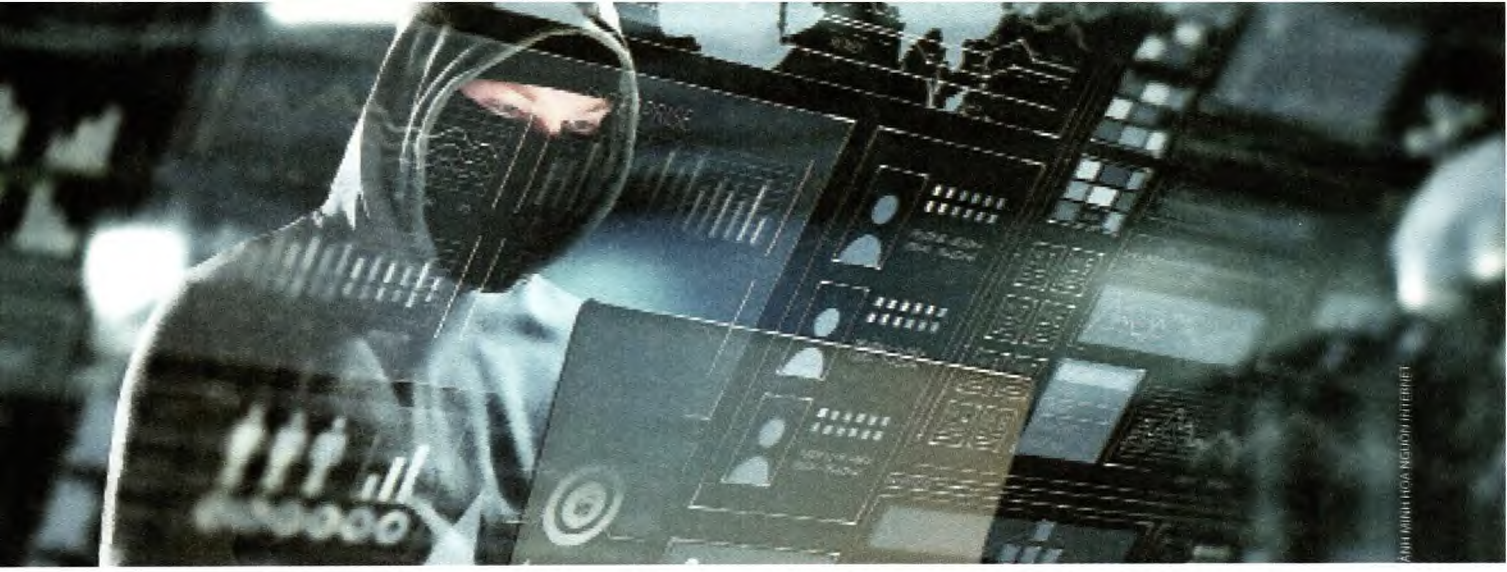

Tội phạm sử dụng công nghệ cao và phòng chống tội phạm sử dụng công nghệ cao tại Việt Nam

▶ PGS, TS. HẠ THỊ THIỀU DAO
▶ THS. LẠI VĂN TÀI

- NGÀY NHẬN BÀI: 3/3/2021
- NGÀY BIÊN TẬP: 5/3/2021
- NGÀY DUYỆT ĐĂNG: 10/8/2021

Tóm tắt: Tội phạm sử dụng công nghệ cao đứng thứ hai trong các loại tội phạm nguy hiểm nhất, sau tội phạm khủng bố và Việt Nam đang đứng trong tốp 7 thế giới về các hoạt động đe dọa tấn công mạng. Số các vụ án mà đối tượng lợi dụng mạng internet để thực hiện hành vi tội phạm sử dụng công nghệ cao ngày càng nhiều và tinh vi hơn, đặc biệt có sự liên kết giữa tội phạm trong và ngoài nước thông qua các phương pháp tấn công vào hệ thống như là Phishing (lừa đảo), Deface (xâm nhập), Malware (phần mềm độc hại) … để tấn công vào người sử dụng. Số liệu tổng hợp trong giai đoạn 2010 – 2019 có 207.353 cuộc tấn công vào Việt Nam, trong đó Phishing là 29.059 cuộc (14,01%), Deface là 105.971 cuộc (chiếm 51,11%), Malware là 72.323 cuộc (chiếm 34,88%). Bài viết phân tích tình hình tội phạm sử dụng công nghệ cao tại Việt Nam và các biện pháp phòng chống để nâng cao tính bảo mật, an toàn của môi trường mạng. Bài viết cũng phân tích tình hình bảo mật và an ninh thông tin thông qua chỉ số an toàn thông tin mạng toàn cầu (Global Cypersecrurity Index), chỉ số an toàn thông tin Việt Nam (Vietnam Cybersecurity Index). Dựa trên những số liệu này, bài viết đề xuất các chính sách để cải thiện và hạn chế tình hình hoạt động của tội phạm công nghệ cao và sự cố an ninh mạng.

Từ khóa: an ninh mạng, tội phạm công nghệ cao, lừa đảo

HI- TECH CRIME AND THE PREVENTION OF HI-TECH CRIME IN VIETNAM

Abstract: Hi-tech crime ranks second among the most dangerous crimes, just after terrorist crime, and Vietnam is ranked in top 7 in the world in terms of cyber threat activities. The number of cases where the criminals takes advantage of the internet to commit hi- tech crimes is increasing day by day with higher level of sophistication, especially there is a connection between domestic and foreign criminals through attack methods to the system such as Phishing, Deface, Malware.... In the period 2010 - 2019, there were 207,353 attacks on Vietnam, of which Phishing was 29,059 (14.01%), Deface was 105,971 (accounting for 51.11%), Malware was 72,323 (accounting for 34.88%). The article analyzes the current situation of hi-tech crime in Vietnam and prevention measures to improve security and safety of the network environment. The article also analyzes security and information security status through the Global Cybersecurity Index, Vietnam Cybersecurity Index. Based on these data, the article proposes policies to improve and limit hi-tech crime and cyber security incidents.

Keywords: cyber security, hi-tech crime, fraud

1. GIỚI THIỆU

Xu thế tài chính số đang mang đến cho Việt Nam cơ hội to lớn trong tăng khả năng cung cấp sản phẩm dịch vụ hiện đại cho khách hàng. Tuy nhiên, đi đôi với những đổi mới này là nguy cơ rủi ro công nghệ thông tin, rủi ro gian lận với mức độ tác động ngày càng lớn, đặc biệt đối với các lĩnh vực nhạy cảm như tài chính, ngân hàng. Do vậy, việc cung cấp thông tin rộng rãi về an toàn, bảo mật thông tin là hết sức cần thiết.

Mức độ đảm bảo an ninh mạng của các quốc gia, vùng lãnh thổ trên thế giới được các tổ chức liên minh quốc tế, các ủy ban phụ trách an ninh mạng công bố trong các báo cáo hàng năm về ATTT mạng. Bài viết này sử dụng một số chỉ tiêu đo lường mức độ an toàn thông tin ở cấp độ quốc gia để phân tích thực trạng an ninh, bảo mật thông tin nhằm phòng chống tội phạm công nghệ cao tại Việt Nam. Các chỉ tiêu có thể kể:

Chỉ số An toàn thông tin (ATTT) mạng toàn cầu: Chỉ số ANTT hay thường được sử dụng là ATTT) mạng toàn cầu (GCI) được Liên minh Viễn thông Quốc tế ITU công bố từ năm 2015. GCI được tính toán trên cơ sở điểm tổng hợp của bộ tiêu chí gồm 17 tiêu chí cụ thể, phân thành 5 nhóm là pháp lý; kỹ thuật; tổ chức, chính sách; xây dựng năng lực và hợp tác. GCI được đưa vào Nghị quyết 130, Hội nghị toàn quyền của ITU về tăng cường vai trò của ITU trong các hoạt động thuộc lĩnh vực thông tin truyền thông và ATTT mạng. Mục đích của việc công bố GCI là để đánh giá hiện trạng, đồng thời thúc đẩy các quốc gia, vùng lãnh thổ trong việc tăng cường các biện pháp bảo đảm ATTT mạng; thúc đẩy hợp tác quốc tế và thúc đẩy việc trao đổi kinh nghiệm trong lĩnh vực ATTT.

Chỉ số ATTT Việt Nam (Vietnam Cybersecurity Index). Chỉ số ATTT Việt Nam được Cục ATTT (Bộ Thông tin và Truyền thông) phối hợp với Hiệp hội ATTT Việt Nam xây dựng. Bộ tiêu chí về ATTT được tính toán dựa vào khảo sát hàng năm của Hiệp hội ATTT số Việt Nam (VNISA). Đây là kết quả được thống kê dựa trên 9 lĩnh vực quản lý, phát triển và đảm bảo ATTT cho tổ chức và doanh nghiệp, gồm 57 câu hỏi phức hợp với hàng trăm tiêu chí nhỏ cho các tổ chức doanh nghiệp lớn và 46 câu hỏi phức hợp cho các doanh nghiệp vừa và nhỏ. Việc đánh giá dựa trên 360 doanh nghiệp trong đó tập trung vào lĩnh vực: ngân hàng (chiếm tỷ trọng trung bình gần 60%), tài chính, các doanh nghiệp khác. Chỉ số này được thống kê từ năm 2010.

Chỉ số sẵn sàng ứng dụng và phát triển thông tin: Chỉ số sẵn sàng cho phát triển và ứng dụng CNTT-TT Việt Nam (Vietnam ICT Index) do Bộ Thông tin và Truyền thông (Vụ Công nghệ thông tin) phối hợp với Hội Tin học Việt Nam thực hiện, cung cấp các thông tin về thực trạng phát triển và ứng dụng CNTT-TT tại Việt Nam, đồng thời đưa ra những đánh giá, xếp hạng về mức độ sẵn sàng cho phát triển và ứng dụng CNTT-TT dựa trên cơ sở số liệu thu thập được từ Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ; tỉnh, thành phố trực thuộc trung ương; tập đoàn kinh tế, tổng công ty và ngân hàng thương mại. Báo cáo này được thực hiện từ năm 2002, góp phần đưa ra những giải pháp, định hướng phù hợp nhằm cải thiện việc phát triển và ứng dụng CNTT trong các cơ quan tổ chức.

Để phân tích thực trạng tội phạm công nghệ cao và đánh giá mức độ đảm bảo an toàn bảo mật trong môi trường mạng, bài viết sử dụng dữ liệu thứ cấp từ nhiều nguồn: Nguồn số liệu thứ cấp từ Báo cáo tóm tắt chỉ số sẵn sàng cho phát triển và ứng dụng CNTT-TT Việt Nam từ Bộ Thông Tin và Truyền thông và Hội Tin học Việt Nam, báo cáo những rủi ro cao nhất toàn cầu của Diễn đàn Kinh tế Thế giới, Báo cáo Tổng kết và dự báo xu hướng an ninh mạng của BKAV, báo cáo người sử dụng internet của Ngân hàng Thế giới, Báo cáo chỉ số ATTT mạng toàn cầu - GCI của ITU, báo cáo về tình hình tội phạm sử dụng công nghệ cao của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), báo cáo Chỉ số ATTT mạng, của Bộ Thông tin và Truyền thông và Hiệp hội ATTT Việt Nam (VNISA).

Số các vụ án mà đối tượng lợi dụng mạng internet để thực hiện hành vi tội phạm sử dụng công nghệ cao ngày càng nhiều

2. TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO TẠI VIỆT NAM

- Tình hình tội phạm sử dụng công nghệ cao tại Việt Nam

Tại Việt Nam, tội phạm sử dụng công nghệ cao gia tăng nhanh chóng, diễn biến phức tạp và gây ra nhiều hậu quả nghiêm trọng (Bảng 1). Số các vụ án mà đối tượng lợi dụng mạng internet để thực hiện hành vi tội phạm sử dụng công nghệ cao ngày càng nhiều, gây thiệt hại cho tổ chức, cá nhân hàng nghìn tỷ đồng. Số lượng bị can bị khởi tố thông qua các vụ vi phạm mà công an Việt Nam đã triệt phá cho thấy tội phạm sử dụng công nghệ cao ngày càng hoạt động tinh vi theo nhóm được tổ chức chuyên nghiệp và có sự liên kết

giữa tội phạm trong nước và cả nước ngoài. Theo số liệu thống kê của Cục Cảnh sát phòng chống tội phạm sử dụng công nghệ cao (nay là Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao), Bộ Công an, từ năm 2010 đến tháng 6/2014 lực lượng cảnh sát phòng chống tội phạm sử dụng công nghệ cao trên cả nước đã phát hiện và xác minh 11.476 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 do C50 phát hiện; 450 vụ việc và 1.230 đối tượng do công an các địa phương (Nguyên Vũ, 2018).

Theo dự báo, số lượng và các loại tội phạm mạng cũng sẽ tăng nhanh cả về phạm vi, quy mô cũng như hậu quả. Đối tượng tấn công của tội phạm này là cơ sở dữ liệu của các cơ quan Nhà nước, kể cả các cơ quan an ninh, các cơ sở dữ liệu về tài chính, ngân hàng, giao thông, năng lượng, thông tin liên lạc, các công ty thương mại điện tử, các ngân hàng cung cấp dịch vụ thanh toán qua mạng, các máy ATM, bán hàng tự động. Đặc biệt là sự hình thành rõ nét hơn trong việc phối hợp giữa tội phạm trong nước và quốc tế tấn công vào các mạng máy tính, trộm cắp thông tin thẻ tín dụng, sử dụng thông tin thẻ tín dụng làm thẻ trắng giả để rút tiền ở máy ATM, thẻ màu giả để mua hàng, mua vé máy bay, thanh toán tiền khách sạn... Thủ đoạn của các đối tượng này được dự báo là sẽ tấn công cơ sở dữ liệu của hạ tầng thông tin quốc gia, của ngân hàng và các doanh nghiệp lớn (Thanh Loan, 2019).

- Thiệt hại do tội phạm sử dụng công nghệ cao ở Việt Nam

Bên cạnh những thiệt hại kinh tế trực tiếp (tổn thất tài chính) cho các nạn nhân như trộm cắp tiền trong thẻ tín dụng, mã hóa tài liệu, chiếm đoạt thông tin, khống chế, đe dọa cá nhân để tống tiền, chúng còn gây ra những thiệt hại gián tiếp (tổn thất phi tài chính) như: làm mất uy tín, gián đoạn hoạt động của các cơ quan, tổ chức; hoạt động kinh doanh của các doanh nghiệp, đặc biệt là đe dọa đến an ninh quốc gia, trật tự an toàn trên mạng internet. Cùng với sự phát triển mạnh mẽ của công nghệ, viễn thông, tội phạm sử dụng công nghệ cao trên thế giới và Việt Nam cũng đang diễn biến phức tạp. Thiệt hại do tội phạm sử dụng công nghệ cao gây ra qua thời gian càng ngày càng tăng, chỉ trong vòng 10 năm, quy mô thiệt hại đã tăng 620%. Mức thiệt hại được tính dựa trên mức thu nhập của người sử dụng máy tính và thời gian công việc của họ bị gián đoạn do các trục trặc gây ra bởi vi rút máy tính cũng ngày càng gia tăng (Bảng 2).

BẢNG 1: TỘI PHẠM SỬ DỤNG CÔNG CỤ CÔNG NGHỆ CAO ĐÃ PHÁT HIỆN GIAI ĐOẠN 2010-2019

Năm	Số vụ vi phạm	Ước tính thiệt hại	Khởi tố	Giá trị tài sản thu hồi
2010	12 (7 chuyên án)	Gần 20 tỷ đồng, 2.000.000 đô la Úc, 130.242 đô la Mỹ	08 vụ, 14 bị can, xử phạt hành chính 36 vụ	Thu hồi 10 tỷ 238 triệu đồng và 820 máy tính xách tay và nhiều linh kiện điện tử các loại
2011	165 (14 chuyên án)	Khoảng 12 tỷ đồng và 235.000 USD	32 vụ, 81 bị can, xử phạt hành chính 09 vụ	Thu giữ tiền và nhiều tài sản khoảng 12 tỷ đồng và 235.000 USD
2012	192 (17 chuyên án)	Hơn 1300 tỷ đồng	34 vụ, 90 bị can	Đã thu hồi tiền và tài sản trị giá hơn 10 tỷ đồng
2013	210 (30 chuyên án)	Khoảng 16 tỷ đồng	59 vụ, CQĐT đã khởi tố 35 vụ, 175 bị can	Thu giữ nhiều tiền và tài sản trị giá hàng chục tỷ đồng
2014	276 (38 chuyên án)	Gần 329.000 USD	11 chuyên án, 135 vụ khởi tố 167 bị can , xử lý hành chính 05 vụ	329.842 đô la Mỹ và các tài sản khác.
2015	-	-	127 vụ, 215 bị can	-
2016	-	-	217 vụ, 493 bị can	-
2017	-	-	197 vụ, 359 bị can	-
2018	-	-	117 vụ, 196 bị can	-
2019*	-	-	449 vụ, 867 bị can, 187 xử lý hành chính	-

** Số liệu hệ thống nhất được cập nhật theo văn bản 746/TTg-QHĐP bao gồm năm 2018 và quý 1/2019*
Nguồn: Nguyên Vũ (2018), Nguyễn Minh Đức (2014)

BẢNG 2: THỰC TRẠNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO GÂY RA TẠI VIỆT NAM

Năm	2007	2010	2014	2015	2016	2017	2018	2019	2020
Tổng thiệt hại (tỷ đồng)	2.400	5.900	8.500	8.700	10.400	12.300	14.900	20.892	23.900
Thiệt hại trung bình/người (triệu đồng)	-	1,192	1,230	1,253	1,509	-	-		
Số người bị tin nhắn rác làm phiền hàng ngày (% người dùng)	-	-	43	50	50	-	-		
Số máy tính nhiễm vi rút (%)	97	93	85	83	83	-	-	80	
Mã độc Ransomware (% lượng mail)	-	-	-	-	16	11,22	-	-	

Nguồn: Tổng hợp từ BKAV (2009, 2014, 2015, 2016, 2017, 2018, 2019, 2020)

Theo báo cáo tình hình an ninh mạng Việt Nam năm 2020 của Công ty an ninh mạng BKAV, thiệt hại do vi rút máy tính gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 23.900 tỷ đồng. So với báo cáo cũng của BKAV từ cách đây 5 năm, mức thiệt hại này đã tăng lên gấp 5 lần.

- Sự cố an ninh thông tin tại Việt Nam

Thực trạng an toàn, an ninh thông tin tại Việt Nam trong một vài năm qua diễn biến rất phức tạp, khó lường. Năm 2016, Việt Nam đối mặt với sự cố tin tặc tấn công có chủ đích vào hệ thống

của Hãng hàng không Quốc gia Việt Nam và các cuộc tấn công vào hệ thống ngân hàng để lừa đảo chiếm đoạt tài sản. Tuy nhiên, điều tích cực là sau khi xảy ra vụ việc, ý thức của quản trị các hệ thống lớn, quan trọng đã tốt hơn rất nhiều (BKAV, 2017). Trong năm 2017, Việt Nam đã phải đối diện với 3 vấn đề mất an toàn, an ninh thông tin lớn mà trong đó, đáng chú ý là việc hàng loạt các cuộc tấn công mạng diễn ra với quy mô lớn, cường độ cao nhắm vào các lĩnh vực trọng yếu cũng như các công trình quan trọng của quốc gia (Đức Thiện, 2019).

Các nhóm các tội phạm đã sử dụng các phương pháp tấn công vào hệ thống như là Phishing (lừa đảo), Deface (xâm nhập), Malware (phần mềm độc hại)... để tấn công vào người sử dụng. Số liệu tổng hợp trong giai đoạn 2010-2019 có 208.409 cuộc tấn công vào Việt Nam, trong đó Phishing là 29.059 cuộc (14,01%), Deface là 105.971 cuộc (chiếm 51,11%), Malware là 72.323 cuộc (chiếm 34,88%).

- Việt Nam là quốc gia có môi trường mạng dễ tổn thương

Phương thức mà các đối tượng sử dụng công nghệ cao để thực hiện những tội phạm này rất phức tạp. Thông thường tội phạm mạng sử dụng phần mềm bảo mật để ẩn danh các máy chủ proxy che giấu vị trí của mình và định tuyến thông tin liên lạc của họ qua nhiều quốc gia để trốn tránh phát hiện trực tiếp và thực hiện tội phạm ở các quốc gia khác nơi chúng không thể bị truy tố. Các loại tấn công phổ biến nhất được thực hiện bởi các băng nhóm này là lừa đảo bằng mã độc, máy tính ma và phần mềm độc hại, chẳng hạn như Trojan truy cập từ xa (RAT). Động lực của chúng đằng sau các cuộc tấn công này thường là lợi ích tiền tệ và thông tin như tấn công mạng, giả định, tống tiền trực tuyến, gian lận thẻ tín dụng và thậm chí các hoạt động rửa tiền quốc tế.

Việt Nam hiện xếp thứ 7 thế giới về số lượng địa chỉ IP trong nước được dùng trong các mạng máy tính ma tấn công nước khác, chiếm 3,5% tổng số địa chỉ IP trong các mạng máy tính ma quốc tế, trong khi năm 2012 chỉ đứng thứ 23 với tỷ lệ 0,78%. Báo cáo của Symantec (2020), Việt Nam đứng thứ 11 trong danh sách quốc gia hàng đầu khởi phát tấn công mạng (Bảng 3). Thời điểm bùng nổ Internet ở Việt Nam cũng là thời điểm mở rộng hoạt động của nhiều hình thức tội phạm cộng nghệ cao như tổ chức đánh bạc, cá độ bóng đá trên mạng, mua bán các loại giấy tờ giả, đánh cắp thông tin cá nhân, trộm cước viễn thông, lừa đảo huy động tiền ảo...

BẢNG 3: XẾP HẠNG CÁC QUỐC GIA, VÙNG LÃNH THỔ ĐỨNG ĐẦU VỀ ĐIỂM XUẤT PHÁT TẤN CÔNG MẠNG

Xếp hạng	2013		2014		2016		2017		2018
1	Mỹ	2,33	Mỹ	20,69	Mỹ	23,96	Mỹ	26,61	Trung Quốc
2	Trung Quốc	9,39	Trung Quốc	10,65	Trung Quốc	9,63	Trung Quốc	10,95	Mỹ
3	Ấn Độ	5,11	Ấn Độ	3,95	Brazil	5,84	Ấn Độ	5,09	Brazil
4	Hà Lan	3,52	Hà Lan	3,64	Ấn Độ	5,11	Nga	4,12	Nga
5	Đức	3,26	Đức	3,26	Đức	3,35	Đức	3,40	Mexico
6	Nga	2,63	Đài Loan	2,60	Nga	3,07	Nhật Bản	3,39	Nhật
7	Anh	2,58	Anh	2,56	Anh	2,61	Brazil	3,39	Việt Nam
8	Brazil	2,53	Nga	2,54	Pháp	2,35	Anh	2,33	Hàn Quốc
9	Đài Loan	2,45	Việt Nam	2,44	Nhật Bản	2,25	Pháp	2,21	Thổ Nhĩ Kỳ
10			Brazil	2,32	Việt Nam	2,16	Việt Nam	2,07	Ý
11	Việt Nam	2,24	-	-	-	-	-	-	-

** Số trong bảng tỷ lệ các vụ tấn công có xuất phát điểm từ nước trong bảng so với toàn cầu*

Nguồn: Synmatec (2017), Synmatec (2019), Synmatec (2020)

3. THỰC TRẠNG ĐẢM BẢO AN TOÀN BẢO MẬT THÔNG TIN PHÒNG CHỐNG, TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO TẠI VIỆT NAM

- Chỉ số ATTT mạng toàn cầu (GCI)

Trong 2 kỳ ITU công bố báo cáo GCI vào tháng 4/2015 và tháng 7/2017, 11/2019, Việt Nam lần lượt xếp hạng 76/196 và 101/193, 50/168 về ATTT mạng. Xếp hạng về ATTT mạng của Việt Nam trong khu vực ASEAN là 5/11, xếp sau các nước Singapore, Malaysia, Thái Lan, Philippines, Indonesia.

Kết quả đánh giá GCI 2017 cho thấy xét về mặt bằng chung so với thế giới và trong khu vực, mức độ ATTT của Việt Nam và các doanh nghiệp vẫn tương đối thấp. Việt Nam chỉ có 4 tiêu chí đạt mức màu Xanh (có cơ quan, tổ chức có trách nhiệm ứng cứu sự cố an toàn mạng quốc gia; có cơ quan, tổ chức có trách nhiệm ứng cứu sự cố an toàn mạng trong khối chính phủ; có cơ quan, tổ chức chịu trách nhiệm về an toàn thông tin; và có hợp tác quốc tế về an toàn thông tin); có 2 tiêu chí đạt mức màu Vàng (có pháp lý về an toàn thông tin; có cơ quan, tổ chức chịu trách nhiệm tiêu chuẩn hóa về an toàn thông tin); các tiêu chí còn lại đều ở mức màu

Đỏ (chưa tuân thủ). Điểm và xếp hạng ATTT mạng của Việt Nam thấp một phần do Cục ATTT chưa trả lời danh sách các câu hỏi trực tuyến được gửi tới các thành viên ITU trong quá trình thu thập thông tin để tính GCI 2017. Một phần do Việt Nam chưa đáp ứng các tiêu chuẩn về an toàn an ninh mạng (một trong số 60 nước chưa có chiến lược quốc gia về ATTT mạng). Tuy nhiên trong báo cáo năm 2018, Việt Nam đã có bước tiến vượt bậc trong xếp hạng của ITU.

- Chỉ số ATTT Việt Nam

Chỉ số ATTT Việt Nam (VNISA Index) được tính toán dựa vào khảo sát hàng năm của Hiệp hội ATTT số Việt Nam. Đây là kết quả được thống kê dựa trên 9 lĩnh vực quản lý, phát triển và đảm bảo ATTT cho tổ chức và doanh nghiệp gồm 57 câu hỏi phức hợp với hàng trăm tiêu chí nhỏ cho các tổ chức doanh nghiệp lớn và 46 câu hỏi phức hợp cho các doanh nghiệp vừa và nhỏ. Việc đánh giá dựa trên 360 doanh nghiệp trong đó tập trung vào lĩnh vực: ngân hàng (chiếm tỷ trọng trung bình gần 60%), tài chính, các doanh nghiệp khác. Chỉ số này được thống kê từ năm 2010. Chỉ số ATTT của Việt Nam được cải thiện qua các năm, trong đó các ngân hàng vẫn là nhóm doanh nghiệp phát triển năng lực ATTT mạng hàng đầu trong cả nước nhưng cũng chỉ ở mức trên trung bình (Bảng 4). Những con số này phản ánh chính xác thực trạng về ATTT mạng tại Việt Nam, khi vẫn còn khá ít doanh nghiệp có hiểu biết và quan tâm về lĩnh vực ATTT theo từng cấp độ, mặc dù đây đều là những kiến thức căn bản và quan trọng.

BẢNG 4: CHỈ SỐ AN TOÀN THÔNG TIN VIỆT NAM GIAI ĐOẠN 2010-2019

Năm	2012	2013	2014	2015	2016	2017	2018	2019*
Chỉ số chung (%)	26	37,5	39	47,4	59,9	54,2	45,6	58,4
Ngân hàng, tài chính	-	-	-	-	-	59,9	57,5	-

- Phòng chống tội phạm sử dụng công nghệ cao của cơ quan quản lý

Hoạt động của tội phạm sử dụng công nghệ cao và hoạt động phòng chống tội phạm sử dụng công nghệ cao tại Việt Nam giai đoạn 2011-2020 cho thấy tội phạm sử dụng công nghệ cao tại Việt Nam ngày càng tinh vi hơn, số vụ vi phạm nhiều hơn và thiệt hại lớn hơn. Để phòng chống tội phạm sử dụng công nghệ cao, Việt Nam đã cải thiện cơ sở hạ tầng nhân lực, cơ sở hạ tầng kỹ thuật để nâng cao tính bảo mật, an toàn của môi trường mạng.

Lực lượng tham gia phòng chống tội phạm sử dụng công nghệ cao 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. Nhiều bộ chủ quản đã có chuyên trách về an toàn an ninh thông tin cho ngành: Cục Công nghệ Tin học thuộc Ngân hàng Nhà nước, Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an,....

Các cơ quan quản lý đều thực hiện tốt chức trách, nhiệm vụ của mình. Tuy nhiên, vẫn còn một số vấn đề cần điều chỉnh: (1) Chưa có văn bản quy phạm pháp luật về phối hợp, phòng, chống tội phạm sử dụng công nghệ cao; (2) Một số luật còn thiếu một số nội dung liên quan đến tội phạm sử dụng công nghệ cao như Luật các Tổ chức tín dụng chưa có các nội dung Luật thanh toán mới; Luật Giao dịch điện tử, Luật xử lý vi phạm hành chính, Pháp lệnh Thương mại điện tử... chưa có các chế định về các hành vi tội phạm, chứng cứ, các biện pháp ngăn chặn; Bộ luật Tố tụng hình sự chưa có các quy định có liên quan đến chứng cứ điện tử, các thủ tục tố tụng hình sự về việc thu thập, bảo quản, phục hồi và giám định chứng cứ điện tử phù hợp với đặc điểm, tính chất của tội phạm sử dụng công nghệ cao.

Cùng với sự phát triển mạnh mẽ của công nghệ, viễn thông, tội phạm sử dụng công nghệ cao trên thế giới và Việt Nam cũng đang diễn biến phức tạp

4. MỘT SỐ GỢI Ý CHÍNH SÁCH VỀ PHÒNG CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

Mặc dù gặt hái nhiều thành công trong phòng chống tội phạm sử dụng công nghệ cao nhưng hiện tại Việt Nam vẫn đứng trong tốp 7 thế giới về các hoạt động đe dọa tấn công mạng cũng xuất phát tấn công mạng. Do vậy, Việt Nam cần phải có điều chỉnh trong các hoạt động:

Chính phủ cần xây dựng cơ chế phối hợp giữa các cơ quan thuộc chính phủ, tạo cơ chế chia sẻ thông tin nhằm đảm bảo an ninh mạng và phòng chống tội phạm sử dụng công nghệ cao. Cần nhanh chóng xây dựng quy chế phối hợp giữa ngân hàng với các cơ quan chức năng liên quan trong đó Cục Công nghệ thông tin - Ngân hàng Nhà nước; Cục An ninh mạng và Phòng, chống tội phạm sử dụng công nghệ cao, Trung tâm Thông tin an toàn, Trung tâm Cảnh

báo, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam... trong phòng ngừa, phát hiện, đấu tranh với các loại tội phạm sử dụng công nghệ cao.

Bộ Công an tăng cường phối hợp với các đơn vị có liên quan để giải quyết các yêu cầu phát hiện, xác minh, điều tra tội phạm sử dụng công nghệ cao một cách kịp thời, triệt để; chủ trì, phối hợp với các bộ, ngành hữu quan như: Viện Kiểm sát Nhân dân Tối cao, Tòa án Nhân dân Tối cao, Bộ Tư pháp, Bộ Thông tin và Truyền thông, Ngân hàng Nhà nước xây dựng Thông tư liên ngành về phòng, chống tội phạm sử dụng công nghệ cao. Đây chính là cơ sở pháp lý quan trọng để các bên tham gia hợp tác, chia sẻ, cung cấp, quản lý và sử dụng thông tin, tài liệu phục vụ cho công tác phòng, chống tội phạm sử dụng công nghệ cao và đảm bảo an ninh, an toàn trong hoạt động. Bên cạnh đó, phần lớn các tội phạm sử dụng công nghệ cao hiện nay là người nhập cư trái phép từ nước ngoài, Bộ Công an cần có các biện pháp tăng cường kiểm soát ở các tuyến biên giới để tránh không cho các đối tượng lợi dụng sơ hở nhập cảnh trái phép vào sâu trong nội địa thực hiện hành vi phạm tội. Bộ Công an cần đề xuất với Chính phủ giao cho Bộ Công an chỉ đạo công tác xây dựng, phát triển lực lượng cảnh sát phòng, chống tội phạm sử dụng công nghệ cao ngang tầm nhiệm vụ trong tình hình mới. Bộ Công an cần chỉ đạo kiện toàn tổ chức bộ máy và triển khai thành lập các đơn vị cảnh sát phòng, chống tội phạm sử dụng công nghệ cao trực thuộc các phòng chức năng ở công an các tỉnh, thành phố trực thuộc trung ương nhằm xây dựng một hệ thống cảnh sát phòng, chống tội phạm sử dụng công nghệ cao trên phạm vi toàn quốc.

Bộ Thông tin và Truyền thông: (1) Chịu trách nhiệm về đảm bảo an toàn về tài nguyên viễn thông, đối với vòng ngoài về truyền thông mạng, định danh và định tuyến, ứng cứu sự cố ATTT mạng cấp quốc gia; (2) Xây dựng Chiến lược đưa Việt Nam trở thành cường quốc an toàn, an ninh mạng; phối hợp với Bộ Công an trong việc xây dựng các văn bản hướng dẫn Luật An ninh mạng; đầu mối tập trung về mặt kỹ thuật, chỉ đạo các doanh nghiệp cung cấp dịch vụ viễn thông, Internet thực hiện các hoạt động, nhiệm vụ bảo đảm an toàn, an ninh mạng; triển khai thu thập thông tin, tổng hợp, phân tích, theo dõi và dự báo, cảnh báo sớm xu hướng về các hoạt động, diễn biến trên không gian mạng Việt Nam; triển khai các chương trình diễn tập, tập trận phòng thủ, đào tạo, tập huấn, bồi dưỡng nâng cao kiến thức, kỹ năng về ATTT cho các cơ quan, tổ chức và doanh nghiệp; thúc đẩy phát triển các nhóm sản phẩm, dịch vụ về hệ sinh thái số Việt Nam; giám sát tin chính xác/sử dụng trí tuệ nhân tạo phân loại, đánh giá tin từ không gian mạng; (3) Triển khai xây dựng Nghị định về xác thực và định danh điện tử; Quy hoạch bảo đảm ATTT mạng đến năm 2030; Kế hoạch bảo đảm ATTT mạng giai đoạn 2021-2025; Đề án đảm bảo ATTT cho đô thị thông minh; Đề án áp dụng thí điểm tiêu chuẩn TCVN:11930 cho hệ thống thông tin của cơ quan, tổ chức nhà nước; Hồ sơ đề xuất cấp độ mẫu cho hệ thống thông tin cấp độ 5 và tiêu chí quy trình đánh giá phần mềm phòng chống phần mềm độc hại; (4) Triển khai hệ thống chia sẻ và phân tích thông tin về nguy cơ, rủi ro mất an toàn, an ninh mạng trong các nước ASEAN và đưa Việt Nam thành một trong những Trung tâm chia sẻ nguy cơ an toàn, an ninh mạng của ASEAN; phát triển Trung tâm Giám sát an toàn không gian mạng quốc gia, đẩy mạnh hoạt động của Trung tâm này để triển khai giám sát an toàn trên toàn bộ không gian mạng Việt Nam.

Bộ Giáo dục và Đào tạo thông tin về cảnh báo, phòng ngừa việc lạm dụng, thiếu hiểu biết pháp luật dẫn đến vi phạm pháp luật, nhất là giới học sinh, sinh viên. Bộ Khoa học và Công nghệ xây dựng và công bố bộ tiêu chuẩn chất lượng, đặc biệt cho các sản phẩm dịch vụ tài chính, ngân hàng◆

TÀI LIỆU THAM KHẢO

- PCERT (2016, 2017, 2018, 2019). APCERT_Annual_Report_2016.

- BKAV (2014, 2015, 2016, 2017, 2018, 2019, 2020). Tổng kết an ninh mạng năm và dự báo xu hướng các năm sau.

- Đức Thiện (2019).Tấn công mạng có chủ đích gây thiệt hại ngày càng khủng. Tham khảo từ https://congnghe.tuoitre.vn/tan-cong-mang-co-chu-dich-gay-thiet-hai-ngay-cang-khung-20190214102213118.htm.

- ITU (2016), Global Cybersecurity Index 2015. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

- ITU (2018). Global Cybersecurity Index 2017. https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf.

- ITU (2019). Global Cybersecurity Index 2018 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

- Nguyễn Minh Đức (2014). Báo cáo Tổng kết của Cục cảnh sát phòng chống tội phạm sử dụng công nghệ cao; Kỷ yếu hội thảo khoa học "Phòng, chống tội phạm sử dụng công nghệ cao - Những vấn đề đặt ra trong công tác đào tạo", 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> (truy cập ngày 02/4/2018).

- Nguyên Vũ (2018) Bộ trưởng Công an: Tội phạm công nghệ cao khó phòng ngừa và đấu tranh hơn trước, http://vneconomy.vn/bo-truong-cong-an-toi-pham-cong-nghe-cao-kho-phong-ngua-va-dau-tranh-hon-truoc-20180813084443184.htm

- Symantec (2014). Internet Security Threat Report. Vol 19. 2014.

- Symantec (2016). Symantec report 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-appendices-en.pdf

- Symantec (2017). Internet Security Threat Report. Vol 22. 2017. https://www.symantec.com/content/dam/symantec/docs/reports/gistr22-government-report.pdf

*- Symantec (2018). Internet Security Threat Report. http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_*

- Symantec (2019).How Do Cybercriminals Get Caught?.https://us.norton.com/internetsecurity-emerging-threats-how-do-cybercriminals-get-caught.html.

- Symantec (2020), Internet Security Threat Report. https://docs.broadcom.com/doc/istr-24-2019-en

- Thanh Loan (2019).Ấm ảnh tội phạm mạng thời công nghệ số. http://tapchitaichinh.vn/tai-chinh-phap-luat/am-anh-toi-pham-mang-thoi-cong-nghe-so-301562.html.

- VNISA (2018), Overview Report Vietnam Information Security Day 2018, https://drive.google.com/file/d/12DgkTjdNxLHdZeqxSD5bUuZTxXzyxMme/view,

- VNISA (2019), Tài liệu báo cáo Ngày ATTT Việt Nam 2019, https://vnisa.org.vn/tai-lieu-bao-cao-ngay-an-toan-thong-tin-viet-nam-2019/