BÀI
AN TOÀN THÔNG TIN VÀ PHÒNG, CHỐNG VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG

I. THỰC TRẠNG AN TOÀN THÔNG TIN HIỆN NAY

1. Một số khái niệm

- An toàn thông tin:"*An toàn thông tin là an toàn kỹ thuật cho các hoạt động của các cơ sở hạ tầng thông tin, trong đó bao gồm an toàn phần cứng và phần mềm theo các tiêu chuẩn kỹ thuật do Nhà nước ban hành; duy trì các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng*".

- An toàn thông tin mạng:"*An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin*".

- An ninh mạng:"*An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân*".

- Tội phạm công nghệ cao:

Theo Từ điển Nghiệp vụ Công an nhân dân Việt Nam (2019), tội phạm sử dụng công nghệ cao là loại tội phạm sử dụng những thành tựu mới của khoa học – kỹ thuật và công nghệ hiện đại làm công cụ, phương tiện để thực hiện hành vi phạm tội một cách cố ý hoặc vô ý, gây nguy hiểm cho xã hội. Chủ thể của loại tội phạm này thường là những người có trình độ học vấn, chuyên môn cao, có thủ đoạn rất tinh vi, khó phát hiện.

Trong những hành vi phạm tội sử dụng công nghệ cao có những hành vi tác động trực tiếp đến ba đặc điểm quan trọng nhất của an toàn thông tin (ATTT). ATTT yêu cầu đảm bảo ba đặc điểm là: Tính bí mật (*Confidentiality*), tính toàn vẹn (*Integrity*) và tính sẵn sàng (*Availability*)

2. Thực trạng an toàn thông tin trong khu vực và trên thế giới

- Trong cuộc cách mạng công nghiệp 4.0, thông tin là một dạng tài nguyên. Chính vì thế, đảm bảo an ninh, ATTT là nhiệm vụ quan trọng và cấp thiết. Tuy nhiên hiện nay, các mối đe dọa từ không gian mạng không ngừng tăng lên và thay đổi nhanh chóng. An ninh mạng đang trở thành vấn đề nóng, đặt ra nhiều thách thức đối với tất cả các quốc gia trên toàn thế giới.

- Tình hình ATTT mạng diễn biến phức tạp, liên tục xảy ra các vụ tấn công, xâm nhập, đánh cắp dữ liệu trên hệ thống mạng của các cơ quan chính phủ, các cơ sở an ninh quốc phòng, tập đoàn kinh tế, cơ quan truyền thông của nhiều quốc gia, như các vụ tấn công vào hệ thống thư điện tử của Bộ Ngoại giao Mỹ, hệ thống máy tính của Nhà trắng, Hạ viện Đức, Bộ Ngoại giao, Bộ Thương mại và Cảnh sát liên bang Australia…

- Các mục tiêu tấn công đã thay đổi, kỹ thuật trở nên phức tạp hơn, hướng tấn công đa dạng hơn và công cụ tấn công được thiết kế chuẩn xác hơn. Những kẻ tấn công đã nghiên cứu kỹ các nạn nhân để có những chiến lược tấn công phù hợp, nhằm tạo ra những ảnh hưởng lớn nhất có thể.

- Tài chính là mục tiêu lớn nhất thúc đẩy tin tặc hành động, với 73% số lượng các cuộc tấn công mạng; chính trị, tình báo là mục tiêu lớn thứ hai, với 21% các cuộc tấn công.

- Các nhóm tội phạm mạng có tổ chức xuất hiện nhiều hơn. Chiến tranh mạng và đội quân tác chiến mạng cũng được chú trọng hơn. Trong cuộc chạy đua vũ trang trên không gian mạng toàn cầu, các quốc gia đang xây dựng các trung tâm chỉ huy không gian mạng, nhằm củng cố hệ thống phòng thủ chống lại các cuộc tấn công mạng vào các cơ quan và cơ sở hạ tầng. Bên cạnh đó, sự phát triển và phổ biến của mạng xã hội đã làm nảy sinh một nguy cơ ATTT nữa đó là việc lan truyền tin tức giả mạo thông qua mạng xã hội, gây ảnh hưởng đến cá nhân, tổ chức, thậm chí là tình hình an ninh, chính trị của cả một đất nước. Tiền ảo và các hành vi tội phạm liên quan đến tiền ảo cũng đang tiếp tục phát triển, bao gồm lây nhiễm phần mềm độc hại đào tiền ảo tới máy tính, máy chủ; lây nhiễm mã độc đào tiền ảo tới một trang web, sử dụng tài nguyên thiết bị của người tải trang web; đánh cắp tiền từ giao dịch tiền ảo.

3. Thực trạng an toàn thông tin ở Việt Nam

- Báo cáo của hãng bảo mật Kaspersky và Symantec cho thấy, Việt Nam đứng thứ 3 (3,96%) sau Nga (4%) và Ấn Độ (8%) về số người dùng di động bị mã độc tấn công nhiều nhất trên thế giới; thứ 6 trên thế giới về số lượng địa chỉ IP trong nước được dùng trong các mạng máy tính ma tấn công nước khác; thứ 7 trên thế giới về phát tán tin nhắn rác và đứng thứ 12 trên thế giới về các hoạt động tấn công mạng.

Năm 2011 có trên 1.500 cổng thông tin Việt Nam bị tin tặc sử dụng mã độc gián điệp dưới hình thức tập tin hình ảnh xâm nhập, kiểm soát, cài mã độc thay đổi giao diện trang chủ.

Trong năm 2012 - 2013, Bộ Công an đã phát hiện gần 6.000 lượt cổng thông tin, trang tin điện tử của Việt Nam (trong đó có hơn 300 trang của cơ quan nhà nước) bị tấn công, chỉnh sửa nội dung và cài mã độc.

Năm 2014, Bộ Công an phát hiện gần 6.000 trang bị tấn công, chiếm quyền quản trị, chỉnh sửa nội dung (có 246 trang tên miền gov.vn). Vào cuối năm 2014, tin tặc cũng đã mở đợt tấn công vào trung tâm dữ liệu của VCCorp khiến nhiều tờ báo mà công ty này đang vận hành kỹ thuật như Dân trí, Người lao động, Soha, VNEconomy, Kenh14… bị tê liệt.

Năm 2015 có trên 2.460 website của các cơ quan, doanh nghiệp bị xâm nhập. Nguy cơ từ mã độc và Internet of Things (IoT) bùng nổ tạo "thị trường" lớn cho hacker là hai trong số những nguy cơ an ninh mạng mà người dùng phải đối mặt.

Năm 2016, nổi bật là cuộc tấn công mạng vào một số màn hình hiển thị thông tin chuyến bay tại khu vực làm thủ tục chuyến bay của các sân bay quốc tế Tân Sơn Nhất, Sân bay quốc tế Nội Bài, sân bay quốc tế Đà Nẵng, sân bay Phú Quốc. Các màn hình của sân bay đã bị chèn những hình ảnh và nội dung xuyên tạc về biển Đông. Hệ thống phát thanh của sân bay cũng phát đi những thông điệp tương tự. Đồng thời website của

Vietnam Airlines cũng bị tấn công với 411.000 dữ liệu của hành khách đi máy bay đã bị hacker thu thập và phát tán.

Năm 2017, mã độc tống tiền (ransomware) có tên là Wanna Cry trở thành mối nguy hiểm của ngành công nghệ thông tin và nó lây nhiễm với tốc độ chóng mặt ở gần 100 quốc gia, hơn 100 nghìn máy tính. Tại Việt Nam, ghi nhận hơn 100 máy tính bị nhiễm độc. Wanna Cry là một loại mã nhiễm độc tấn công vào máy nạn nhân qua tệp tin đính kèm email hoặc đường link độc hại, như các dòng ransomware khác.

Năm 2018, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 14.900 tỷ đồng, tương đương 642 triệu USD, nhiều hơn 21% so với mức thiệt hại của năm 2017.

Năm 2019, số cuộc tấn công mạng vào các hệ thống thông tin Việt Nam có chiều hướng giảm. Trong 6 tháng đầu năm 2019, Bộ TT&TT ghi nhận 3.159 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam, giảm 2.684 cuộc, tương đương 45,9% so với cùng kỳ năm 2018.

Theo Cục ATTT (Bộ TT&TT) trong 4 tháng đầu năm 2020 tổng cộng 1.056 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam dẫn đến sự cố (553 cuộc Phishing, 280 cuộc Deface, 223 cuộc Malware), đã giảm 51,4% với 4 tháng đầu năm 2019.

II. CÁC HÀNH VI VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG

1. Spam, tin giả trên mạng xã hội, thư điện tử

a) Spam

- Spam hay còn gọi là tin rác, là viết tắt của Stupid Pointless Annoying Messages, từ này có ý nghĩa là những thông điệp vô nghĩa và gây phiền toái cho người nhận, được gửi đến nhiều người dùng với cùng một nội dung.

- Thuật ngữ spam lần đầu xuất hiện vào năm 1978, khi một người đàn ông gửi thư có nội dung y hệt nhau đến 393 người cùng lúc để quảng cáo sản phẩm mới của mình. Ngày nay, spam xuất hiện trên nhiều phương tiện như spam chat, spam tin tức, spam tin nhắn, spam trong forum, spam trên những mạng xã hội.

b) Tin giả

Theo định nghĩa của từ điển Collins, tin giả là "những thông tin sai sự thật, thường là tin giật gân, được phát tán dưới vỏ bọc tin tức".

Tin giả được tạo ra bằng nhiều hình thức tinh vi. Đặc biệt, hiện nay nhiều đối tượng đã sử dụng CNTT làm giả tiếng, giả hình, giả video để tạo ra tin giả.

- Giả hình: Công nghệ cắt ghép tạo hình ảnh người giả y như thật để tạo ra tin tức giả, nhiều người nổi tiếng đã là nạn nhân. Và nguy hại hơn nếu họ cắt ghép với hình ảnh những chính trị gia, người có uy tín cộng đồng để tạo dư luận giả.

- Giả tiếng: Sử dụng công nghệ TTP (công cụ chuyển văn bản thành tiếng nói - text to speech) để tạo ra các cuộc gọi tự động với giọng robot thu sẵn. Từ nhiều năm trước đã có những người sử dụng công nghệ này để thay họ đọc thông tin, tin tức do họ "xào nấu" ra. Hiện nhiều người đang dùng công nghệ này cho các chương trình trên YouTube.

- Giả video: Thực hiện bằng cách cắt ghép hình ảnh người dẫn chương trình lồng vào dẫn bản tin giả. Clip giả nhưng có người dẫn chương trình sống động như thật. Loại hình ảnh giả này "buộc" người xem nghĩ đó là những thông tin thật vì có hình ảnh quen mặt của người dẫn chương trình truyền hình.

Tin giả có thể được tạo và lan truyền nhằm các mục đích sau:

- Chính trị: Tin giả được lợi dụng vào các âm mưu chính trị và làm rối loạn xã hội.

- Thương mại: Ngày càng nhiều người biết cách tận dụng công cụ hiện đại, những nền tảng mạng xã hội để phát tán thông tin giả. Số lượng tin giả đối với doanh nghiệp, kinh doanh cũng tăng lên tỷ lệ thuận với tin giả trong các lĩnh vực khác nói chung.

c) Xử lý hành vi tạo và lan truyền tin giả:

Nghị định 15/2020/NĐ-CP của Chính phủ Quy định xử phạt vi phạm hành chính lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử, ban hành ngày 03/02/2020, có hiệu lực 15/4/2020, quy định:

- Điều 101: phạt tiền từ 10-20 triệu đồng đối với hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân; cung cấp, chia sẻ thông tin bịa đặt, gây hoang mang trong nhân dân, kích động bạo lực, tội ác, tệ nạn xã hội, đánh bạc hoặc phục vụ đánh bạc.

- Nghị định 15 quy định rất cụ thể các hành vi vi phạm về chống thư rác, tin nhắn rác và cung cấp dịch vụ nội mạng. Mức phạt lên đến 80 triệu đồng đối với hành vi gửi hoặc phát tán thư điện tử rác, tin nhắn rác, phần mềm độc hại. Riêng đối với hành vi không ngăn chặn, thu hồi số thuê bao được dùng để phát tán tin nhắn rác thì mức phạt tiền sẽ từ 180-200 triệu đồng.

- Đối với các hành vi kể trên, ngoài phạt tiền còn bị áp dụng thêm các hình thức xử phạt bổ sung, biện pháp khắc phục hậu quả như: đình chỉ hoạt động cung cấp dịch vụ từ 1-3 tháng; tước quyền sử dụng mã số quản lý, tên định danh từ 1-3 tháng; buộc thu hồi đầu số, kho số viễn thông.

- Ngoài phạt tiền, người vi phạm còn bị buộc áp dụng các biện pháp khắc phục hậu quả: gỡ bỏ thông tin sai sự thật, gây nhầm lẫn hoặc thông tin vi phạm pháp luật do thực hiện hành vi vi phạm.

2. Đăng tải các thông tin độc hại vi phạm ANQG, trật tự ATXH

Điều 8 - Luật An ninh mạng năm 2018, các hành vi bị nghiêm cấm bao gồm:

- Sử dụng không gian mạng để thực hiện hành vi sau đây:

+ Hành vi quy định tại khoản 1 Điều 18 của Luật này;

+ 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.

- Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; 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.

- 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.

- 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.

- 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.

- Hành vi khác vi phạm quy định của Luật này.

Theo Khoản 1, Điều 16. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

+ Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

+ Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

+ Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

Theo Khoản 2, Điều 16. Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm:

+ Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

+ Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

3. Chiếm đoạt tài khoản mạng xã hội

-Hình thức Phishing: Đây là hình thức chiếm đoạt một tài khoản facebook phổ biến nhất hiện nay và cho đến bây giờ nó vẫn là cách được hacker sử dụng nhiều nhất. Không riêng gì facebook mà hầu hết các loại website nào mà có account đăng nhập đều sử dụng được hình thức này.

- Dò mật khẩu: Đây là một hình thức phổ biến tuy xác xuất thành công không cao nhưng không thể không nói đến nó vì có nhiều người dùng sử dụng những mật khẩu quá đơn giản kiểu như: 123456 , matkhau, số điện thoại, họ và tên…Đây là những sai lầm ở phía người dùng khi đặt mật khẩu facebook.

- Sử dụng trojan, Keylog: Kẻ tấn công sẽ chèn một đoạn mã vào một ứng dụng,tập tin nào đó rồi gửi thông qua inbox, comment trên facebook hay bất cứ đâu. Khi người dùng click vào đường dẫn đó thì ứng dụng, tập tin đó sẽ được tự động tải về máy, sau đó keylog sẽ ghi lại tất cả những thao tác trên bàn phím của người 6ung rồi gửi về cho kẻ tấn công.

- Sử dụng chương trình khuyến mãi – trúng thưởng hay Mini Game: Hacker sẽ giả chương trình trúng thưởng – khuyến mãi trên danh nghĩa của Facebook (trúng thưởng xe máy, ô tô, tiền mặt… có giá trị cao) và yêu cầu người dùng xác nhận bằng cách truy cập vào đường link lạ.

- Lỗ hổng bảo mật facebook: Là hình thức tấn công nick facebook mạng tên "3 Friends". Đây là hình thức lấy lại mật khẩu của facebook thông qua việc sử dụng 3 người bạn facebook bất kì trong danh sách bạn bè. Ví dụ khi bạn quên mật khẩu thì bạn có thể gửi yêu cầu để facebook gửi 3 mã code về cho 3 người bạn này.

4. Chiếm quyền giám sát Camera IP

- *Cách thứ nhất*: Tấn công trực tiếp vào thiết bị Camera bằng cách Quét (Scan) IP và Port của Camera rồi sau đó Hacker tìm cách xâm nhập vào hệ thống để xem hình ảnh, video trái phép. Cách này rất phổ biến, bởi đa số người dùng camera hiện tại thường sử dụng Password mặc định của nhà cung cấp.

- *Cách thứ hai*: Hacker sẽ dùng một phần mềm gián điệp cài trên Camera quan sát để tạo thành một mạng Botnet sử dụng trong một hình thức tấn công nổi tiếng đó là DDOS.

5. Lừa đảo chiếm đoạt tài sản

- Kịch bản lừa đảo thông báo trúng thưởng với giải thưởng cực lớn đang quay trở lại hoành hành trên Facebook. Sau khi chiếm đoạt tài khoản Facebook cá nhân, nhiều đối tượng còn tung ra nhiều chiêu trò để lừa đảo khiến nhiều người dùng mất đi một khoản tiền không hề nhỏ. Ngay sau khi có tài khoản đã được đánh cắp, đối tượng sẽ thực hiện ngay việc chat với bạn bè, người thân hỏi thăm về sức khỏe, công việc và sau đó nhờ nhận hộ một số tiền chuyển từ nước ngoài về. Nạn nhân không biết tài khoản Facebook kia đã bị tấn công nên tin tưởng và sẵn sàng giúp đỡ.

- Không chỉ vậy, nạn nhân còn có nguy cơ bị tấn công lấy tài khoản ngân hàng thông qua hình thức tấn công phishing. Sau khi thống nhất số tiền sẽ chuyển, đối tượng lừa đảo dùng một số điện thoại từ nước ngoài sẽ gửi 1 tin nhắn giả mạo thông

báo từ Western Union đến số điện thoại của nạn nhân với nội dung đề nghị truy cập đường link trong tin nhắn SMS và xác nhận để có thể nhận được tiền Western Union.

- Nạn nhân không biết đây là trang web phishing (một hình thức lừa đảo giả mạo các tổ chức uy tín như ngân hàng) nên đã nhập các thông tin tài khoản, mật khẩu internet banking vào trang web giả mạo rồi gửi đi và đối tượng lừa đảo sẽ nhận được. Từ đó, đối tượng lừa đảo dùng thông tin internet banking vừa chiếm được từ nạn nhân để thực hiện giao dịch qua cổng thanh toán trực tuyến VTC Pay và cổng thanh toán VNPAY.

6. Deep web và Dark web

a) Deep web

- Web trên bề mặt (tiếng Anh: Surface web): Theo tạp chí PC Magazine, web bề mặt là một phần web có sẵn cho công chúng, hoàn chỉnh với những liên kết được công cụ tìm kiếm lập chỉ mục. BrightPlanet, một dịch vụ web thông minh, xác định web bề mặt chỉ chứa những trang web được lập chỉ mục và có thể được tìm kiếm bởi các công cụ tìm kiếm phổ biến như Google, Bing, Yahoo. Đôi khi, chúng còn được gọi là web hữu hình. Web bề mặt thường bao gồm những trang web có tên miền kết thúc bằng .com, .org, .net, .vn hoặc các biến thể tương tự. Nội dung của các trang web này không yêu cầu bất kỳ cấu hình đặc biệt nào để truy cập.

- Web chìm (tiếng Anh: Deep web) hay còn gọi là web ẩn (invisible web, undernet, hay hidden web) là từ dùng để chỉ các trang hoặc nội dung trên thế giới mạng World Wide Web không thuộc về Web nổi (surface Web). Chúng gồm những trang không được đánh dấu, chỉ mục (index) và không thể tìm kiếm được khi dùng các công cụ tìm kiếm thông thường.

- Web chìm bao gồm nhiều ứng dụng rất phổ biến như web mail và ngân hàng trực tuyến nhưng nó cũng bao gồm các dịch vụ mà người dùng phải trả tiền, và được bảo vệ bởi một paywall, như video theo yêu cầu, một số tạp chí và báo chí trực tuyến, và nhiều hơn nữa.

b) Dark web

- Mỗi thiết bị được kết nối với Internet đều có địa chỉ IP (Internet protocol) duy nhất. Tên và địa chỉ vật lý của một người có thể có được thông qua một nhà cung cấp dịch vụ Internet với sự cho phép hợp pháp, còn IP cho phép bất cứ ai xác định vị trí của máy tính được kết nối. Do đó, các bên liên quan sẽ dễ dàng tìm được một người sử dụng Internet cụ thể.

- Với mong muốn ẩn danh - đặc biệt là chính phủ khi tìm cách bảo vệ những thông tin, mạng lưới tình báo nhạy cảm - đã dẫn đến sự ra đời và phát triển của The Onion Router (Tor) do đội ngũ nhân viên phòng thí nghiệm nghiên cứu Hải Quân Hoa Kỳ tạo ra. Tên Onion (củ hành) bắt nguồn từ việc bạn phải lột ra nhiều "lớp vỏ" để có thể tìm thấy danh tính thật sự của người dùng.

- Tor, được phát hành miễn phí cho người dùng vào năm 2004, cung cấp sự riêng tư bằng cách mã hóa và điều hướng lưu lượng truy cập thông qua một sê-ri "đường hầm ảo (virtual tunnel)", phân phối các giao dịch qua nhiều máy tính ngẫu

nhiên trên Internet, do đó, không một máy tính nào liên kết người dùng đến cơ sở hoặc điểm đến của họ. Không giống như những trang web bề mặt (kết thúc bằng .com, .org, .net hoặc các biến thể tương tự), các trang Tor kết thúc bằng .onion và chỉ có thể được mở bằng phần mềm Tor.

- Dark web (tạm dịch: web tối) là những nội dung mạng World Wide Web không thể truy cập bằng những cách thông thường mà phải sử dụng các phần mềm chuyên biệt. Dark web là một phần nhỏ của deep web, một thế giới mạng mà các công cụ tìm kiếm như Google hay Bing không hiển thị ra.

- Một số hoạt động thường thấy ở Dark Web:

+ Chợ đen: Nhiều hoạt động thương mại bất hợp pháp diễn ra trên Dark web, ví dụ như: buôn bán tiền giả, thẻ ngân hàng hay tài khoản mạng bị đánh cắp, súng, ma túy và các chất kích thích, các sản phẩm không rõ nguồn gốc khác.

+ Khủng bố: Vì tính ẩn danh cao, nhiều tổ chức tội phạm khủng bố như IS sử dụng không gian Dark web để phát tán các nội dung đến người dùng. Nói đến khủng bố thì không chỉ là IS mà còn có các tổ chức Mafia khác sử dụng mạng lưới này, đã từng có trường hợp chúng nhận hợp đồng thanh toán một người và hợp đồng đó đã ở trạng thái được thực thi.

+ Khiêu dâm: Khiêu dâm trẻ em, ngược đãi hoặc làm tình với động vật, phát tán video quay lén là những nội dung hiện hữu trên dark web. Các nội dung này đều bị các tổ chức bảo vệ trẻ em cũng như các nước trên thế giới lên án và cố gắng dẹp bỏ

+ Lừa đảo: Không hiếm những trường hợp lừa tiền hoặc thanh toán người khác trên Dark Web được thực thi.

III. PHÒNG, CHỐNG VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG

1. Cơ sở pháp lý

a) Bộ luật Hình sự năm 2015,sửa đổi bổ sung năm 2017

- Bộ luật Hình sự năm 2015, sửa đổi bổ sung năm 2017 có hiệu lực thi hành từ ngày 01/01/2018.

- Bộ luật hình sự gồm 26 chương và 526 điều.

Các điều khoản trong luật thực hiện với các hành vi vi phạm pháp luật trên không gian mạng được quy định tại Mục 2. Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông -Chương XXI gồm các Điều 285 đến 294.

b) Luật An toàn thông tin năm 2015

- Luật An toàn thông tin mạng ban hành ngày 19/11/2015, có hiệu lực thi hành từ ngày 01/7/2016.

- Luật An toàn thông tin mạng gồm 08 chương và 54 điều, bao gồm:

Chương I. Những quy định chung

Chương II. Bảo đảm an toàn thông tin mạng

Chương III. Mật mã dân sự

Chương IV. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng

Chương V. Kinh doanh trong lĩnh vực an toàn thông tin mạng

Chương VI. Phát triển nguồn nhân lực an toàn thông tin mạng

Chương VII. Quản lý nhà nước về an toàn thông tin mạng

Chương VIII. Điều khoản thi hành

c) Luật An ninh mạng năm2018

- Luật An ninh mạng ban hành ngày 12/6/2018, có hiệu lực thi hành từ ngày 01/01/2019.

- Luật An ninh mạng gồm 07 chương, 43 điều, bao gồm:

Chương I. Những quy định chung,

Chương II. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Chương III. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng

Chương IV. Hoạt động bảo vệ an ninh mạng

Chương V. Bảo đảm hoạt động bảo vệ an ninh mạng

Chương VI. Trách nhiệm của cơ quan, tổ chức, cá nhân

Chương VII. Điều khoản thi hành

2. Các biện pháp

- Giáo dục nâng cao nhận thức về bảo vệ chủ quyền quốc gia, các lợi ích và sự nguy hại đến từ không gian mạng.

- Tuyên truyền, phổ biến, giáo dục các quy định của pháp luật về quản lý không gian mạng.

-Bồi dưỡng kỹ năng nhận diện các âm mưu, thủ đoạn tấn công mạng và các hình thái phát sinh trên không gian mạng.

- Nâng cao ý thức phòng tránh, tự vệ và sử dụng biện pháp kỹ thuật để khắc phục hậu quả trong trường hợp bị tấn công trên không gian mạng.

- Phát huy vai trò, trách nhiệm của các cơ quan chuyên trách an ninh mạng, lãnh đạo, quản lý các địa phương, cơ quan, đơn vị, doanh nghiệp, nhà trường trong giáo dục nâng cao ý thức làm chủ và bảo vệ không gian mạng.

3. Trách nhiệm của sinh viên

Một là, Mỗi cá nhân cần nghiên cứu, hiểu rõ ý nghĩa, giá trị, nội dung của Luật An ninh mạng, quyền lợi, nghĩa vụ, trách nhiệm và những hành vi bị cấm khi tham gia hoạt động trên không gian mạng.

Luật An ninh mạng nhằm bảo vệ người dùng hợp pháp trên không gian mạng; phòng ngừa, đấu tranh, làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống Nhà nước, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, kích động biểu tình, phá rối của các thế lực phản động. Phòng ngừa, ngăn chặn, ứng

phó, khắc phục hậu quả của các đợt tấn công mạng, khủng bố mạng và phòng, chống nguy cơ chiến tranh mạng.

Luật An ninh mạng quy định rõ những hành vi bị cấm như: sử dụng không gian mạng để tuyên truyền chống Nhà nước; tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước; xuyên tạc lịch sử...). Những quy định này không xâm phạm đến quyền con người, không cản trở tự do ngôn luận, không tạo rào cản, không cản trở hoạt động bình thường, đúng luật của các tổ chức, cá nhân như những thông tin trên mạng xã hội, blog, web phản động tuyên truyền, xuyên tạc trong thời gian vừa qua. Thực hiện đúng Luật là bảo vệ chính mình, người thân và gia đình, đồng thời, góp phần bảo vệ an ninh mạng quốc gia.

Hai là, Tự trau dồi kỹ năng nhận diện âm mưu, thủ đoạn gây nguy cơ mất an ninh mạng, nhất là âm mưu, thủ đoạn "diễn biến hòa bình", bạo loạn lật đổ của các thế lực thù địch. Nhận diện được các tổ chức chống đối hoạt động trên không gian mạng; các thủ đoạn tạo vỏ bọc "xã hội dân sự", "diễn đàn dân chủ"... để chống phá; các website giả mạo, các trang mạng có nhiều nội dung thông tin xấu, độc.

Mỗi người cần nắm chắc các thủ đoạn tấn công mạng như đánh sập các website; cài gắm vào máy tính cá nhân hoặc lấy tài khoản và mật khẩu; đánh cắp dữ liệu cá nhân (hình ảnh, video); tấn công bằng mã độc (theo tệp đính kèm trong email hoặc ẩn trong quảng cáo Skype); tấn công ẩn danh bằng những phần mềm độc hại; tấn công qua USB, đĩa CD…

Ba là, Nâng cao ý thức phòng tránh, tự vệ khi tham gia mạng xã hội. Nghiên cứu kỹ trước khi like hoặc chia sẻ các file, các bài viết hoặc các đường link; cảnh giác với trang web lạ (web đen), E-mail chưa rõ danh tính và đường dẫn đáng nghi ngờ; tuyệt đối không a dua, hiếu kỳ, hoặc tham tiền bạc cùng với những lời kích động, xúi giục của các đối tượng xấu. Kịp thời cung cấp thông tin, thực hiện yêu cầu và hướng dẫn của cơ quan nhà nước có thẩm quyền, người có trách nhiệm.

Sử dụng tốt các biện pháp kỹ thuật bảo đảm an toàn thông tin như tạo thói quen quét virus; thực hiện sao lưu dự phòng trên ổ cứng ngoài, trên mạng nội bộ hoặc trên các dịch vụ lưu trữ đám mây; kiểm tra lộ lọt thông tin tài khoản cá nhân qua Trung tâm xử lý tấn công mạng Việt Nam. Khi phát hiện bị tấn công mạng, nhanh chóng ngắt kết nối mạng; sử dụng các công cụ giải mã độc; báo cho người có trách nhiệm qua đường dây nóng.

Bốn là, cần biết cách tận dụng, sử dụng mạng xã hội một cách đúng đắn và hiệu quả, biến mạng xã hội thành một phương tiện, một kênh hữu ích để mở mang kiến thức, cùng nhau xây dựng môi trường văn hóa mạng xã hội lành mạnh, tránh bị các thông tin ảo chi phối tác động, góp phần phòng chống, ngăn chặn những tư tưởng, quan điểm sai trái, thù địch một cách có hiệu quả.

Năm là, Phổ biến, tuyên truyền trong gia đình, người thân, bạn bè và Nhân dân nơi cư trú các quy định của Luật An ninh mạng để mọi người nắm, hiểu và không thực hiện các hành vi vi phạm liên quan đến an ninh mạng, góp phần xây dựng "không gian mạng lành mạnh từ cơ sở".