiếu nại.[55]

[52] Blog A1dighub: Digital trends 2019: Xu hướng Internet Thế giới năm 2019.
[53] Báo cáo tháng 12 năm 2018 của Trung tâm Nghiên cứu Chiến lược và Quốc tế (CSIS).
[54] Trung tâm tiếp nhận các khiếu nại về tội phạm công nghệ cao của FBI.
[55] Xem phụ lục 3.

Châu Á

Chỉ tính riêng Châu Á năm 2011 đã có đến 45% (khoảng 943 triệu) người dùng Internet tại Châu Á và Thái Bình Dương (tức là Châu Á và Châu Đại Dương)[56]. Theo thống kê có thể thấy rằng, số người dùng Internet ở khu vực Châu Á vào năm 2011 đã tăng nhanh chóng, đây cũng chính là một trong những lí do khiến TPCNC càng phát triển và khó kiểm soát.[57] Ngoài ra theo thống kê vào năm 2012 thì số người sử dụng Internet trên toàn cầu đạt ngưỡng 2,4 tỷ, trong đó tại Châu Á con số người dùng lên đến 1,1 tỷ. Thực tế trên cho thấy rằng Châu Á là một trong những khu vực sử dụng Internet hàng đầu thế giới.[58]

Hơn 60% tổng số người dùng Internet là tại các quốc gia đang phát triển, tại Châu Á, theo báo cáo thì Trung Quốc là nước có các hoạt động tấn công mạng bằng phần mềm độc hại phát triển mạnh nhất trong khu vực, tiếp theo là Hàn Quốc, Ấn Độ, Đài Loan và Nhật Bản. Symantec đã phát hiện ra rằng hầu hết các cuộc tấn công đến từ Hoa Kỳ, tiếp theo là Trung Quốc, Hàn Quốc và Nhật Bản.[59] Trung Quốc cũng có nhiều máy tính bị nhiễm botnet nhất được phát hiện ở khu vực Châu Á- Thái Bình Dương và Nhật Bản cho giai đoạn 2006 - 2010 trong khi Đài Loan xếp thứ hai, tiếp theo là Hàn Quốc và Ấn Độ. Một khảo sát năm 2010 nhận thấy 83% số người được hỏi từ Trung Quốc đã bị TPCNC tấn công theo nhiều phương thức khác nhau, bao gồm cả vi-rút máy tính hoặc một số hình thức của crime-ware. Con số này cao hơn nhiều so với mức trung bình toàn cầu là 65%. Ngoại trừ Nhật Bản có tỷ lệ nạn nhân thấp hơn (36%), các quốc gia khác trong Khu vực Châu Á và Thái Bình Dương như Úc (65%), Ấn Độ (75%) và New Zealand (70%) đều cao hơn mức trung bình toàn cầu (Norton, 2010).[60]

[56] Roderic Broadhurst và Lennon Y.C.Chang, Cyber in Asia: Trends and Challenges.
[57] Xem phụ lục 4.
[58] Roderic Broadhurst và Lennon Y.C.Chang, Cyber in Asia: Trends and Challenges.
[59] Báo cáo của Symantec-nhà cung cấp phần mềm bảo mật máy tính.
[60] Báo cáo của công ty Norton (một công ty thuộc sở hữu của Symantec), một nhà cung cấp chống vi-rút- Symantec, 'Facts and fgures', Internet Security Threat Report (ISTR).

Châu Âu

Tại Châu Âu, các vụ tấn công mạng đến từ cả trong và ngoài biên giới lãnh thổ châu lục này. Xu hướng tấn công mạng thịnh hành tại Châu Âu là sử dụng Email chứa mã độc. Theo thống kê thì Áo, Đức, Hungary, Ý, Nga, Tây Ban Nha và Vương quốc Anh là các nước đứng đầu toàn cầu về việc tấn công bằng email có chứa mã độc hay phát tán phần mềm độc hại. Hay các nước như Hà Lan, Hungary, Bồ Đào Nha và Áo đứng đầu về việc bị phát tán các Email có nội dung lừa đảo. Còn tại Bulgaria và Romania thì TPCNC hoạt động bằng cách gian lận thanh toán chiếm tỉ lệ lớn.[61] Riêng tại Anh, trong 2012-2013 đã có sự gia tăng 60% số lượng báo cáo về TPCNC gây thiệt hại cho nền kinh tế Anh 81 tỷ bảng.[62]

Châu Mỹ

Châu Mỹ, đặc biệt tại Hoa Kỳ, là mục tiêu hàng đầu của các cuộc tấn công mạng. Trong lĩnh vực công nghiệp đã ghi nhận nhiều vụ tấn công bằng phần mềm độc hại di động. Ngoài ra, Mỹ đã trở thành máy chủ lớn thứ hai trên thế giới của sự hình thành các botnet hay việc thiết bị IoT bị xâm nhập kể từ năm 2016. Tương tự như Hoa Kỳ, Brazil cũng được mệnh danh là một trong những nơi có nhiều các trang web lừa đảo và tại một số báo cáo chỉ ra rằng Brazil cũng là một trong mười mục tiêu hàng đầu trên thế giới của TPCNC. Tại Mexico là quốc gia phải hứng chịu nhiều nhất các cuộc tấn công mạng chỉ sau Brazil.[63]

Việt Nam

Tội phạm công nghệ trong giai đoạn đầu hình thành, với trình độ văn hóa, nền kinh tế tương đối thấp, tuy đã có sự xâm nhập của Internet nhưng chưa phổ biến thì diễn biến tội phạm trong lĩnh vực CNTT chủ yếu là sử dụng CNTT là mục đích nhằm xâm phạm an ninh, an toàn mạng máy tính diễn ra phức tạp, tiềm ẩn nhiều nguy cơ đối với an ninh quốc gia và trật tự

[61] Internet organised crime threat assessment (IOCTA) 2018.
[62] Phát biểu của Bernard Hogan-Howe ủy viên cảnh sát thủ đô nước Anh, vào tháng 11 năm 2013.
[63] Internet organised crime threat assessment (IOCTA) 2018.

an toàn xã hội. Tuy nhiên, từ những năm 1999 sự phát triển như vũ bão của nền CNTT, thì diễn biến tội phạm trong lĩnh vực CNTT chủ yếu là sử dụng CNTT là một công cụ, phương tiện phạm tội. Tội phạm nhìn nhận công nghệ như một miếng mồi màu mỡ và sử dụng triệt để công nghệ như một công cụ đắc lực phục vụ hàng loạt hành vi phạm tội phạm tội. Có thể coi đây là một loại tội phạm mới trong tội phạm truyền thống nhưng sử dụng công nghệ để thực hiện hành vi bất hợp pháp. Ba ngành bị tấn công nhiều nhất ở nước ra là: khối tài chính (các ngân hàng, tổ chức tín dụng, doanh nghiệp kinh doanh, kiểm toán, kế toán…) tỉ lệ 41%; khối dịch vụ chuyên ngành tỉ lệ 30%; khối sản xuất với tỉ lệ 29%.[64] TPCNC đã và đang trở thành những mối lo ngại đối với tất cả cá nhân, tổ chức, cơ quan ban hành. Tội phạm sử dụng những thủ đoạn phổ biến để thực hiện hành vi bất hợp pháp của mình.

Đối với lĩnh vực an toàn, trật tự tội phạm thực hiện hành vi "tấn công từ chối dịch vụ *DDoS"* làm tê liệt hoạt động của trang web bị hại và "Tấn công deface" lợi dụng lỗ hổng bảo mật của các trang web để chiếm quyền điều khiển máy chủ xâm nhập trái phép hệ thống thông tin để thu thập, trộm cắp, sửa đổi dữ liệu hoặc phá hủy cơ sở dữ liệu của trang web. Ví dụ như vào tháng 7-2016 đã xảy ra vụ tiến công vào hệ thống mạng của hàng không Việt Nam theo hình thức APT (tiến công có chủ đích) làm ảnh hưởng hơn 100 chuyến bay, đồng thời làm rò rỉ dữ liệu của hơn 400 nghìn tài khoản khách hàng thường xuyên của hãng. Nguy hiểm hơn nữa là hình thành các ổ nhóm đối tượng "đánh thuê", có tổ chức, được trả tiền để tấn công vào các mục tiêu trên mạng, phục vụ mục đích riêng của các đối tượng bỏ tiền thuê như: phá hoại hoạt động sản xuất, kinh doanh của doanh nghiệp để cạnh tranh không lành mạnh hoặc vì các mục đích vụ lợi khác hay thủ đoạn"Phát tán virus, phần mềm gián điệp" làm phát tán qua dịch

[64] Lê Thanh Tâm, Phạm Thị Thu Thảo, Tội phạm công nghệ cao đối với ngành Ngân hàng Việt Nam trong bối cảnh cách mạng công nghiệp 4.0: thực trạng và một số khuyến nghị chính sách, Tạp chí Khoa học & Đào tạo Ngân hàng Số 192, Tháng 5. 2018.

vụ web nhằm lây lan vào máy tính cá nhân để lấy thông tin cá nhân như mật khẩu của e-mail, tài khoản chat.[65] Các đối tượng cũng mở rộng các hình thức phát tán các loại phần mềm độc hại qua thư điện tử, website khiêu dâm, diễn đàn trên mạng,… mua bán các thiết bị, phần mềm gián điệp để cài đặt trên điện thoại thông minh, máy tính với quy mô, phạm vi rộng lớn, xâm phạm nghiêm trọng quyền riêng tư của công dân, tiềm ẩn nhiều nguy cơ đối với an ninh quốc gia, trật tự an toàn xã hội. Điển hình là vụ hệ thống mạng của Tập đoàn Dầu khí quốc gia Việt Nam bị tin tặc liên tiếp tấn công bằng nhiều phương thức khác nhau, làm ngưng trệ hoạt động và xóa sạch toàn bộ dữ liệu website; vụ Công ty Cổ phần Bảo hiểm AAA tại TP. Hồ Chí Minh bị đối tượng tấn công làm tê liệt hệ thống mạng máy tính, mã hóa dữ liệu, đe dọa tống tiền trên 2 triệu đô la Mỹ.

Đối với lĩnh vực thương mại điện tử tội phạm đây là một trong những lĩnh vực trọng điểm, tiềm ẩn nhiều nguy cơ lừa đảo. Tội phạm tiến hành các thủ đoạn lừa đảo qua quảng cáo, bán hàng trực tuyến; Lừa trên các sàn giao dịch ảo như ngoại tệ, vàng, bất động sản, huy động vốn tín dụng; Xâm phạm thiết bị điện tử, thiết bị số của ngân hàng, cá nhân, tổ chức*;* Lừa đảo lấy cắp thông tin cá nhân; Trộm cắp, mua bán và sử dụng trái phép thẻ ngân hàng giả... lợi dụng tâm lý hám tiền, tham lợi, tham giàu nhanh mà không muốn bỏ công sức lao động của nhiều người dân, các đối tượng đã lập lên những trang web với vỏ bọc là các trang thương mại điện tử, nhưng thực chất là một tổ chức lừa đảo, huy động vốn theo kiểu kinh doanh đa cấp. Phổ biến tình trạng sử dụng mạng Internet, Facebook để buôn bán hàng lậu (hàng xách tay), hàng giả (hàng fake), hàng cấm, ma túy, vũ khí, tài sản do phạm tội mà có, văn bằng giấy tờ giả… hoặc lập các các diễn đàn để trao đổi, mua bán phần mềm "lậu", vi phạm bản quyền sở hữu trí tuệ, phát tán phim lậu, phim sex… Bên cạnh đó, vẫn tồn tại nhiều hành vi lừa

[65] Nguyễn Ngọc Thương**,** Một số giải pháp phòng ngừa tội phạm sử dụng công nghệ cao**,** Tạp chí CSND, T32 (19/1/2017).

đảo chiếm đoạt tài sản qua mạng Internet như: Lập các Website giả mạo Website của các doanh nghiệp, tổ chức; Thỏa thuận mua bán hàng hóa qua mạng Internet nhưng không chuyển hàng hoặc chuyển hàng giả, hàng kém chất lượng.[66] Điển hình, Tháng 01/2015, phòng cảnh sát phòng, chóng TPCNC (PC50) Hà Nội phối hợp với phòng cảnh sát điều tra tội phạm về trật tự xã hội Công an Hà Nội thực hiện khám xét khẩn cấp tại trụ sở chính của Công ty HGI ở tòa nhà Artex, số 172 Ngọc Khánh, Hà Nội và chi nhánh của HGI tại Đà Nẵng ở tòa nhà Trung tâm Tài chính Dầu khí Đà Nnẵng, quận Hải Châu, Đà Nẵng. Cơ quan điều tra xác định Công ty HGI được thành lập vào tháng 5/2009 và hoạt động kinh doanh vàng tài khoản từ năm 2009. Công ty này tổ chức sàn giao dịch vàng trên tài khoản websitehgi.com.vn, sử dụng phần mềm MT4 được mua của đối tác nước ngoài, sử dụng cho các nhà đầu tư tư tham gia đầu tư vàng, bạc, dầu và 8 cặp ngoại tệ trên mạng. Theo dữ liệu Cơ quan điều tra thu giữ được, thời điểm bị triệt phá, sàn HGI có hơn 3.000 nạn nhân góp vốn kinh doanh, trong đó có khoảng 300 nhà đầu tư có dấu hiệu bị lừa đảo với số tiền 270 tỷ đồng.[67] Hiện nay, chỉ cần số điện thoại và password sử dụng một lần là người dùng có thể mua hàng hóa và thanh toán trực tuyến. Lợi dụng kẽ hở này, các đối tượng chiếm đoạt sim điện thoại của khách hàng có sử dụng dịch vụ Internet Banking và thực hiện các giao dịch mua hàng hóa trực tuyến để chiếm đoạt. Theo các chuyên gia bảo mật, hacker sử dụng thủ đoạn "phishing"[68] để đánh cắp tài khoản của khách hàng rồi sử dụng Internet banking để rút tiền từ tài khoản này sang một tài khoản khác[69]. Bên

[66]http://csnd.vn/Home/Nghien-cuu-Trao-doi/301/Ket-qua-va-kinh-nghiem-phong-chong-toi-pham-su-dung-cong-nghe-cao-cua-PC50-Cong-an-thanh-pho-Ha-Noi-va-nhung-van-de-dat-ra-trong-cong-tac-dao-tao-can-bo.

[67] Đinh Thế Hưng, Lê Thị Hồng Xuân, Tội phạm công nghệ cao trong lĩnh vực tài chính, ngân hang ở việt nam hiện nay – (phòng pháp luật hình sự- Viện nhà nước và pháp luật), Tạp chí TAND số 7 /2019(Kỳ I tháng 4/2019).

[68] "Phishing" có thể hiểu là việc xây dựng những hệ thống lừa đảo nhằm đánh cắp các thông tin nhạy cảm, như tên đăng nhập, mật khẩu hay thông tin về các loại thẻ tín dụng của người dùng.

[69] http://antg.cand.com.vn/Ho-so-Interpol/Toi-pham-cong-nghe-cao-2016-Lam-nguy-co-nhieu-thach-thuc-423161/ ngày 29/12/2016.

cạnh đó, một số khách hàng của các ngân hàng như HSBC, Vietcombank, BIDV, ACB... cũng nhận được các cuộc gọi đến xưng danh là cán bộ của ngân hàng thông báo việc khách đã trúng thưởng, đề nghị khách hàng chuyển tiền để làm thủ tục nhận thưởng hoặc thông báo thẻ tín dụng có vài vấn đề và yêu cầu cung cấp những thông tin liên quan để điều chỉnh; Xưng danh là cán bộ điều tra yêu cầu nộp tiền vào một tài khoản khác để bảo lãnh, phục vụ việc điều tra[70] hay một thủ đoạn khác là mua bán các loại thiết bị, phần mềm có chức năng nghe lén cuộc gọi thoại, trộm cắp thông tin cá nhân trong điện thoại di động diễn ra rất phổ biến, trắng trợn. Vụ án Công ty TNHH Công nghệ Việt Hồng kinh doanh trái phép phần mềm nghe lén điện thoại. Ước tính có hơn 14000 điện thoại ở Việt Nam bị nghe lén, trộm cắp dữ liệu cá nhân. Tình hình lừa đảo trong lĩnh vực thương mại điện tử và thanh toán điện tử gia tăng, dẫn đến tình trạng nhiều nước không chấp nhận giao dịch qua mạng Internet có địa chỉ IP xuất phát từ Việt Nam, ảnh hưởng nghiêm trọng đến uy tín và hình ảnh của Việt Nam trong lĩnh vực thương mại điện tử nói riêng và lĩnh vực kinh tế quốc tế nói chung.

Đối với lĩnh vực viễn thông tội phạm đang có xu hướng gia tăng trong lĩnh vực này theo đó tội phạm thực hiện thủ đoạn lừa đảo trên đầu số dịch vụ giá trị gia tăng (GTGT) trên Internet, viễn thông tức tin nhắn gài bẫy có hai kiểu lừa đảo là "Phần mềm lừa đảo" tức sử dụng phần mềm gián điệp cài trên điện thoại smat phone tự động gửi tin nhắn đến đầu số GTGT (wap charging).[71]Vụ án Công ty CP IMMC, địa chỉ: số 28, ngõ 139, đường Lê Thanh Nghị, phường Đồng Tâm, quận Hai Bà Trưng, Hà Nội có website: mmoney.vn đăng tải các ứng dụng có chức năng tự động gửi tin nhắn đến

[70] Trần Thế Hệ, Thực trạng tội phạm công nghệ cao trong lĩnh vực ngân hàng ở Việt Nam. http://lsvn.vn/nghien-cuu-trao-doi/phan-tich-nghien-cuu/thuc-trang-toi-pham-cong-nghe-cao-trong-linh-vuc-ngan-hang-o-viet-nam-31401.html

[71] Nguyễn Minh Đức, Đặc điểm tội phạm học của tội phạm sử dụng công nghệ cao và giải pháp nâng cao hiệu quả phòng ngừa, đấu tranh. http://csnd.vn/Home/Nghien-cuu-Trao-doi/307/Dac-diem-toi-pham-hoc-cua-toi-pham-su-dung-cong-nghe-cao-va-giai-phap-nang-cao-hieu-qua-phong-ngua-dau-tranh.

các đầu số dịch vụ để trừ tiền của người sử dụng rồi chiếm đoạt số tiền. "Hack SIM" là thủ đoạn phạm tội không chỉ nhằm lấy được tiền trong tài khoản mà còn có thể bán tài khoản ấy cho người khác hoặc lấy hết tiền trong ngân hàng khi SIM được liên kết với tài khoản ngân hàng.[72] Đặc biệt là thủ đoạn đánh bạc trực tuyến và cá độ bóng đá qua mạng Internet trở nên phổ biến và lan rộng trên cả nước với nhiều diễn biến phức tạp, khó lường. Các website chuyên tổ chức đánh bạc, cá độ trong và ngoài nước thường đặt máy chủ tại nước ngoài và cấu kết với người Việt Nam hình thành các đường dây đánh bạc, cá độ có quy mô lớn, được tổ chức thành mạng lưới nhiều tầng. Số lượng người chơi lên đến hàng trăm nghìn người, lượng tiền đánh bạc lên đến hàng chục ngàn tỷ đồng. Ví dụ điển hình, vụ án ông Nguyễn Thanh Hóa – Nguyên cục trưởng Cục Phòng chống TPCNC (C50) đã cho thấy việc đánh bạc thông qua hình thức game online là vô cùng lớn, với hình thức sử dụng công nghệ cao để làm công cụ, phương tiện thực hiện hành vi phạm tội, tính chất đặc biệt nghiêm trọng. Vụ việc này đã gõ lên hồi chuông cảnh báo đối với cơ quan chức năng trong việc phòng, chống TPCNC.

Tội phạm công nghệ hoạt động hầu hết trên các lĩnh vực liên quan đến công nghệ. Có thể thấy rằng, chúng ngày càng trở lên phức tạp, khó lường, về chủ thể, quy mô, tính chất, hậu quả, mức độ thiệt hại đều không ngừng tăng nhanh và nghiêm trọng hơn so với thời gian trước. Những phương thức thủ đoạn trên được quy tụ trên môi trường ảo với các tổ chức diễn đàn gọi là "thế giới ngầm - Underground" trong đó chứa nhiều nội dung vi phạm pháp luật như phản động, khiêu dâm, cờ bạc, cá độ bóng đá qua mạng, mua bán thông tin thẻ tín dụng do trộm cắp được, tiền ảo... đặt hoặc thuê máy chủ tại nước ngoài, mạng lưới hoạt động trên nhiều quốc gia với hình thức hoạt động tinh vi nhằm tránh sự kiểm soát, xử lý của các cơ quan

[72] Nguyễn Minh Đức**:** Đặc điểm tội phạm học của tội phạm sử dụng công nghệ cao và giải pháp nâng cao hiệu quả phòng ngừa, đấu tranh.

chức năng. Những trang web, diễn đàn nước ngoài và trong nước về bảo mật thường xuyên cung cấp, trao đổi những thông tin về việc công bố lỗ hổng bảo mật, chia sẻ các công cụ, phương pháp khai thác tấn công hệ thống mạng máy tính. Hoạt động của tội phạm có sự phân công nhiệm vụ cụ thể, sử dụng nhiều thủ đoạn tinh vi để che giấu hành vi phạm tội của mình hoặc liên tục thay đổi phương thức hoạt động phạm tội nhằm trốn tránh sự phát hiện của các cơ quan chức năng. Qua đó có thể thấy rằng, TPCNC là mối đe dọa an ninh rất lớn đối với các quốc gia, có thể xếp ngang hàng với các loại tội phạm vũ khí hóa học, hạt nhân, khủng bố.

2.1.2. Thực trạng hoạt động của tội phạm công nghệ cao theo lĩnh vực Chính trị

Với sự phát triển nhanh chóng của TPCNC, các mối đe dọa an ninh mạng là một trong những thách thức của an ninh quốc gia, an toàn công cộng và kinh tế mà mọi quốc gia phải đối mặt trong thế kỷ XXI. Năm 2016 đánh dấu một sự thay đổi trong động cơ của TPCNC với sự gia tăng của tội phạm về số lượng các cuộc tấn công nhằm vào thao túng chính trị. Tất cả các quốc gia tin rằng an ninh mạng là một công cụ để đạt được lợi ích quốc gia của nhà nước. Trong khi đó, một số quốc gia thấy an ninh mạng là công cụ để tác động đến đối thủ. Điều kiện này được xây dựng dựa trên sự ảnh hưởng của các cuộc tấn công mạng. Sự khác biệt giữa các phương pháp an ninh quốc gia này là cách sử dụng công cụ được sử dụng để đạt được mục tiêu. Chính vì vậy, an ninh mạng có một vai trò quan trọng và đặc biệt trong chính trị thế giới.

Hoa Kỳ, là một nước đi đầu trong lĩnh vực CNC. Đến nay, kinh nghiệm của Hoa Kỳ trong lĩnh vực bảo mật thông tin rất tiến bộ. An ninh quốc gia của Hoa Kỳ ngày nay hoàn toàn phụ thuộc vào cơ sở hạ tầng CNTT. Chính vì vậy, hệ thống CNTT rất quan trọng đối với Hoa Kỳ, họ sử dụng máy tính và Internet để quản lý hầu như tất cả mọi lĩnh vực dẫn đến an ninh mạng là vấn đề cần được quan tâm hàng đầu của chính phủ.

Trong chiến lược an ninh mạng quốc gia của Hoa Kỳ, tổng thống Donald Trump khẳng định "Bảo mật không gian mạng là nền tảng cho chiến lược của chúng tôi và đòi hỏi tiến bộ kỹ thuật và hành chính hiệu quả trên toàn Chính phủ Liên bang và khu vực tư nhân. Chính quyền cũng nhận ra rằng một cách tiếp cận thuần túy công nghệ đến không gian ảo là không đủ để giải quyết bản chất của những vấn đề mới mà chúng ta phải đối mặt. Hoa Kỳ cũng phải có lựa chọn chính sách áp đặt chi phí nếu hi vọng nó ngăn chặn hoạt động khủng bố mạng và ngăn chặn sự leo thang hơn nữa của TPCNC".[73]

Tại Đức, các cuộc tấn công mạng trên các mạng của chính phủ Đức xảy ra hàng ngày. Các cuộc tấn công được phát hiện thường xuyên nhất tại Cục Quản lý Liên bang liên quan đến các email có chứa phần mềm độc hại. Bằng việc sử dụng biện pháp tự động chống vi-rút thì trung bình có 28.000 email được chặn trong thời gian một tháng trước khi người nhận mở nó. Trong số này trung bình có khoảng 6.000 e-mail độc hại được thu thập mỗi tháng chỉ bằng cách sử dụng chữ ký chống vi-rút được tạo một cách đặc biệt.[74] Với những số liệu thống kê trên, chính phủ Đức cũng đã đưa ra những chiến lược an ninh mạng để kịp thời kiểm soát tình huống xảy ra. Theo chính phủ Đức, an ninh mạng ở Đức phải được đảm bảo ở mức tương xứng với tầm quan trọng và sự bảo vệ cần thiết bởi thông tin liên kết cấu trúc, mà không cản trở các cơ hội và việc sử dụng không gian mạng.[75] Trong bối cảnh này, mức độ an toàn an ninh mạng đạt được là sự phối hợp của tất cả các quốc gia và các biện pháp quốc tế được thực hiện để bảo vệ sự sẵn có của thông tin và công nghệ truyền thông và tính toàn vẹn, xác thực và bảo mật dữ liệu trong không gian ảo.

Kinh tế

[73] Nhà trắng: Chiến lược An ninh mạng Hoa Kỳ, tháng 9 năm 2018.
[74] Horst Seehofer và Arne Schönbohm, The State of IT Security in Germany 2018.
[75] Bộ nội vụ Liên bang : Chiến lược An ninh mạng Đức, tháng 2 năm 2011.

Một lĩnh vực tiềm năng khác mà TPCNC hướng đến đó là kinh tế với mục tiêu là các tài khoản ngân hàng, tài khoản cá nhân, ... Vì nhiều chủ tài khoản không biết thực hiện các biện pháp bảo vệ cơ bản nhất, và nhiều sản phẩm thiếu công nghệ bảo mật đầy đủ. Trong khi đó tội phạm mạng lại sử dụng các công nghệ đơn giản và tiên tiến để xác định mục tiêu, tự động hóa việc tạo phần mềm và bắt đầu cuộc tấn công và kiếm tiền từ những gì họ ăn cắp.Trong lĩnh vực kinh tế, ngân hàng là mục tiêu hàng đầu của TPCNC, điều này đã xảy ra suốt hơn một thập kỷ. Theo điều tra của CSIS- Trung tâm Nghiên cứu chiến lược quốc tế, Nga, Bắc Triều Tiên và Iran là những nước mà việc hack các tổ chức tài chính phát triển nhất.[76] Theo báo cáo của ICSPA[77] TPCNC đang trở thành mối nguy hại lớn trên giới với thiệt hại gây ra khoảng 400 tỷ USD/năm, cao hơn số tiền mà tội phạm buôn bán ma túy thu được và cứ 14 giây lại xảy ra 01 vụ phạm tội sử dụng công nghệ cao. Phương thức thông thường của TPCNC nhắm đến các ngân hàng thường là trộm thông tin của khách hàng, giả mạo ngân hàng gửi tin nhắn cho khách hàng và cuối cùng trộm tiền từ cái tài khoản và hành vi này được gọi là gian lận thẻ tín dụng. Mục đích của gian lận thẻ tín dụng là mua hàng hóa mà không phải trả tiền, hoặc ăn cắp tiền từ tài khoản tín dụng của người khác. Tội phạm lợi dụng máy tính và Internet, sử dụng những mánh khóe và các thủ đoạn để bằng mọi cách ăn cắp thông tin cá nhân của nạn nhân từ các ngân hàng. Những nhân viên ngân hàng thường là những người chỉ có trình độ máy tính trung bình cho nên việc xâm nhập vào hệ thống ngân hàng là không khó. Việc này không đòi hỏi những tội phạm có trình độ kỹ thuật chuyên ngành cao như việc hack các hệ thống khác, chỉ cần vài thao tác là tội phạm có thể dễ dàng lấy được hàng loạt thông tin cá nhân của khách hàng. Nếu như tội phạm truyền thống phải trực tiếp đến ngân hàng, có các thông tin cá nhân và giả mạo chữ kí của nạn nhân thì với các

[76] CSIS– Trung tâm Nghiên cứu Chiến lược và Quốc tế.
[77] Liên minh bảo vệ an ninh mạng quốc tế.

công cụ công nghê cao hỗ trợ, tội phạm có thể ngồi cách ngân hàng hàng ngàn kilomet vẫn có thể lấy được hàng tỷ đô từ các tài khoản của nạn nhân.

Doanh nghiệp

Hiện nay các doanh nghiệp hiện là mục tiêu của các TPCNC. Cũng như các ngành khác, doanh nghiệp sử dụng không gian mạng để quản lý hoạt động của mình, từ các bí mật kinh doanh, thông tin khách hàng hay nội bộ công ty đều được đưa vào các trang web để thuận tiện cho việc theo dõi và vận hành. Ở Canada, TPCNC khá phổ biến ở các doanh nghiệp, với 69% báo cáo một số loại tấn công trong thời hạn mười hai tháng. Tổng cộng có 5,866 cuộc tấn công đã được báo cáo hoặc 16,5 cuộc tấn công cho mỗi doanh nghiệp bị ảnh hưởng.[78] Hay tại Anh, đến năm 2017 đã đánh dấu một loạt các cuộc tấn công đến các tổ chức, doanh nghiệp lớn như : Yahoo, Uber, Equifax,… Các cuộc tấn công mạng đến các tổ chức doanh nghiệp không chỉ gây thiệt hại về kinh tế mà còn các yếu tố khác như danh tiếng hay về sở hữu trí tuệ,…Để phá hủy danh tiếng của một doanh nghiệp, tội phạm thường xâm nhập vào hệ thống và lấy cắp thông tin cá nhân của khách hàng và công khai. Việc này sẽ làm cho khách hàng mất tin tưởng vào các tổ chức doanh nghiệp dẫn đến danh tiếng sẽ bị suy giảm đáng kể. Nếu doanh nghiệp gặp phải một cuộc tấn công mạng nhằm đánh cắp ý tưởng của công ty, chiến dịch tiếp thị hoặc kế hoạch mở rộng kinh doanh, doanh nghiệp đó sẽ mất lợi thế cạnh tranh mà nó từng có so với các doanh nghiệp khác trong thị trường. Hay nếu tin tặc đánh cắp tài sản trí tuệ, chẳng hạn như thiết kế sản phẩm, dù là nhỏ hay lớn, nó có thể là một nguyên nhân gây phá sản cho doanh nghiệp. Với các công ty, sẽ mất một nguồn doanh thu bất ngờ khi sản phẩm cạnh tranh gia nhập thị trường. Vụ trộm tài sản trí tuệ chiếm ít nhất một phần tư về chi phí của tội phạm mạng và khi nó liên quan đến kỹ thuật công nghệ quân sự sẽ tạo ra rủi ro cho an ninh quốc gia. Và so với tội phạm truyền thống TPCNC nguy hiểm hơn rất nhiều bởi vì

[78] Theo ICSPA Canada cybercrime report của Liên minh bảo vệ an ninh mạng quốc tế (ICSPA).

chúng có thể gây thiệt hại nghiêm trọng hay thậm chí một cuộc tấn công mạng vào các doanh nghiệp tổ chức có thể gây hại tới hàng ngàn cá nhân hay ảnh hưởng tới nhiều doanh nghiệp liên quan khác. Hàng năm, số lượng doanh nghiệp bị ảnh hưởng bởi TPCNC tăng lên và điều này một phần là do ngày càng có nhiều doanh nghiệp, đồng thời cũng là do tội phạm đang trở nên thông minh hơn với những cách thức tiến bộ hơn và các công ty không thể khống chế được. Cách tốt nhất để vượt lên trước những tên tội phạm này là luôn cập nhật những tội phạm mạng mới nhất có thể ảnh hưởng đến doanh nghiệp và phát triển công nghệ của các doanh nghiệp. Ngoài ra, hiểu được tác động của tội phạm mạng trong kinh doanh và xã hội sẽ là động lực cần thiết để bảo vệ dữ liệu và tài sản của các doanh nghiệp một cách tốt nhất.

Xã hội

TPCNC không chỉ dừng lại ở các hoạt động chính trị hay kinh tế, chúng còn gây nên những ảnh hưởng tiêu cực đến xã hội. Các trang web khiêu dâm, buôn bán, đấu giá các sản phẩm hàng hóa bất hợp pháp trên Internet đang tạo nên những tác động tiêu cực cho xã hội. Đầu tiên phải kể đến hành vi truyền tải nội dung khiêu xâm trên mạng Internet, hiện nay nội dung khiêu dâm trên mạng bị cấm ở nhiều quốc gia và được hợp pháp hóa ở một số nước. Theo thống kê năm 2005, có khoảng 4.2 triệu trang web khiêu dâm - chiếm khoảng 12% tổng số các trang web. Quy mô của ngành công nghiệp khiêu dâm là khoảng 57 tỷ đô la Mỹ trên toàn thế giới - mang lại nhiều hơn doanh thu so với các mạng truyền hình ABC, CBS và NBC cộng lại, và nhiều hơn cả bóng rổ, và nhượng quyền bóng chày thể thao kết hợp. Năm 2005, hơn 40 triệu người trưởng thành (72% nam, 28% nữ) nói rằng họ thường xuyên truy cập trang web khiêu dâm dành cho người lớn và 20% nam giới được khảo sát nói rằng họ thường xuyên xem nội dung khiêu

dâm trực tuyến trong khi làm việc.[79] Nội dung liên quan đến tình dục là một trong những nội dung đầu tiên được phân phối thương mại trên Internet. Việc truyền tải các nội dung khiêu dâm trên mạng đưa lại nhiều lợi ích hơn cho các tội phạm như trao đổi các phương tiện như hình ảnh, phim,… mà không phải tốn chi phí, phạm vi truy cập trên toàn thế giới, số lượng người tiếp cận tăng lên đáng kể so với việc bán lẻ hay một tiện ích của Internet có lợi cho việc truy cập vào các nội dung khiêu dâm đó là chế độ ẩn danh - một khía cạnh mà người truy cập đánh giá cao. Trái ngược với những quan điểm khác nhau về nội dung khiêu dâm người lớn, nội dung khiêu dâm trẻ em bị lên án rộng rãi và hành vi phạm tội liên quan đến nội dung khiêu dâm trẻ em được công nhận rộng rãi là hành vi phạm tội. Lạm dụng tình dục trẻ em trực tuyến và khai thác tình dục trẻ em trực tuyến là việc sử dụng công nghệ thông tin và truyền thông như một phương tiện để lạm dụng tình dục hoặc khai thác tình dục trẻ em. Trong những năm 1970 và 1980, những kẻ phạm tội tham gia trao đổi nội dung khiêu dâm trẻ em phải đối mặt với các mối đe dọa nghiêm trọng. Vào thời điểm đó, thị trường phim khiêu dâm trẻ em thương mại tập trung chủ yếu ở châu Âu và Mỹ và tài liệu này là được sản xuất tại địa phương, đắt tiền và khó mua được. Hiện nay, Internet là kênh chính để giao dịch nội dung khiêu dâm trẻ em và việc truy cập là miễn phí. Nghiên cứu hành vi của những kẻ phạm tội khiêu dâm trẻ em cho thấy 15% những người bị bắt với nội dung khiêu dâm trẻ em liên quan đến Internet đã quảng cáo hơn 1000 hình ảnh trên của họ máy vi tính; 80% có hình ảnh của trẻ em từ 6 đến 12 tuổi trên máy tính của họ, 19 % có hình ảnh của những đứa trẻ nhỏ hơn 3 tuổi; và 21 phần trăm có hình ảnh mô tả bạo lực.[80]

Dữ liệu cá nhân

[79] Bernadette H. Schella, Cyber child pornography: A review paper of the social and legalissues and remedies—and a proposed technological solution, March 2006.
[80] Understanding cybercrime: Phenomena, challenges and legal response, September 2012.

Báo cáo của Microsoft cho thấy TPCNC ngày càng trở nên tinh vi hơn khi thực hiện việc mô hình hóa hoạt động của chúng dưới dạng các quy trình nghiệp vụ phổ biến để lừa người sử dụng nhằm đánh cắp và gian lận các thông tin quan trọng. Không chỉ nguy hiểm với người dùng máy vi tính cá nhân, cùng với sự phổ biến các dòng điện thoại thông minh, tội phạm ảo đang chuyển mạnh hướng tấn công sang điện thoại di động truy cập Internet. Nghiên cứu của Unisys[81] cho biết có đến 60% người dùng điện thoại không sử dụng những biện pháp bảo mật cơ bản nhất là cài password hoặc mã PIN. Theo công ty nghiên cứu IDC, khi tải về ứng dụng hình nền cho điện thoại Android, iPhone, BlackBerry và Windows Mobile, người dùng có thể bị thu thập số điện thoại và hộp thư thoại cùng với dữ liệu có thể được sử dụng để dò ra vị trí của người dùng. Vào năm 2013, Một tỷ tài khoản người dùng bị đánh cắp từ Yahoo, thông tin cá nhân bao gồm tên, số điện thoại, mật khẩu và địa chỉ email được lấy từ gã khổng lồ Internet này.[82]

Tình trạng TPCNC ở quốc tế đang diễn ra hết sức phức tạp và đáng báo động. Tốc độ tăng trưởng của TPCNC đang diễn ra một cách nhanh chóng. Mục tiêu của chúng rất đa dạng và trải dài hầu hết ở các lĩnh vực từ đời sống cho đến kinh tế, chính trị. Sự giúp sức của máy tính khiến chúng trở nên nguy hiểm hơn so với tội phạm truyền thống và còn gây ra những khó khăn trong quá trình điều tra bởi vì tội phạm có thể thực hành vi phạm tội từ một phạm vi rất xa, thậm chí là ngoài lãnh thổ. Hơn nữa, phương thức thực hiện của các tội phạm là nhiều vô kể, với những tội phạm có trình độ kỹ thuật chuyên môn thấp, chúng vẫn có thể dễ dàng thực hiện những cách thức đơn giản như sử dụng email giả mạo hay đánh cắp thông tin với những tội phạm chuyên nghiệp hơn, chúng có thể sáng tạo ra hàng ngàn cách thức khác để đạt được mục tiêu của mình và đây chính là thách thức lớn cho các chuyên gia an ninh mạng.

[81] Unisys Corporation - công ty công nghệ thông tin toàn cầu của Mỹ, chuyên cung cấp các dịch vụ, phần mềm và công nghệ CNTT.

[82]https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/

2.1.3. Thực trạng hoạt động của tội phạm công nghệ cao có tính chất xuyên biên giới

Rất nhiều quốc gia trên thế giới báo cáo rằng, từ 50 đến 100 phần trăm hoạt động của TPCNC là có tính chất xuyên quốc gia.[83] Có thể hiểu TPCNC xuyên quốc gia là tội phạm sử dụng máy tính và Internet để thực hiện hành vi phạm tội trên phạm vi nhiều nước khác nhau hay trên toàn cầu. Tính chất xuyên quốc gia của TPCNC tạo điều kiện cho hậu quả của hành vi phạm tội phạm xảy ra ở nhiều quốc gia mà không yêu cầu tội phạm phải có mặt cùng lúc tại những nơi đó để thực hiện hành vi của mình. Đặc điểm của TPCNC xuyên quốc gia đó là thông thường chúng sẽ hoạt động theo cơ cấu tổ chức thay vì hoạt động đơn lẻ và đồng thời, vị trí hoạt động của các tổ chức tội phạm sẽ nằm ở nhiều nơi khác nhau.

Việc tội phạm TPCNC đang tràn lan qua biên giới một cách nhanh chóng là một thách thức lớn trong việc kiểm soát tội phạm trong không gian mạng. Sự phát triển nhanh chóng của Internet là một trong những nguyên nhân cho sự bùng phát của tội phạm công nghệ cao xuyên quốc gia. Hiện nay, Internet trở thành một phần quan trọng của toàn nhân loại, tạo điều kiện cho thế giới kết nối lại với nhau một cách dễ dàng và tội phạm xuyên quốc gia truyền thống đã lợi dụng để phạm tội một cách hiệu quả hơn. Tội phạm lợi dụng việc dễ dàng kết nối và thuận tiện thực hiện hành vi phạm tội từ xa mà Internet tạo ra để có thể hoạt động trong phạm vi toàn thế giới và việc tội phạm phải thực hiện hành vi phạm tội tại một vị trí cụ thể là không cần thiết và có thể cho phép chúng không phụ thuộc vào một không gian hoặc địa điểm cụ thể. Các cơ hội mới được tạo trong không gian mạng đã tăng cường năng lực của tổ chức phạm tội và mạng lưới tội phạm ngày càng tinh vi và nguy hiểm hơn. Ngoài ra, tính chất xuyên quốc gia của loại tội phạm này cũng gây ra những hạn chế nhất định trong việc kiểm soát tội phạm. Do tính

[83] Thống kê của UNODC Văn phòng Liên Hiệp Quốc về chống Ma túy và Tội phạm tại sách Comprehensive Study on Cybercrime.

chất xuyên biên giới, tội phạm có thể dễ dàng có được những lợi thế đáng kể liên quan đến việc thiếu liên kết về mặt pháp luật giữa các quốc gia. Bởi vì mỗi quốc gia sẽ có một chế định riêng về kiểm soát không gian mạng cũng như việc bảo mật an ninh quốc gia nên sẽ rất khó khăn trong việc xét xử tội phạm mạng xuyên quốc gia vì nó sẽ ảnh hưởng đến lợi ích của mỗi quốc gia khác nhau. Hiện nay, pháp luật quốc tế cũng đã đưa ra nhiều công ước nhằm chống lại tội phạm TPCNC xuyên quốc gia nhưng vẫn còn gặp nhiều khó khăn trong việc kí kết và thực thi. Trong các cuộc điều tra tội phạm mạng, sự hợp tác chặt chẽ giữa các quốc gia liên quan là rất quan trọng. Tuy nhiên các thỏa thuận tương trợ pháp lý giữa các quốc gia hiện còn rất phức tạp điều này gây nên sự tốn kém về mặt thời gian để hoàn thiện các thủ tục và ngoài ra việc điều tra, thu nhập chứng cứ nhằm xác định hành vi phạm tội trên hệ thống máy tính hay không gian mạng giữa các quốc gia còn gặp nhiều khó khăn.

Trên thế giới đã nhiều vụ án TPCNC xuyên quốc gia liên quan đến các cuộc tấn công các trang web, khủng bố mạng. Chẳng hạn, một cuộc tấn công khác có quy mô lớn đó là Vụ tấn công Wanna Cry[84] đã sử dụng phần mềm gián điệp tống tiền với tên gọi WannaCry đã khiến khoảng 300.000 máy tính ở 150 quốc gia bị lây nhiễm vào tháng 05 năm 2017. Phần mềm đã mã hóa các tệp tin và yêu cầu người dùng phải trả tiền để đổi lấy các mã khóa. Cuộc tấn công này đã ảnh hưởng đến Telefónica- một công ty viễn thông đa quốc gia Tây Ban Nha và một số công ty lớn khác ở Tây Ban Nha, cũng như các bộ phận của Dịch vụ Y tế Quốc gia (NHS) của Anh nhiều ngân hàng và các công ty thương mại... Công ty vận chuyển Fedex cho biết họ đã mất hàng trăm triệu USD từ vụ tấn công. Mỹ và Vương quốc Anh đã cáo buộc Triều Tiên đứng sau các vụ tấn công này nhưng phía Triều Tiên đã phủ nhận hoàn toàn những cáo buộc trên, ngoài ra họ còn cho rằng đây là "sự khiêu khích chính trị nghiêm trọng".

[84] Quang Huy, 6 cuộc tấn công mạng làm rung chuyển thế giới, VOV,2019.

Trong khi đó, Việt Nam đã xảy ra rất nhiều vụ án tội phạm TPCNC xuyên quốc gia, và phần lớn, các vụ án đều liên quan đến cá cược bóng đá hay tổ chức đánh bạc bất hợp pháp thông qua mạng Internet. Winxx8.com là trang mạng cá cược (lô đề, cá độ bóng đá) có trụ sở tại Casino Shanghai Resort (Campuchia), đánh bạc theo hình thức thế chấp, tổ chức nhiều loại hình gồm thể thao (bóng đá, bóng rổ, quần vợt), casino trực tuyến… Giao diện website thể hiện nhiều ngôn ngữ khác nhau, trong đó có tiếng Việt. Từ năm 2015, một số người Việt Nam sang làm việc tại các sòng bạc Campuchia, sau khi về nước, những người này đã liên kết, móc nối với các đối tượng tổ chức tại Campuchia để cá độ bóng đá, lô đề, casino trực tuyến cho người Việt Nam đánh bạc tại website Winxx8.com. Các "con bạc" cư trú tại TPHCM và tỉnh Long An đã mở nhiều tài khoản ngân hàng Việt Nam cho các đối tượng tại Campuchia thuê, làm tài khoản đại diện trên trang web để cho các đối tượng đánh bạc nạp tiền. Qua hoạt động nghiệp vụ, Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao đã phát hiện đường dây đánh bạc có quy mô lớn này và thu giữ hơn 1,5 tỷ đồng, 2 máy tính xách tay, nhiều thẻ ngân hàng, nhiều điện thoại di động và giấy tờ, tài liệu liên quan.[85]

2.2. Nguyên nhân của sự hình thành và phát triển của tội phạm công nghệ cao

2.2.1. Nguyên nhân khách quan của sự hình thành và phát triển của tội phạm công nghệ cao

Với tính chất hoạt động trên môi trường ảo và phương thức thực hiện "Phi truyền thống" với niềm tin sẽ không thể hoặc rất khó có thể phát hiện tung tích và hành vi phạm tội của tội phạm. Đây là một trong những yếu tố kích thích hoạt động phạm tội đặc biệt đối với trình độ tri thức của loại tội phạm công nghệ muốn thể hiện bản lĩnh của mình. Trên thực tế, người phạm tội không nhất thiết phải ở nơi diễn ra hành vi phạm tội như các loại

[85] Bùi Thu Hương, Phá đường dây đánh bạc nghìn tỷ xuyên quốc gia, bắt 9 đối tượng, Báo Chính phủ, 2019.

tội phạm khác mà người phạm tội có thể ở bất kỳ nơi nào, bất kỳ thời điểm nào, thời gian tính bằng giây để thực hiện được hành vi phạm tội nên rất khó xác định địa điểm phạm tội.

Bên cạnh đó với sự bùng nổ Internet cùng nhiều lợi ích mà chúng mang lại, tội phạm sử dụng triệt để CNTT chính là công cụ, phương tiện phạm tội của mình nhằm mục đích tư lợi, chiếm hưởng trái phép tài sản của người khác hoặc tội phạm coi CNTT chính là mục đích phạm tội của mình nhằm xâm phạm trật tự an ninh. Sự khác biệt về công cụ, phương tiện phạm tội đã khiến cho TPCNC thực hiện được những hành vi phạm tội mà tội phạm truyền thống không thể làm được. Có thể nói, CNTT là một công cụ hữu hiệu giúp cho tội phạm tiến hành hoạt động của mình một cách nhanh chóng mà ít để lại dấu vết. Điều này làm cho việc phục hồi dữ liệu trở lên vô cùng khó khăn và hoặc nếu có phục hồi thì cũng cần có những phương tiện chuyên dụng kỹ thuật cao và tốn nhiều thời gian với những kỹ sư, chuyên gia giỏi.

Tiếp đến chính sự hấp dẫn về kinh tế đem lại là một trong những động lực lớn đối với loại tội phạm này. Trên môi trường ảo tội phạm thực hiện các hành vi của mình bằng những thủ đoạn gian dối một cách nhanh chóng, dễ dàng đã có thể chiếm đoạt tài sản của một người khác mà lao động bình thường khó có thể có được lợi nhuận nhanh và đem lại khối tài sản lớn.

Sự khác biệt trong hệ thống luật pháp và sự hợp tác quốc tế hạn chế là rào cản làm cho hoạt động đấu tranh phòng, chống TPCNC nói chung và tội phạm mạng máy tính nói riêng còn hạn chế, là điều kiện để tội phạm mạng máy tính trên phạm vi toàn thế giới tiếp tục tồn tại, hoạt động.[86]

2.2.2. Nguyên nhân chủ quan của sự hình thành và phát triển của tội phạm công nghệ cao

Đối với ý thức của người thực hiện hành vi phạm tội, tội phạm trước hết là lợi dụng tâm lý cả tin, hám lợi, tò mò của người sử dụng nhằm thực hiện hành vi phạm tội. Đối với ý thức của cá nhân còn chủ quan, mất cảnh giác và chưa nhận thấy được tầm quan trọng trong việc sử dụng máy tính,

[86]http://csnd.vn/Home/Nghien-cuu-Trao-doi/307/Dac-diem-toi-pham-hoc-cua-toi-pham-su-dung-cong-nghe-cao-va-giai-phap-nang-cao-hieu-qua-phong-ngua-dau-tranh

thiết bị số, mạng thông tin cũng như công tác bảo mật dữ liệu. An ninh thông tin là một vấn đề mới với đa số người dùng. Phần lớn các máy tính, thiết bị số không cài đặt, sử dụng các phần mềm bảo vệ (phần mềm diệt vi rút) hoặc thiết lập tường lửa (firewall) để bảo vệ. Chi phí cho việc mua và sử dụng các phần mềm bảo vệ thường không lớn nhưng do ý thức bảo mật kém nên số lượng người sử dụng vẫn thấp.[87] Đây là nguyên nhân dẫn đến việc lây lan các phần mềm độc hại trở lên nhanh chóng, là tiền đề để đối tượng phạm tội thực hiện các hành vi phạm tội về mạng máy tính.

Các tổ chức, doanh nghiệp, nhà nước có có các hoạt động kinh doanh, quản lý nội bộ bằng cách sử dụng mạng hay các thiết bị công nghệ cao vẫn chưa thực quan tâm đúng mức đến giải pháp bảo mật một cách tổng thể. Không có các khóa đào tạo về an ninh mạng cho các lập trình viên khi được tuyển dụng cũng như công tác giáo dục, đào tạo nguồn nhân lực về CNTT và truyền thông còn có những bất cập.

Dù cho pháp luật và phương pháp nghiên cứu về tội phạm công nghệ cao của các quốc gia trên thế giới và Việt Nam vẫn tồn tại các khác biệt. Tuy nhiên, những nguyên nhân hình thành của TPCNC mà nhóm nghiên cứu tiến hành phân tích ở trên có thể coi là những nguyên nhân chính dẫn đến sự hình thành và phát triển của TPCNC.

2.3 Thực tiễn hoạt động xử lý tội phạm công nghệ cao

2.3.1 Thực tiễn hoạt động xử lý tội phạm công nghệ cao tại các quốc gia trên thế giới

2.3.1.1. Thực tiễn hoạt động xử lý tội phạm công nghệ cao tại các quốc gia trên thế giới

Anh Quốc

Trong cuộc công bố Khảo sát Tội phạm ở Anh và xứ Wales, gần đây nhất vào tháng 3 năm 2018 của Văn phòng Thống kê Quốc gia Anh (ONS), ước tính rằng khoảng 4,5 triệu hành vi phạm tội liên quan đến CNC đã được thực hiện ở Anh và xứ Wales trong khoảng thời gian mười

[87]http://csnd.vn/Home/Nghien-cuu-Trao-doi/307/Dac-diem-toi-pham-hoc-cua-toi-pham-su-dung-cong-nghe-cao-va-giai-phap-nang-cao-hieu-qua-phong-ngua-dau-tranh

hai tháng đó. Trong đó, khoảng 3,24 triệu là tội lừa đảo và khoảng 1,23 triệu liên quan đến lạm dụng máy tính (bao gồm nội dung khiêu dâm trẻ em và hack).[88]

TPCNC được coi là đặc biệt nguy hiểm. Do đó, Vương quốc Anh đã ban hành các quy định pháp luật tương đối nghiêm ngặt về tội phạm liên quan đến máy tính như: Pháp luật có liên quan Đạo luật lạm dụng máy tính 1990; Đạo luật bảo vệ dữ liệu năm 1998; Đạo luật giả mạo năm 1981; Đạo luật truyền thông độc hại năm 1998; Luật Truyền thông năm 2003.[89]

Bên cạnh hoạt động xây dựng pháp luật thực định thì Anh Quốc còn chú trọng trong việc bảo đảm các chế tài xử phạt được thực thi một cách nghiêm minh có hiệu quả trong việc ngăn chặn và xử lý loại TPCNC. Một trong đó là hoạt động nhằm nâng cao hiệu quả truy tố TPCNC của The Crown Prosecution Service- Cơ quan truy tố vương miện (CPS)[90] thực hiện. CPS đưa ra hướng dẫn trong việc truy tố tội phạm mạng rất rõ ràng với phạm vi truy tố rộng bao gồm hầu hết các lĩnh vực như: phá hủy chức năng máy tính, tội phạm mạng liên quan đến kinh tế, sở hữu trí tuệ, di động ảo, thông tin và truyền thông. Theo đó, các hành vi sẽ bị truy tố hình sự bao gồm: tạo ra một mối đe dọa giết người, quấy rối hoặc theo dõi bất hợp pháp, tống tiền, tiết lộ hình ảnh tình dục riêng tư mà không có sự đồng ý của nạn nhân, phát tán các nội dung khiêu dâm liên quan đến trẻ em. Thời hạn truy tố đối với TPCNC được CPS quy định là từ 3 năm kể từ ngày hành vi phạm tội được thực hiện và 6 tháng từ khi công tố đã chuẩn bị đủ bằng chứng và sẵn sang để tiến hành xét xử. Ngoài ra để hòa hợp với các điều ước quốc tế đã kí kết như Công ước quốc tế về xóa bỏ mọi hình thức phân biệt chủng tộc (năm 1965), Công ước về quyền của người khuyết tật (2006), Tuyên ngôn quốc tế về quyền con người (1948) và Tuyên bố xóa

[88]Sandra Henshaw, Cybercrime Statistics 2019: An In Depth Look at UK Figures and Trends, November 9, 2018.
[89] https://www.cps.gov.uk/cyber-online-crime
[90] Cơ quan khởi tố các vụ án hình sự đã được điều tra bởi cảnh sát và các tổ chức điều tra khác ở Anh và xứ Wale.

bỏ mọi hình thức không khoan dung và phân biệt đối xử dựa trên tôn giáo hoặc tín ngưỡng (1981), cơ quan CPS đã tăng nặng hình phạt với loại tội phạm " Hate Crime"- tội phạm mà bị cáo thể hiện thái độ thù địch với nạn nhân dựa trên đặc điểm được bảo vệ của nạn nhân như chủng tộc, tôn giáo, khuyết tật, khuynh hướng tình dục hoặc danh tính của người chuyển giới.

Ngoài ra, Vương Quốc Anh còn tiến hành xây dựng các lực lượng phòng chống TPCNC như: Trụ sở Truyền thông Chính phủ (GCHQ) [91] và Đơn vị tội phạm mạng quốc gia (NCCU) đã hợp tác để phát triển các kỹ năng và công nghệ cần thiết để chống lại mối đe dọa TPCNC đối với Vương quốc Anh như phát triển các kỹ năng công nghệ để chống lại các mối đe dọa tội phạm mạng. Ngoài ra đối với hoạt động xử lý các TPCNC quốc gia có tính chất nghiêm trọng sẽ do Cơ quan tội phạm quốc gia (NCA)[92] tiến hành và hơn 3.500 sĩ quan của NCA đã hoàn thành khóa đào tạo nâng cao nhận thức kỹ thuật số.[93]

Đối với mục đích nhằm xử lý và ngăn chặn TPCNC có tính chất xuyên quốc gia, Anh Quốc đã tiến hành mở rộng và củng cố các mạng lưới song phương và đa phương bằng cách hợp tác với các quốc gia khác và thông qua EU, NATO, Khối thịnh vượng chung và các cơ quan phi chính phủ khác.Vào tháng 1 năm 2015, Thủ tướng Anh và Tổng thống Hoa Kỳ Obama đã công bố một loạt các biện pháp dự kiến sẽ tăng cường hợp tác trong lĩnh vực phòng chống TPCNC như: Thứ nhất, thiết lập một "tế bào mạng" chung ở cả hai bờ Đại Tây Dương, nơi các nhóm không gian mạng của Anh và Hoa Kỳ sẽ làm việc cùng nhau để chia sẻ thông tin về các mối đe dọa từ TPCNC. Thứ hai, thực hiện một chương trình tập trận chung quy mô lớn để kiểm tra khả năng phục hồi của cả Anh và Mỹ trước các cuộc tấn

[91] GCHQ là Trụ sở Truyền thông Chính phủ là một tổ chức tình báo và an ninh chịu trách nhiệm cung cấp tín hiệu tình báo và đảm bảo thông tin cho chính phủ và các lực lượng vũ trang của Vương quốc Anh

[92] NCA là Cơ quan tội phạm quốc gia của Anh có nhiệm vụ xử lý tội phạm nghiêm trọng và có tổ chức có nguy cơ lớn nhất đối với Vương quốc Anh.

[93]https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security

công mạng. Thứ ba, xây dựng và phát triển các chương trình đào tạo "những người bảo vệ không gian mạng" cũng như sự hợp tác quốc tế về an ninh mạng giữa Đại học Cambridge và MIT (Viện Công nghệ Massachusetts) để giải quyết các thách thức an ninh mạng kỹ thuật. Vào tháng 6 năm 2014, Vương quốc Anh đã trở thành thành viên chính thức của Trung tâm xuất sắc hợp tác mạng NATO.[94] Chương trình an ninh mạng quốc gia (NCSP) đã tài trợ cho Tổ chức viễn thông khối thịnh vượng chung để phát triển mô hình quản trị mạng quốc gia cho các quốc gia Khối thịnh vượng chung.

Chính những nỗ lực cả về hoạt động xây dựng và thực thi pháp luật cùng với sự phát triển khoa học cộng nghệ đã tạo ra những kết quả to lớn trong chiến dịch đấu tranh với TPCNC tại Anh Quốc. Theo thống kê vào tháng 6 năm 2018, CSEW[95] ước tính rằng các hành vi phạm tội liên quan đến lạm dụng máy tính cho thấy giảm 30% so với năm 2017. Các sự cố liên quan đến quyền truy cập trái phép vào thông tin cá nhân (bao gồm cả hack) cũng có xu hướng giảm. Mặc dù thực trạng hoạt động của TPCNC có xu hướng giảm nhờ sự phát triển của pháp luật và ý thức về các biện pháp tự bảo vệ của người sử dụng công nghệ. Tuy nhiên vấn đề vướn mắc trong hoạt động truy tố và kết án tội phạm mạng còn tồn tại và có xu hướng giảm theo từng năm. Theo thống kê vào năm 2016 chỉ có 57 vụ truy tố TPCNC, giảm so với 61 năm 2015.[96] Năm 2017 chỉ có 47 vụ truy tố tội phạm mạng. Và số vụ truy tố gian lận đã giảm một phần ba kể từ năm 2011.[97] Nguyên nhân của thực trạng này được biết đến là do việc sử dụng máy chủ mã hóa và proxy của TPCNC khiến cho Cảnh sát cực kỳ khó khăn trong việc cảnh sát theo dõi, thu thập chứng cư, hoặc để xác định nơi họ

[94] Trung tâm xuất sắc hợp tác mạng NATO tên tiếng Anh là the NATO Cooperative Cyber Defence Centre of Excellence đây là một cơ sở nghiên cứu và đào tạo về an ninh mạng.

[95] Khảo sát tội phạm ở Anh và xứ Wales được thực hiện bởi Kantar Public (một tổ chức nghiên cứu độc lập) .

[96] Báo cáo của hang luật RPC (Reynold Porter Chamberlain) là một công ty luật bảo hiểm và doanh nghiệp có trụ sở tại London , Vương quốc Anh có văn phòng tại Bristol, Singapore và Hồng Kông.

[97]https://www.independent.co.uk/news/business/news/cyber-crime-prosecutions-fall-police-law-firm-reynolds-porter-chamberlain-a7853591.html.

đang hoạt động nhằm đưa tội phạm ra truy tố. Ngoài ra tính chất xuyên biên giới của TPCNC cũng khiến cho hoạt động truy tố loại tội phạm khó được thực hiện.

Hoa Kì

Nước Mỹ, là mục tiêu hàng đầu của các cuộc tấn công mạng. Quốc gia này được mệnh danh là máy chủ lớn thứ hai trên thế giới của sự hình thành các botnet hay việc thiết bị IoT bị xâm nhập kể từ năm 2016. Đối mặt với thực trạng đáng báo động của tội phạm mạng, Hoa Kỳ đã xây dựng cho mình chế tài nhằm ngăn chặn và xử lý loại tội phạm nguy hiểm này.

Điển hình là các chế tài xử phạt đối với TPCNC được thiết lập tại Đạo luật lạm dụng và gian lận máy tính (CFAA) đã mang lại những hiểu quả tích cực cho nước Mỹ trong hoạt động kiểm soát TPCNC với rất nhiều vụ án dân sự[98], hình sự [99] về loại tội phạm này đã được xử lý triệt để. CFAA đưa ra chế tài xử phạt cho các hoạt động phổ biến của TPCNC. Chẳng hạn, hành vi xâm phạm máy tính của chính phủ bị kết án 1 năm tù trong khi hành vi lấy cắp thông tin an ninh quốc gia sẽ bị phạt 10 năm đây cũng là mức phạt tù cao nhất trong các hành vi của TPCNC. Ngoài ra, đạo luật cũng quy định các mức phạt cho những hành vi xâm phạm đến dữ liệu cá nhân như buôn bán mật khẩu sẽ phải chịu 1 năm tù trong sử dụng máy tính để tống tiền sẽ bị phạt 5 năm tù giam. Như vậy, trong Đạo luật lạm dụng và gian lận máy tính của Hoa Kỳ, hình phạt thấp nhất của TPCNC là 1 năm và cao nhất là 10 năm và tăng nặng 20 năm trong trường hợp tội phạm chịu hai bản án. Ngoài ra, những tài sản được sử dụng để tạo điều kiện hoặc thực hiện hành vi phạm tội và tài sản mà tội phạm thu được sẽ bị tịch thu. [100]Bên cạnh CFAA, Luật Hình sự Hoa Kỳ cũng đưa ra khung pháp lý cho TPCNC. Theo đó, những hành vi bị xét xử hình sự bao gồm: truy cập bất hợp pháp vào dữ liệu lưu trữ truyền thông, trộm cắp danh tính, lừa đảo qua

[98] https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#Civil_cases.
[99] https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act#Criminal_cases.
[100] Phụ lục 5.

đường dây, qua các phương tiện truyền thông. Đối tội truy cập hợp pháp vào dữ liệu truyền thông, các hình phạt gồm ba trường hợp. Đối với vi phạm lần đầu không được cam kết không đúng quy định mục đích (nghĩa là không cam kết với mục đích lợi thế thương mại, phá hủy hoặc thiệt hại độc hại, hoặc lợi ích thương mại tư nhân, hoặc để tiếp tục của bất kỳ hành vi phạm tội hoặc hành vi đồi bại nào), hình phạt tối đa là một năm tù và phạt $ 100.000. Nếu lặp lại vi phạm không được thực hiện cho mục đích không phù hợp hoặc vi phạm lần đầu với các hành vi bất hợp pháp, hình phạt tối đa là năm năm phạt tù và phạt $ 250.000. Đối với các vi phạm lặp lại đã cam kết cho một mục đích không phù hợp, hình phạt tối đa là mười năm tù và phạt $ 250.000. Với hành vi trộm cắp danh tính được quy định tại 18 U.S.Code §□1028, người phạm tội vi phạm mục 1028 (a) (7) sẽ bị phạt tiền và lên tới 15 năm tù nếu như thiệt hại từ $ 1.000 trở lên trong thời gian một năm. Trong hầu hết các trường hợp khác, thời hạn tù tối đa là 5 năm. Tuy nhiên, tòa án có thể áp dụng các bản án cao hơn nếu hành vi phạm tội tạo điều kiện cho tội phạm buôn bán ma túy, tội phạm bạo lực hoặc hành vi khủng bố, hoặc nếu người phạm tội có tiền án. Ngoài ra, một tòa án có thể ra lệnh cho người phạm tội trả tiền bồi thường cho nạn nhân của hành vi trộm cắp danh tính với số tiền bằng với giá trị mà nạn nhân nỗ lực khắc phục dự định hoặc thiệt hại thực tế do gây ra bởi hành vi phạm tội để đảm bảo rằng nạn nhân của hành vi trộm cắp danh tính có thể được bồi thường.

Không chỉ hoàn thiện về mặt pháp luật trong việc xét xử truy tố TPCNC, Hoa Kỳ còn xây dựng các tổ chức điều tra nhằm thực hiện hiệu quả hơn việc điều tra loại tội phạm này như : Cục Điều tra Liên bang (FBI) đã thành lập Trung tâm khiếu nại Internet(IC3) để nhận các vụ khiếu nại của người dân về TPCNC cũng như cung cấp những thông tin chính xác cho Cục Điều tra Liên bang hay Nhóm hành động mạng (CAT) nhằm xử lý nhanh chóng, kịp thời các sự cố xâm nhập máy tính có quy mô lớn và các trường hợp khẩn cấp liên quan đến mạng. Ngoài ra Hoa Kỳ còn tổ chức

hợp tác giữa các cơ quan như Đơn vị hợp nhất tài nguyên và sáng kiến mạng (CIRFU) của bộ phận điều tra mạng FBI đã kết hợp với Liên minh pháp y và Đào tạo điện tử quốc gia (NCFTA) nhằm thu hút các thông tin tình báo từ hàng trăm thành viên, nhân viên tình báo của NCFTA, nhóm phản ứng khẩn cấp của Đại học Carnegie Mellon và trung tâm IC3 nhằm xây dựng chiến lược quan trọng trong việc đối phó với TPCNC.[101]

Hoa Kỳ còn tổ chức phối hợp chặt chẽ trong các vấn đề liên quan đến an ninh mạng với Liên minh Châu Âu EU. Nhóm làm việc giữa EU và Hoa Kỳ về tội phạm mạng và an ninh mạng được thành lập trong bối cảnh Hội nghị thượng đỉnh Mỹ - EU Lisbon 2010, Nhóm công tác này đóng vai trò là khuôn khổ cho sự hợp tác giữa hai bên nhằm tăng cường các hoạt động an ninh mạng nhằm góp phần chống lại các mối đe dọa an ninh mạng toàn cầu. Tại cuộc Đối thoại điện tử EU-Hoa Kỳ tại Brusssels ngày 10 tháng 9 năm 2018, Liên minh Châu Âu và Hoa Kỳ đã tái khẳng định mối quan hệ hợp tác để ủng hộ một không gian mạng ổn định và an toàn.[102]Chính các chế tài xử phạt này là một công cụ hữu hiệu giúp Hoa Kỳ thực hiện hiệu quả trong việc điều tra, truy tố và kết án TPCNC đặc biệt những tội phạm trong những vụ án lớn gây ra những thiệt hại nghiêm trọng. Điển hình là Sonya Martin, chủ mưu của vụ hack máy tính và rút tiền thông qua máy tính một cách tinh vi đã bị kết án với tội danh âm mưu phạm tội lừa đảo và bị phạt 2 năm 6 tháng tù giam.[103] Hay một trường hợp khác liên quan đến việc tấn công vào các trang web chính phủ Hoa Kỳ, Max Butler đã bị kết án 13 năm tù và bồi thường 27,5 triệu đô la cho việc truy cập trái phép vào

[101]https://www.fbi.gov/investigate/cyber?fbclid=IwAR3kY_extO53Cd1n4wVBVZ7CTuz1slMvLl21x_XE4EQR4r-EaWcxY-21RXI

[102] https://uk.usembassy.gov/fact-sheet-u-s-eu-cyber-cooperation/

[103]https://archives.fbi.gov/archives/atlanta/press-releases/2012/sentencing-in-major-international-cyber-crime-prosecution?fbclid=IwAR3MYrwVnYNPTwuTYQJkrcrEqx5gu8tbG2-3nbN8lv68bwTYeaL0DQKfDY8

các căn cứ quân sự và các bộ phận hạt nhân của Hoa Kỳ và ăn cắp gần 2 triệu thẻ tín dụng từ các ngân hàng và doanh nghiệp.[104]

2.3.1.2. Thực tiễn hoạt động Hợp tác quốc tế nhằm xử lý tội phạm công nghệ cao của các quốc gia trên thế giới

Trong quá khứ, TPCNC chủ yếu là cá nhân hoặc nhóm nhỏ. Nhưng ngày nay thế giới đang được chứng kiến sự hình thành của các mạng lưới tội phạm phức tạp, có tổ chức và mang tính toàn cầu. Các tổ chức tội phạm có xu hướng ngày càng chuyển sang khai thác Internet để phục vụ cho hành vi phạm tội nhằm tối đa hóa lợi nhuận của trong thời gian ngắn nhất. Các tội phạm sử dụng công nghệ cao tiên tiến như hack, tấn công phần mềm độc hại và tống tiền DDoS đặt ra mối đe dọa lớn đối với an ninh của các chính phủ, doanh nghiệp và các cá nhân đồng thời đưa ra những thách thức đối với đối với hoạt động thực thi pháp luật của các quốc gia khi nhiều chính phủ vẫn chưa trang bị đủ kiến thức hoặc kỹ năng cần thiết để đương đầu với loại tội phạm nguy hiểm này. Bên cạnh đó với tính chất không biên giới của không gian mạng đã đặt ra những thách thức trong việc điều tra các sự cố TPCNC. Những thông tin và bằng chứng liên quan đến nghi phạm, nạn nhân và tội phạm có thể nằm ở nhiều quốc gia. Do đó nhu cầu về việc xây dựng các tổ chức liên minh giữa các quốc gia nhằm mục đích nâng cao và xử lý tội phạm công nghệ cao trong thời đại hiện nay là vô cùng cần thiết.

Interpol - Tổ chức Cảnh sát hình sự quốc tế được thành lập ngày 7 tháng 9 năm 1923 tại Viên, Áo, là một trong những tổ chức quốc tế đã có những đóng góp hiệu quả trong hoạt dộng đấu tranh phòng chống TPCNC quốc tế. Interpol không phải là một cơ quan thực thi pháp luật, thay vào đó nó là một tổ chức quốc tế có mạng lưới là các cơ quan thực thi pháp luật hình sự tại các quốc gia khác nhau. Tổ chức này có chức năng là một cơ

[104]B. Lynn Winmill, David L. Metcalf and Michael E. Band, Cybercrime: Issues and challenges in the United States.

quan liên lạc hành chính giữa các cơ quan thực thi pháp luật của các nước thành viên, cung cấp thông tin liên lạc và cơ sở dữ liệu hỗ trợ, hỗ trợ thông qua trụ sở trung ương ở Lyon, Pháp. Interpol hoạt động độc lập, tôn trọng chủ quyền các quốc gia thành viên, không can thiệp vào công việc nội bộ. Đối tượng điều tra chỉ là tội phạm hình sự ở ba lĩnh vực chính là: khủng bố, tội phạm có tổ chức và tội phạm mạng. Interpol giúp điều phối các hoạt động điều tra và theo dõi hoạt động của tội phạm mạng xuyên quốc gia tại chỗ hoặc từ xa, đảm bảo cảnh sát quốc gia có thông tin chính xác nhất để thuận lợi trong việc hành động ngăn chặn và xử lý TPCNC. Interpol duy trì một hệ thống các văn phòng tại 190 quốc gia trên thế giới. Các bộ phận của văn phòng thường được hoạt động với sự kết hợp cùng các cơ quan thực thi pháp luật quốc gia. Thông qua trực tuyến hệ thống I-24/7 (Internet 24/7), văn phòng có thể tạo điều kiện cho các yêu cầu hợp tác cảnh sát song phương hoặc đa phương không chính thức, hoặc truyền yêu cầu hỗ trợ pháp lý chính thức từ cơ quan trung ương này sang cơ quan khác - thông qua cơ quan trung ương quốc gia.[105]

Ứng phó với những thách thức mới do đó hoạt động thực thi pháp luật nhằm chống lại TPCNC đòi hỏi một cách tiếp cận mới. Lực lượng cảnh sát quốc tế Interpol là tổ chức đi đầu trong việc nghiện cứu và áp dụng các hình thức truy bắt tội phạm hiện đại phù hợp với tính chất phức tạp của TPCNC. Đầu tiên có thể kể đến là hoạt động hỗ trợ phân tích dữ liệu thông minh của Interpol đã tạo điều kiện cho việc nhanh chóng trao đổi, nắm bắt thông tin về TPCNC, góp phần giúp cảnh sát quốc gia nâng cao tốc độ truy bắt, điều tra tội phạm mạng và pháp y kỹ thuật số. Chia sẻ dữ liệu, thông tin, bằng chứng của cảnh sát trên toàn cầu là vô quan trọng, góp phần tạo nên thành công khi xử lý, truy bắt TPCNC. Bên cạnh đó Interpol còn đóng vai trò là một kho dữ liệu đa quốc gia. Tổ chức này là cầu nối tạo nên sự liên kết giữa các quốc gia trong hoạt động nghiên cứu, phân tích và kết nối

[105] Comprehensive study on cybercrime by United Nations office on drugs and crime, pages 187.

với các chuyên gia trên toàn thế giới nhằm nghiên cứu tính chất, đặc điểm, phương thức hoạt động của TPCNC nhằm tạo ra các phương pháp mới để đảm bảo cung cấp kinh nghiệm, tri thức cho các nước thành viên để đối đầu với các mối đe dọa mạng mới nhất cũng như khuyến khích các quốc gia tiến hành thông báo cho Interpol để cảnh báo trên toàn thế giới về các mối đe dọa mới đến từ tội phạm mạng. Đây cũng là nền tảng để Interppol nghiên cứu phát triển các công cụ mới nhằm ngăn chặn và xử lý TPCNC.

Với bản chất xuyên quốc gia vốn có của TPCNC, rất có khả năng là bằng chứng về hành vi phạm tội sẽ được đặt trên các khu vực pháp lý khác nhau. Tuy nhiên hiện nay, nhiều cơ quan thực thi pháp luật không có đủ khả năng tiến hành phân tích dữ liệu cần thiết để tiếp tục điều tra TPCNC gây ảnh hưởng nghiêm trọng đến sự an toàn của công dân và cơ sở hạ tầng an ninh quốc gia. Sự ra đời của Interpol góp phần tạo nên một môi trường hợp tác quốc tế trong lĩnh vực phòng chống TPCNC.

Có thể kể đến những thành tích nổi bật của tổ chức này trong hoạt động truy bắt tội phạm như: Bắt giữ thành công người đứng đầu một mạng lưới tội phạm kinh tế đứng sau hàng ngàn vụ lừa đảo trực tuyến. Chính nhờ sự kết hợp của Interpol, Ủy ban Tội phạm kinh tế và tài chính Nigeria (EFCC) mà Công dân Nigeria 40 tuổi, được gọi là "Mike", được cho là đứng sau các vụ lừa đảo với tổng trị giá hơn 60 triệu USD liên quan đến hàng trăm nạn nhân trên toàn thế giới đã được xử lý.[106] Ngoài ra Interpol còn hợp tác với các cơ quan điều tra trong khu vực ASEAN để xác định máy chủ đã phát tán và kiểm soát các loại phần mềm độc hại khác nhau làm cho 270 trang web bị xâm nhập bao gồm các trang web của chính phủ được xác định liên quan đến một người Nigeria và do một tên tội phạm

[106] INTERPOL, Ringleader of global network behind thousands of online scams arrested in Nigeria, 2016.

Indonesia bán bộ dụng cụ lừa đảo và đăng video Youtube cho khách hàng biết cách sử dụng các phần mềm bất hợp pháp đó.[107]

Bên cạnh đó trong phạm vi khu vực Châu Âu**,** Europol cũng đang tài trợ cho một Trung tâm tội phạm mạng mới của châu Âu để cung cấp trợ giúp về kỹ thuật, phân tích và pháp y trong các cuộc điều tra. Trung tâm tội phạm công nghệ Châu Âu (EC3 hoặc EC³) là cơ quan của Văn phòng Cảnh sát (Europol) của Liên minh châu Âu (EU), có trụ sở tại The Hague. Cơ quan này điều phối các hoạt động thực thi pháp luật xuyên biên giới chống lại tội phạm máy tính và hoạt động như một trung tâm kỹ thuật chuyên môn về lĩnh vực này. Europol đã thành lập EC3 vào năm 2013 để tăng cường việc thực thi pháp luật TPCNC ở khu vực EU. Mục tiêu của EC3 là bảo vệ công dân, doanh nghiệp và chính phủ Châu Âu khỏi loại tội phạm này.

Kể từ khi thành lập, EC3 đã đóng góp đáng kể vào cuộc chiến chống TPCNC: tổ chức đã tham gia vào nhiều hoạt động, triển khai hỗ trợ hoạt động dẫn đến tội phạm bị bắt giữ, ngoài ra EC3 còn phân tích dữ liệu của các tập tin và phần lớn trong đó được phát hiện là tập tin độc hại.Đặc biệt vào năm 2018, dưới sự can thiệp của EC3, 95 kẻ lừa đảo chuyên nghiệp và thành viên của các mạng lưới tội phạm dựa trên Internet bị nghi ngờ có hoạt động lừa đảo trực tuyến đã bị bắt trong Hành động thương mại điện tử 2018 (ecomm 2018), với hơn 20000 giao dịch gian lận với thẻ tín dụng bị xâm nhập, với giá trị ước tính vượt quá 8 triệu EUR.[108] Hành động ngăn chặn và xử lý tổ chức TPCNC này được điều phối bởi EC3 từ trụ sở của Europol ở The Hague, cùng sự hỗ trợ trực tiếp từ các thương nhân, công ty hậu cần, ngân hàng và các chương trình thẻ thanh toán. Europol cũng hỗ trợ các nhà chức trách quốc gia tại chỗ bằng cách cung cấp các dịch vụ phân tích trong các cuộc điều tra.

2.3.2. Thực tiễn hoạt động xử lý tội phạm công nghệ cao tại Việt Nam

[107] INTERPOL, INTERPOL-led cybercrime operation across ASEAN unites public and private sectors 2017.
[108] Europol, 95 e-commerce fraudsters arrested in international operation, 2018.

2.3.2.1. Thực tiễn xử lý của tội phạm công nghệ cao tại Việt Nam

Theo số liệu thống kê của Cục Cảnh sát phòng chống tội phạm (PCTP) sử dụng công nghệ cao (C50), Bộ Công an, từ năm 2010-6/2014 lực lượng Cảnh sát PCTP sử dụng công nghệ cao trên cả nước đã phát hiện và xác minh 1.1476 đầu mối vụ việc có dấu hiệu vi phạm pháp luật liên quan đến yếu tố công nghệ cao với 3.220 đối tượng, trong đó 823 vụ việc và 1.990 đối tượng là do C50; 450 vụ việc và 1.230 đối tượng là do Công an các địa phương. Tổng thiệt hại do loại tội phạm trong lĩnh vực này gây ra lên tới hàng chục ngàn tỷ đồng. Số liệu thống kê các vụ án phát hiện, khởi tố điều tra và kết quả đạt năm 2010 – năm 2014.[109]

Qua nhưng số liệu cho thấy tuy đã đạt những kết quả nhưng tình hình tội phạm công nghệ cao diễn biến hết sức phức tạp, số lượng phát hiện cao nhưng khởi tố điều tra thì rất ít, số lượng năm sau cao hơn năm trước. Trong các giai đoạn thì có thể nói năm 2011 được coi là năm "báo động đỏ" của an ninh mạng Việt Nam với rất nhiều vụ tấn công, phá hoại, lây nhiễm virus, phầm mềm gián điệp, mã tin học độc hại..., nhằm vào hệ thống mạng của cơ quan, doanh nghiệp, tập đoàn kinh tế của Nhà nước với mức độ, tính chất ngày càng nghiêm trọng, làm rối loạn hoạt động của hệ thống và lộ lọt thông tin.[110] Qua những số liệu những năm 2010 – 2014 tội phạm công nghệ bùng phát được coi là báo động đỏ đối với tình hình trật tự an ninh xã hội.[111] Có thể thấy rằng, do mới thành lập nên lực lượng để phòng chống đối với tội phạm này còn non trẻ, chưa nắm bắt kịp thời được tình hình, thủ đoạn cũng như phương thức hoạt động của tội phạm để đưa ra những phương án, chiến lược, kế hoạch để phòng ngừa, phát hiện, xử lí tội phạm hiệu quả mà đặc thù của loại tội phạm là tính lây lan nhanh chóng và hành vi phạm tội biến đổi tinh vi khó lường.

---

[109] Phụ lục 6

[110] http://tks.edu.vn/thong-tin-khoa-hoc/chi-tiet/79/687

[111] Cao Anh Đức, Tính chất của tình hình tội phạm sử dụng công nghệ cao tại Việt Nam, thủ đoạn phạm tội và dự báo: http://nguoibaovequyenloi.com/User/ThongTin_ChiTiet.aspx?MaTT=289201551832859903&MaMT=23.

Những năm tiếp theo 2015 đến 2018 tình hình TPCNC đã có những chuyển biến mạnh mẽ hơn so với những năm trước, được thể hiện qua bảng báo cáo về kết quả đấu tranh của lực lượng Công an các cấp.[112] Cục Cảnh sát phòng chống tội phạm sử dụng công nghệ cao (C50) Bộ Công an đã phối hợp với một số đơn vị nghiệp vụ khám phá nhiều chuyên án, bắt giữ nhiều "quái nhân" lợi dụng mạng Internet để phạm tội. Trong đó đã phát hiện, triệt phá nhiều vụ án lớn như: Vụ án công ty CNC tổ chức đánh bạc, đánh bạc trực tuyến trên mạng Internet bằng hình thức game bài với gần 43 triệu tài khoản tham gia đánh bạc; 25 đại lý cấp 1 và 5.877 đại lý cấp 2 trên phạm vi toàn quốc để giao dịch mua, bán Rik (tiền ảo) với tổng số tiền thu lợi bất chính trên 9.853 tỷ đồng, thu giữ trên 1.760 tỷ đồng; khởi tố điều tra, làm rõ 105 bị can về các tội danh liên quan.[113]

Nhận thấy sự gia tăng và tinh chất nguy hiểm của TPCNC, pháp luật Việt Nam đã có những quy định về chế tài xử lý loại tội phạm này như sau: Theo quy định của Bộ luật Hình sự năm 1999 (sửa đổi, bổ sung năm 2009), TPCNC chủ yếu bị xử lý theo 5 điều luật 224, 225, 226, 226a, 226b thuộc Chương XIX về các tội phạm trong lĩnh vực CNTT, viễn thông và Bộ luật hình sự 2015 tội phạm sử dụng công nghệ cao bị xử lí theo các điều luật 285 đến điều 294 thuộc mục 2 Chương XXI các tội phạm xâm phạm an toàn công cộng,trật tự công cộng. Đặc biệt tại Điều 226b thì phạm tội thuộc một trong các trường hợp chiếm đoạt tài sản có giá trị từ năm trăm triệu đồng trở lên; gây hậu quả đặc biệt nghiêm trọng có thể bị phạt tù từ mười hai năm đến hai mươi năm hoặc tù chung thân. Ngoài ra, trên thực tế có một số hành vi trong quá trình phạm tội có sử dụng CNTT, viễn thông thì cũng có thể bị xử lý theo các điều Điều 155 (Tội sản xuất, tàng trữ, vận chuyển, buôn bán hàng cấm), Điều 159 (Tội kinh doanh trái phép), Điều 248 (Tội đánh bạc), Điều 249 (Tội tổ chức đánh bạc hoặc gá bạc), Điều 251 (Tội rửa

[112] Xem tại phụ lục 7

[113]http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2018-08-13/toi-pham-cong-nghe-cao-trong-linh-vuc-tien-te-gia-tang-60921.aspx

tiền), Điều 253 (Tội truyền bá văn hóa phẩm đồi trụy)…Bên cạnh đó, ngày 7/4/2014, Chính phủ ban hành Nghị định số 25/2014/NĐ-CP quy định về phòng, chống tội phạm và các vi phạm pháp luật khác có sử dụng công nghệ cao. Nghị định này quy định về hoạt động phòng ngừa, phát hiện, xử lý tội phạm và vi phạm pháp luật khác có sử dụng CNC; Hợp tác quốc tế trong phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng CNC; Trách nhiệm của cơ quan, tổ chức, doanh nghiệp và cá nhân trong phòng, chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao.[114]

Tóm lại đây mới chỉ là số vụ việc được phát hiện, còn theo đánh giá của cơ quan, chuyên môn thì số vụ còn ẩn là vô cùng lớn do đặc thù của tội phạm hoạt động thế giới "ảo". Với đặc thù của TPCNC là tính lây lan nhanh chóng mà thực tiễn xử lí còn nhiều vướng mắc khó khăn trong hoạt động phát hiện, ngăn ngừa và xử lí tội phạm. Có thể nhìn thấy qua tỉ lệ số vụ phạm tội qua các năm có xu hướng tăng dần. Điều này cho thấy tình hình tội phạm sử dụng công nghệ cao đang có chiều hướng ngày càng phức tạp, với diễn biến tăng cả về số vụ và tính chất, mức độ, hậu quả. Thực tế số vụ vi phạm pháp luật hình sự phát hiện tương đối nhiều, nhưng số vụ khởi tố và truy tố rất thấp, bởi chủ thể tội phạm thực hiện trên không gian mạng, có thể ở một nơi nhưng lại gây ra hậu quả toàn cầu, do đó rất khó xác định chủ thể để truy tìm và bắt giữ, do rào cản về không gian mạng và lãnh thổ.

2.3.2.2 Thực tiễn hợp tác quốc tế về thực thi pháp luật, phòng chống tội phạm công nghệ cao của Việt Nam

Hiệp định tương trợ tư pháp về hình sự

Qua các quá trình nghiên cứu, đánh giá cho thấy TPCNC là một loại tội phạm hết sức nghiêm trọng có tổ chức và xuyên quốc gia ảnh hưởng lớn đến các vấn đề chính trị - xã hội, kinh tế và trật tự an ninh, quốc phòng của

[114]http://cand.com.vn/Phap-luat/Toi-pham-su-dung-cong-nghe-cao-se-bi-xu-ly-nhu-the-nao-266415//

quốc gia. Hiệp định tương trợ tư pháp về hình sự là một trong những điều ước quốc tế quan trọng trong lĩnh vực tư pháp hình sự, là cơ sở pháp lý để các bên ký kết dành cho nhau sự tương trợ tối ta trong quá trình điều tra, truy tố, xét xử nhằm thu thập tài liệu, chứng cứ và thực hiện các thủ tục tố tụng giúp việc giải quyết các vụ án hình sự của mỗi bên đạt kết quả cao. Các Điều ước Việt Nam đã ký kết trong lĩnh vực hình sự trong đó bao gồm tội phạm công nghệ như là : Việt Nam - Ấn Độ; Việt Nam – An giê ri ; Việt Nam – Ba Lan; Việt Nam – Ba La Rút; Việt Nam – Campuchia; Việt Nam- Cu Ba; Việt Nam – Hàn Quốc; Việt Nam – Hungari; Việt Nam – Inđôđêxia; Việt Nam - Lào; Việt Nam – Mông Cổ; Việt Nam – Nga; Việt Nam – Tiệp Khắc (Séc và Xlô-va-ki-a kế thừa); Việt Nam – Triều Tiên; Việt Nam – Trung Quốc; Việt Nam – ASEAN; Việt Nam – Tây Ban Nha.

Hiệp định về hợp tác trong lĩnh vực phòng chống và xử lý tội phạm

Bên cạnh đó nhận thấy mối hiểm họa nguy hiểm từ TPCNC, Việt Nam đã tiến hành kí kết các hiệp định về hợp tác trong lĩnh vực phòng chống tội phạm như: Thứ nhất, Hiệp định giữa Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam và Chính phủ nước Cộng hòa Mô-dăm-bích về hợp tác trong lĩnh vực phòng, chống tội phạm, ký tại Ma-pu-tô ngày 10 tháng 6 năm 2011, có hiệu lực kể từ ngày 06 tháng 10 năm 2011. Với mong muốn tiếp tục phát triển mối quan hệ hữu nghị và hợp tác giữa hai nước theo tinh thần thống nhất và đoàn kết; nhận thức được tầm quan trọng của việc hợp tác giữa các cơ quan bảo vệ pháp luật của hai nước trong việc phòng, chống có hiệu quả các loại tội phạm liên quan đến hai nước; trên cơ sở tôn trọng độc lập, chủ quyền, không can thiệp vào công việc nội bộ của nhau, bình đẳng, hiểu biết lẫn nhau và cùng có lợi, phù hợp với luật pháp quốc tế và pháp luật hiện hành của mỗi nước. Hiệp định quy định phạm vi

hợp tác trong đó có hợp tác phòng chống TPCNC và các vấn đề liên quan được quy định tại khoản 6, Điều 1 Hiệp định[115].

Thứ hai, Hiệp định giữa Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam và Chính phủ nước Cộng hòa I-ta-li-a về hợp tác đấu tranh phòng, chống tội phạm, ký tại Rô-ma ngày 09 tháng 7 năm 2014, có hiệu lực từ ngày 30 tháng 11 năm 2016. Hiệp định này quy định về các lĩnh vực hợp tác trong đó có hợp tác về TPCNC và tội phạm có tổ chức xuyên quốc gia đây cũng là một trong tính chất của tội phạm công nghệ tại điều khoản f điều 3.[116] Nhằm mục đích tăng cường hợp tác thông qua trao đổi thông tin nghiệp vụ và kinh nghiệm công tác, đồng thời đào tạo cho các cơ quan thực

---

[115] Điều 1. Phạm vi hợp tác

Hai Bên tiến hành hợp tác ngăn chặn và đấu tranh chống các loại tội phạm sau đây:

1. Các hoạt động khủng bố quốc tế;

2. Sản xuất, tàng trữ, vận chuyển, lưu hành tiền giả cũng như các loại giấy tờ có giá giả khác;

3. Sản xuất, tàng trữ, vận chuyển và mua bán trái phép các chất ma túy, các chất hướng thần và các tiền chất;

4. Chế tạo, tàng trữ, vận chuyển, sử dụng, mua bán trái phép các loại vũ khí đạn dược, vật liệu nổ, chất cháy, chất độc và chất phóng xạ và hạt nhân;
5. Rửa tiền;
6. Tội phạm sử dụng công nghệ cao;
7. Sản xuất, tàng trữ, vận chuyển, buôn bán hàng cấm, hàng giả và buôn lậu;
8. Buôn bán, tàng trữ và vận chuyển trái phép các di sản văn hóa và cổ vật bị đánh cắp;
9. Truyền bá văn hóa phẩm đồi trụy;
10. Tổ chức đưa người xuất nhập cảnh trái phép;
11. Mua bán người;
12. Tội phạm về môi trường;
13. Hoạt động phạm tội có tổ chức xuyên quốc gia khác nếu hai Bên thấy cần thiết.

[116] Điều 3: lĩnh vực hợp tác
1. Các Bên triển khai hợp tác theo quy định tại Điều 1 trên các lĩnh vực sau:
(a) Tội phạm có tổ chức xuyên quốc gia;
(b) Tội phạm sản xuất, vận chuyển, mua bán và/hoặc tàng trữ trái phép các chất ma túy, chất hướng thần và tiền chất;
(c) Tội phạm mua bán người và đưa người di cư trái phép;
(d) Tội phạm mua bán trái phép vũ khí, đạn dược, chất nổ, nguyên liệu hạt nhân, các chất phóng xạ và chất độc;
(e) Tội phạm kinh tế, rửa tiền, và tội phạm xâm phạm quyền sở hữu, đồng thời cũng nhằm phát hiện tài sản có nguồn gốc bất hợp pháp;
(f) Tội phạm sử dụng công nghệ cao;
(g) Bất kỳ tội phạm nào khác các Bên cùng quan tâm.
2. Các Bên cũng sẽ hợp tác phòng và chống các vụ tấn công khủng bố theo quy định pháp luật hiện hành của mỗi nước và các Công ước quốc tế mà các Bên tham gia.
3. Hiệp định này không gây ảnh hưởng tới các hoạt động dẫn độ và tương trợ tư pháp về hình sự".

thi pháp luật của các bên nhằm đấu tranh chống tội phạm có tổ chức xuyên quốc gia, tội phạm công nghệ và các loại tội phạm khác.

Thứ ba, Hiệp định khung về đối tác và hợp tác toàn diện giữa một bên là nươc cộng hòa xã hội chủ nghĩa Việt Nam và một bên là liên minh Châu Âu và các quốc gia thành viên; với mục đích tăng cường quan hệ song phương, các bên sẽ tiến hành đối thoại toàn diện và tăng cường hơn nữa hợp tác trên tất cả các lĩnh vực cùng quan tâm. Tại Điều 2 hiệp định đã nêu ra mục tiêu của hợp tác trong đó có đề cập đến lĩnh vực tội phạm công nghệ: (e) Tiến hành hợp tác trong lĩnh vực tư pháp và an ninh, bao gồm hợp tác pháp quyền và pháp luật, bảo vệ dữ liệu, di cư, chống tội phạm có tổ chức, rửa tiền và chống ma túy bất hợp pháp; (f) Thúc đẩy hợp tác trong các lĩnh vực khác cùng quan tâm, bao gồm nhân quyền, chính sách kinh tế, dịch vụ tài chính, thuế, chính sách công nghiệp và doanh nghiệp vừa và nhỏ, CNTT và truyền thông, khoa học và công nghệ, năng lượng, vận tải, qui hoạch và phát triển đô thị. Với tình hình TPCNC hiện nay, việc kí kết PCA có giá trị thúc đẩy quá trình đào tạo, nâng cao trình độ, phát triển khoa học – công nghệ góp phần vào công tác phòng chống TPCNC đạt hiệu quả.

Hợp tác trong công tác đấu tranh phòng chống tội phạm công nghệ cao

TPCNC hoạt động ngày càng gia tăng với mức độ, cách thức tổ chức, quy mô lớn và mang tính xuyên quốc gia. Do đó để công tác phòng chống tội phạm hiệu quả nhà nước đã tiến hành hợp tác quốc tế về hoạt động thực thi pháp luật cụ thể.

Việt Nam hợp tác với Cảnh sát Liên bang Australia (AFP) là đại diện cảnh sát của Chính phủ Australia tại Việt Nam. AFP và Bộ Công an (BCA) Việt Nam đã hợp tác trong công tác đấu tranh phòng chống tội phạm nguy hiểm xuyên quốc gia và có tổ chức kể từ khi Văn phòng đại diện thực thi luật pháp mở tại Băng-cốc năm 1993. Văn phòng đầu tiên của AFP mở tại

Hà Nội ngày 01/04/1999 và sau đó là Văn phòng AFP tại Thành phố Hồ Chí Minh mở ngày 13/06/2003. AFP và Bộ công an (BCA) hợp tác với nhau ở cấp độ chiến lược, chia sẻ thông tin nghiệp vụ, tiến hành các chuyên án chung và cùng làm việc để phát triển năng lực. Số lượng các băng nhóm tội phạm xuyên quốc gia đã bị triệt phá và những thành viên trong các băng nhóm đã bị truy tố, kết án và trừng trị vì những tội phạm nghiêm trọng của chúng. Một khối lượng lớn hàng hóa phi pháp đã bị tịch thu. Những vụ điều tra phối hợp với nhiều loại tội phạm trong đó có TPCNC. Để hỗ trợ những chuyên án này, đã có nhiều đoàn các sỹ quan cảnh sát được gửi sang giữa hai nước nhằm thực hiện những nỗ lực chung. Về mặt chiến lược, trong những năm qua AFP đã được trao cơ hội, trao đổi những công cụ, phân tích thông tin nghiệp vụ và các thiết bị quan trọng để giúp các đồng nghiệp Việt Nam của mình phát triển năng lực trong các lĩnh vực như TPCNC.[117] Năm 2010 Việt Nam tiếp tục hợp tác với Trung tâm Phối hợp chống Tội phạm Xuyên quốc gia Việt-Úc (JTCC) và Việt Nam và AFP hợp tác với đối tác là Trường Đại học RMIT Đồng quản lý và phối hợp tổ chức chương trình ARLEMP Chương trình Quản lý Thực thi Luật pháp Khu vực Châu Á (ARLEMP).

Bộ Công an Việt Nam tăng cường hợp tác với Cơ quan Điều tra Liên bang Hoa Kỳ (FBI) thời gian qua, từng bước đạt được những kết quả tích cực, góp phần cụ thể hóa quan hệ Đối tác toàn diện Việt Nam - Hoa Kỳ. Hai bên đã ký, triển khai hiệu quả nội dung các văn bản hợp tác như: Bản ghi nhớ về phòng, chống tội phạm xuyên quốc gia ký năm 2019; Thỏa thuận chuyển giao công nghệ phần mềm giám định ADN ký năm 2015... Những văn bản, thỏa thuận này đã tạo cơ sở pháp lý quan trọng cho lực lượng Công an Việt Nam và FBI chủ động triển khai nhiều hoạt động hợp tác tư pháp hình sự, phối hợp nghiệp vụ và đạt được những kết quả tích cực trong đấu tranh phòng, chống tội phạm xuyên quốc gia liên quan đến hai

[117] https://vietnam.embassy.gov.au/hnoivietnamese/Police_liaison.html

nước và quan hệ Đối tác toàn diện Việt Nam - Hoa Kỳ nói chung trong thời gian tới. Hai bên đã triển khai có hiệu quả các văn bản hợp tác đã ký về phòng, chống tội phạm xuyên quốc gia, chia sẻ thông tin đối tượng khủng bố...; Trao đổi thông tin đấu tranh chuyên án, hỗ trợ điều tra, truy tố, xét xử tội phạm, nhất là TPCNC. Tạo khuôn khổ hợp tác tư pháp hình sự như: thường xuyên trao đổi, tiếp nhận, xử lý thông tin tội phạm giữa Văn phòng INTERPOL Việt Nam và Cơ quan Điều tra Liên bang Hoa Kỳ trong công tác đấu tranh phòng, chống tội phạm có tổ chức xuyên quốc gia liên quan đến hai Bên, đặc biệt là TPCNC và các loại tội phạm hình sự khác; trao đổi về phương thức, thủ đoạn tội phạm mới nổi nhằm phục vụ công tác dự báo trong phòng, chống các loại tội phạm xuyên quốc gia, thông qua hình thức trao đổi đoàn hoặc tổ chức các cuộc họp song phương nhằm tham vấn, đánh giá định kỳ; kịp thời trao đổi thông tin tội phạm, chia sẻ kinh nghiệm. Tăng cường hợp tác trên lĩnh vực bảo đảm an ninh mạng nói chung, phòng, chống TPCNC nói riêng.

Trong những năm gần đây, tình hình TPCNC giữa đối tượng người Việt Nam và Trung Quốc thực hiện có nhiều diễn biến phức tạp. Tuy nhiên công tác phối hợp, trao đổi, cung cấp thông tin giữa các cơ quan phòng, chống tội phạm hai nước còn chậm, không đầy đủ trong khi tội phạm diễn ra rất nhanh, các đối tượng sau khi rút tiền sẽ nhanh chóng tẩu thoát do đó kết quả đấu tranh với tội phạm này vẫn còn nhiều hạn chế. Đặc biệt, việc thu thập, xác minh địa chỉ IP để xác định vị trí, địa điểm, đối tượng hoạt động gặp rất nhiều khó khăn và kéo dài vì thế Việt Nam hợp tác với Trung Quốc trong lĩnh vực phòng, chống TPCNC hai bên đã tiến hành hội nghị hợp tác phòng, chống tội phạm lần thứ 6 Việt Nam-Trung Quốc đã được tổ chức tại thủ đô Bắc Kinh (Trung Quốc) để góp phần nâng cao hiệu quả hơn nữa trong hợp tác thực thi pháp luật giữa Bộ Công an Việt Nam và Bộ Công an Trung Quốc trong thời gian tới, hai bên thống nhất nghiêm túc triển khai nhận thức chung quan trọng đạt được giữa lãnh đạo cấp cao hai

Đảng, hai Nhà nước và các nội dung thỏa thuận hai Bộ đã thống nhất trong các văn bản hợp tác đã ký; duy trì triển khai hoạt động đoàn các cấp; tiếp tục đẩy mạnh phối hợp đấu tranh phòng, chống tội phạm, trong đó đặc biệt là TPCNC.[118] [119]

[118]http://baochinhphu.vn/Doi-ngoai/Viet-Nam-Trung-Quoc-Day-manh-phoi-hop-dau-tranh-phong-chong-toi-pham/349058.vgp

[119] Xem thêm: Trần Văn Doanh, Hợp tác quốc tế trong PCTP sử dụng CNC và vấn đề đặt ra trong công tác đào tạo, bồi dưỡng cán bộ.
http://hvcsnd.edu.vn/nghien-cuu-trao-doi/giao-duc-dao-tao/hop-tac-quoc-te-trong-pctp-su-dung-cnc-va-van-de-dat-ra-trong-cong-tac-dao-tao-boi-duong-can-bo-3285

TỔNG KẾT CHƯƠNG 2

Chương hai của bài nghiên cứu đã nêu rõ thực trạng hoạt động của TPCNC theo khu vực địa lý và các lĩnh vực chuyên ngành; Đồng thời làm rõ tính chất xuyên biên giới của loại tội phạm này. Từ đó khẳng định xu thế gia tăng, diễn biến vô cùng phức tạp với mức độ, phương thức mới, thủ đoạn tinh vi, quy mô lớn của tội phạm công nghệ cao hiện nay. Qua đó rút ra nguyên nhân khách quan và chủ quan của sự hình thành và phát triển TPCNC. Thực tiễn xử lí TPCN tuy đạt được một số kết quả nhưng cũng gặp rất nhiều khó khăn, bất cập. Cuối cùng chỉ ra sự hợp tác quốc tế nhằm nâng cao kết quả trong công tác đấu tranh phòng chống TPCNC.

CHƯƠNG 3: KINH NGHIỆM QUỐC TẾ VÀ BÀI HỌC CHO VIỆT NAM TRONG HOẠT ĐỘNG XỬ LÝ TỘI PHẠM CÔNG NGHỆ CAO

3.1. Kinh nghiệm quốc tế về hoạt động xử lý tội phạm công nghệ cao

Với lịch sử hình thành và phát triển của ngành khoa học công nghệ từ lâu đời, các quốc gia phát triển trên thế giới đã trải qua những quá trình dài nghiên cứu và cải tiến các công cụ công nghệ cao cũng như hoàn thiện cơ chế pháp lý tương đối toàn diện nhằm ngăn chặn, giảm thiểu và xử lý tác động của TPCNC đến đời sống con người

3.1.1. Kinh nghiệm về lập pháp trong hoạt động xử lý tội phạm công nghệ cao

Nhiều quốc gia đã nhận thức rõ về những mối đe dọa đối với an ninh quốc gia từ không gian mạng, coi đây là thách thức mới, mối đe dọa mới có tầm quan trọng và nguy hiểm cao. Do đó các nước tiên tiến trên thế giới đã thiết lập hành lang pháp lý chặt chẽ nhằm phòng chống TPCNC từ rất sớm. Cụ thể như: Năm 1986, Mỹ đã ban hành Luật Lừa đảo và lạm dụng máy tính. Luật này đã được điều chỉnh một số lần vào các năm 1989, 1994, 1996, 2001, 2002 và 2008; Nhật Bản ban hành Luật Truy cập máy tính trái phép vào năm 1999; Australia ban hành Luật Tội phạm ảo năm 2001; Philippines ban hành Luật Phòng tránh tội phạm ảo tháng 12/2012.Các nước không có luật riêng về TPCNC thì đều định danh loại tội phạm này trong BLHS.

Có thể thấy các quốc gia trên thế giới luôn nỗ lực cập nhật, sửa đổi, bổ sung các văn bản quy phạm pháp luật để nhanh chóng bắt kịp với sự thay đổi và phát triển của xã hội cùng với đó là sự biến đổi, gia tăng nhanh chóng các loại tội phạm, đặc biệt là tội phạm sử dụng công nghệ cao. Điển hình là Vương quốc Anh, quốc gia này từ rất sớm đã xếp TPCNC là loại tội đặc biệt nguy hiểm và nước Anh đã ban hành các quy định pháp luật tương

đối nghiêm ngặt về tội phạm liên quan đến máy tính như: Đạo luật lạm dụng máy tính 1990, Đạo luật bảo vệ dữ liệu năm 1998, Đạo luật giả mạo năm 1981, Đạo luật truyền thông độc hại năm 1998 , Luật Truyền thông năm 2003. Có thể thấy các quy định về TPCNC đã được quốc gia này xây dựng dựa trên các lĩnh vực khác nhau từ truyền thông, dữ liệu cho đến máy tính. Hay tại Singapo, Đạo luật về Chứng cứ được sửa đổi vào năm 2012 đã thừa nhận các thông tin có được từ hệ thống máy tính là chứng cứ. Từ đó, BLTTHS đã trao quyền cho cảnh sát được yêu cầu cung cấp các bằng chứng điện tử ở dạng máy tính có thể đọc dữ liệu được, từ đó giúp điều tra viên, công tố viên phân tích nội dung hồ sơ vụ án tội phạm sử dụng công nghệ cao một cách dễ dàng hơn.[120]

Không chỉ dừng lại ở việc tạo ra các quy định pháp luật giúp quá trình định danh, xác định TPCNC một cách rõ ràng chi tiết mà các quốc gia trên thế giới còn tập trung xây dựng các văn bản hướng dẫn hoạt động truy tố loại tội phạm này. Giúp việc truy bắt và xử lý nhanh chóng TPCNC. Tại Vương Quốc Anh, The Crown Prosecution Service- Cơ quan truy tố vương miện (CPS)[121] đã xây dựng các hướng dẫn trong việc truy tố TPM rất rõ ràng với phạm vi truy tố rộng bao gồm hầu hết các lĩnh vực như: phá hủy chức năng máy tính, TPM liên quan đến kinh tế, sở hữu trí tuệ, di động ảo, thông tin và truyền thông.

3.1.2. Kinh nghiệm về hợp tác quốc tế về xử lý tội phạm công nghệ cao

Ý thức được tính chất xuyên biên giới của TPCNC, các quốc gia trên thế giới không chỉ dừng lại ở việc xây dựng các quy định pháp luật quốc gia về xử lý TPCNC mà còn tiến hành hợp tác xây dựng, kí kết các hiệp định song phương, đa phương giữa các quốc gia nhằm nâng cao hiệu quả trong công tác đấu tranh với TPCNC. Trong đó có thể kể đến Công ước

[120] https://kiemsat.vn/kinh-nghiem-truy-to-toi-pham-su-dung-cong-nghe-cao-cua-vien-cong-to-singapore-50807.html

[121] Cơ quan khởi tố các vụ án hình sự đã được điều tra bởi cảnh sát và các tổ chức điều tra khác ở Anh và xứ Wale.

Budapest về tội phạm mạng năm 2001 của Châu Âu hay Châu Phi đã đưa ra dự thảo Công ước Liên minh Châu Phi về thiết lập một pháp lý Khung có lợi cho An ninh mạng ở Châu Phi và năm 2012. Bên cạnh việc xây dựng pháp luật chung các quốc gia trên thế giới còn tích cực cùng nhau thành lập, tham gia các tổ chức quốc tế hợp tác về nghiên cứu TPCNC như Liên minh Viễn thông quốc tế (ITU), Tổ chức hợp tác Thượng Hải (SCO). Ngoài ra, Công ước của Hội đồng Châu Âu về tội phạm mạng đã đưa ra quy định thành lập trung tâm " Mạng lưới 24/7" gồm các nước thành viên trong công ước hoạt động 24 giờ một ngày và 7 ngày trong một tuần để đảm bảo ứng phó kịp thời với các sự cố mạng. Việc ban hành các luật chung và các tổ chức trong khu vực sẽ giúp cho các nước thành viên có thể dễ dàng chia sẻ thông tin và điều tra về TPCNC đặc biệt là những hành vi phạm tội có tính chất xuyên biến giới cần phải có sự hợp tác giữa các quốc gia.

3.1.3. Kinh nghiệm về xây dựng đội ngũ con người trong hoạt động xử lý tội phạm công nghệ cao

Để các cơ quan chuyên môn hoạt động hiệu quả, các quốc gia cũng chú trọng đầu tư về nhân sự. Hầu hết các quốc gia đều đưa ra những chính sách đào tạo liên quan đến an ninh mạng cho các chuyên viên thực thi pháp luật chuyên ngành và không chuyên ngành. Các chuyên viên đó sẽ được đào tạo nhiều chủ đề, từ định hướng công nghệ, điều tra cơ bản, thu thập bằng chứng và các vấn đề pháp y. Phạm vi của chương trình đào tạo cho các sĩ quan rất đa dạng. Ở một số quốc gia, tất cả các sĩ quan chuyên ngành đều được đào tạo TPM theo phương thức trực tuyến hay đào tạo từ xa.Việc đào tạo nhân sự ở các quốc gia không chỉ dừng lại ở các khóa học ngắn hạn mà tổ chức các khóa đào tạo thường xuyên, điều này giúp cho các sĩ quan có thể cập nhật những diễn biến mới nhất và các hành vi tinh vi nhất của TPCNC.

Ví dụ ở Hoa Kỳ, để trở thành một chuyên viên của cơ quan phòng chống TPCNC cần đáp ứng những điều kiện khắt khe như: có ít nhất 3 năm kinh nghiệm thực thi pháp luật để làm quen với vai trò là một đặc vụ cũng

như hiểu rõ hệ thống tư pháp Hoa Kỳ. Ngoài ra, họ cũng phải là người có khuynh hướng kỹ thuật cao và sở hữu những phẩm chất cần thiết để trở thành nhân viên điều tra TPM. Các thành viên mới sẽ được đào tạo hết sức bài bản trước khi trở thành một nhân viên chuyên ngành cơ quan đó. Chẳng hạn, các thành viên mới của đơn vị sẽ chịu trách nhiệm hỗ trợ các chuyên viên thu thập, bảo vệ và phân tích bằng chứng, xử lý giấy tờ để đáp ứng các yêu cầu của nhóm công tố, hoàn thành và lưu trữ các báo cáo cho mục đích thu thập dữ liệu và thực hiện nhiều cuộc điện thoại và các cuộc đối thoại trực tiếp liên quan đến các sự cố cụ thể với nạn nhân, nhân chứng và người cung cấp thông tin. Sau thời gian thử việc một năm, các thành viên mới sẽ được giao các vụ án đơn giản như gian lận thẻ tín dụng trực tuyến, giả mạo kỹ thuật số hay trộm cắp tài sản qua Internet với thiệt hại dưới $1000. Ngoài ra, trong thời gian thử việc, các thành viên mới sẽ được yêu cầu tham gia các cuộc hội thảo về công nghệ để thường xuyên cập nhật những kiến thức, xu hướng của TPCNC.[122]

Bộ Quốc phòng Anh đã ban hành một số miễn trừ đặc biệt để mở rộng cơ hội tuyển dụng cho các chuyên gia máy tính giỏi. Quy định của Nữ hoàng Anh cho phép loại bỏ một số yêu cầu dành cho nam về đầu tóc gọn gàng; tân binh trong lực lượng dự bị không gian mạng được miễn kiểm tra thể lực. Chính phủ Nhật Bản đã thông qua kế hoạch đào tạo gần 1.000 chuyên gia an ninh mạng trong 4 năm tới nhằm tăng cường năng lực phòng thủ đối với các cuộc tấn công mạng trong thời gian diễn ra Olympic 2020 tại Tokyo. Kể từ năm 2017, Nhật Bản sẽ cung cấp một khoản hỗ trợ ưu đãi cho các nhân viên, yêu cầu các cơ quan chính phủ đề ra kế hoạch bồi dưỡng, đề cử lãnh đạo "giám sát an ninh mạng và thông tin hóa" để quản lý công tác đào tạo. Các nhân viên ưu tú nhất sẽ được chuyển đến Trung tâm An ninh mạng Nội các (NISC) và các doanh nghiệp tư nhân, chịu trách nhiệm giám sát các hoạt động tấn công mạng nhằm vào chính phủ.

[122] Sameer Hinduja, Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future, 2007.

3.1.4. Kinh nghiệm về giáo dục và phổ biến kiến thức cho người dân về xử lý tội phạm công nghệ cao

Với sự tăng trưởng nhanh chóng của TPCNC, để hạn chế tối đa hậu quả mà TPM lại, người dùng Internet cần phải chủ động bảo vệ mình trong không gian mạng. Việc chủ động bảo vệ bản thân trong không gian mạng sẽ giảm thiểu khả năng bị trở thành nạn nhân cũng như những hậu quả mà TPM đem lại. Ở các nước trên thế giới, khái niệm tội phạm đã được biết đến rộng rãi và mọi người đã nhận thức được nguy cơ của TPCNC. Chẳng hạn, một khảo sát ở các nước Châu Âu,[123] cho thấy 70% cá nhân đã nghe hoặc thấy thông tin TPM trong những năm qua, chủ yếu từ truyền hình, báo chí, Internet, bạn bè hay đài phát thanh. Tuy nhiên, đó chỉ là một cách tiếp nhận thông tin bình thường và họ không cảm thấy nhất thiết phải được cảnh báo về TPM. Chỉ 7% trong số đó cho rằng việc được cảnh báo về TPM là hữu ích. Trong các cuộc khảo sát người sử dụng máy tính, ở các nước phát triển hay đang phát triển, bây giờ hầu hết người dùng đều thực hiện một số biện pháp phòng ngừa an ninh cơ bản. Trong cuộc khảo sát với 13000 người dùng Internet ở 24 quốc gia, gần 90% số người được hỏi báo cáo rằng họ đã xóa các email đáng ngờ từ người gửi không xác định; khoảng 80% người số người được hỏi báo cáo sử dụng ít nhất phần mềm diệt vi-rút đơn giản và không mở tệp đính kèm hoặc liên kết trong email hoặc văn bản mà không rõ nguồn gốc. Bên cạnh đó, một nửa trong số họ cài đặt chế độ riêng tư của mạng xã hội để chia sẻ thông tin và chỉ hơn 35% đã chấp nhận "yêu cầu kết bạn" từ những người họ không quen biết. Sự nhận thức của người sử dụng Internet là một chiến lược quan trọng trong chiến lược giảm thiểu TPM. Từ các thống kê trên cho thấy, hầu hết hiện nay người sử dụng Internet ở các nước trên thế giới đã có ý thức bảo vệ bản thân khỏi những cuộc tấn công của TPCNC. Người dùng bước đầu đã có những sự phòng vệ nhất định và phổ biến như không mở các email không rõ nguồn gốc hay bị cho là thư rác, sử dụng phần mềm virut máy tính, sử dụng mật khẩu dài, đa

[123] United Nations Office on Drugs and Crime: Comprehensive Study on Cybercrime, 2013.

dạng cho mọi dịch vụ trực tuyến mà họ đăng ký. Các biện pháp này nhìn chung dễ dàng cho mọi người sử dụng và có thể ngăn chặn những mục tiêu thông thường của TPCNC như đánh cắp thông tin, trộm cắp tài sản trong thẻ tín dụng hay hạn chế việc hack các thiết bị điện tử. Đồng thời với sự phổ biến của các trang mạng xã hội hiện nay - một cách tội phạm thực hiện hành vi phạm tội của mình, và theo thống kê trên, người sử dụng đã có những hành vi phòng tránh như đặt mật khẩu phức tạp cho các tài khoản, không kết bạn với những người xa lạ hay hạn chế mở tin nhắn từ những người không quen, hạn chế chia sẻ thông tin lên mạng xã hội,…

Việc cá nhân chủ động bảo vệ thông tin của mình là chưa đủ, mà các doanh nghiệp, tổ chức cần phải kết hợp với các cá nhân, các cơ quan chính quyền để bảo vệ bí mật của doanh nghiệp cũng như thông tin người dùng. Các tổ chức doanh nghiệp không chỉ chứa bí mật kinh doanh của họ mà còn hàng ngàn thông tin của khách hàng vì vậy, doanh nghiệp cần giảm thiểu tối đa các hành vi bị tấn công từ TPM để tránh ảnh hưởng đến nhiều người khác. Các doanh nghiệp tư nhân trên thế giới khi được hỏi về thực tiễn bảo đảm an ninh mạng với mục đích ngăn chặn nạn nhân của TPM, thông tin các công ty trình bày đều tham khảo từ nguyên tắc bảo vệ hệ thống thông tin và mạng của Tổ chức Hợp tác và Phát triển Kinh tế (OCED). Hướng dẫn này của OCED đã được đề cập trong nghị quyết Đại hội đồng liên quan đến việc tạo ra Văn hóa an ninh mạng toàn cầu. Phòng Thương mại và Quốc tế cũng đã sử dụng hướng dẫn này để đưa ra một hướng dẫn ngắn về "đảm bảo an toàn thông tin cho giám đốc điều hành". Các hướng dẫn của OCED nhấn mạnh ba nhóm nguyên tắc an ninh mạng bào gồm nguyên tắc nền tảng, nguyên tắc xã hội và nguyên tắc vòng đời bảo mật.[124] Trên cở sở hướng dẫn bảo vệ an toàn thông tin và mạng của OCED, nhiều doanh nghiệp được hỏi đã nhấn mạnh tầm quan trọng của cách tiếp cận toàn diện đối với an ninh mạng của doanh nghiệp. Hiện nay,

[124] United Nations Office on Drugs and Crime: Comprehensive Study on Cybercrime, 2013.

phần lớn công ty trên thế giới hay bao gồm cả các nhà cung cấp dịch vụ và các công ty công nghệ đã chủ động thực hiện các bước để chống lại hành vi của TPM bao gồm việc sử dụng các biện pháp pháp lý. Ngoài ra, để hạn chế tối đa rủi ro, các doanh nghiệp giải quyết bằng cách thông qua đào tạo đội ngũ nhân viên, cùng với các chính sách và giám sát của nhân viên, khách hàng và bên thứ ba. Những biện pháp này được thực hiện nội bộ với chi phí khác nhau tùy theo quy mô tổ chức. Hầu hết các doanh nghiệp nước ngoài đều có một trung tâm với những nhân viên chuyên môn để xử lý các vấn đề về mạng. Các nhân viên thường xử lý việc bảo quản dữ liệu thông tin của doanh nghiệp với một số giám sát các mối đe dọa và theo dõi xu hướng TPM đồng thời hợp tác thực thi pháp luật. Các doanh nghiệp cũng tiến hành các giả pháp kỹ thuật để ngăn chặn TPM như tường lửa, bảo quản bằng chứng kỹ thuật số và hạn chế đối với các kết nối địa chỉ IP cụ thể. Ngoài việc tập trung tình hình mạng của riêng mình, các công ty đã thực hiện một cách tiếp cận chủ động từ bên ngoài để điều tra và ngăn chặn kịp thời các cuộc tấn công mạng đe dọa đến hệ thống an ninh mạng của họ. Những biện pháp này, khi được kết hợp với các cơ quan thực thi pháp luật giảm thiểu được rất nhiều các cuộc tấn công của tội phạm. Tuy nhiên, không phải tất cả các doanh nghiệp đều tiến hành các biện pháp phòng chống TPCNC, việc này phần lớn chỉ do các doanh nghiệp lớn tiến hành, các doanh nghiệp vừa và nhỏ không thực hiện đủ các bước để bảo vệ hệ thống hoặc họ nhận thức không chính xác sự nguy hại mà TPCNC cao sẽ mang lại. Nguyên nhân là bởi vì những hạn chế về nguồn nhân lực và kinh phí hay họ đều nghĩ rằng họ chỉ là doanh nghiệp nhỏ và sẽ không có sự tấn công nào từ bọn tội phạm và không chú trọng trong việc bảo vệ hệ thống thông tin. Trên thực tế, các doanh nghiệp vừa và nhỏ bị mất dữ liệu thông tin do phương tiện rất đơn giản và không được thực hiện đầy đủ các hành vi bảo mật.

3.1.5. Kinh nghiệm về xây dựng và tăng cường quản lý của các cơ quan chuyên môn chính phủ về hoạt động xử lý tội phạm công nghệ cao

Việc phòng chống TPM có hiệu quả đòi hỏi phải có sự lãnh đạo tập trung và tăng cường các nguồn lực của cơ quan chính phủ để phối hợp hài hòa các chiến lược phòng chống tội phạm. Nhiều nước trên thế giới cho biết họ đã chỉ định một tổ chức chính phủ lãnh đạo chịu trách nhiệm điều phối công tác phòng chống TPM và phần lớn là cảnh sát quốc gia hoặc cơ quan quan thi hành pháp luật. Phần lớn ở các nước trên thế giới đã thành lập những cơ quan chuyên môn nhằm kiểm soát hiệu quả hơn TPCNC.

Theo thống kê của Văn phòng Liên hiệp quốc về chống Ma túy và Tội phạm (UNODC),[125] hiện nay có hơn 90% quốc gia đã bắt đầu có những cơ quan chuyên ngành để điều tra TPM và tội phạm liên quan các thiết bị công nghệ cao. Trong đó, có 75% quốc gia hiện có một tổ chức chuyên môn trong các cơ quan thực thi và 15% quốc gia có một cơ quan về các vấn đề liên quan đến TPM. Chẳng hạn, ở Mỹ có Trung tâm khiếu nại Tội phạm Internet (IC3) với mục đích tiếp nhận, đưa ra các khiếu nại hình sự liên quan đến Internet. IC3 không chỉ đưa ra các báo cáo đáng tin cậy cho công chúng mà còn đưa ra những thông tin giúp cho Cục điều tra Liên bang Mỹ (FBI) thuận tiện trong việc điều tra, bắt giữ TPCNC. Việc thành lập các trung tâm chuyên môn với các chuyên gia chuyên ngành sẽ giúp cho việc kiểm soát không gian mạng dễ dàng hơn trong việc kịp thời ngăn chặn những cuộc tấn công mạng và kịp thời khắc phục hậu do TPCNC gây ra.

Hiện nay, hầu hết các cơ quan chính phủ Hoa Kỳ đều có trách nhiệm trong việc thực hiện đấu tranh phòng chống TPCNC. Từ việc kiểm soát không gian mạng cho đến điều tra bắt giữ, mỗi cơ quan đều được quy định rõ trách nhiệm và hoạt động của mình. Chẳng hạn Bộ quốc phòng Hoa Kỳ là cơ quan chủ chốt trong việc điều hành, chỉ đạo các hoạt ộng kiểm soát tội phạm sử dụng thiết bị công nghệ cao. Cơ quan này phụ thuộc vào các chuyên gia bảo mật công nghệ cao, bao gồm nhiều sinh viên đại học tốt

[125] United Nations Office on Drugs and Crime: Comprehensive Study on Cybercrime, 2013.

nghiệp, để giữ an toàn cho thông tin nội bộ (DoDIN), hỗ trợ cho các chỉ huy thực hiện các nhiệm vụ trên khắp toàn cầu và tăng cường khả năng sống sót của các cuộc tấn công mạng hay Bộ an ninh nội địa (DHS), cơ quan này gồm 240.000 nhân viên và một trong số này thực hiện nhiệm vụ bảo mật không gian mạng. Những chuyên gia an ninh mang phải chịu trách nhiệm rất lớn trong việc bảo vệ cơ sở hạ tầng được kiểm soát bởi các mạng, các nhân viên cũng điều tra cũng điều tra những hành vi của các TPM. Trong hoạt động tiến hành điều tra, bắt giữ TPCNC, Hoa Kỳ tập trung hai lực lượng chính là Cơ quan tình báo trung ương (CIA) và Cục điều tra liên bang (FBI) trong đó CIA là cơ quan đứng đầu trong việc thu thập thông tin của chính phủ. Trung tâm điều hành thông tin của cơ quan này (IOC) đặc biệt tập trung vào các hoạt động xảy ra trên Internet nhằm thu thập thông tin dữ liệu bằng chứng cho các cuộc tấn công mạng. Trong khi đó, FBI là cơ quan hàng đầu trong việc điều tra các cuộc tấn công mạng của TPM, là nhân tố chủ chốt trong việc điều tra và bắt giữ TPCNC.[126]

Vương Quốc Anh tiến hành xây dựng các lực lượng phòng chống TPCNC như: Trụ sở Truyền thông Chính phủ (GCHQ) [127] và Đơn vị tội phạm mạng quốc gia (NCCU) đã hợp tác để phát triển các kỹ năng và công nghệ cần thiết để chống lại mối đe dọa TPCNC đối với Vương quốc Anh như phát triển các kỹ năng công nghệ để chống lại các mối đe dọa TPM. Ngoài ra đối với hoạt động xử lý các TPCNC quốc gia có tính chất nghiêm trọng sẽ do Cơ quan tội phạm quốc gia (NCA)[128] tiến hành. Bên cạnh đó cơ quan An ninh (MI5) chịu trách nhiệm đảm bảo an ninh hệ thống cơ sở hạ tầng trọng yếu quốc gia và trực tiếp tiến hành điều tra các vụ tấn công mạng; Bộ Quốc phòng chịu trách nhiệm phòng vệ không gian mạng quốc gia trước các cuộc tấn công mạng mang tính quân sự.

[126]https://programs.online.utica.edu/articles/government-agencies-that-utilize-cyber-security-professionals

[127] GCHQ là trụ sở Truyền thông Chính phủ là một tổ chức tình báo và an ninh chịu trách nhiệm cung cấp tín hiệu tình báo và đảm bảo thông tin cho chính phủ và các lực lượng vũ trang của Vương quốc Anh.

[128] NCA là Cơ quan tội phạm quốc gia của Anh có nhiệm vụ xử lý tội phạm nghiêm trọng và có tổ chức có nguy cơ lớn nhất đối với Vương quốc Anh.

3.1.6. Kinh nghiệm về xây dựng Thực hiện các chính sách ưu tiên, khuyến khích, thu hút, tuyển lựa nhân tài phục vụ công tác xử lý tội phạm công nghệ cao

Thu hút, trọng dụng người có tài năng luôn có vị trí quan trọng công tác phòng chống TPCNC. Với tính chất tinh vi, phức tạp và hiện đại của loại tội phạm nguy hiểm này, các quốc gia trên thế giới đã tích cực trong hoạt động tìm kiếm, giáo dục và sử dụng nhân tài nhằm tối đa hóa khả năng đấu tranh và phòng ngừa TPCNC.

Bộ Quốc phòng Anh đã ban hành một số miễn trừ đặc biệt để mở rộng cơ hội tuyển dụng cho các chuyên gia máy tính giỏi. Quy định của Nữ hoàng Anh cho phép loại bỏ một số yêu cầu dành cho nam về đầu tóc gọn gàng; tân binh trong lực lượng dự bị không gian mạng được miễn kiểm tra thể lực. Chính phủ Nhật Bản đã thông qua kế hoạch đào tạo gần 1.000 chuyên gia an ninh mạng trong 4 năm nhằm tăng cường năng lực phòng thủ đối với các cuộc tấn công mạng trong thời gian diễn ra Olympic 2020 tại Tokyo. Kể từ năm 2017, Nhật Bản sẽ cung cấp một khoản hỗ trợ ưu đãi cho các nhân viên, yêu cầu các cơ quan chính phủ đề ra kế hoạch bồi dưỡng, đề cử lãnh đạo "giám sát an ninh mạng và thông tin hóa" để quản lý công tác đào tạo. Các nhân viên ưu tú nhất sẽ được chuyển đến Trung tâm An ninh mạng Nội các (NISC) và các doanh nghiệp tư nhân, chịu trách nhiệm giám sát các hoạt động tấn công mạng nhằm vào chính phủ.[129]

3.2. Giải pháp xử lý tội phạm công nghệ cao ở Việt Nam hiện nay

3.2.1. Giải pháp hoàn thiện các quy phạm pháp luật về tội phạm công nghệ cao

Hệ thống pháp luật là cơ sở pháp lí vững chắc do đó cần tiếp tục ban hành các chính sách, biện pháp cụ thể đảm bảo công tác đấu tranh phòng chống TPCNC được hiệu quả. Việt Nam cần tiến hành hoàn thiện thống

[129]http://duthaoonline.quochoi.vn/DuThao/Lists/DT_DUTHAO_LUAT/View_Detail.aspx?ItemID=1382&TabIndex=2&TaiLieuID=2900

văn bản quy phạm pháp luật liên quan đến công tác phòng ngừa, ngăn chặn, phát hiện, đấu tranh, xử lý tội phạm sử dụng công nghệ cao. Trong đó, cần tập trung nghiên cứu bổ sung kịp thời các chế định về các hành vi tội phạm, chứng cứ, các biện pháp ngăn chặn, khung hình phạt, trình tự thủ tục, trách nhiệm của các cơ quan và thời hạn tố tụng... trong Luật Hình sự, Luật Tố tụng hình sự, Luật Giao dịch điện tử, Luật xử lý vi phạm hành chính, Pháp lệnh Thương mại điện tử... Đẩy mạnh công tác xây dựng thông tư liên ngành; Ban hành nhanh chóng nghị định hướng dẫn luật an ninh mạng 2018 phù hợp với đặc thù và yêu cầu của công tác đấu tranh phòng chống tội phạm sử dụng công nghệ cao; Tăng cường hợp tác quốc tế; Triển khai thành lập các đơn vị cảnh sát phòng chống TPCNC nhằm xây dựng một hệ thống lực lượng cảnh sát phòng chống tội phạm sử dụng công nghệ cao trên phạm vi cả nước.[130]

3.2.2. Giải pháp xây dựng chính sách tạo động lực cho hoạt động phòng chống và xử lý tội phạm công nghệ cao

Xây dựng các chính sách nhằm tạo động lực vật chất và tinh thần mạnh mẽ cho các cá nhân hoạt động khoa học và công nghệ. Đồng thời cần phải trọng dụng và tôn vinh nhân tài khoa học và công nghệ bằng việc thực hiện cơ chế cạnh tranh lành mạnh, thực thi chế độ đãi ngộ tương xứng với cống hiến của các nhà khoa học và công nghệ hoặc ban hành chính sách khen thưởng đối với cá nhân có thành tích khoa học và công nghệ có giá trị khoa học và thực tiễn cao; chính sách khuyến khích cán bộ khoa học và công nghệ làm việc tại địa bàn có điều kiện kinh tế, xã hội khó khăn và đặc biệt khó khăn.

Bên cạnh đó cần phải chú trọng trong việc đổi mới chính sách đào tạo, tuyển chọn cán bộ khoa học và công nghệ, đẩy mạnh việc tuyển chọn và gửi học sinh, sinh viên, cán bộ khoa học và công nghệ đi đào tạo một cách đồng bộ ở các nước có trình độ khoa học và công nghệ tiên tiến, trước mắt

[130] Lê Hồng Xuân, Nguyễn Thị Thùy Linh, Tội phạm mạng trong kỷ nguyên cách mạng công nghiệp 4.0, Tạp chí TAND số 18 kỳ II tháng 9/2018.

là trong một số lĩnh vực khoa học và công nghệ trọng điểm quốc gia. Quá trình đào tạo các học viên mới cần phải đảm bảo cả nghiệp vụ Công an và nghiệp vụ kỹ thuật, đề nghị học viện tăng cường tổ chức lớp bồi dưỡng nghiệp vụ Công an và lớp bồi dưỡng nghiệp vụ kỹ thuật đào tạo chuyên sâu về hệ thống an ninh, an toàn mạng, bảo mật; đào tạo về khai thác, sử dụng các thiết bị chuyên dụng để thu thập, phục hồi dữ liệu, chứng cứ điện tử..[131] phối hợp chặt chẽ giữa việc đào tạo với cơ quan sử dụng cán bộ khoa học và công nghệ chú trọng đào tạo, bồi dưỡng nhân tài. Huy động tối đa và hỗ trợ các thành phần kinh tế tham gia trực tiếp vào quá trình đào tạo nhân lực khoa học và công nghệ; xây dựng cơ chế, chính sách đa dạng hóa nguồn vốn đầu tư cho hoạt động khoa học và công nghệ; khuyến khích các doanh nghiệp đầu tư đổi mới công nghệ có tính năng quản lí và bảo mật cao.

3.2.3. Giải pháp về nâng cao hiệu quả trong thực tiễn phát triển nghiên cứu giáo dục công tác đấu tranh xử lý tội phạm công nghệ cao

Khuyến khích mở các trường đại học, viện nghiên cứu công nghệ quốc tế hoặc khu vực tại Việt Nam. Thu hút các viện nghiên cứu, trường đại học có uy tín của nước ngoài liên kết hoặc mở phân viện, phân hiệu hoặc tổ chức các chương trình đào tạo nhân lực khoa học và công nghệ tại Việt Nam.

Tập trung xây dựng một số tổ chức khoa học và công nghệ và cơ sở hạ tầng đạt trình độ trung bình tiên tiến trong khu vực cho một số hướng khoa học và công nghệ trọng điểm. Tập trung đầu tư xây dựng một số tổ chức khoa học và công nghệ trong một số hướng khoa học và công nghệ trọng điểm, đảm bảo cho các cơ quan này có đầy đủ những trang thiết bị nghiên cứu, thực nghiệm, thông tin-tư liệu, đội ngũ cán bộ khoa học và công nghệ đạt trình độ tiên tiến trong khu vực. Thực hiện đầu tư đồng bộ giữa xây dựng cơ sở vật chất-kỹ thuật với đào tạo cán bộ khoa học và công nghệ đáp ứng nhu cầu phòng chống tội phạm đạt hiệu quả cao.

[131]http://csnd.vn/Home/Nghien-cuu-Trao-doi/301/Ket-qua-va-kinh-nghiem-phong-chong-toi-pham-su-dung-cong-nghe-cao-cua-PC50-Cong-an-thanh-pho-Ha-Noi-va-nhung-van-de-dat-ra-trong-cong-tac-dao-tao-can-bo

TỔNG KẾT CHƯƠNG 3

Từ những vấn đề lý luận và thực tiễn áp dụng pháp luật đã được trình bày tại chương một và chương hai của bài nghiên cứu. Có thể khẳng định rằng, Việt Nam là một quốc gia đang phát triển với bước đầu hội nhập quốc tế, sự hình thành của thời đại kỉ nguyên số tại nước ta đã tạo nên sự thay đổi về mọi mặt kinh tế - xã hội dẫn đến sự xuất hiện của loại tội phạm mới - TPCNC. Để khắc phục tình trạng và nâng cao hiệu quả đấu tranh phòng chống tội phạm. Do đó, tại chương ba bài nghiên cứu đã tiến hành đưa ra giải pháp hoàn thiện hệ thống pháp luật; Xây dựng chính sách; Nâng cao hiệu quả trong thực tiễn công tác đấu tranh phòng chống TPCNC thông qua bài học kinh nghiệm của các quốc gia phát triển trên thế giới; Nhằm mục đích hoàn thiện hơn hệ thống pháp luật Việt Nam, tạo nên khung pháp lý vững chắc trong hoạt động phòng ngừa, đấu tranh với loại tội phạm mới đặc biệt nguy hiểm này.

KẾT LUẬN ĐỀ TÀI NGHIÊN CỨU KHOA HỌC

Từ những vấn đề lý luận đến thực tiễn áp dụng pháp luật trên thực tế trong quá trình nghiên cứu vừa qua. Trong điều kiện kinh tế, xã hội như hiện nay tội phạm công nghệ cao đã và đang trở thành một trong những tội phạm tồn tại phổ biến trong xã hội. Các đối tượng phạm tội rất đa dạng về thành phần, lứa tuổi, với xu hướng phát triển mạnh mẽ về kinh tế cũng như công nghệ hiện nay thì các đối tượng phạm tội với thủ đoạn ngày càng tinh vi với quy mô lớn và có tính nguy hiểm cao. Trước những diễn biến phức tạp của tội phạm, việc nghiên cứu để có được những nhận thức chính xác về tội phạm công nghệ cao đồng thời tìm ra nguyên nhân dẫn đến sự phát triển của tội phạm, để từ đó có những biện pháp phòng ngừa, xử lí thích hợp, kịp thời là vấn đề cấp thiết được đặt ra không chỉ cho các nhà nghiên cứu về tội phạm học, các cơ quan chức năng mà bên cạnh đó chúng ta phải phối hợp chặt chẽ giữa các cơ quan Nhà nước, các tổ chức xã hội và toàn thể bộ phận nhân dân để ngăn ngừa tác động của tội phạm công nghệ cao, góp phần giữ vững an ninh chính trị, trật tự an toàn xã hội của toàn đất nước.

Trong phạm vi đề tài, nhóm đã góp phần làm rõ những vấn đề lý luận và quy định pháp luật về tội phạm công nghệ cao của các quốc gia; Cùng các thỏa thuận song phương, đa phương về xử lí tội phạm công nghệ cao trên thế giới. Thông qua đó học hỏi các ưu điểm của quy định pháp luật về tội phạm công nghệ cao của các quốc gia trên thế giới cũng như hoàn thiện những thiếu xót còn tồn tại trong pháp luật Việt Nam. Từ đó, đề xuất một số giải pháp, kinh nghiệm quốc tế để phòng ngừa, đẩy lùi tội phạm công nghệ cao. Việc lựa chọn và hoàn thành đề tài nghiên cứu *Pháp luật Quốc tế và thực tiễn về xử lí tội phạm công nghệ cao – Kinh nghiệm cho Việt Nam* cũng là mong muốn có thể góp một phần nhỏ vào công tác đấu tranh, phòng chống tội phạm, nâng cao ý thức, giữ gìn trật tự, an ninh, xã hội. Xây dựng một xã hội tốt đẹp, trong sạch hơn.

Nhóm nghiên cứu cam đoan số liệu và kết quả nghiên cứu trong đề tài là trung thực, các kết quả nghiên cứu do chính chủ nhiệm đề tài và những người tham gia thực hiện, các tài liệu tham khảo đã được trích dẫn đầy đủ. Do điều kiện nghiên cứu và khả năng bản thân còn hạn chế nên chắc chắn 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.

Một lần nữa nhóm xin chân thành cám ơn!

DANH MỤC TÀI LIỆU THAM KHẢO

A. Các văn bản pháp luật

I. Các văn bản pháp luật tiếng Việt.

1. Bộ luật hình sự năm 1999.
2. Bộ luật hình sự năm 1999(sửa đổi bổ sung 2009).
3. Theo Bộ luật Hình sự 2015.
4. Luật an toàn thông tin mạng 2015.
5. Luật an ninh mạng 2018.
6. Luật công nghệ cao 2008.
7. Nghị định số 25/2014/NĐ-CP của Chính phủ ngày 07 tháng 4 năm 2014 Nghị định quy định về phòng chống tội phạm và vi phạm pháp luật khác có sử dụng công nghệ cao.
8. Quyết định số 3317/ QĐ-BTC ngày 24 tháng 12 năm 2014 của Bộ Tài chính quy định về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính.
9. Theo hướng dẫn 16/HD-BCA-C41 ngày 31/12/2013 của Bộ Công an hướng dẫn thực hiện một số quy định trong các Thông tư 18, 19, 20, 21, 22 ngày1/4/2013 của Bộ trưởng Bộ Công an quy định về công tác nghiệp vụ cơ bản của lực lượng Cảnh sát nhân dân có hướng dẫn việc phân chia các nhóm đối tượng phạm tội có sử dụng công nghệ cao.
10. Công văn 2132/BTTTT-VNCERT V/v Hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử.
11. 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.

II. Các văn bản pháp luật Tiếng Anh:

1. Computer Misuse Act 1990.
2. China's cybersecurity law 2019.
3. Computer Fraud and Abuse Act 1986.
4. Budapest Convention on Cybercrime 2001.

B. Sách giáo khoa, giáo trình, sách tham khảo, Luận văn, báo cáo, công trình nghiên cứu

I. Sách giáo khoa, giáo trình, sách tham khảo, Luận văn, báo cáo, công trình nghiên cứu Tiếng Việt

1. TS. Phạm Văn Lợi (chủ biên) - Tội phạm trong lĩnh vực công nghệ thông tin của: nhà xuất bản tư pháp Hà Nội 2007.
2. PGS.TS Lê Thanh Tâm, Phạm Thị Thu Thảo - Tội phạm công nghệ cao đối với ngành Ngân hàng Việt Nam trong bối cảnh cách mạng công nghiệp 4.0: thực trạng và một số khuyến nghị chính sách - Tạp chí Khoa học & Đào tạo Ngân hàng Số 192- Tháng 5. 2018.
3. Trung tá, NCS Đào Trung Hiếu: Quy trình thu thập, chuyển hóa dữ liệu điện tử thành chứng cứ trong ddieeuf tra tội phạm sử dụng công nghệ cao-Tạp chí khoa học kiểm sát số 06 (14)-2016).
4. Trần Thị Hồng Lê: Các tội phạm trong lĩnh vực tin học theo luật hình sự Việt Nam - Đại học quốc gia Hà Nội.

II. Sách giáo khoa, giáo trình, sách tham khảo, Luận văn, báo cáo, công trình nghiên cứu Tiếng Anh

1. Philip N. Ndubueze, High-tech crimes, boundaryless policing and cyber security policy in digital nigeria: a periscope by Philip N. Ndubueze. (Xem tại: https://www.researchgate.net/publication/326658556_HIGH-TECH_CRIMES_BOUNDARYLESS_POLICING_AND_CYBER_SECURITY_POLICY_IN_DIGITAL_NIGERIA_A_PERISCOPE)
2. Murughendra Tubake, Cyber Crime: An Overview - Online International Interdisciplinary Research Journal, {Bi-Monthly}, ISSN2249-9598, Volume-III, Issue-II, Mar-Apr 2013

3. ITU, Understanding cybercrime: Phenomena, challenges and legal response, 2012.
4. Prof. Dr.Ulrich Sieber: Legal Aspects of Computer-Related Crime in the Information Society.
5. Johannes Xingan Li: Cybercrime and Legal countermeasures: A history Analysis.
6. Chief Judge B. Lynn Winmill, David L. Metcalf and Michael E. Band, Cybercrime: issues and challenges in the United State – SAS Journals.
7. Office of Legal Education Executive Office for United States Attorneys: Prosecuting Computer Crimes.
8. Babak Akhgar, Andrew Staniforth and Francesca Bosco, Cyber Crime and Cyber Terrorism Investigator's Handbook.
9. United Nations office on drugs and crime, Comprehensive study on cybercrime.
10. Roderic Broadhurst và Lennon Y.C.Chang: Cyber in Asia: Trends and Challenges.
11. Horst Seehofer và Arne Schönbohm: The State of IT Security in Germany 2018.
12. Bernadette H. Schella, Cyber child pornography: A review paper of the social and legalissues and remedies-and a proposed technological; March 2006; accepted 28 March 2006.
13. Sameer Hinduja, Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future, 2007.

C. Bài báo

I. Bài báo Tiếng Việt:

1. Hoàng Việt Quỳnh: Một số trao đổi về tội phạm sử dụng công nghệ cao theo quy định pháp luật Việt Nam - Tạp chí KHGD CSND số 79 tháng 8/2016.
   (Xem tại http://tks.edu.vn/thong-tin-khoa-hoc/chi-tiet/79/776).

2. TS. Hồ Thế Hòe, Giải pháp nâng cao hiệu quả đấu tranh với tội phạm sử dụng công nghệ cao trong bối cảnh toàn cầu.
(Xem tại: http://tks.edu.vn/thong-tin-khoa-hoc/chi-tiet/79/687).
3. Lê Thị Hồng Xuân – Nguyễn Thị Thùy Linh -Tội phạm mạng trong kỷ nguyên cách mạng công nghiệp 4.0. Tạp chí TAND số 18/2018 (kỳ II tháng 9/2018).
4. TS. Đinh Thế Hưng- ThS. Lê Thị Hồng Xuân -Tội phạm công nghệ cao trong lĩnh vực tài chính, ngân hang ở việt nam hiện nay - (phòng pháp luật hình sự- Viện nhà nước và pháp luật)- Tạp chí TAND số 7 /2019 (Kỳ I tháng 4/2019).
5. Nguyễn Ngọc Thương -Một số giải pháp phòng ngừa tội phạm sử dụng công nghệ cao- - Tạp chí CSND - T32
(Xem tại http://csnd.vn/Home/Nghien-cuu-Trao-doi/2257/Mot-so-giai-phap-phong-ngua-toi-pham-su-dung-cong-nghe-cao, ngày 19/7/2019).
6. Thiếu tướng, GS,TS.Nguyễn Ngọc Anh: Một số quy định của pháp luật về tội phạm công nghệ cao
(Xem tại: http://canhsatnhandan.vn/Home/Print/286/Mot-so-quy-dinh-cua-phap-luat-ve-toi-pham-cong-nghe-cao, ngày17/11/2014).
7. Đại tá, PGS.TS Nguyễn Minh Đức- Giám đốc Trung tâm Nghiên cứu Tội phạm học và điều tra tội phạm, Đặc điểm tội phạm học của tội phạm sử dụng công nghệ cao và giải pháp nâng cao hiệu quả phòng ngừa, đấu tranh – Học viện CSND ngày 17/11/2014
(Xem tại: http://www.csnd.vn/Home/Nghien-cuu-Trao-doi/307/Dac-diem-toi-pham-hoc-cua-toi-pham-su-dung-cong-nghe-cao-va-giai-phap-nang-cao-hieu-qua-phong-ngua-dau-tranh).
8. Nguyễn Thị Xuân Thu: Nhận diện một số phương thức thủ đoạn của tội phạm sử dụng công nghệ cao - Tạp chí nghiên cứu, lý luận, nghiệp vụ khoa học của học viện cảnh sát nhân dân.
(Xem tại: http://csnd.vn/Home/Nghien-cuu-Trao-doi/4453/Nhan-dien-mot-so-phuong-thuc-thu-doan-cua-toi-pham-su-dung-cong-nghe-cao)

9. Tội phạm công nghệ cao 2016: Lắm nguy cơ, nhiều thách thức.
(Xem tại: http://antg.cand.com.vn/Ho-so-Interpol/Toi-pham-cong-nghe-cao-2016-Lam-nguy-co-nhieu-thach-thuc-423161/, ngày 29/12/2016)
10. ThS. Trần Đoàn Hạnh: Hoàn thiện khung khổ pháp lý xử phạt tội phạm công nghệ thông tin, mạng viễn thông.
(Xem tại: http://tapchitaichinh.vn/nghien-cuu--trao-doi/trao-doi-binh-luan/ hoan-thien-khung-kho-phap-ly-xu-phat-toi-pham-cong-nghe-thong-tin-mang-vien-thong-112331.html, ngày 25/9/2016).
11. KSV.Cao Anh Đức: chất của tình hình tội phạm sử dụng công nghệ cao tại Việt Nam, thủ đoạn phạm tội và dự báo.
(http://nguoibaovequyenloi.com/User/ThongTin_ChiTiet.aspx?MaTT=289201551832859903&MaMT=23, ngày 28/09/2015).

II. Bài báo Tiếng Anh

1. Nick Beckett, A guide for businesses to China's first cyber security law, 2017.
(Xem tại: https://www.computerweekly.com/opinion/Chinas-first-cyber-security-law-what-it-means-for-companies)
2. Cybercrime Statistics 2019: An In Depth Look at UK Figures and Trends by Sandra Henshaw - November 9, 2018.
(Xem tại: https://www.tigermobiles.com/blog/cybercrime-statistics/)
3. Ben Chapman, Cybercrime proseccutions fell last year because police are under-sourced top law firm says.
(Xem tại: https://www.independent.co.uk/news/business/news/cyber-crime-prosecutions-fall-police-law-firm-reynolds-porter-chamberlain a7853591.html).
4. Social Media - Guidelines on prosecuting cases involving communications sent via social media.
(Xem tại :https://www.cps.gov.uk/legal-guidance/social-media- guidelines -prosecuting-cases-involving-communications-sent-social- media)

5. Cybercrime Statistics 2019: An In Depth Look at UK Figures and Trends.
(Xem tại: https://www.tigermobiles.com/blog/cybercrime-statistics/)
6. Learn more about computer fraud and abuse act.
(https://www.sciencedirect.com/topics/computer-science/computer-fraud-and-abuse-act)
7. International and regional instruments
(Xem tại: https://www.unodc.org/e4j/en/cybercrime/module-3/key issues/ international-and-regional-instruments.html)

BẢNG PHỤ LỤC

Phụ lục 1: Các bộ luật có liên quan đến hoạt động xử lý tội phạm công nghệ cao của nước Anh.

1. Đạo luật lạm dụng máy tính 1990.
2. Quy định của Đạo luật Quyền hạn Điều tra 2000.
3. Đạo luật bảo vệ dữ liệu năm 1998.
4. Đạo luật giả mạo và giả mạo 1981.
5. Đạo luật ghi video 2010.
6. Đạo luật thiết kế đã đăng ký 1949.
7. Đạo luật truyền thông độc hại 1998.
8. Luật Truyền thông 2003.
9. Đạo luật Bảo vệ khỏi Quấy rối 1997.

Phụ lục 2: Danh sách các công ước điều chỉnh hoạt động xử lý tội phạm công nghệ cao trên thế giới.

1. Liên minh châu Phi, 2012. Dự thảo Công ước về việc thiết lập một khung pháp lý dẫn đến an ninh mạng ở châu Phi (Dự thảo Công ước Liên minh châu Phi).
2. Thị trường chung cho Đông và Nam Phi (COMESA), 2011. Dự luật mô hình dự thảo an ninh mạng. (Dự thảo mô hình dự thảo COMESA).
3. Commonwealth, 2002. (i) Dự luật về tội phạm liên quan đến máy tính và máy tính và (ii) Luật mẫu về chứng cứ điện tử (Luật mô hình khối thịnh vượng chung).
4. Liên bang các quốc gia độc lập, 2001. Thỏa thuận hợp tác trong việc chống lại các hành vi phạm tội liên quan đến thông tin máy tính (Liên minh các quốc gia độc lập).
5. Hội đồng Châu Âu, 2001. Công ước về tội phạm mạng và Nghị định thư bổ sung cho Công ước về tội phạm mạng, liên quan đến việc hình sự hóa các hành vi phân biệt chủng tộc và bài ngoại được thực hiện thông qua các hệ thống máy tính (Hội nghị / Nghị định thư về tội phạm mạng của Hội đồng châu Âu).
6. Hội đồng châu Âu, năm 2007 Công ước về bảo vệ trẻ em chống bóc lột tình dục và lạm dụng tình dục (Công ước bảo vệ trẻ em của Hội đồng châu Âu).
7. Cộng đồng kinh tế của các quốc gia Tây Phi (ECOWAS), 2009. Dự thảo Chỉ thị về Chống tội phạm mạng trong ECOWAS (Chỉ thị Dự thảo ECOWAS).
8. Liên minh châu Âu, 2000. Chỉ thị 2000/31 / EC của Nghị viện châu Âu và của Hội đồng về các khía cạnh pháp lý nhất định của dịch vụ xã hội thông tin, đặc biệt là thương mại điện tử, trong Thị trường nội bộ (Chỉ thị của EU về thương mại điện tử).

9. Liên minh châu Âu, 2001. Quyết định khung của Hội đồng 2001/413 / JHA chống gian lận và làm giả các phương tiện thanh toán không dùng tiền mặt (Quyết định của EU về gian lận và giả mạo).

10. Liên minh châu Âu, 2002. Chỉ thị 2002/58 / EC của Nghị viện châu Âu và của Hội đồng liên quan đến việc xử lý dữ liệu cá nhân và bảo vệ quyền riêng tư trong lĩnh vực truyền thông điện tử (Chỉ thị của EU về bảo vệ dữ liệu).

11. Liên minh châu Âu, 2005. Quyết định khung của Hội đồng 2005/222 / JHA về các cuộc tấn công chống lại các hệ thống thông tin (Quyết định của EU về các cuộc tấn công chống lại các hệ thống thông tin).

12. Liên minh châu Âu, 2006. Chỉ thị 2006/24 / EC của Nghị viện châu Âu và của Hội đồng về việc lưu giữ dữ liệu được tạo hoặc xử lý liên quan đến việc cung cấp dịch vụ liên lạc điện tử có sẵn công khai hoặc của các mạng truyền thông công cộng (Chỉ thị của EU về lưu giữ dữ liệu) .

13.

Liên minh châu Âu, năm 2010 Đề xuất COM (2010) 517 cho Chỉ thị của Nghị viện châu Âu và của Hội đồng về các cuộc tấn công chống lại hệ thống thông tin và bãi bỏ Quyết định khung của Hội đồng 2005/222 / JHA (Đề xuất chỉ thị của EU về tấn công hệ thống thông tin).

14. Liên minh châu Âu, 2011. Chỉ thị 2011/92 / EU của Nghị viện châu Âu và của Hội đồng về chống lạm dụng tình dục và khai thác tình dục trẻ em và khiêu dâm trẻ em, và thay thế Quyết định khung của Hội đồng 2004/68 / JHA (Chỉ thị của EU về Khai thác trẻ em) .

15. Liên minh Viễn thông Quốc tế (ITU) / Cộng đồng Caribbean (CARICOM) / Liên minh Viễn thông Caribbean (CTU), 2010. Mô hình các văn bản lập pháp về Bằng chứng điện tử / Tội phạm điện tử (ITU / CARICOM / CTU Mô hình lập pháp).

16. Liên minh các quốc gia Ả Rập, 2010. Công ước Ả Rập về Chống vi phạm công nghệ thông tin (Công ước Liên minh các quốc gia Ả Rập).

17. Liên minh các quốc gia Ả Rập, 2004. Mô hình Luật Ả Rập về Chống lại các Vi phạm liên quan đến Hệ thống Công nghệ Thông tin (Luật Mô hình Liên minh các Quốc gia Ả Rập).

18. Tổ chức Hợp tác Thượng Hải, 2010. Thỏa thuận hợp tác trong lĩnh vực bảo mật thông tin quốc tế (Thỏa thuận tổ chức hợp tác Thượng Hải).

19. Liên hợp quốc, 2000. Nghị định thư không bắt buộc đối với Công ước về quyền trẻ em về bán trẻ em, mại dâm trẻ em và khiêu dâm trẻ em (Liên hợp quốc OP-CRC-SC).

Phụ lục 3: Bảng thống kê 10 nước có nhiều khiếu nại nhiều nhất về tội phạm công nghệ cao năm 2018 của IC3

(Thống kê này không bao gồm Hoa Kỳ)

STT	QUỐC GIA	SỐ VỤ KHIẾU NẠI IC3 NHẬN ĐƯỢC
1	Ấn Độ	4,556
2	Anh	3,970
3	Canada	2,880
4	Australia	1,227
5	Georgia	1,144
6	Đức	622
7	Brazil	605
8	Mexico	591
9	Greece	514
10	Philipines	511

Phụ lục 4: Thống kê số người dùng Internet ở khu vực Châu Á vào năm 2011

STT	Quốc gia	Số lượng người dùng Internet	% Dân số 2011	% Dân số 2002
1	Trung Quốc	485 000 000	36.3	3.5
2	Ấn Độ	100 000 000	8.4	0.7
3	Nhật Bản	99 182 000	78.4	48.0
4	Indonexia	39 600 000	16.1	1.8
5	Hàn quốc	39 440 000	80.9	52.7
6	Philippines	29 700 000	29.2	2.5
7	Việt Nam	29 268 606	32.3	0.5
8	Pakistan	20 431 000	10.9	0.3
9	Thái Lan	18 310 000	27.4	5.7
10	Australia	17 033 826	78.3	46.0
11	Malaysia	16 902 600	58.8	24.4
12	Đài Loan	16 147 000	70.0	49.8
13	Hồng Kong	4 878 713	68.5	64.1
14	Singapore	3,658,400	77.2	55.6
15	New Zealand	3,600,000	83.9	
16	Sri Lanka	1,776,900	8.3	0.8
17	Bangladesh	1,735,020	1.1	0.1
18	Nepal	1,072,900	3.7	0.2
19	Lào	527,400	8.1	0.2
20	Mongolia	350,000	11.2	1.6

Bảng phụ lục 5: Hình phạt xử lý tội phạm công nghệ cao theo luật CFAA của Hoa Kỳ

Hành vi	Phần	Kết án theo năm
Lấy thông tin an ninh quốc gia	(a) (1)	10 (20)
Truy cập máy tính và lấy cắp thông tin	(a) (2)	1 hoặc 5 (10)
Xâm phạm máy tính của chính phủ	(a) (3)	1(10)
Truy cập máy tính để lừa đảo & lấy giá trị	(a) (4)	5(10)
Cố ý phá hủy bằng cách lan truyền	(a) (5)(A)	1 hoặc 10(20)
Thiệt hại bất ngờ do truy cập có chủ ý	(a) (5)(B)	1 hoặc 5 (20)
Truy cập có chủ ý gây ra thiệt hại	(a) (5)(C)	1(10)
Buôn bán mật khẩu	(a) (6)	1(10)
Sử dụng máy tính để tống tiền	(a) (7)	5(10)

Bảng phụ lục 6: Bảng báo cáo kết quả đấu tranh 2010-2014

Năm	Tổng số vụ phát hiện	Khởi tố	Bị can
2010	121	08	14
2011	165	32	81
2012	192	34	90
2013	210	35	175
2014	146	12	71

Kết quả: Năm 2010: (bao gồm 7 chuyên án) , gây thiệt hại ước tính gần 20 tỷ đồng, 2.000.000 đô la Úc, 130.242 đô la Mỹ, 820 máy tính xách tay và nhiều linh kiện điện tử các loại. Chuyển Thanh tra chuyên ngành các cấp xử phạt hành chính 36 vụ; thu hồi 10 tỷ 238 triệu đồng và 112.842 đô la Mỹ. Năm 2011 (bao gồm 14 chuyên án): Thu giữ tiền và nhiều tài sản khoảng 12 tỷ -đồng và 235.000 USD. Chuyển Thanh tra các cấp xử phạt hành chính 09 vụ; Năm 2012: (bao gồm 17 chuyên án); gây thiệt hại ước tính hơn 1300 tỷ đồng; đã thu hồi tiền và tài sản trị giá hơn 10 tỷ đồng; Năm 2013: (bao gồm 30 chuyên án, 178 vụ việc và vụ án). Đã chuyển CQĐT các cấp: 59 vụ, (trong đó có 20 chuyên án, 151 bị can và 15 vụ án, 24 bị can); chuyển Thanh tra các Bộ, ngành và các cơ quan chức năng xử lý hành chính 30 vụ; thu giữ nhiều tiền và tài sản trị giá hàng chục tỷ đồng; Sáu tháng đầu năm 2014: (bao gồm 11 chuyên án, 135 vụ việc và vụ án). Đã chuyển CQĐT các cấp: 23 vụ, (trong đó có 04 chuyên án, 18 bị can và 08 vụ án, 53 bị can); chuyển Thanh tra các Bộ, ngành và các cơ quan chức năng xử lý hành chính 05 vụ.

Bảng phụ lục 7: Bảng báo cáo kết quả đấu tranh xử lý tội phạm công nghệ cao tại Việt Nam 2015-2018

Năm	**2015**	**2016**		**2017**		**Đầu năm 2018**	
	Số lượng	Số lượng	So với Năm 2015	Số lượng	So với năm 2016	Số lượng	So với năm 2017 cùng kỳ
Khởi tố điều tra	124	214	Tăng 75%	197	Giảm 9,22%	117	Giảm 13,97%
Bị can	473	493	Tăng 129,3%	359	Giảm 27,18%	196	Tăng 4,26%