**TÀI LIỆU BỒI DƯỠNGKỸ NĂNG, NGHIỆP VỤ CHO CÁN BỘ
PHÁP CHẾ DOANH NGHIỆP NĂM 2019 TẠI TP. HỒ CHÍ MINH**

**-------------------------------------------------**

**Chuyên đề: *“Bồi dưỡng cho cán bộ pháp chế và những nội dung về
Luật An ninh mạng 2018 với các doanh nghiệp ngành công nghệ,
truyền thông và nội dung số”***

# I. TÍNH CẤP THIẾT XÂY DỰNG, BAN HÀNH LUẬT AN NINH MẠNG

## 1. Thực trạng, tình hình an ninh mạng đặt ra yêu cầu cấp thiết phải xây dựng, ban hành Luật An ninh mạng

***\**** Khởi nguồn từ công cụ phục vụ chiến tranh, Internet đã trở thành lõi cho sự hình thành không gian mạng. Ngày nay, với sự phát triển và ứng dụng mạnh mẽ công nghệ thông tin vào đời sống xã hội, không gian mạng đang làm thay đổi thế giới, thay đổi cuộc sống của con người, sự phát triển như vũ bão của khoa học công nghệ, không gian mạng trở thành một bộ phận cấu thành không thể thiếu và đóng vai trò quan trọng trong xây dựng xã hội thông tin và phát triển kinh tế tri thức. Sự phát triển bùng nổ của công nghệ mang tính đột phá như trí tuệ nhân tạo, Internet của vạn vật, máy tính lượng tử, điện toán đám mây, dữ liệu lớn, dữ liệu nhanh… đã làm không gian mạng thay đổi sâu sắc cả về chất và lượng, được dự báo sẽ mang lại những lợi ích chưa từng có cho xã hội loài người nhưng cũng làm xuất hiện những nguy cơ tiềm ẩn vô cùng lớn.

 Theo thống kê của Bộ Công an, mỗi năm có hàng nghìn trang mạng của Việt Nam bị tin tặc tấn công nhằm đánh cắp thông tin, chiếm quyền điều khiển, thay đổi, chèn nội dung, cài cắm mã độc… Trong 6 tháng đầu năm 2019, Bộ Công an đã phát hiện trên 2.500 trang tin, cổng thông tin điện tử tên miền quốc gia Việt Nam bị tấn công; hàng trăm ngàn máy tính bị nhiễm mã độc. Đáng lưu ý, Việt Nam xếp thứ 4 trong Top 10 quốc gia bị kiểm soát bởi mạng máy tính ma botet.

 Cùng với đó, hoạt động sử dụng mạng xã hội nước ngoài để đăng tải tin giả với mục đích làm nhục, vu khống, bôi nhọ, xúc phạm các tổ chức, cá nhân diễn ra tràn lan trên không gian mạng, xâm phạm trực tiếp quyền, lợi ích hợp pháp của các tổ chức, cá nhân. Năm 2018, Bộ Công an đã phát hiện hơn 800 trang blog, gần 6.000 tài khoản mạng xã hội đăng tải hàng trăm nghìn tin, bài có nội dung tuyên truyền xuyên tạc, vu cáo, phỉ bang, xúc phạm nhân phẩm….

 “Tại Việt Nam, thời gian qua đã ghi nhận hàng chục vụ tự tử, giết người, cố ý gây thương tích… xuất phát từ nguyên nhân sử dụng mạng xã hội để thách đố, kích động bạo lực, vu cáo, xúc phạm người khác. Đặc biệt, trong đó nhiều nạn nhân là trẻ em và vị thành niên”, Đại tá Đỗ Anh Tuấn cho biết.

 Đáng lưu ý, hoạt động sử dụng Internet vào mục đích khủng bố nổi lên như một thách thức toàn cầu, đe dọa nghiêm trọng tới an ninh quốc gia của các nước trong đó có Việt Nam. Theo các chuyên gia an ninh bảo mật quốc tế, hiện trên thế giới có khoảng 50 tỷ điểm kết nối IoT đang hoạt động, đây là những điểm yếu có thể bị lợi dụng để tạo ra những cuộc tấn công mạng quy mô lớn gây thiệt hại nghiêm trọng về tài sản và sinh mạng người dân với mục đích khủng bố. Trong khi đó, các phần tử Hồi giáo cực đoan quá khích đang xây dựng một môi trường tư tưởng mới trên không gian mạng toàn cầu. Internet trở thành môi trường lý tưởng để tội phạm khủng bố trao đổi, thu thập thông tin, kết nối và tuyển mộ lực lượng. Theo thống kê của Liên Hợp Quốc, IS đã tích cực sử dụng truyền thông xã hội để tuyển mộ chiến binh, truyền bá tư tưởng cực đoan và hành động bạo lực với khoảng 40.000 thông điệp/ngày (Twitter); tuyển mộ thành công hàng ngàn chiến binh từ hơn 90 quốc gia thông qua Internet….

 Lý giải cho tình trạng trên thì gồm có 05 lý do chính:

 *Một là*, sự phát triển nhanh chóng của CNTT, viễn thông, Internet vừa tạo ra cơ hội, động lực để phát triển kinh tế - xã hội, nhưng cũng làm nảy sinh những nguy cơ, lỗ hổng, tạo điều kiện cho tội phạm mạng, tin tặc triệt để lợi dụng để tiến hành các hoạt động vi phạm pháp luật, đặc biệt là tội phạm trong lĩnh vực tài chính – ngân hàng.
 *Hai là*, công tác bảo mật dữ liệu và bảo vệ bí mật Nhà nước tại nhiều cơ quan, đơn vị của các Bộ, ngành, địa phương, trong đó có các tổ chức tài chính – ngân hàng chưa được quan tâm đúng mức; hiệu quả công tác tuyên truyền, phổ biến quán triệt nội dung các quy định về bảo mật dữ liệu và bảo vệ bí mật nhà nước chưa cao; ý thức, nhận thức của cán bộ có bước chuyển biến, song vẫn còn hạn chế, chưa thực hiện nghiêm quy định, quy trình bảo mật dữ liệu và bảo vệ bí mât nhà nước, vẫn tồn tại tình trạng soạn thảo, lưu trữ, truyền đưa tài liệu mật trên môi trường mạng.

 *Ba là*, việc đầu tư thiết bị đảm bảo an toàn, an ninh mạng chưa tương xứng với thực tại và tương lai. Sự phát triển như vũ bão về khoa học - công nghệ đã khiến cho vòng đời của sản phẩm an ninh mạng ngắn lại, yêu cầu đầu tư để theo kịp sự phát triển, không bị lạc hậu trong điều kiện kinh tế đất nước còn nhiều khó khăn là một trong những thách thức được đặt ra. Song song với đó, nghiên cứu, ứng dụng và phát triển khoa học – công nghệ trong lĩnh vực đảm bảo an ninh mạng ở nước ta còn chưa theo kịp tốc độ phát triển khoa học – công nghệ của thế giới; chưa tự chủ, sản xuất được các thiết bị công nghệ thông tin dẫn đến gần như lệ thuộc vào các sản phẩm bên ngoài.Trong khi đó, các hệ thống mạng thông tin ở Việt Nam, trong đó có các hệ thống tài chính – ngân hàng chưa tuân theo một tiêu chuẩn thống nhất, chưa có thẩm định, kiểm tra, đánh giá về an ninh mạng; việc áp dụng các biện pháp bảo đảm an toàn, an ninh thông tin chưa được các cơ quan, tổ chức, doanh nghiệp chú trọng; nhiều cơ quan Bộ, ngành sử dụng các thiết bị mạng lõi của một số tập đoàn công nghệ vẫn tồn tại lỗ hổng bảo mật, nguy cơ bị theo dõi, giám sát, thu thập thông tin từ xa là rất lớn.

 *Bốn là*, công tác đào tạo nguồn nhân lực, chuyên gia an ninh mạng chưa theo kịp yêu cầu về số lượng và chất lượng, chưa hình thành đội ngũ chuyên gia an ninh mạng, thiếu lực lượng chuyên gia chuyên trách bảo vệ an ninh mạng, việc thực hiện chính sách còn khó khăn nên khó phát huy hết năng lực chuyên môn.

 *Năm là*, công tác quản lý nhà nước trên lĩnh vực viễn thông, Internet, an ninh mạng còn nhiều bất cập, chưa đáp ứng yêu cầu đặt ra. Hệ thống văn bản quy phạm pháp luật về lĩnh vực bảo đảm an ninh thông tin, an ninh mạng đang trong quá trình hoàn thiện, chưa đầy đủ, tạo sơ hở cho các đối tượng lợi dụng hoạt động vi phạm pháp luật. Hoạt động thương mại điện tử, thanh toán trực tuyến và các dịch vụ trực tuyến ở nước ta phát triển mạnh nhưng công tác quản lý còn chưa theo kịp, tạo sơ hở cho hoạt động lừa đảo, chiếm đoạt tài sản, xâm hại nghiêm trọng đến chủ quyền không gian thanh toán và hệ sinh thái kỹ thuật số.

 Thế giới cũng đang phải đối phó với nhiều nguy cơ, thách thức do không gian mạng đem lại, những năm gần đây, tình hình an ninh mạng diễn biến ngày càng phức tạp với hàng loạt chiến dịch gián điệp mạng nhằm vào những cơ quan, tổ chức và tập đoàn kinh tế lớn trên thế giới, chiếm đoạt hàng nghìn tài liệu quan trọng, bí mật, gây ra những hậu quả khôn lường. Các đơn vị tình báo mạng, tin tặc quốc tế xuất hiện ngày càng nhiều, đã tiến hành nhiều đợt tấn công APT (Advanced Persisdent Threat - Tấn công có chủ đích) kéo dài nhiều năm vào hàng trăm mục tiêu trên thế giới. Không gian mạng là môi trường thuận lợi để kích hoạt các vũ khí mạng trong việc lật đổ thể chế chính trị của một quốc gia mà sự kiện “mùa xuân Ả rập” hay “cách mạng hoa Lài” theo cách gọi của các nước phương Tây là sự thể hiện rõ nét nhất. Hoạt động sử dụng không gian mạng để hoạt động khủng bố, truyền bá chủ nghĩa khủng bố, cực đoan, tuyển quân ngày càng đe dọa nghiêm trọng đến an ninh các quốc gia, nổi lên là hoạt động của tổ chức “Nhà nước Hồi giáo tự xưng IS”.

Với đặc tính nặc danh và lan truyền nhanh, rộng khắp, không gian mạng có khả năng mở rộng phạm vi tác động, vượt qua các rào cản ngôn ngữ, khoảng cách địa lý và các nỗ lực ngăn chặn để gây thiệt hại trên diện rộng. Nhiều quốc gia đã nhận thức rõ về những mối đe dọa đối với an ninh mạng, coi đây là thách thức mới, mối đe dọa mới có tầm quan trọng và nguy hiểm cao nên đã cụ thể hóa thành các văn bản chính sách, văn bản pháp luật như luật hoặc văn bản dưới luật tại hơn 80 quốc gia, tổ chức, liên minh quốc tế như Mỹ[[1]](#footnote-1), Anh, Trung Quốc[[2]](#footnote-2), Đức, Hà Lan, Pháp, Canada, Hàn Quốc, NATO... nhằm tạo ra các thiết chế, cơ sở pháp lý chống lại các nguy cơ đe dọa đến an ninh quốc gia 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 tội phạm mạng.

Ngoài việc quy phạm các hành vi vi phạm pháp luật trên không gian mạng, Luật về an ninh mạng của một số quốc gia nêu trên còn là văn bản pháp lý, là tuyên bố chủ quyền của quốc gia đối với lãnh thổ, lợi ích họ đã thiết lập. Không gian mạng vấn đề có khả năng xảy ra tranh chấp, giống như tranh chấp lãnh thổ trên biển, trên không gian, vũ trụ. Tình hình biển Đông là minh chứng rõ ràng nhất, nếu không xác định sớm và có tuyên bố chủ quyền bằng một văn bản luật, lợi ích quốc gia trên không gian mạng sẽ bị ảnh hưởng.

Lãnh thổ không gian mạng là vùng thông tin được tạo ra từ các tín hiệu điện từ, được thiết lập, lưu trữ, xử lý và trao đổi trên cơ sở hạ tầng không gian mạng, có tính mở, không cố định, không phụ thuộc vào địa lý và nằm trong không gian mạng toàn cầu. Chủ quyền quốc gia trên không gian mạng là quyền quản lý, kiểm soát đối với cơ sở hạ tầng không gian mạng và thông tin được tạo ra, lưu trữ, xử lý, trao đổi trên đó, xác lập được chủ quyền, quyền tài phán theo luật pháp quốc tế đối với cơ sở hạ tầng mạng thuộc sở hữu cả ở trong nước và ngoài lãnh thổ quốc gia. Xác định chủ quyền quốc gia trên không gian mạng cần căn cứ vào lãnh thổ trên không gian mạng.

Thực tế công tác an ninh mạng đã chứng minh, muốn bảo vệ được chủ quyền, lãnh thổ quốc gia trên không gian mạng phải xác định được biên giới mạng, cửa khẩu mạng. Biên giới mạng là đường giới hạn lãnh thổ nước ta trên không gian mạng. Cửa khẩu mạng là cửa ngõ cho các hoạt động trao đổi lưu lượng mạng từ lãnh thổ quốc gia ra thế giới và ngược lại. Biên phòng mạng chính là lực lượng quản lý cửa khẩu mạng, cho phép hoặc không cho phép (bên chúng tôi hay gọi là xuất cảnh - nhập cảnh) một địa chỉ mạng tham gia hoạt động trên lãnh thổ không gian mạng Việt Nam. Đây chính là cốt lõi để phát hiện, ngăn chặn, xử lý các hoạt động, phá hoại từ bên ngoài; giải quyết vấn đề các nhà cung cấp dịch vụ xuyên biên giới hiện nay đang hoạt động tại Việt Nam mà không chịu sự quản lý của Nhà nước, không chịu nộp thuế kinh doanh mặc dù họ thu lợi rất nhiều.

Một số đạo luật điển hình là:

**- Mỹ**: Ngoài việc ban hành các đạo luật chung, Mỹ đã ban hành tới 06 đạo luật liên quan các vấn đề về an ninh mạng là:

**(1)** Đạo luật Đánh giá Lực lượng An ninh mạng**,** ban hành ngày 18/12/2014, đánh giá khả năng của lực lượng an ninh mạng và định hướng chiến lược phát triển toàn diện lực lượng an ninh mạng, trong đó chú trọng đào tạo phát triển nguồn nhân lực trong lĩnh vực an ninh mạng.

**(2)** *Đạo luật Tăng cường An ninh Mạng năm 2014*, ban hành ngày 18/12/2014, quy định việc hợp tác giữa nhà nước và tư nhân trong lĩnh vực an ninh mạng nhằm giảm thiểu các nguy cơ đe dọa an ninh mạng và tăng cường khả năng ứng phó với các sự cố mạng; đào tạo và phát triển nguồn nhân lực đáp ứng yêu cầu đảm bảo an ninh và ổn định trên không gian mạng.

**(3)** *Đạo luật Bảo vệ An ninh mạng Quốc gia 2014***,** ban hành ngày 18/12/2014, bổ sung cho Bộ luật An ninh nội địa Mỹ 2002, luật hóa hoạt động của Trung tâm Hội nhập Truyền thông và An ninh mạng Quốc gia (một đơn vị tác chiến mạng của Mỹ) trong đó có hoạt động chia sẻ thông tin, tác chiến mạng, hỗ trợ kỹ thuật, tìm ra nguyên nhân, giảm thiểu tác hại, khắc phục hậu quả và tăng cường bảo vệ các hệ thống thông tin chống lại các rủi ro và sự cố mạng.

**(4)** *Đạo luật hiện đại hóa An ninh Thông tin Liên bang năm 2014*,ban hành ngày 18/12/2014, đưa ra các quy định về hiện đại hóa an ninh thông tin Liên bang, bổ sung vào Bộ luật Mỹ phụ chương An ninh thông tin để xây dựng một khuôn khổ pháp lý toàn diện bảo đảm tính hiệu quả của việc kiểm soát an ninh thông tin đối với các nguồn thông tin liên quan đến hoạt động của Liên bang; quy định trách nhiệm của các cơ quan chính phủ là phải bảo đảm an ninh thông tin, ngăn chặn việc truy cập trái phép, sử dụng, tiết lộ, làm gián đoạn, biến đổi, hoặc phá hủy hệ thống thông tin và hỗ trợ các biện pháp kỹ thuật kịp thời cho người điều khiển hệ thống thông tin liên quan đến sự cố an ninh.

**(5)** *Dự luật Chia sẻ thông tin An ninh mạng năm 2015*,đệ trình ngày 15/04/2015, quy định việc tăng cường chia sẻ thông tin về các nguy cơ đe dọa an ninh mạng mà vẫn đảm bảo tính bảo mật, các quyền tự do dân sự và quyền riêng tư; chia sẻ các biện pháp phòng thủ và các chỉ báo về nguy cơ đe dọa an ninh mạng như các cuộc tấn công, chiếm đoạt thông tin hay rò rỉ dữ liệu trên mạng liên quan tới tất cả các lĩnh vực trong đời sống xã hội.

**(6)** *Dự luật Tăng cường Bảo vệ An ninh mạng Quốc gia năm 2015*, đệ trình ngày 23/04/2015, bổ sung cho Bộ luật An ninh nội địa Mỹ 2002, tăng cường sự chia sẻ thông tin theo nhiều hướng liên quan đến các mối đe dọa an ninh mạng như quy định về quy trình và cấu trúc chia sẻ thông tin, hoạt động của Trung tâm Hội nhập Truyền thông và An ninh mạng Quốc gia Mỹ và các tổ chức phân tích và chia sẻ thông tin khác. Dự luật cũng đưa racác kế hoạch ứng phó với sự cố mạng bất ngờ, chiến dịch nâng cao nhận thức về an ninh mạng và phát triển các hệ thống bảo vệ cơ sở hạ tầng trọng yếu của quốc gia*.*

**- Trung Quốc** xây dựng dự thảo **Luật An ninh mạng** với mục đích bảo đảm an ninh mạng, duy trì chủ quyền không gian mạng, an ninh quốc gia và lợi ích chung của Trung Quốc. Dự thảo gồm 7 chương với 68 điều phân định rõ trách nhiệm của các Bộ, ngành chức năng của Trung Quốc trong việc điều phối tổng thể công tác an ninh mạng và công tác quản lý giám sát liên quan đến an ninh mạng; quy định các nội dung bảo vệ thông tin cá nhân của người sử dụng Internet, mở rộng quyền lực của chính phủ Trung Quốc trong việc tiếp cận, thu giữ hồ sơ dữ liệu và ngăn chặn sự phát tán các thông tin cá nhân bị coi là bất hợp pháp; quy định trách nhiệm của người sử dụng Internet là phải khai báo tên thật khi tham gia các hoạt động trên không gian mạng; các nhà cung cấp dịch vụ Internet phải lưu trữ dữ liệu thu thập được trong phạm vi lãnh thổ Trung Quốc, cung cấp hoặc lưu trữ dữ liệu ở nước ngoài để phục vụ mục đích kinh doanh phải thông qua biện pháp đánh giá an ninh của Chính phủ Trung Quốc; các cơ quan chức năng Trung Quốc sẽ đưa ra hướng dẫn về an ninh mạng trong các lĩnh vực trọng yếu như: viễn thông, phát thanh truyền hình, năng lượng, giao thông, thủy lợi, tài chính. Đặc biệt, Văn phòng Thông tin mạng Trung Quốc có thẩm quyền đưa ra các quy định cụ thể nhằm theo dõi mọi hoạt động về mạng trên mọi lĩnh vực. Đối với các thiết bị mạng, phải đáp ứng các tiêu chuẩn do Chính phủ Trung Quốc quy định; yêu cầu các nhà kinh doanh mạng Internet phải tiến hành những biện pháp cần thiết để khắc phục các lỗ hổng an ninh, kịp thời xử lý nhằm ngăn chặn nguy cơ tấn công mạng; các nhà cung cấp dịch vụ Internet phải ký thỏa thuận bảo mật an ninh với cơ quan quản lý và ký thỏa thuận hoặc ký xác nhận với người dùng khi cung cấp dịch vụ, đánh giá các rủi ro an ninh ít nhất 01 năm/lần; cho phép tạm thời hạn chế việc truy cập Internet tại một số khu vực nhưng không định nghĩa rõ về “mối đe dọa an ninh”.

- **Nigeria** đã ban hành **Đạo luật An ninh mạng**, quy định các vấn đề về cơ sở hạ tầng thông tin trọng yếu quốc gia; nêu rõ, bất kỳ hệ thống, tài sản thông tin nào mà việc phá hủy nó dẫn đến hệ quả suy yếu an ninh quốc gia, ổn định kinh tế, an toàn và sức khỏe cộng đồng đều là cơ sở hạ tầng thông tin trọng yếu quốc gia và cần bảo vệ. Theo đó, hệ thống máy tính hoặc các mạng lưới (có thể là vật lý hay ảo), các chương trình máy tính, dữ liệu máy tính hoặc dữ liệu lưu lượng truy cập quan trọng đối với Nigeria đều là khách thể bảo vệ của Đạo luật; quy định những hành vi phạm tội cụ thể cùng chế tài đi kèm; quy định trách nhiệm cụ thể của tổ chức Tài chính, nhà cung cấp dịch vụ; chỉ định Văn phòng Cố vấn An ninh Quốc gia Nigeria là cơ quan chịu trách nhiệm chính trong việc điều phối và thực thi Đạo luật; thành lập một Hội đồng Tư vấn về tội phạm mạngbao gồm các thành viên là đại diện của một số Bộ ngành và cơ quan chính phủ; Quỹ An ninh mạng quốc gia; quy định một số trình tự, thủ tục Tố tụng như bắt giam, khám xét, tạm giữ, khởi tố...; đồng thời, cũng đề cập đến một số quy định hợp tác quốc tế trong xử lý các vấn đề liên quan đến tội phạm mạng.

**- EU**: Ngày 7/12/2015, Hội đồng và Nghị viện Châu Âu đã ban hành **Chỉ thị An ninh thông tin và mạng** nhằm tăng cường các khả năng an ninh mạng của các quốc gia thành viên, tăng cường sự hợp tác của các quốc gia thành viên trong lĩnh vực an ninh mạng, yêu cầu các nhà cung cấp dịch vụ quan trọng trong các lĩnh vực năng lực, vận tải, ngân hàng và y tế, cùng với các nhà cung cấp các dịch vụ kỹ thuật số cốt yếu khác như điện toán đám mây và công cụ tìm kiếm thực hiện các biện pháp an ninh phù hợp và báo cáo các sự cố cho các nhà chức trách.

\* Tình hình an an ninh mạng trong nước và thế giới đang diễn biến phức tạp, cấp thiết phải có một văn bản luật chuyên ngành để điều chỉnh

*- Chiến tranh mạng đã cận kề, trở thành nguy cơ đối với hòa bình và an ninh thế giới; tình báo mạng, gián điệp mạng, khủng bố đang là vấn nạn đặt ra đối với nhiều quốc gia*

Năm 1957, hoảng sợ trước việc Liên Xô phóng thành công vệ tinh Sputink có khả năng phát tín hiệu radio khi bay quanh quỹ đạo trái đất, giới quân sự, khoa học Mỹ đặc biệt lo ngại việc Liên Xô tấn công hủy diệt toàn bộ hệ thống truyền dẫn viễn thông. Để đối phó với điều này, họ nghiên cứu trong nhiều năm và năm 1969 cho ARPAnet ra đời. Đây là hệ thống mạng được coi là tiền thân của Internet, được coi là vũ khí để chống lại hoạt động của Liên Xô. Ngày nay, với nhiều lợi ích mang lại, nhiều người đã quên và thậm chí không biết rằng, Internet khởi nguồn là một thứ vũ khí quân sự và hiện nay, nó vẫn là một thứ vũ khí quân sự.

Chiến tranh mạng là có thể được hiểu theo nghĩa rộng và nghĩa hẹp. Theo nghĩa rộng là việc sử dụng thông tin trên mạng để đạt được mục đích quốc gia, theo nghĩa hẹp là sự đối kháng giữa các hệ thống thông tin quân sự. Với các quốc gia có lợi ích toàn cầu như Nga, Mỹ, Trung Quốc… chiến tranh mạng luôn được hiểu theo nghĩa rộng và các quốc gia khác trên thế giới cũng bắt đầu tính toán đến việc đó. Chiến tranh mạng là hình thái chiến tranh mới, vượt khỏi khuôn khổ khái niệm về chiến tranh quân sự truyền thống. Nếu không được quy phạm và bắt tay vào công cuộc chuẩn bị ngay từ bây giờ, với hệ thống thông tin ăn sâu vào mọi lĩnh vực của đời sống xã hội như hiện nay, chỉ cần một cú nhấp chuột, chiến tranh mạng có thể khiến hạ tầng quốc gia (*hệ thống thông tin, liên lạc, quân sự, điện, tài chính, nước, giao thông…*) bị phá hủy, gây tổn thất về nhân mạng, thiệt hại gây ra có thể nặng nề hơn nhiều so với vũ khí quân sự thông thường.

Nhiều quốc gia trên thế giới đã mặc nhiên thừa nhận sự tồn tại của hoạt động tình báo mạng, gián điệp mạng. Nhiều đơn vị tình báo mạng của Trung Quốc đã bị các công ty bảo mật vạch trần như 61398, 61478… Edward Snowden đã khiến thế giới bàng hoàng khi công bố hoạt động tình báo mạng, gián điệp mạng của Cơ quan An ninh Quốc gia Mỹ (NSA), Cơ quan Tình báo Trung ương Mỹ (CIA). Từ góc độ an ninh quốc gia của Việt Nam, không gian mạng đã tạo nên những thay đổi căn bản trong hoạt động tình báo, gián điệp của cơ quan đặc biệt nước ngoài, hình thành nên phương thức gián điệp mới - gián điệp mạng. Phương thức này khác về bản chất so với việc sử dụng các phương tiện kỹ thuật phục vụ hoạt động gián điệp dù các phương tiện này có thể được sử dụng trong hầu hết các mặt, các khâu của hoạt động gián điệp. Bởi, không gian mạng là không gian xã hội, nơi con người có thể tương tác trực tiếp với nhau một cách tức thời cũng như thực hiện được các hành vi xã hội như giao tiếp, hội họp, học tập, lao động, sáng tạo… như ngoài đời thực. Qua thực hiện Kế hoạch kiểm tra, đánh giá an toàn, an ninh thông tin tại 26 bộ, ngành, địa phương, Tổ công tác liên ngành của Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông đã phát hiện nhiều thông tin, dữ liệu là bí mật nhà nước bị đánh cắp, chiếm đoạt.

Hiện nay, khủng bố mạng nổi lên như một thách thức toàn cầu, diễn ra theo ba hình thức chủ yếu: (1)tấn công hệ thống mạng thông tin nhằm mục đích khủng bố; (2)sử dụng không gian mạng tài trợ, tuyên truyền, lôi kéo, tuyển mộ, đào tạo, huấn luyện lực lượng để thực hiện hành vi khủng bố; (3)tán phát thông tin lên mạng nhằm khủng bố tinh thần. Mỹ đã sử dụng mã độc Stuxnet tấn công các hệ thống điều khiển giám sát và thu thập dữ liệu (SCADA), gây đình trệ hoạt động, phá hủy hàng nghìn máy làm giàu uranium của nhà máy điện hạt nhân Busher của Iran, vụ việc này được đánh giá là đã làm chậm chương trình hạt nhân của Iran từ 2 - 5 năm. Biến thể của Stuxnet được cho là đã xâm nhập hệ thống điều khiển, kích nổ các tên lửa đạn đạo, phá hủy kho chứa tên lửa đạn đạo Sejil - 2 tại căn cứ quân sự của lực lượng Vệ binh cách mạng hồi giáo Iran vào ngày 12/11/2011, làm 17 chuyên gia, trong đó có thiếu tướng Hassan Moghaddam thiệt mạng. Tháng 10/2011, hai vệ tinh khí tượng của Mỹ bị tin tặc xâm nhập, khống chế nhưng rất may chưa bị phá hủy. Tháng 12/2011 và tháng 12/2012, bằng tấn công mạng, Iran đã kiểm soát hành trình và lần lượt bắt giữ 02 máy bay do thám tàng hình không người lái RQ-170 Sentinel và Scan Eagle của Mỹ ngay khi vừa xâm nhập không phận Iran. Tháng 7/2015, tin tặc kiểm soát hệ thống tên lửa phòng không Patriot của Đức đặt tại Thổ Nhĩ Kỳ, gần biên giới với Syria, “ép” hệ thống này thực hiện một số mệnh lệnh và khiến sĩ quan chỉ huy không thể điều khiển được, rất may tin tặc không có ý định sử dụng hệ thống này để tấn công quân đồng minh. Thực tế, không gian mạng đã trở thành môi trường cho các tổ chức khủng bố quốc tế hoạt động tuyên truyền, tuyển lựa, huấn luyện và chỉ đạo hoạt động như Al-Qaeda, Tổ chức Nhà nước Hồi giáo tự xưng (IS). Tại Việt Nam, mỗi năm có hàng nghìn cổng thông tin điện tử bị tấn công phá hoại. Cơ quan chức năng của Bộ Công an đã phát hiện và đấu tranh với hoạt động của một số tổ chức PĐLV sử dụng không gian mạng chỉ đạo đối tượng trong nước thực hiện hành vi khủng bố. Tháng 11/2015, nhóm tin tặc “New King Team”, gồm các đối tượng là học sinh ở Đắk Lắk, Bình Định, Bà Rịa - Vũng Tàu đã chiếm dụng trái phép tài khoản facebook “Timz Zhunusov”, thay đổi ảnh đại diện (avatar), đăng tải thông tin có nội dung kích động IS tấn công khủng bố Việt Nam.

*- Hoạt động xâm phạm an ninh quốc gia trên không gian mạng đang diễn biến phức tạp*

Với đặc tính “không biên giới”, Internet đã và đang được Mỹ và các nước phương Tây triệt để sử dụng nhằm tác động, chuyển hóa thể chế chính trị của các quốc gia trên thế giới dưới chiêu bài tự do, dân chủ, nhân quyền. Các thế lực thù địch, phản động chống Việt Nam hiện nay đang triệt để sử dụng Internet, ráo riết thực hiện âm mưu “diễn biến hoà bình”, tuyên truyền phá hoại tư tưởng, mưu toan tiến hành “cách mạng màu” nhằm xóa bỏ vị trí, vai trò lãnh đạo của Đảng Cộng sản Việt Nam, xóa bỏ chế độ XHCN ở Việt Nam.

Nhiều hình thức chống phá trên Internet mới được các thế lực thù địch, phản động sử dụng như: phát động các chiến dịch chống phá, tổ chức các cuộc thi, thành lập các đài phát thanh, hệ thống liên lạc và các phần mềm chuyên dụng để tuyên truyền chống Việt Nam. Việc tập hợp lực lượng, tài trợ tiền, tổ chức đào tạo lực lượng trong nước phục vụ cho các hoạt động chống phá được thực hiện ngay trên Internet. Việc vận động chính quyền các nước phương Tây can thiệp, gây sức ép với Việt Nam về dân chủ, nhân quyền trở nên dễ dàng, nhanh chóng và hiệu quả hơn trước đây. Đáng chú ý là, các tổ chức phản động tăng cường đầu tư công nghệ, hạ tầng thông tin, trang thiết bị, nhân lực và thông qua sự viện trợ, hậu thuẫn của các quốc gia, tổ chức đối lập để tiến hành chống phá. Theo thống kê của cơ quan chức năng Bộ Công an, từ năm 2012 đến nay, các đối tượng đã sử dụng hơn 500 trang mạng, blog, hàng nghìn chuyên trang trên mạng xã hội đăng tải hàng chục nghìn bài viết có nội dung chống Đảng, Nhà nước; kích động 55 đợt tụ tập, biểu tình tại 19 địa phương trong cả nước; thành lập 29 “hội”, “nhóm” trá hình hoạt động xâm phạm ANQG, gây mất ổn định chính trị.

*- Tội phạm sử dụng công nghệ cao diễn biến hết sức phức tạp và gia tăng với mức độ ngày càng nghiêm trọng*

Theo báo cáo của tổ chức Cảnh sát Hình sự quốc tế (Interpol), tội phạm sử dụng công nghệ cao đang trở thành mối nguy hại lớn trên thế giới với thiệt hại mỗi năm khoảng 400 tỷ USD, 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 và đang trở thành mối quan tâm chung của nhiều quốc gia. Trong những năm qua, tại Việt Nam, tình trạng tội phạm sử dụng công nghệ thông tin, truyền thông để hoạt động phạm tội diễn biến rất phức tạp, gia tăng cả về số vụ, tính chất, mức độ nghiêm trọng, với các hành vi như: trộm cắp, làm giả thẻ tín dụng, lừa đảo, tống tiền, rửa tiền, kinh doanh trái phép, đánh bạc, cá độ bóng đá, trộm cắp, gian lận cước viễn thông, làm giả bằng cấp, mại dâm, buôn bán hàng cấm, phát tán văn hóa phẩm đồi trụy, xâm phạm an toàn mạng máy tính, hệ thống tài chính ngân hàng, thương mại điện tử, viễn thông. Tội phạm sử dụng công nghệ cao xảy ra trên tất cả các lĩnh vực của đời sống xã hội, tập trung chủ yếu tại các thành phố lớn và đang có xu hướng lan rộng ra các tỉnh, thành phố trên toàn quốc, với phương thức, thủ đoạn phạm tội ngày càng tinh vi, kín đáo và có sự thay đổi liên tục nhằm tránh sự phát hiện của các cơ quan chức năng. Từ năm 2004 đến giữa năm 2019, lực lượng Công an toàn quốc đã phát hiện, xử lý gần 1.300 vụ tội phạm sử dụng công nghệ cao và các hành vi phạm pháp luật khác trên lĩnh vực viễn thông, Internet; tiến hành bắt giữ, xử lý 1.110 đối tượng liên quan, trong đó có hơn 600 đối tượng người nước ngoài.

*- Các nguy cơ đối với an ninh quốc gia, đời sống xã hội liên tục xuất hiện trên không gian mạng*

Theo báo cáo của các hãng bảo mật trên thế giới, Việt Nam là một trong 5 nước đứng đầu thế giới về tỉ lệ tán phát thư rác, xếp thứ 12 thế giới về mức độ đe dọa bị tấn công bằng mã độc, xếp thứ 33 thế giới về hệ thống máy chủ bị lợi dụng lừa đảo trực tuyến, xếp thứ 45 thế giới về mức độ đe dọa máy tính bị nhiễm phần mềm điều khiển của tin tặc. Hoạt động tấn công mạng thông tin Việt Nam đang diễn ra nghiêm trọng, hàng nghìn trang mạng bị tin tặc tấn công, chỉnh sửa, chèn thêm nội dung, cài mã độc mỗi năm, trong đó có hàng trăm trang tên miền .gov.vn của các cơ quan Nhà nước. Theo thống kê của cơ quan chức năng Bộ Công an, từ năm 2010 đến nay, đã có hơn 18.000 trang mạng tên miền .vn bị tin tặc tấn công, chỉnh sửa, chèn thêm nội dung (chiếm 3.72 % tổng số tên miền .vn cả nước), trong đó có 1.083 trang tên miền .gov.vn của các cơ quan Nhà nước (chiếm 44.07% tổng số tên miền .gov.vn cả nước). Từ năm 2010 đến nay, Bộ Công an đã phát hiện 172 vụ lộ, lọt bí mật nhà nước trên Internet, trong đó có nhiều tài liệu có đóng dấu “Tuyệt mật”, “Tối mật”, “Mật”, tài liệu nội bộ, tài liệu không đăng công báo của các Bộ, ngành, địa phương.

*- Hệ thống mạng thông tin Việt Nam phát triển nhanh nhưng không đáp ứng được yêu cầu bảo đảm an ninh mạng*

|  |
| --- |
| Tại Việt Nam, Internet chính thức xuất hiện từ năm 1997 và phát triển nhanh chóng, ngày càng thâm nhập sâu rộng vào mọi mặt đời sống xã hội, đóng góp quan trọng vào các thành tựu phát triển KT-XH, văn hóa, giáo dục, QP-AN... Việt Nam đứng thứ 3 Đông Nam Á; đứng thứ 8 Châu Á và đứng thứ 17 thế giới về số lượng người dùng Internet. Theo thống kê của Bộ Thông tin và Truyền thông, đến năm 2018 số lượng người dùng Internet tại Việt Nam có trên 55 triệu người sử dụng (tăng 15 lần so với năm 2000), đạt tỷ lệ trên 53% dân số, cao hơn mức trung bình thế giới là 46,64%; trong đó, 100% các cơ quan Trung ương, Bộ, ngành, tỉnh, thành phố trực thuộc Trung ương và các tập đoàn kinh tế xây dựng cổng/trang TTĐT và ứng dụng CNTT vào công tác quản lý, điều hành, kinh doanh, liên lạc. CNTT đã trở thành một ngành kinh tế - kỹ thuật hiện đại, tạo ra nhiều việc làm và đóng góp ngày càng lớn vào quá trình phát triển đất nước. Ứng dụng CNTT đã góp phần quan trọng cải thiện năng lực cạnh tranh của nền kinh tế; đẩy mạnh công nghiệp hóa, hiện đại hóa và hội nhập quốc tế. Tuy nhiên Việt Nam là 1 trong 8 quốc gia Châu Á đứng trước hiểm họa an ninh mạng, xếp thứ 3 sau Nga và Ấn Độ về số lượng người sử dụng thiết bị di động bị mã độc tấn công nhiều nhất thế giới, xếp thứ 4 trên thế giới với gần 50% người dùng có nguy cơ bị nhiễm mã độc khi sử dụng Internet trên máy tính, đứng thứ 6 thế giới về số lượng địa chỉ IP trong nước được dùng trong các mạng máy tính ma (botnet) tấn công nước khác, đứng thứ 12 thế giới về các hoạt động tấn công mạng và tiếp tục nằm trong danh sách các quốc gia đứng đầu thế giới về tỷ lệ phát tán thư rác. Đáng chú ý, các cuộc tấn công bằng mã độc nhằm lấy cắp tiền thông qua dịch vụ online banking ở Việt Nam vẫn tiếp tục tăng và đứng thứ 8 trên thế giới.Hệ thống mạng, cổng thông tin điện tử của các cơ quan chính phủ và doanh nghiệp của Việt Nam tiếp tục là mục tiêu tấn công chính của các nhóm tin tặc trong và ngoài nước. Trung bình mỗi tháng xuất hiện hơn 1.000 trang giả mạo Facebook đánh cắp thông tin tài khoản, lừa tiền người sử dụng, 13,9 triệu tin nhắn rác được phát tán mỗi ngày, 30% websites ngân hàng tồn tại lỗ hổng bảo mật (2/3 số này ở mức độ nguy hiểm trung bình và cao). Hoạt động tấn công bằng thư điện tử giả mạo đính kèm các loại mã độc nguy hiểm vẫn là phương thức tấn công chủ yếu của các tổ chức gián điệp mạng, trong đó nổi lên là hoạt động tấn công xâm nhập, đánh cắp thông tin của các nhóm tin tặc nước ngoài.Các dịch vụ trên Internet được sử dụng phổ biến tại Việt Nam chủ yếu là trang mạng (website), diễn đàn (forum), MXH (social network), thư điện tử (email), blog, các dịch vụ ứng dụng trên OTT, chat (Skype, Paltalk)... trong đó, MXH được sử dụng nhiều nhất, như Facbook, Twitter, Youtube, MySpace, Google Plus… Các nhà cung cấp dịch vụ tại Việt Nam cũng xây dựng, phát triển các MXH như Zalo, Zing Me, YuMe, Tamtay… đến cuối năm 2018, Zalo đã có trên 80 triệu tài khoản. Facebook và Youtube hiện là hai MXH có sức ảnh hưởng lớn nhất tại Việt Nam, số lượng người sử dụng Facebook khoảng hơn 55 triệu tài khoản, phần lớn đều dưới 34 tuổi, trung bình cứ 03 giây có 01 người Việt Nam đăng ký và tham gia Facebook; đối với Youtube có hơn 30 triệu tài khoản được sử dụng trung bình mỗi ngày có khoảng 2 tỷ lượt xem, chiếm 10% lưu lượng truyền tải qua Internet trên toàn thế giới, nghĩa là cứ 10 người truy cập Internet thì có 1 người xem video trên Youtube. Những con số trên cho thấy, khả năng phổ biến và sức lan truyền của MXH có tác động trực tiếp đến thế giới thực, CNTT và Internet góp phần tích cực làm thay đổi nhiều mặt của đời sống, xã hội. |

Tuy phát triển nhanh nhưng hệ thống mạng thông tin Việt Nam còn tồn tại nhiều bất cập về an ninh mạng. Đó là:

- Mức độ trung bình áp dụng các giải pháp bảo đảm an toàn thông tin thấp, chỉ đạt 22,42%; tỷ lệ các đơn vị nhận biết được các loại hình tấn công mạng, xâm nhập trái phép chỉ đạt trung bình 17,32%; tỷ lệ các đơn vị ban hành quy chế, về an toàn thông tin chỉ đạt 34,9%; tỷ lệ đơn vị ban hành quy trình thao tác chuẩn phản ứng xử lý sự cố máy tính: 26,2%; tỷ lệ đơn vị có cán bộ chuyên trách hoặc bán chuyên trách về an toàn thông tin: 69,6%; tỷ lệ đơn vị có kế hoạch đào tạo an toàn thông tin: 59,8%. Đây là những chỉ số cơ bản về an toàn thông tin, trong khi vấn đề an ninh mạng hầu như chưa được chú trọng.

- Các cổng thông tin điện tử, website, hệ thống mạng thông tin ở nước ta không theo một tiêu chuẩn thống nhất, thiếu sự thẩm định về an ninh thông tin, an ninh mạng; các phần mềm và thiết bị phần cứng không được nâng cấp thường xuyên, việc cập nhật vá lỗ hổng bảo mật chưa được chú trọng, tồn tại nhiều lỗi bảo mật ở mức nguy hiểm nhưng chưa được khắc phục kịp thời. Hệ thống máy chủ đặt tại nhà cung cấp dịch vụ trong dải mạng yếu, không có “tường lửa” bảo vệ hoặc có nhưng không đủ mạnh, không có biện pháp phòng chống mã độc, phòng chống tấn công mạng. Chính sách phân quyền người điều hành và quyền ứng dụng chưa được thiết lập chặt chẽ, vẫn cho phép chế độ đăng nhập tự do, không mật khẩu, mở nhiều cổng dịch vụ không cần thiết. Không có hệ thống dự phòng khi xảy ra tấn công hoặc bị lỗi phần cứng thì lúng túng, gặp khó khăn trong khắc phục. Không có hệ thống cảnh báo, phát hiện và ngăn chặn xâm nhập; hệ thống ghi nhật ký rời rạc.

- Đội ngũ quản trị viên các trang tin điện tử chưa được quan tâm bồi dưỡng chuyên môn, chế độ chính sách không thỏa đáng, chưa phát huy hết trình độ chuyên môn. Ý thức bảo vệ an ninh, an toàn thông tin khi sử dụng hệ thống máy tính của người dùng còn hạn chế, có tâm lý chủ quan trong bảo đảm an ninh thông tin, an ninh mạng. Nhiều nơi, máy tính dùng chung cho hai mục đích: soạn thảo, lưu trữ tài liệu nội bộ và kết nối Internet. Nhiều phần mềm sử dụng không có bản quyền, không được cập nhật và nâng cấp thường xuyên, thiếu biện pháp bảo vệ.

- Không kiểm tra an ninh thông tin, an ninh mạng trước khi lắp đặt và sử dụng các thiết bị và phần mềm công nghệ thông tin. Nhiều Bộ, ngành, địa phương dùng thiết bị tiềm ẩn nhiều nguy cơ mất an ninh thông tin, an ninh mạng của ZTE, Huawei.

*- Công tác quản lý nhà nước về an ninh thông tin, an ninh mạng chưa đáp ứng được yêu cầu trong tình hình mới*

Trước sự phát triển nhanh, mạnh của công nghệ thông tin và tình hình an ninh thông tin, an ninh mạng, việc ứng dụng công nghệ thông tin vào phát triển kinh tế, xã hội, nhiều cơ quan, doanh nghiệp mới chỉ dừng lại ở lợi ích kinh tế, xem nhẹ vấn đề bảo đảm an ninh thông tin, an ninh mạng, chưa ban hành các quy định chặt chẽ về công tác bảo đảm an ninh thông tin, an ninh mạng khi sử dụng máy tính và mạng máy tính, dẫn tới việc vi phạm các nguyên tắc bảo đảm an ninh thông tin, an ninh mạng. Trong khi đó, ý thức bảo vệ an ninh thông tin, an ninh mạng khi sử dụng hệ thống máy tính của người dùng còn hạn chế.

Về nguồn nhân lực, đội ngũ cán bộ làm công tác quản lý nhà nước về an ninh thông tin vừa thiếu lại vừa yếu. Công tác đào tạo nguồn nhân lực có trình độ cao về an ninh thông tin, an ninh mạng chưa theo kịp yêu cầu hiện nay, cả về số lượng và chất lượng.

Về công nghệ, kỹ thuật phục vụ công tác quản lý nhà nước về an ninh thông tin, an ninh mạng, hệ thống mạng thông tin của Việt Nam sử dụng công nghệ không đồng bộ. Việc triển khai hệ thống thông tin, các thiết bị phần cứng chưa bảo đảm an toàn, tồn tại nhiều nguy cơ mất an ninh thông tin, an ninh mạng khi sử dụng các thiết bị nhập khẩu từ nước ngoài, đặc biệt là Trung Quốc. Các nhà cung cấp dịch vụ ở Việt Nam chưa có công nghệ nguồn, còn phụ thuộc nhiều vào công nghệ của nước ngoài. Chưa ban hành được tiêu chuẩn thống nhất về an ninh thông tin, an ninh mạng trong việc xây dựng các cổng thông tin điện tử, website, hệ thống mạng thông tin ở nước ta. Sự phát triển của các thiết bị di động cầm tay có kết nối mạng đang đặt ra nhiều thách thức đối với công tác quản lý.

***Những năm gần đây, công tác quản lý nhà nước đối với các loại hình dịch vụ viễn thông, internet đã đạt được những kết quả thiết thực góp phần bảo vệ an ninh quốc gia:***

*- Hoạt động cung cấp, sử dụng dịch vụ viễn thông, internet của các doanh nghiệp cung cấp dịch vụ và một số cơ sở hoạt động kinh doanh dịch vụ viễn thông, internet tại Việt Nam được từng bước quản lý chặt chẽ*, đã phát hiện, xử lý hàng trăm trang web có tên miền, máy chủ tại Việt Nam đăng tải thông tin vi phạm pháp luật. Công tác kiểm tra, ngăn chặn thông tin xấu, độc hại, phản động trên mạng đã được tăng cường và thực hiện tương đối hiệu quả, duy trì ngăn chặn khoảng 2.700 trang web, blog, địa chỉ mạng xã hội có nội dung xấu, phản động và những từ khóa SMS nhạy cảm.

*- Công tác quản lý nhà nước đối với báo điện tử, mạng xã hội trong nước được Bộ Thông tin và Truyền thông cấp phép đã được tăng cường*, chủ động xác minh và xử lý sai phạm của hàng chục trang mạng xã hội trong nước có hành vi vi phạm pháp luật, đăng tải tài liệu có nội dung phản động, yêu cầu gỡ bỏ thông tin xấu, thiết lập cơ chế kiểm duyệt thông tin hoặc dừng hoạt động trang mạng. Kiên quyết xử lý sai phạm, hoạt động vi phạm pháp luật của một số báo, đài truyền hình.

*- Bước đầu thực hiện quản lý nhà nước đối với trò chơi trực tuyến*, trong đó thực hiện nghiêm bước thẩm định nội dung, kịch bản các trò chơi trước khi cấp phép hoạt động theo quy định của Thông tư số 24/2014/TT-BTTTT ngày 29/12/2014 của Bộ Thông tin và Truyền thông quy định chi tiết về hoạt động quản lý, cung cấp và sử dụng dịch vụ trò chơi điện tử trên mạng.

*- Hoạt động quản lý “SIM rác” được tăng cường*, trong đợt kiểm tra thu hồi SIM kích hoạt sẵn đăng ký sai thông tin thuê bao được Bộ Thông tin và Truyền thông cùng các nhà mạng triển khai vào cuối năm 2016, đã có khoảng 10,7 triệu thuê bao bị thu hồi và khóa SIM.

***Tuy nhiên, công tác quản lý nhà nước về an ninh mạng trên một số mặt chưa đáp ứng yêu cầu:***

*- Công tác quản lý nhà nước đối với báo chí điện tử, mạng xã hội chưa chặt chẽ.* Hoạt động của báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên không gian mạng ngày càng phong phú, đa dạng, phức tạp, trong khi công tác quản lý còn bất cập. Một số báo chí điện tử đưa tin thiếu chính xác, sa vào thông tin giật gân, câu khách. Các trang thông tin điện tử hoạt động có xu hướng chiếm ưu thế về nguồn phát thông tin và thực chất nhiều trang hoạt động như cơ quan báo chí nhưng chưa được quản lý chặt chẽ. Bên cạnh đó, mạng xã hội, blog và các loại hình truyền thông khác đang trở thành công cụ đắc lực cho hoạt động chống phá của các đối tượng thù địch trong và ngoài nước nhưng không có biện pháp quản lý hữu hiệu.

*- Công tác quản lý nhà nước đối với các dịch vụ qua biên giới còn nhiều sơ hở.* Chưa có quy định quản lý phù hợp với tình hình thực tiễn đối với các doanh nghiệp cung cấp dịch vụ qua biên giới vào Việt Nam. Công tác thanh tra, kiểm tra và xử lý sai phạm còn hạn chế, chế tài xử lý chưa đủ mạnh, chưa đạt được hiệu quả răn đe cần thiết, năng lực kỹ thuật xử lý, ngăn chặn thông tin sai phạm từ các máy chủ đặt tại nước ngoài phát tán vào Việt Nam còn nhiều bất cập.

*- Tính pháp lý và hiệu lực thi hành của các văn bản quy phạm pháp luật đã ban hành về quản lý, cung cấp dịch vụ, bảo đảm an ninh mạng còn chưa cao, tồn tại nhiều sơ hở để kẻ địch lợi dụng hoạt động xâm phạm an ninh quốc gia*. Một số văn bản quy phạm pháp luật ban hành nhưng chậm triển khai thực hiện, nhiều nội dung lạc hậu so với tình hình mới. Phân công, phân cấp quản lý nhà nước trên lĩnh vực viễn thông, Internet giữa một số bộ, ngành chức năng còn chồng chéo, chưa thống nhất.

***\**** Ở nước ta, ứng dụng và phát triển mạnh mẽ công nghệ thông tin trong các lĩnh vực của đời sống đã góp phần to lớn đẩy nhanh quá trình công nghiệp hóa, hiện đại hóa đất nước, phát triển kinh tế, văn hóa, xã hội, nâng cao chất lượng y tế, giáo dục, phát huy sức sáng tạo và quyền làm chủ của nhân dân, giữ vững an ninh, quốc phòng. Tuy nhiên, vẫn còn những tồn tại, hạn chế về an ninh mạng như sau:

(1) Tiềm lực quốc gia về an ninh mạng của nước ta chưa đủ mạnh, chưa huy động, khai thác được sức mạnh tổng hợp để đối phó với các mối đe dọa trên không gian mạng[[3]](#footnote-3).

(2) Không gian mạng và một số loại hình dịch vụ, ứng dụng đang bị các thế lực thù địch, phản động sử dụng thực hiện âm mưu tiến hành “cách mạng màu”, “cách mạng đường phố”, “diễn biến hòa bình” nhằm xóa bỏ chế độ chính trị ở nước ta. Tình trạng đăng tải thông tin sai sự thật, làm nhục, vu khống tổ chức, cá nhân tràn lan trên không gian mạng nhưng chưa có biện pháp quản lý hữu hiệu, dẫn tới nhiều hậu quả đáng tiếc về nhân mạng, tinh thần, thậm chí ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự an toàn xã hội.

(3) Ngày càng xuất hiện nhiều cuộc tấn công mạng với quy mô lớn, cường độ cao, gia tăng về tính chất nghiêm trọng, mức độ nguy hiểm đe dọa trực tiếp đến an ninh quốc gia và trật tự an toàn xã hội[[4]](#footnote-4). Khủng bố mạng nổi lên như một thách thức đe dọa nghiêm trọng tới an ninh quốc gia. Hoạt động phạm tội trên không gian mạng ngày càng gia tăng về số vụ, thủ đoạn tinh vi gây thiệt hại nghiêm trọng về kinh tế, ảnh hưởng đến tư tưởng, văn hóa, xã hội.

(4) Dữ liệu quốc gia trên không gian mạng chưa được xác định, bảo vệ đúng mức và đang bị tình trạng chiếm đoạt, sử dụng, lạm dụng vào các hoạt động kinh tế, chính trị, thậm chí là hành vi phạm tội[[5]](#footnote-5).

(5) Hệ thống thông tin quan trọng về an ninh quốc gia chưa được xác định và bảo vệ bằng các biện pháp tương xứng[[6]](#footnote-6).

(6) Tình hình lộ, lọt bí mật nhà nước qua không gian mạng rất đáng lo ngại, nhiều văn bản thuộc bí mật nhà nước bị đăng tải trên không gian mạng[[7]](#footnote-7).

(7) Sự phụ thuộc vào thiết bị công nghệ thông tin có nguồn gốc nước ngoài[[8]](#footnote-8).

(8) Hệ thống văn bảnquy phạm pháp luật về an ninh mạng chưa được xây dựng, các văn bản hiện hành chưa đáp ứng được yêu cầu phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng vi phạm pháp luật[[9]](#footnote-9).

Trong những năm qua, nước ta đã ban hành nhiều văn bản quy phạm pháp luật liên quan đến lĩnh vực công nghệ thông tin, viễn thông, Internet. Tuy nhiên, đến nay chưa có văn bản quy phạm pháp luật về an ninh thông tin, an ninh mạng (gồm cả Luật, Nghị định, Thông tư); chưa có quy định để điều chỉnh các vấn đề, nội dung an ninh thông tin, an ninh mạng mới phát sinh, đặc biệt là những quy định về những hành vi phạm tội liên quan đến lĩnh vực viễn thông, Internet như: gián điệp mạng, tình báo mạng, khủng bố mạng, chiến tranh mạng, bảo đảm an ninh quốc gia trên không gian mạng; một số quy định còn chưa nhất quán, thiếu tính khả thi; các quy định về chế tài chưa đủ sức răn đe, không đáp ứng được yêu cầu thực tiễn của công tác an ninh đặt ra trong tình hình mới, gây khó khăn, vướng mắc trong tổ chức, triển khai các phương án bảo đảm an ninh thông tin, an ninh mạng cũng như trong công tác phòng ngừa, đấu tranh ngăn chặn các hoạt động lợi dụng Internet để xâm phạm an ninh quốc gia, trật tự an toàn xã hội. Trước yêu cầu bức thiết hiện nay, việc xây dựng một văn bản Luật để điều chỉnh toàn hiện hoạt động an ninh mạng là phù hợp với sự phát triển của đất nước và yêu cầu của công tác bảo vệ an ninh quốc gia.

Tuy ngày 19/11/2015, Chủ tịch Quốc hội Nguyễn Sinh Hùng đã ký ban hành Luật An toàn thông tin mạng (số 86/2015/QH13), chính thức có hiệu lực thi hành kể từ ngày 01/7/2016 nhưng nội dung của Luật An toàn thông tin mạng không quy phạm những nội dung liên quan an ninh mạng. An toàn thông tin là điều kiện cơ bản để bảo đảm an ninh mạng, là một trong những nội dung của an ninh mạng. Không thể dùng các quy phạm về an toàn để áp dụng cho công tác an ninh. Trong khi đó, Luật An toàn thông tin mạng chỉquy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng. Luật An ninh quy định về hoạt động an ninh mạng; quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an ninh mạng; quản lý nhà nước về an ninh quốc gia trên lĩnh vực viễn thông, Internet; đấu tranh với hoạt động xâm phạm an ninh quốc gia trên không gian mạng; đảm bảo an ninh hệ thống mạng thông tin quốc gia; xây dựng các văn bản quy phạm pháp luật, quy định, quy chuẩn về bảo đảm an ninh mạng thông tin quốc gia; phát hiện, kiến nghị xử lý các tổ chức, cá nhân có hành vi vi phạm pháp luật trên lĩnh vực an ninh mạng; phát hiện, ngăn chặn, đấu tranh vô hiệu hóa hoạt động xâm nhập mạng thông tin; bảo vệ bí mật nhà nước trên mạng máy tính...

**Thực trạng trên đã đặt đất nước ta trước những nguy cơ sau:**

**Một là**, an ninh quốc gia bị đe dọa khi sự phát triển của mạng xã hội cũng tạo môi trường thuận lợi cho các hoạt động tác động, chuyển hóa chính trị, khủng bố ở nhiều quốc gia và vùng lãnh thổ.

**Hai là**, mất kiểm soát trên không gian mạng khi sự phát triển của trí tuệ nhân tạo đã và đang tạo ra những thành tựu khoa học công nghệ vượt trội, đóng vai trò ngày càng quan trọng trong nhiều lĩnh vực của đời sống xã hội nhưng cũng được dự báo sẽ gây nên “thảm họa” nếu không được kiểm soát chặt chẽ.

**Ba là**, đối mặt với các cuộc tấn công mạng quy mô lớn, gây thiệt hại nghiêm trọng khi các thiết bị kết nối internet ngày càng phổ biến không chỉ mang lại những lợi ích to lớn cho cuộc sống con người, phát triển kinh tế - xã hội, bảo đảm quốc phòng - an ninh mà còn có thể bị sử dụng để tiến hành các cuộc tấn công mạng quy mô lớn.

**Bốn là**, các hệ thống thông tin quan trọng về an ninh quốc gia bị tấn công, phá hủy, gây đình trệ hoạt động của một hoặc nhiều lĩnh vực trọng yếu của đất nước. Các cuộc tấn công mạng có chủ đích (Advanced Peristent Threat - APT) không chỉ có thể phá hoại các mục tiêu, công trình quan trọng về an ninh quốc gia mà còn chiếm đoạt thông tin, tài liệu bí mật, chiếm đoạt để sử dụng các hệ thống dữ liệu lớn, dữ liệu nhanh phục vụ ý đồ chính trị và hoạt động phạm tội.

Thực trạng, nguy cơ trên đã đặt ra yêu cầu bức thiết phải xây dựng và ban hành văn bản luật về an ninh mạng để phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

**2. Hoạt động sử dụng không gian mạng và công nghệ cao xâm phạm trật tự, an toàn xã hội**

Những năm gần đây, tội phạm sử dụng công nghệ cao gia tăng với mức độ ngày càng nghiêm trọng,tại Việt Nam, tình trạng tội phạm sử dụng công nghệ thông tin, truyền thông để hoạt động phạm tội diễn biến rất phức tạp, gia tăng cả về số vụ, tính chất, mức độ nghiêm trọng, với các hành vi như: trộm cắp, làm giả thẻ tín dụng, lừa đảo, tống tiền, rửa tiền, kinh doanh trái phép, đánh bạc, cá độ bóng đá, trộm cắp, gian lận cước viễn thông, làm giả bằng cấp, mại dâm, buôn bán hàng cấm, phát tán văn hóa phẩm đồi trụy, xâm phạm an toàn mạng máy tính, hệ thống tài chính ngân hàng, thương mại điện tử, viễn thông. Từ năm 2006 đến nửa năm 2019, lực lượng Công an toàn quốc đã phát hiện, xử lý 1.295 vụ tội phạm sử dụng công nghệ cao và các hành vi phạm pháp luật khác trên lĩnh vực viễn thông, Internet; tiến hành bắt giữ, xử lý 1.300 đối tượng liên quan, trong đó có hơn 500 đối tượng người nước ngoài. Trong năm 2018 và 6 tháng đầu năm 2019, Bộ Công an đã phát hiện và xử lý 1.467 vụ án, vụ việc liên quan sử dụng không gian mạng thực hiện hành vi phạm tội, phá 93 chuyên án, xác minh làm rõ 540 vụ việc, vụ án, chuyển CQĐT khởi tố 252 vụ, 444 bị can.

Trung bình mỗi tháng xuất hiện hơn 1.000 trang giả mạo Facebook đánh cắp thông tin tài khoản, lừa tiền người sử dụng, 13,9 triệu tin nhắn rác được phát tán mỗi ngày, 30% websites ngân hàng tồn tại lỗ hổng bảo mật (2/3 số này ở mức độ nguy hiểm trung bình và cao). Đặc biệt, các vụ tấn công mạng thông qua thiết bị IoT liên tục diễn ra, gây thiệt hại nghiêm trọng cho nhiều quốc gia trên thế giới, đây là minh chứng rõ nét cho thấy tác động vô cùng nguy hiểm đến an ninh quốc gia của các thiết bị IoT *(Theo công ty bảo mật RiskIQ – Mỹ, cứ mỗi phút, có 2,7 triệu người trở thành nạn nhân của tin tặc và 1,1 triệu USD bị thiệt hại bởi tấn công mạng)*.

Tội phạm phát tán phần mềm có chức năng nghe lén cuộc gọi thoại, phần mềm tấn công mạng wifi, hệ thống camera… nhằm lấy cắp thông tin cá nhân và các tài khoản Email, tài khoản mạng xã hội, tài khoản ngân hàng hoặc phát tán các phần mềm trên để thu lợi bất chính diễn ra phức tạp. Tình trạng mua bán thông tin cá nhân diễn ra phổ biến, công khai trên mạng Internet tiểm ẩn nhiều nguy cơ, tạo điều kiện thuận lợi cho một số loại tội phạm gia tăng như phát tán tin nhắn rác, lừa đảo qua mạng xã hội, tội phạm trong lĩnh vực ngân hàng, tội phạm lừa đảo viễn thông…

Các đối tượng lợi dụng các dịch vụ thanh toán của ngân hàng, dịch vụ viễn thông để chiếm đoạt tài sản; thuê mở tài khoản, mua lại tài khoản ngân hàng, tài khoản thẻ, tài khoản ghi nợ quốc tế để nhận các khoản tiền do hành vi lừa đảo trên mạng, qua dịch vụ viễn thông sau đó rút chiếm đoạt tiền ở nước ngoài. Tháng 4/2018, các nhà cung cấp dịch vụ viễn thông đã dừng việc thanh toán thẻ cào điện thoại cho các dịch vụ nội dung số do nhiều bất cập khi thẻ cào được sử dụng như một phương tiện thanh toán và bị lợi dụng vào các trò chơi đánh bạc trực tuyến, quảng cáo trái phép, lừa đảo mua bán hàng hóa trên mạng… với doanh số, trị giá giao dịch lớn. Các đơn vị quản lý Nhà nước đang nghiên cứu đề xuất biện pháp quản lý cho phù hợp để các doanh nghiệp viễn thông được sử dụng thẻ cào điện thoại để thanh toán dịch vụ nội dung số.

Tình trạng trộm cắp, mua bán thông tin thẻ tín dụng để làm giả thẻ thanh toán dịch vụ mua hàng hóa tiếp tục diễn biến phức tạp, gây thiệt hại nghiêm trọng: (1) Tình trạng lắp đặt thiết bị sao chép, trộm cắp dữ liệu ngân hàng (Skiming) tại các máy ATM của các ngân hàng tại Việt Nam; (2) Tình trạng các đối tượng người nước ngoài vào Việt Nam sử dụng trái phép thông tin thẻ tín dụng móc nối với các đối tượng trong nước thực hiện các giao dịch khống qua POS để rút tiền, chiếm đoạt hàng chục tỷ đồng.

Tình trạng khách du lịch nước ngoài (chủ yếu Trung Quốc) nhập cảnh vào Việt Nam, thực hiện giao dịch bằng các thẻ nội địa do ngân hàng Trung Quốc phát hành tại máy mPOS (máy chấp nhận thanh toán thẻ không dây dùng SIM điện thoại) của Trung Quốc được chuyển trái phép vào Việt Nam, không thông qua hệ thống ngân hàng và trung gian thanh toán Việt Nam, ảnh hưởng lớn an ninh tiền tệ quốc gia, vi phạm quy định về quản lý ngoại hối của Nhà nước, không bảo vệ được người tiêu dùng và người bán hàng; thất thu thuế do các giao dịch được hoàn toàn xử lý tại Trung Quốc.

Tại nhiều địa phương tiếp tục tái diễn tình trạng các đối tượng thiết lập tổng đài viễn thông, sử dụng dịch vụ thoại trên nền Internet (VoIP) giả danh các cơ quan chức năng (bưu điện, công an, tòa án, Viện kiểm sát…) gọi điện cho người dân để lừa đảo chiếm đoạt tài sản.

Hoạt động lừa đảo chiếm đoạt tài sản trên mạng xã hội (Facebook, Zalo, Viber, Whatapp…) diễn biến phức tạp, nổi lên là tình trạng người nước ngoài câu kết với một số người Việt Nam làm quen với người bị hại, tạo lòng tin, hứa gửi tiền, quà tặng có giá trị, sau đó giả mạo nhân viên hải quan gọi điện yêu cầu nạn nhân chuyển tiền làm các thủ tục thông quan để chiếm đoạt. Tại một số địa phương hình thành các tụ điểm tội phạm sử dụng công nghệ cao chuyên lừa đảo chiếm đoạt tài sản bằng hình thức nhắn tin thông báo trúng thưởng qua mạng xã hội như một số tỉnh: Quảng Trị, Quảng Nam…

Hoạt động kinh doanh theo mô hình đa cấp dù được các cơ quan chức năng tập trung quản lý, giám sát nhưng vẫn diễn biến phức tạp. Các đối tượng lợi dụng hoạt động bán hàng đa cấp để chiếm đoạt tài sản với nhiều thủ đoạn, phương thức mới hết sức tinh vi như: (1) lập website để tổ chức huy động vốn trả lãi suất cao nhằm CĐTS; (2) lợi dụng hoạt động từ thiện để lừa đảo CĐTS; (3) lập sàn giao dịch cho - nhận tiền để lừa đảo CĐTS; (4) lập và tạo ra nhiều sàn giao dịch các loại tiền ảo hoạt động theo mô hình đa cấp như Onecoin, ILcoin, Gemcoin… để thu hút các nhà đầu tư nhằm CĐTS hoặc kinh doanh tiền ảo trái phép để rửa tiền, ship hàng, trả tiền cá độ bóng đá…; (5) các đối tượng thành lập các công ty, giả mạo các dự án công ty nước ngoài huy động vốn trả lãi suất và hoa hồng theo mô hình đa cấp để CĐTS của người tham gia.

Từ đầu năm 2018 đánh dấu sự bùng phát mạnh mẽ của tiền ảo, tiền điện tử, hoạt động huy động vốn bằng tiền điện tử (ICO)…, trên thị trường có đến hàng ngàn đồng tiền điện tử, trong đó có một số đồng tiền có vốn hóa trị trường lên đến hàng chục triệu đến hàng tỷ USD, được chấp nhận thanh toán tại một số quốc gia. Tuy nhiên hoạt động trên chưa được công nhận tại nhiều quốc gia trên thế giới, tiềm ẩn nguy cơ lớn gây ảnh hưởng về ANTT.

Các hình thức lừa đảo chiếm đoạt tài sản khác qua hoạt động thương mại điện tử tiếp tục diễn ra với phương thức, thủ đoạn như: lập các website rao bán các mặt hàng chính hãng giảm giá từ 40 - 60% nhưng gửi hàng kém chất lượng, không rõ xuất xứ, không đúng như thỏa thuận, rao bán tiền giả, các loại bằng cấp giả để chiếm đoạt tiền; hacker xâm nhập, chiếm đoạt tài khoản email của doanh nghiệp, sau đó theo dõi các giao dịch kinh doanh rồi chọn thời điểm thay đổi thông tin người nhận tiền để chiếm đoạt số tiền trong hợp đồng kinh tế do đối tác của doanh nghiệp gửi.

Truyền bá, phát tán văn hóa phẩm đồi trụy: tiếp tục diễn ra tình trạng các website, diễn đàn chia sẻ những hình ảnh, bộ phim có nội dung khiêu dâm, đồi trụy, ảnh hưởng nghiêm trọng đến thuần phong mỹ tục. Đặc biệt, tình trạng truyền bá phim ảnh khiêu dâm trẻ em đã và đang gây ra nhiều hệ lụy cho xã hội, ảnh hưởng đến sự phát triển tâm sinh lý của trẻ em, làm gia tăng tình trạng lạm dụng tình dục trẻ em hiện nay. Thông qua các trang web đen này, hacker phát tán nhiều loại mã độc, phần mềm nghe lén nhằm thu thập trái phép thông tin người dùng Internet để hoạt động phạm tội.

Tổ chức đánh bạc và đánh bạc trên mạng Internet có giảm nhưng vẫn diễn biến rất phức tạp, tiềm ẩn và diễn ra dưới những hình thức khác nhau. Các đối tượng nhà cái ở nước ngoài thường móc nối với các đối tượng trong nước (các đại lý) xây dựng các đường dây lớn tổ chức cho cả người Việt Nam và người nước ngoài.

Vi phạm bản quyền phần mềm: bản quyền nhạc số, phim số; quyền tác giả, tác phẩm và bản quyền truyền hình đang trở thành mối lo ngại lớn. Theo Liên minh phần mềm doanh nghiệp (BSA), tính tới tháng 4/2018, tỷ lệ vi phạm bản quyền ở Việt Nam là 78%, Việt Nam được coi là một quốc gia có tỷ lệ vi phạm bản quyền cao thứ hai thế giới (sau Trung Quốc). Tình trạng vi phạm bản quyền phần mềm đang làm giảm sức cạnh tranh của các nền kinh tế trong khu vực, ảnh hưởng xấu đến khả năng phát triển các sản phẩm mới, đồng thời các phần mềm không bản quyền sẽ dẫn tới nguy cơ cao bị tấn công bằng mã độc.

Tình trạng lừa đảo, chiếm đoạt tài sản, đăng tin sai sự thật thông qua trang thông tin điện tử cá nhân xảy ra thường xuyên, trong đó tập trung chủ yếu vào các hành vi như đăng tin để “câu view” nhằm mục đích kinh doanh; bán hàng đa cấp qua mạng; kinh doanh sàn vàng, huy động vốn trái phép; lừa đảo thông qua các giao dịch, bán hàng trực tuyến; trộm cắp tài khoản MXH (Facebook, Zalo,...), sau đó sử dụng để lừa đảo các nạn nhân thông qua việc nhờ nạp thẻ điện thoại, thẻ game, chuyển tiền; mạo danh cơ quan, cán bộ thực thi pháp luật gọi điện yêu cầu công dân nộp tiền để chiếm đoạt... Thời gian gần đây, một số cá nhân còn đăng tin đồn, bịa đặt gây bức xúc trong dư luận về việc bắt cóc trẻ em, người dân “đốt” xe máy, “đánh chết” kẻ trộm chó hay tung tin đồn máy bay rơi ở Nội Bài trên các trang MXH nhằm câu view, tăng lượt người theo dõi phục vụ hoạt động bán hàng trên mạng. Mặc dù, lực lượng chức năng đã kịp thời phát hiện, xử lý theo quy định của pháp luật và công bố trên các phương tiện truyền thông đại chúng để cảnh báo, răn đe nhưng hiện tượng này vẫn không có dấu hiệu suy giảm.

Tình trạng đánh bạc trực tuyến và cá độ bóng đá qua các dịch vụ của trang thông tin điện tử cá nhândiễn ra phức tạp. Các đối tượng tại Việt Nam móc nối với các đối tượng cầm đầu đường dây tổ chức đánh bạc, cá độ bóng đá trực tuyến tại nước ngoài, tổ chức đánh bạc trực tuyến dưới nhiều hình thức. Để đối phó với sự quản lý của các cơ quan chức năng, chúng liên tục lập ra hàng nghìn website, tên miền, địa chỉ IP… chủ yếu là trang thông tin điện tử cá nhân để “ẩn danh”, tránh sự truy vết của cơ quan chức năng, qua đó quảng bá, lôi kéo con bạc tham gia, khi bị lực lượng chức năng xử lý, chặn lọc thì các đối tượng lập trang mới để tiếp tục hoạt động. Trước tình hình đó, lực lượng Công an triển khai thực hiện kế hoạch nhằm triển khai các biện pháp đấu tranh phòng, chống loại tội phạm này và phát hiện, triệt phá hàng loạt các đường dây lớn chuyên tổ chức đánh bạc, cá độ bóng đá trên mạng Internet.

Trong lĩnh vực kinh doanh trò chơi trực tuyến (Game Online): Tính đến tháng 6/2019, tại Việt Nam đã có trên 300 trò chơi trực tuyến được cấp phép và đang hoạt động, tuy nhiên qua công tác nắm tình hình hiện còn hơn 100 trò chơi trực tuyến đang hoạt động trái phép, thường xuyên sử dụng trang thông tin điện tử cá nhân để quảng bá, lôi kéo người chơi gây ra những tác động tiêu cực đáng kể cho xã hội.

## 3. Tình hình an ninh mạng thế giới có tác động đến Việt Nam

|  |
| --- |
| 3.1. Tình báo, gián điệp mạng: Gián điệp mạng ngày càng chiếm vị trí quan trọng trong chính sách phát triển không gian mạng của các quốc gia**Gián điệp mạng** là phương thức gián điệp với đầy đủ các đặc điểm của phương thức gián điệp truyền thống kết hợp với đặc trưng riêng của công nghệ thông tin, truyền thông, không phụ thuộc vào không gian, địa giới hành chính, lãnh thổ. Hoạt động gián điệp mạng có độ an toàn cao, tránh được chế tài hành chính, hình sự của đối phương trong trường hợp bị phát hiện.- Hoạt động thu thập thông tin tình báo |
| **[1] TRUNG QUỐC**Tháng 5/2013, Mỹ cáo buộc Trung Quốc đánh cắp các thiết kế của hơn hai mươi loại vũ khí hiện đại của nước này, trong đó có máy bay tàng hình F-35 Joint Strike, hệ thống phòng thủ tên lửa Patriot, hệ thống phòng thủ chống tên lửa đạn đạo trang bị cho tàu chiến Aeges, máy bay không người lái Global Hawker, tầu chiến tàng hình cận bờ, máy bay F/A-18, trực thăng V-22 Osprey và Black Hawk...Các đơn vị 61398, 61478 thuộc Quân Giải phóng nhân dân Trung Quốc (PLA) bị chứng minh là đã trực tiếp thực hiện nhiều đợt tấn công APT kéo dài nhiều năm vào hàng trăm mục tiêu trên thế giới, tập trung chủ yếu vào cơ quan chính phủ, các công ty công nghệ cao và lĩnh vực năng lượng của Mỹ, chiếm đoạt hàng trăm Terabyte dữ liệu quan trọng của ít nhất 141 doanh nghiệp thuộc 20 ngành công nghiệp chính trên thế giới. Ngày 19/5/2014, Bộ Tư pháp Mỹ đã phát lệnh truy nã 05 thành viên đơn vị 61398 về hành vi gián điệp.Đầu năm 2015, Văn phòng Quản lý Nhân sự (OPM) của chính phủ Mỹ bị tin tặc (được cho là của Trung Quốc) lấy đi khoảng 20 triệu dữ liệu, bao gồm dấu vân tay và mẫu đơn khai an ninh, của các nhân viên Liên bang. Sau sự kiện này, CIA đã rút các nhân viên hoạt động ở Trung Quốc về nước.Nhiều thiết bị công nghệ của TQ, nhất là của các hãng Hauwei và ZTE bị phát hiện cài sẵn phần mềm, thiết bị gián điệp điều khiển từ xa trước khi xuất xưởng.- Điện thoại “RedMi 1S” của công ty Xiaomi bị phát hiện tự động gửi dữ liệu nhạy cảm của người sử dụng về máy chủ đặt tại TQ.- Các router sản xuất ở TQ gồm Netcore, Netis có chứa sẵn cửa hậu (backdoor) cho phép xâm nhập từ xa, bí mật theo dõi và chiếm đoạt thông tin người sử dụng.- Hãng bảo mật Kryptowire (Mỹ) phát hiện hơn **700 triệu smartphone Android** của các hãng điện thoại Trung Quốc như Huawei, ZTE,... đã bị cài sẵn phần mềm bí mật theo dõi người dùng, thậm chí còn có trường hợp cứ mỗi 72 giờ, toàn bộ tin nhắn của người dùng sẽ được gửi về máy chủ ở Trung Quốc.- Đại sứ quán Mỹ tại Afghanistan sẽ hủy bỏ cài đặt tất cả các camera giám sát của công ty Hikvision (một trong các nhà cung cấp thiết bị camera giám sát lớn nhất thế giới) được kiểm soát bởi chính phủ Trung Quốc, sau khi có thông tin camera Hikvision sẽ truyền các hình ảnh ghi lại đến Trung Quốc, chính phủ Trung Quốc có thể đăng nhập vào hệ thống camera này bất kỳ lúc nào, Hikvision còn bị cáo buộc đã cài “backdoor” trong thiết bị, cho phép các nhà sản xuất có thể giám sát từ xa.- Hai doanh nghiệp cung cấp dịch vụ chính tại Trung Quốc là China Telecom và China Unicom bị phát đã lây nhiễm nội dung độc hại vào lưu lượng mạng của người dùng truy cập một tên miền thuộc quản lý của hai doanh nghiệp trên.- Hãng công nghệ Baidu của Trung Quốc bị cáo buộc đã cố tình tạo ra các “cửa hậu” trên các bộ phát triển phần mềm Android của hãng này để thu thập dữ liệu người dùng và chuyển về máy chủ. Hãng bảo mật Citizen Lab vừa cảnh báo mất an toàn nghiêm trọng trên hàng ngàn ứng dụng Android xây dựng dựa trên mã lập trình của công ty Baidu - Trung Quốc. Những vấn đề này ảnh hưởng tới trình duyệt web của Baidu, cũng như hàng ngàn phần mềm khác được xây dựng dựa trên bộ kit của Android.Một nhóm tin tặc dưới sự bảo trợ của Chính phủ Trung Quốc đang nắm giữ quyền truy cập vào hầu hết hệ thống ngân hàng toàn cầu. Theo đó, nhóm đã khai thác hầu hết lỗ hổng bảo mật, lập bản đồ hệ thống ngân hàng toàn cầu suốt 8 năm (từ 2006 đến 2013) và hiện đang rao bán một số lỗ hổng đã hoàn thành mục đích. Danh sách nạn nhân gồm các ngân hàng ở Hoa Kỳ, Châu Mỹ Latin và Châu Á. Nhóm tin tặc này còn là thủ phạm đứng sau vụ hack 81 triệu USD tại Ngân hàng Trung ương Bangladesh tháng 02/2016, giống vụ tấn công ngân hàng TP Bank của Việt Nam tháng 05. Đây có thể là giai đoạn đầu của cuộc khủng hoảng ngân hàng toàn cầu.Trung Quốc bị phát hiện thực hiện hàng loạt các chiến dịch gián điệp mạng quy mô lớn như LURID, Operation Shady RAT, Byzantine Hades… nhằm vào hàng chục quốc gia như Mỹ, Anh, Đức, Pháp, Hà Lan, Ấn Độ, Nhật, Úc, New Zealand, Indonesia, Việt Nam… Mới đây là các chiến dịch gián điệp mạng “Zombie Zero” nhằm vào các doanh nghiệp vận tải và hậu cần trên toàn cầu, chiến dịch do thám “Operation Snowman” (Chiến dịch người tuyết) nhằm vào các giới chức quân sự, chiến dịch “Những con rồng” (Dragons) nhằm vào hệ thống mạng của các nhà cung cấp dịch vụ Internet (ISP), công ty cung cấp dịch vụ điện toán đám mây và trò chơi trực tuyến trên thế giới. |
| **[2] MỸ****Mỹ** đã tiến hành hoạt động tình báo mạng quy mô rất lớn nhằm vào hệ thông thông tin toàn cầu. Theo tiết lộ của Edward Snowden, cựu nhân viên kỹ thuật CIA và một số cựu nhân viên Cơ quan An ninh Quốc gia Mỹ (NSA), NSA đã bí mật thu thập thông tin qua các đường truyền cáp nước ngoài và hợp tác với 100 công ty Mỹ thu thập thông tin cá nhân của khách hàng từ đầu thập niên 1970. Sau vụ khủng bố 11/9/2001, Tổng thống George W. Bush đã cho phép NSA kết nối hệ thống của mình với các đường truyền cáp quang ra, vào nước Mỹ để thu thập thông tin về các email trung chuyển qua các máy chủ đặt ở Mỹ. Từ tháng 11/2007, NSA và FBI đã sử dụng chương trình thu thập thông tin bí mật **PRISM** truy cập trực tiếp vào máy chủ của 09 hãng công nghệ hàng đầu thế giới là Yahoo, Apple, Microsoft, Google, Facebook, Paltalk, AOL, Skype, Youtube để thu thập thông tin người dùng. NSA còn sử dụng chương trình **XKeyscore** giám sát gần như tất cả thông tin người sử dụng trên toàn thế giới khi truy cập Internet. Xkeyscore có khả năng thu thập, phân tích, tìm kiếm trên các cơ sở dữ liệu khổng lồ chứa các thư điện tử, các cuộc trò chuyện trực tuyến và lịch sử duyệt web của hàng triệu người dùng Internet. Sức mạnh của Xkeycore khiến NSA vô cùng tự hào và gọi là **“hệ thống tiếp cận rộng lớn nhất”**. Theo tài liệu mới nhất do cựu nhân viên CIA Mỹ Edward Snowden tiết lộ, Tòa án Giám sát Tình báo Mỹ (FISC) đã cho phép NSA theo dõi **193 quốc gia và vùng lãnh thổ cùng nhiều tổ chức quốc tế** (trừ 04 nước thuộc nhóm “Five Eyes” là Anh, Canada, Australia, New Zealand). NSA đã triển khai chương trình “**Physical subversion”** truy cập vào các hệ thống truyền thông toàn cầu để thu thập thông tin bằng cánh sử dụng hệ thống **QUANTUMINSERT** để chuyển hướng người dùng đến một máy chủ web của NSA có tên mã là FOXACID, từ đó lây nhiễm mã độc vào máy tính của người dùng và tấn công các máy trong cùng mạng thông qua mã độc có tên AirPwn.NSA và Cơ quan Tình báo Chính phủ Anh (GCHQ) đã giám sát các cơ quan viễn thông và cơ quan tiêu chuẩn để **xâm nhập thành công 701/985 (71,16%) mạng điện thoại di động trên toàn thế giới** qua hệ thống thống theo dõi điện thoại **“AURORAGOLD”.**NSA và Cơ quan tình báo Anh (GCHQ) đã phát triển công cụ cho phép **kiểm soát, giám sát điện thoại thông minh ngay cả khi chúng đã được tắt.****Mới đây nhất, Wikileaks tiết lộ hàng nghìn tài liệu về hoạt động tình báo mạng của CIA.** Theo đó, CIA có khả năng xâm nhập, kiểm soát, định vị từ xa thiết bị công nghệ mà hàng tỉ người trên thế giới đang sử dụng, bao gồm các loại smartphone, máy tính bảng, smart TV và cả những loại xe có hệ thống định vị. CIA đang nắm trong tay một hệ thống theo dõi mạng phủ khắp gần như toàn thế giới. Đối với từng dòng thiết bị công nghệ, CIA có các bộ phận riêng chuyên hack mỗi dòng đó.Đối với smartphone: CIA có các công cụ chuyên tấn công iOS (tức iPhone, iPab) và có tới 24 công cụ khai thác lỗi ‘zero days’ nhắm vào các thiết bị sử dụng hệ điều hành Android.Tất cả những công cụ nói trên cho phép CIA qua mặt các hệ thống mã hóa của hàng loạt ứng dụng như WhatsApp, Signal, Telegram, Weibo, Confide và Cloackman bằng cách chiếm quyền kiểm soát các smartphone, theo dõi vị trí mục tiêu, kích hoạt các camera và microphone của thiết bị để nghe lén các đoạn ghi âm và xem trộm các thông điệp văn bản trước khi chúng được mã hóa. Điều này đồng nghĩa, CIA đã không phá vỡ quá trình mã hóa của các ứng dụng chạy trên thiết bị, mà thay vào đó đi trước một bước, thu thập toàn bộ thông tin trước khi quá trình mã hóa diễn ra.CIA có trong tay rất nhiều chương trình các loại để xâm nhập và điều khiển máy tính sử dụng hệ điều hành Windows. Chúng bao gồm virus Hammer Drill có thể ảnh hưởng đến các máy tính và điện thoại chưa kết nối internet, các công cụ xâm nhập nhằm vào các ổ cứng USB, hệ thống giấu dữ liệu, và đặc biệt là các phần mềm có thể lẩn trốn các chương trình bảo mật. WikiLeaks cũng cáo buộc CIA có những phương án tấn công mạng bằng phần mềm độc hại có thể điều khiển máy tính sử dụng Windows và Mac OS X. Các chương trình này mang tên HIVE, Cutthroat và SwindleMột tiết lộ rúng động khác từ các tài liệu của Wikileaks có liên quan đến một phần mềm tấn công của CIA, có mã định danh “Weeping Angel” (Thiên thần than khóc). Đây là một công cụ xâm nhập vào các ti vi thông minh kết nối mạng như smartTV Samsung và biến chúng thành thiết bị nghe lén. Theo đó, ngay cả khi người dùng đã bấm nút tắt, tivi vẫn hoạt động như một “rệp điện tử", thu các lời thoại trong phòng và gửi qua đường truyền Internet về một máy chủ của CIA.Từ năm 2014, WikiLeaks đã tuyên bố CIA đang nghiên cứu khả năng kiểm soát các loại xe hiện đại. Mặc dù chưa rõ mục đích, WikiLeaks cho rằng việc này có thể dùng để thực hiện ám sát từ xa mà không bị phát hiện.WikiLeaks còn tiết lộ sự phân ban trong bộ phận mạng máy tính của CIA. Bộ phân chuyên sản xuất vũ khí mạng của CIA là Nhóm Thiết kế phát triển (EDG), hoạt động dưới sự kiểm soát của Trung tâm Tình báo Mạng (CCI). Ban Thiết bị Di động (MDB) chuyên phát triển các công cụ và kỹ thuật để có thể truy cập và kiểm soát các loại điện thoại thông tin và máy tính bảng phổ biến từ xa.Ngày 31/8/2017, Wikileak tiếp tục công bố các thông tin cho rằng CIA sở hữu công cụ tên là Angelfire có thể đột nhập vào các máy tính sử dụng hệ điều hành Windows trên khắp thế giới |
| - Hoạt động phá hoại cơ sở vật chất, kỹ thuật |
| Cơ quan An ninh quốc gia Mỹ (NSA) và đơn vị tình báo quân đội 8200 của Israel đã hợp tác triển khai chiến dịch mang tên **“Olympic Games”**, tạo ra mã độc **Stuxnet** tấn công hệ thống điều khiển, gây đình trệ hoạt động, **phá hủy hàng nghìn máy làm giàu uranium** của nhà máy điện hạt nhân Busher của Iran, vụ việc này được đánh giá là đã **làm chậm chương trình hạt nhân của Iran từ 2 - 5 năm**. Biến thể của Stuxnet được cho là đã xâm nhập hệ thống điều khiển, kích nổ các tên lửa đạn đạo, phá hủy kho chứa tên lửa đạn đạo Sejil - 2 tại căn cứ quân sự của lực lượng Vệ binh cách mạng hồi giáo Iran vào ngày 12/11/2011, làm 17 chuyên gia, trong đó có thiếu tướng Hassan Moghaddam thiệt mạng.Để đáp trả, tháng 12/2011 và tháng 12/2012, Iran đã tấn công mạng, kiểm soát hành trình và lần lượt bắt giữ 02 máy bay do thám tàng hình không người lái RQ-170 Sentinel và Scan Eagle của Mỹ.Trong bối cảnh căng thẳng gia tăng với Nga, ¼ lưới điện Ukraine bị ngừng trệ trong suốt 6 giờ do mã độc mã hóa tấn công hệ thống điều hành lưới điện.Các nhà sản xuất máy công nghiệp Pháp và một số công ty của Đức trở thành mục tiêu tấn công của mã độc giống sâu Stuxnet có tên **“Havex”** được lập trình để lây nhiễm lên phần mềm hệ thống điều khiển công nghiệp (SCADA) và thiết bị điều khiển công nghiệp (ICS), có khả năng vô hiệu hóa các đập thủy điện, làm quá tải các nhà máy điện hạt nhân, đánh sập hệ thống điện lưới quốc gia.Mới đây nhất, ngày 14/12/2017, hãng bảo mật FireEye đã phát hiện mã độc Triton, dòng mã độc mới chuyên tấn công các hệ thống kiểm soát công nghiệp (ICS), được thiết kế để phá hủy hoặc vô hiệu hóa các thiết bị kiểm soát an toàn công nghiệp Triconex của hãng Schneider, thiết bị thường được sử dụng cho các nhà máy lọc dầu, cơ sở hạt nhân và nhà máy sản xuất, việc phá hủy hoặc vô hiệu hóa thiết bị kiểm soát an toàn này có thể dẫn đến những vụ nổ hoặc rò rỉ nghiêm trọng. |
| - Hoạt động tác động chuyển hóa chính trị |
| **“Mùa xuân Ả Rập”**Tại Trung Đông – Bắc Phi, Internet và nhất là mạng xã hội đã trở thành công cụ đắc lực để tuyên truyền, kích động biểu tình, bạo loạn, lật đổ chính quyền với tên gọi “Mùa xuân Ả rập”, hay “Cách mạng hoa lài”.- Tại **Tunisia**, vào ngày 17/12/2010, hình ảnh Mohamed Bouazzi tự thiêu tại quảng trưởng Tahir được ghi lại bằng máy quay phim, điện thoại di động và được tung lên các trang mạng xã hội Facebook, Twitter, Youtube… đã nhanh chóng “truyền lửa”, châm ngòi cho hàng loạt cuộc biểu tình, bạo loạn liên tiếp nổ ra trên khắp Tunisia. Chỉ sau 04 tuần, hơn 329 triệu thông điệp kêu gọi biểu tình đã liên tục trao đổi trên các mạng xã hội, trở thành tác nhân chính dẫn đến sự sụp đổ của chính quyền của Tổng thống Ben Ali. Các phân tích về vai trò của Facebook trong sự kiện này cho thấy, chỉ trong vòng 15 ngày đầu tháng 01/2011 – thời gian xảy ra các cuộc biểu tình - Facebook đã tăng 8% số lượng người dùng ở Tunisia; số người dùng Facebook ở các nước Ả Rập đạt 21,3 triệu với tỷ lệ tăng trưởng gần 80%. - Tại **Ai Cập**, ông Mubarack thậm chí đã ra lệnh cắt Internet và sóng điện thoại di động nhưng cũng không kịp ngăn chặn làn sóng biểu tình chống đối, chỉ sau 18 ngày kể từ lời kêu gọi đầu tiên được phát đi trên Facebook, chính quyền của Tổng thống Mubarak đã sụp đổ sau 30 năm cầm quyền ***(18 ngày là thời gian kỷ lục của một cuộc cách mạng từ lúc bắt đầu kêu gọi đến lúc kết thúc thắng lợi trong lịch sử loài người)****.*Trong làn sóng này, Wael Ghonim, mật danh ElShaheed được nhắc đến như là người đóng vai trò chính trong việc kích động giới trẻ Ai Cập thông qua Facebook khi lập một trang Facebook kết nối hơn 400.000 người Ai Cập, chủ yếu là giới trẻ và phát động cuộc biểu tình chống chính phủ đầu tiên cùng với hàng loạt các thông báo, hình ảnh, video, tờ rơi có thể tải xuống. Trả lời báo chí, Ghonim khẳng định, ***“Không có Facebook, không có Twitter, không có Google, không có Youtube, các cuộc cách mạng này sẽ không bao giờ xảy ra. Chắc chắn đây là cuộc cách mạng Internet. Tôi gọi nó là cuộc cách mạng 2.0”.*** Tuy nhiên, Ghonim cũng thừa nhận, ***“mọi thứ đã vượt khỏi tầm kiểm soát”***.- Tại **Syria**, mạng xã hội Twitter và Facebook được các nhóm biểu tình chống đối Chính phủ sử dụng để trao đổi thông tin, liên lạc; đăng tải những lời kêu gọi và khẩu hiệu biểu tình; trang Facebook “Cách mạng Syria 2011” có 120.000 thành viên tham gia. “Cách mạng hoa lài” lây lan qua trang mạng xã hội, điện thoại di động và các phương tiện truyền thông khác tới hàng loạt các nước Trung Đông – Bắc Phi khác như Yemen, Bahraihn, Algeria, Jordan, Moritani, Bangladesh, Bolivia, Cyrus, Gabong, Iran…Theo nhận xét của Hoàng thân Alwaleed, thành viên hoàng gia Arab Saudi – đồng minh thân cận của Mỹ, biến động chính trị tại Trung Đông – Bắc Phi đánh dấu một phong trào nổi dậy đòi dân chủ, phá bỏ “chế độ độc tài” lan rộng với tốc độ nhanh chưa từng thấy kể từ sau cách mạng Châu Âu 1848.**Nga can thiệp bầu cử Tổng thống Mỹ 2016**Theo báo cáo *“Đánh giá hành động và âm mưu của Nga trong cuộc Bầu cử Tổng thống Mỹ 2016”* của Cộng đồng tình báo Mỹ:- Tổng thống Nga Vladimir Putin đã ra lệnh tiến hành một chiến dịch tổng lực can dự và gây ảnh hưởng nhằm làm suy yếu niềm tin công chúng vào tính minh bạch của bầu cử Mỹ; bóp méo thông tin, tung tin giả, bôi nhọ nhằm giảm khả năng trúng cử của bà Hillary Clinton; đồng thời, tuyên truyền ủng hộ ông Donald Trump đắc cử.- Tổng cục Tình báo Bộ Tổng tham mưu Nga (GRU), cơ quan tiến hành chiến dịch tác chiến mạng này, đã tiến hành các hoạt động gián điệp mạng đánh cắp thông tin bí mật, từ đó, chọn lựa thông tin nhạy cảm cung cấp cho những chiến dịch truyền thông dài hơi, với sự tham gia của cơ quan thông tấn công khai của Nga, các hãng truyền thông tư nhân và hoạt động tấn công chính trị rộng rãi trên mạng xã hội.- Hoạt động gián điệp mạng của Nganhắm đến các nhân vật chính trị ở cả hai đảng Dân chủ, Cộng hòa và các cơ quan trọng yếu khác của Mỹ. GRU đã xâm nhập thành công vào nhiều hộp thư điện tử cá nhân của các quan chức Đảng Dân chủ, mạng máy tính của Uỷ ban Dân chủ Quốc gia (DNC) và chiếm đoạt khối lượng lớn dữ liệu nhạy cảm. GRU cũng thu thập dữ liệu từ một số mục tiêu của Đảng Cộng hòa nhưng để sử dụng trong chiến dịch truyền thông ủng hộ ông D. Trump. Tình báo Nga cũng được xác định đã xâm nhập thành công một số hệ thống máy tính của Ban Bầu cử địa phương và Liên bang Mỹ. GRU đã sử dụng tin tặc có biệt danh *Guccifer 2.0* và các trang *DCLeaks.com*, *WikiLeaks.com* để công bố các dữ liệu thu thập được trong các chiến dịch tấn công mạng hoặc cung cấp độc quyền cho các hãng truyền thông lớn trên thế giới để thực hiện kế hoạch lan truyền thông tin. Từ tháng 03/2016, các hãng truyền thông lớn của Nga đã phối hợp chặt chẽ với Chính phủ triển khai chiến dịch công khai ủng hộ ông D. Trump thông qua các bài viết, bản tin tiếng Anh và nhiều ngôn ngữ khác nhằm vào khán giả quốc tế. RT đã sử dụng mạng xã hội như một kênh truyền thông chủ lực, vừa nhằm tránh các quy định về phát sóng trên truyền hình truyền thống vừa giúp mở rộng đối tượng tiếp cận trên toàn thế giới.Chính quyền của ông Barack Obama đã trục xuất 35 nhà ngoại giao Nga để trả đũa. Thượng viện và Hạ viện tổ chức nhiều phiêu điều trần về nghi vấn trên. Ủy ban Tình báo Thượng viện Mỹ tuyên bố mở cuộc điều tra về các hoạt động gián điệp mạng của Nga. Giám đốc Cục Điều tra Liên bang (FBI) khẳng định, “FBI đang điều tra những nỗ lực của chính phủ Nga can thiệp vào cuộc bầu cử 2016 ở Mỹ, bao gồm cả những mối liên hệ với chiến dịch tranh cử của Tổng thống Donald Trump”. Chủ tịch Ủy ban Quân vụ, Thượng nghị sĩ John McCain (đảng Cộng hòa) coi sự cai thiệp của Nga là “hành động chiến tranh”. Phó Tư lệnh Bộ Chỉ huy tối cao NATO tại châu Âu, tướng Adrian Bradshaw cho rằng, sự can thiệp của Nga vào bầu cử Tổng thống Mỹ có thể được coi là một “hành động chiến tranh” và có thể dẫn đến một phản ứng quân sự từ NATO.**Ngoài Mỹ, Nga cũng bị tố cáo sử dụng tin tặc can thiệp vào các cuộc bầu cử của nhiều nước khác,**Tháng 11/2016, Thủ tướng Đức Angela Merken tuyên bố, không loại trừ khả năng tin tặc Nga can thiệp vào cuộc bầu cử liên bang của nước này. Ngày 1/9/2017, Cục An ninh công nghệ thông tin liên bang Đức (BSI) bày tỏ lo ngại cuộc tổng tuyển cử tại Đức vào ngày 24/9/2017 có thể trở thành mục tiêu của các cuộc tấn công mạng.Tháng 2/2017, Cơ quan tình báo Na Uy (PST) cáo buộc nhóm tin tặc APT29 (Nga) đã thực hiện hàng loạt cuộc tấn công mạng vào Bộ Ngoại giao, cơ quan tình báo quốc phòng và các cơ quan cấp cao của nước này. Tháng 5/2017, Pháp tố cáo các nhóm tin tặc APT28 tấn công vào hệ thống mạng của Ủy ban bầu cử của ứng cử viên Emmanuel Marcon để can thiệp vào quá trình vận động tranh cử vòng 2 bầu cử Tổng thống Pháp theo hướng có lợi cho ứng cử viên Marine Le Pen... **Sử dụng dữ liệu Facebook can thiệp bầu cử Tổng thống Mỹ 2016**Công ty Cambridge Analytica đã sử dụng một phương pháp để phân tích con người dựa trên hành vi của họ trên Facebook theo từng phút để giúp Trump thắng cử. Đây là phương pháp đo lường tính cách của một người dựa trên **5 chiều cá tính** (OCEAN): **Độ mở** (Bạn cởi mở với những điều mới như thế nào?), **Sự tận tâm** (Bạn là người cầu toàn như thế nào?), **Hướng ngoại** (Bạn là người hoà đồng?), **Dễ chịu** và **nhạy cảm** (bạn dễ bị tổn thương như thế nào?). Dựa vào dữ liệu từ Facebook, phương pháp này cho phép dự đoán hành vi của một người với độ chính xác cao: **Phân tích 10 like đã hiểu nhân cách đối tượng tốt hơn đồng nghiệp của họ, sau 70 like – tốt hơn cả bạn thân, sau 150 – hơn cả bố mẹ, sau 300 – hơn cả bạn tình, nếu nghiên cứu nhiều hành động hơn thì có thể biết về đối tượng hơn cả chính họ** (Đây là bộc lộ từ chính Nhà tâm lý học Michal Kosinski - người sáng tạo ra phương pháp trên, chính Michal Kosinski cũng cảnh báo về phương pháp của mình rằng “có thể tạo ra nguy hiểm cho đời sống, tự do hay thậm chí tính mạng mọi người”.)Công ty Cambridge Analytica được cho là đã giúp dự đoán khả năng một cử chi cụ thể có xu hướng lựa chọn Đảng Dân chủ hay Công hòa để từ đó **“tinh chỉnh”** chiến dịch truyền thông cho từng đối tương cụ thể nhằm hướng đến kết quả có lợi cho Đảng Cộng hòa.Ngay sau khi Trump thắng cử, CEO Alexander James Ashburner Nix phát biểu rằng: **"Chúng tôi rất vui mừng rằng cách tiếp cận truyền thông được định hướng bởi dữ liệu mang tính cách mạng của chúng tôi có đóng góp nền tảng vào chiến thắng của ông Donald Trump”.** |
| 3.2. Khủng bố mạng |
| **[1] Tấn công mạng để khủng bố**Hoạt động phổ biến của dạng này là: tấn công từ chối dịch vụ; tấn công xâm nhập để phá hủy cơ sở dữ liệu; mã hóa dữ liệu để ra yêu sách (giống như hoạt động tống tiền); tấn công xâm nhập, chiếm đoạt và công khai dữ liệu bí mật.Trên thế giới đã diễn ra nhiều hoạt động khủng bố mạng quy mô lớn, điển hình là hoạt động của các nhóm tin tặc quốc tế như Anonymous, Luzlsec, Lizard Squad..., với nhiều hoạt động tấn công gây thiệt hại lớn nhằm vào các cơ quan chính phủ của Mỹ, EU, NATO, Nga, Đức, Pháp... và các tập đoàn lớn như Visa, PayPal, Master, Google, Microsoft... Không chỉ gây đình trệ hệ thống, tiết lộ các thông tin nhạy cảm, mà số đối tượng khủng bố mạng còn công khai nhiều tài liệu mật của các quốc gia, gây nên các tổn thất khó lường về chính trị, ngoại giao. Điển hình như tổ chức tin tặc Anonymous đã cung cấp cho Wikileak khoảng 5,5 triệu thư điện tử cho thấy các bằng chứng về hoạt động gián điệp mạng và mối liên hệ bí mật giữa Stratfor, công ty phân tích tình báo có trụ sở tại Mỹ với những tập đoàn lớn như Bhopal’s Dow Chemical Co, Lockheed Martin và một số cơ quan chính phủ của Mỹ, trong đó có Bộ An ninh nội địa. Anonymous cũng đã tấn công vào hệ thống mạng của Trung tâm quốc gia về phòng chống tội phạm mạng của Ý (CNAIPIC) và công bố 8 GB dữ liệu đánh cắp được cho thấy hoạt động thu thập tình báo của CNAIPIC đối với các cơ quan, tổ chức khắp nôi trên thế giới. Tổ chức Wikileaks do Julian Assange sáng lập đã chiếm đoạt và công khai hàng trăm nghìn điện tín ngoại giao của Mỹ trong nhiều năm và từ khắp nơi trên thế giới, trong đó có nhiều điện mật; quy mô tác hại của sự kiện này thậm chí còn được ví như khủng bố 11/9 đối với nền ngoại giao của Mỹ.**Từ đầu năm 2016 đến nay:**- Nhóm tin tặc Anonymous tuyên bố đã tấn công, xâm nhập thành công vào hệ thống mạng của Bộ Quốc phòng Pháp, đánh cắp các thông tin nhạy cảm nhằm phản đối chính sách tăng cường xuất khẩu vũ khí của Chính phủ Pháp. - Nhóm tin tặc Anonymous tại Ý triển khai chiến dịch tấn công từ chối dịch vụ vào một số tổ chức, chính quyền địa phương vùng Apulia và vùng Basilicata nhằm phản đối dự án Đường ống dẫn khí xuyên biển Adriatic (TAP - đường ống dẫn khí đốt từ Azerbaijan đến Thổ Nhĩ Kỳ, Hy Lạp, Albania, Ý và một số nước Tây Âu khác) do nhóm này cho rằng, dự án TAP không quan tâm đến các vấn đề môi trường và bảo vệ địa danh lịch sử của Apulia.- Hệ thống cổng thông tin của một số cơ quan, tổ chức của Bỉ như trang mạng của Thủ tướng, Bộ trưởng Bộ Quốc phòng, Bộ trưởng Bộ Giáo dục Pháp ngữ, Liên đoàn Wallonie-Bruxells,… đã bị nhóm tin tặc Down - Sec tấn công nhằm lên án sự thụ động của chính quyền Bỉ trong việc bảo vệ trẻ vị thành niên bị quấy nhiễu trên mạng xã hội.- Trung tâm dữ liệu của Cơ quan An ninh quốc gia Mỹ đã hứng chịu 300 triệu cuộc tấn công mạng mỗi ngày, số lượng này gia tăng mạnh kể từ khi Edward Snowden (cựu nhân viên CIA) tiết lộ chương trình do thám Big Brother của NSA vi phạm quyền riêng tư của công dân Mỹ. - Nhóm tin tặc Anonymous tuyên bố sẽ tái khởi động chiến dịch tấn công mạng #OpTrump đánh sập trang web tranh cử của ông Donald Trump từ ngày 01/4/2016 vì cho rằng những hành động và phát biểu của ông này trong quá trình tranh cử đã gây chia rẽ và kích động mâu thuẫn sắc tộc sâu sắc trong nội bộ nước Mỹ và thế giới. - Nhóm tin tặc Anonymous tại Bồ Đào Nha tuyên bố đã đánh sập 20 trang web của Chính phủ Angola nhằm phản đối việc bỏ tù 17 nhà vận động hòa bình trẻ. Nhiều trong số các trang web này vẫn không thể hoạt động lại sau khi nhóm tin tặc tuyên bố trên trang Facebook.**- Hãng bảo mật Verizon** vừa công bố báo cáo cho biết một nhóm tin tặc đã tấn công thay đổi hệ thống ICS/SCADA của nhà máy xử lý nước Kemuri (Mỹ) và thay đổi lượng hóa chất dùng để xử lý nước gây nguy hiểm cho sức khỏe người dùng. Nhóm này đã truy cập vào hệ thống AS400 (kết nối mạng nội bộ của công ty và hệ thống SCADA), tắt hệ thống SCADA và thay đổi giá trị xử lý nước. Tuy nhiên, chức năng cảnh báo của hệ thống đã hoạt động đúng lúc và cảnh báo nguy hiểm liên quan đến nồng độ hóa chất bất thường trong nước, kịp thời ngăn chặn nguy cơ gây ngộ độc cho người dùng.- Theo trang Tech Worm, từ năm 2006 đến 2012, tin tặc người Colombia Andress Sepulveda đã thao túng kết quả các cuộc bầu cử bằng cách tấn công các máy bỏ phiếu tại 9 quốc gia Mỹ Latin, gồm Colombia, El Salvado, Costa Rica, Mexico, Panama, Guatemala, Nicaragua, Venezuela và Honduras để nhận khoản thù lao khổng lồ từ 12.000 USD mỗi tháng.- Tháng 3/2016, xảy ra vụ gián điệp mạng đình đám, còn gọi là vụ “Hồ sơ Panama”, được cho là do các cựu quan chức Bộ Ngoại giao, nhân viên CIA và các đặc vụ khác của Mỹ đạo diễn. Tin tặc đã tấn công vào hệ thống mạng của hãng luật Mossack Fonseca, đánh cắp và công bố 2.6 TetaByte dữ liệu của hãng này liên quan đến các giao dịch trốn thuế, rửa tiền bất hợp pháp của các quan chức, nhân vật nổi tiếng trên thế giới, nhằm chia rẽ, gây mất ổn định chính trị một số nước không theo Mỹ và Phương Tây như Nga, Trung Quốc, Syria… |
| **[2] Hoạt động của các tổ chức khủng bố trên không gian mạng:** Không gian mạng đã trở thành môi trường cho các tổ chức khủng bố quốc tế hoạt động tuyên truyền, tuyển lựa, huấn luyện và chỉ đạo hoạt động của các mạng lưới. Các tổ chức khủng bố hoạt động nổi hiện nay như IS, al-Qaeda... đều có các hoạt động này, trong đó hoạt động tuyển lựa qua mạng xã hội của IS đã gây ra mối lo ngại sâu sắc cho cộng đồng quốc tế.Đáng chú ý, **trong vụ khủng bố tại Paris** ngày 13/11/2015, các đối tượng đã thông qua hệ thống game PlayStation 4 của Sony để trao đổi và lên kế hoạch tấn công.**Tại Anh,** ngày 25/3/2017, đối tượng Khalid Masood đã sử dụng ứng dụng WhatsApp để mã hóa thông tin trao đổi trước khi thực hiện vụ tấn công bằng xe ô tô ở Thủ đô Luân Đôn, Anh khiến cơ quan an ninh Anh rất khó khan để giải mã.Ngoài ra, không gian mạng còn trở thành nơi phát động các cuộc biểu tình, phá rối an ninh, bạo loạn quy mô lớn:Điển hình như bạo động tại Anh lan rộng và gây thiệt hai nghiêm trong chỉ sau 03 ngày, từ ngày 06 - 09/8/2011. Thủ tướng David Cameron sau đó cho rằng: *“Mọi người sẽ bị sốc khi chứng kiến cách các cuộc bạo loạn được tổ chức bằng các phương tiện truyền thông xã hội.*Tại Mỹ, phong trào biểu tình “Chiếm phố Wall” phát động từ mạng xã hội lan rộng trên khắp đất nước, sau đó lan ra hơn 1.500 thành phố trên toàn thế giới chỉ sau 01 tháng. |
| **[3] Khủng bố thông tin**Không gian mạng với đặc tính nặc danh, lan truyền nhanh đã trở thành môi trường thuận lợi cho hoạt động tán phát thông tin riêng tư, bịa đặt, xuyên tạc hoặc thật giả lẫn lộn lên mạng nhằm khủng bố tinh thần và tạo dư luận xã hội trên cộng đồng mạng phục vụ các ý đồ đen tối, gây phương hại đến ổn định chính trị và trật tự, an toàn xã hội.Ủy ban Châu Âu (EC) đã yêu cầu các công ty Facebook, Twitter, Google+ áp dụng các biện pháp ngăn chặn những thông tin lừa đảo, gian lận xuất hiện trên các trang mạng này.Đức dự kiến thành lập Trung tâm phòng chống tin tức sai lệch, phạt các doanh nghiệp cung cấp dịch vụ tới 50 triệu Euro nếu không gỡ bỏ thông tin sai sự thật trong vòng 24 giờ sau khi có yêu cầu của chính quyền. Các hãng Facebook, Google và một số cơ quan thông tin khác thực hiện “kiểm chứng chéo” thông tin nhằm ngăn chặn những thông tin sai lệch trên Internet tại Pháp. Facebook đưa ra chính sách cấm sử dụng dữ liệu thu thập được từ người dùng Facebook cho mục đích giám sát, bao gồm cả việc giám sát các nhà hoạt động và những người biểu tình; tuyển dụng thêm 3.000 nhân viên để kiểm duyệt, ngăn chặn các video bạo lực và thông tin sai lệch.Ngày 25/8/2017, Văn phòng Thông tin Internet quốc gia Trung Quốc đã ban hành một loạt quy định mới, trong đó người dùng Internet nếu muốn bình luận vào các bài đăng sẽ phải đăng ký tài khoản online bằng tên thật của mình. Người dùng Internet tại Trung Quốc vẫn có thể dùng bút danh nhưng nó phải gắn với đặc tính cụ thể của người bình luận |
| 3.3. Chiến tranh mạng |
| Năm 1957, hoảng sợ trước việc Liên Xô phóng thành công vệ tinh Sputink có khả năng phát tín hiệu radio khi bay quanh quỹ đạo trái đất, giới quân sự, khoa học Mỹ đặc biệt lo ngại việc Liên Xô tấn công hủy diệt toàn bộ hệ thống truyền dẫn viễn thông. Để đối phó với điều này, họ nghiên cứu trong nhiều năm và năm 1969 cho ARPAnet ra đời. Đây là hệ thống mạng được coi là tiền thân của Internet, được coi là vũ khí để chống lại hoạt động của Liên Xô. Ngày nay, với nhiều lợi ích mang lại, nhiều người đã quên và thậm chí không biết rằng, Internet khởi nguồn là một thứ vũ khí quân sự và hiện nay, nó vẫn là một thứ vũ khí quân sự.Chiến tranh mạng là có thể được hiểu theo nghĩa rộng và nghĩa hẹp. Theo nghĩa rộng là việc sử dụng thông tin trên mạng để đạt được mục đích quốc gia, theo nghĩa hẹp là sự đối kháng giữa các hệ thống thông tin quân sự. Với các quốc gia có lợi ích toàn cầu như Nga, Mỹ, Trung Quốc… chiến tranh mạng luôn được hiểu theo nghĩa rộng và các quốc gia khác trên thế giới cũng bắt đầu tính toán đến việc đó. Chiến tranh mạng là hình thái chiến tranh mới, vượt khỏi khuôn khổ khái niệm về chiến tranh quân sự truyền thống. Nếu không được quy phạm và bắt tay vào công cuộc chuẩn bị ngay từ bây giờ, với hệ thống thông tin ăn sâu vào mọi lĩnh vực của đời sống xã hội như hiện nay, chỉ cần một cú nhấp chuột, chiến tranh mạng có thể khiến hạ tầng quốc gia (*hệ thống thông tin, liên lạc, quân sự, điện, tài chính, nước, giao thông…*) bị phá hủy, gây tổn thất về nhân mạng, thiệt hại gây ra có thể nặng nề hơn nhiều so với vũ khí quân sự thông thường.**Hình thái chiến tranh mới**. Theo dự thảo Chiến lược An ninh mạng quốc gia, *Chiến tranh mạng là trạng thái xã hội đặt biệt của đất nước khi lực lượng quân sự nước ngoài tấn công quy mô lớn trên không gian mạng gắn với hoạt động vũ trang nhằm gây chiến tranh xâm lược hoặc phương hại đến độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của nước CHXHCN Việt Nam.***Chiến tranh mạng vượt khỏi khuôn khổ chiến tranh quân sự truyền thống.***(1) Về mục đích*, chiến tranh truyền thống hướng đến sự thống trị về địa lý để qua đó đạt được các mục đích về chính trị, xã hội, kinh tế, tôn giáo…, còn chiến tranh mạng hướng đến sự chiếm đoạt thông tin, thao túng hoặc hủy diệt các hệ thống thông tin của đối phương nhằm đạt được các mục đích quốc gia. Tuy có thể gắn liền hoặc khởi đầu cho các phản ứng quân sự, các cuộc xâm nhập, chiếm cứ về địa lý nhưng đó không phải là bản chất của chiến tranh mạng.*(2) Về mục tiêu*, chiến tranh truyền thống nhắm đến con người và các vật hữu hình có ảnh hưởng trực tiếp đến đời sống con người; còn chiến tranh mạng chủ yếu hướng đến mục tiêu vô hình là thông tin, qua đó tác động đến các mục tiêu hữu hình và có thể dẫn đến các tác động trực tiếp hoặc gián tiếp đến đời sống con người. Mặt khác, các cuộc tấn công trong chiến tranh mạng nhắm trước hết và chủ yếu vào các mục tiêu phi quân sự, thay vì các mục tiêu quân sự như trong chiến tranh truyền thống.*(3) Về phạm vi*, chiến tranh truyền thống xảy ra trong khu vực địa lý nhất định, yếu tố “biên giới” và chiến tuyến (địch - ta) khá rõ rệt. Trong khi đó, chiến tranh mạng không có biên giới, không có chiến tuyến, có thể xảy ra ở mọi nơi. Đây là điểm đặc biệt khiến cho việc phòng bị, phát hiện, ngăn chặn, tổ chức đấu tranh trong chiến tranh mạng rất khó khăn, bởi nó có thể được phát động từ bất cứ đâu, yếu tố địch - ta (chiến tuyến) không rõ ràng và khó dự đoán trước mục tiêu bị tấn công.*(4) Về thành phần tham gia*, chiến tranh truyền thống với đặc trưng vũ trang có sự tham gia và đóng vai trò nòng cốt của các lực lượng quân sự và bán quân sự, còn trong chiến tranh mạng, tất cả mọi người đều có thể tham gia, không phân biệt quân sự hay dân sự, trong hay ngoài lãnh thổ. Điều này cũng có nghĩa, chiến tranh mạng có thể do các lực lượng phi quân sự tiến hành. Đây là đặc điểm rất quan trọng, tác động đến việc xây dựng thế trận và tổ chức lực lượng phòng chống chiến tranh mạng. Nó cũng chỉ ra rằng, phòng chống chiến tranh mạng cần có tư duy mới, không chỉ bó hẹp trong tư duy về quân sự; sự tham gia của các cấp, các ngành và toàn xã hội là tất yếu. *(5) Về thời gian*, chiến tranh truyền thống diễn ra trong khoảng thời gian tương đối dài, ngược lại, chiến tranh mạng diễn ra trong một khoảng thời gian tương đối ngắn hơn. Tốc độ triển khai và mở rộng của chiến tranh mạng thường cực nhanh. Những cuộc “tập kích” bất ngờ trong chiến tranh mạng nhằm vào các hạ tầng thông tin trọng yếu thậm chí chỉ cần diễn ra trong vài giây nhưng vẫn có thể dẫn đến những hậu quả nặng nề *(như nhận định của nguyên Thứ trưởng Quốc phòng Mỹ William Lynn: “chỉ cần gõ bàn phím ở một nước này cũng có thể tác động đến phần còn lại của thế giới chỉ trong chớp mắt”)*. Xét thời gian cần phục hồi sau chiến tranh, thời gian này thường kéo dài hơn trong chiến tranh truyền thống, còn trong chiến tranh mạng thì ngắn hơn. Tuy vậy, trong trường hợp chiến tranh mạng dẫn đến sự phá hủy trên thực tế, như trường hợp siêu vũ khí Stuxnet tấn công nhà máy hạt nhân Busher của Iran hay biến thể của nó tấn công kho chứa tên lửa Sejil-2, thì thời gian cần để phục hồi cho hai hình thái chiến tranh này không có khác biệt.*(6) Về chi phí*, so với chiến tranh truyền thống, chiến tranh mạng có chi phí thấp hơn, do nó không dẫn đến các cuộc hành binh, triển khai lực lượng, phương tiện, vũ khí bên ngoài lãnh thổ, không sử dụng khí tài quân sự truyền thống mà sử dụng các vũ khí mạng được lập trình, có thể tự động nhân bản, tự động thực hiện nhiệm vụ và nhiều tác vụ thông minh khác; việc điều khiển vũ khí mạng không đòi hỏi sự di chuyển về nhân lực, phương tiện mà có thể thực hiện ngay tại trụ sở nhưng phạm vi tác chiến trên toàn thế giới; chiến tranh mạng không nhất thiết phải là một lực lượng hùng hậu mà có thể chỉ do một nhóm vài người, thậm chí chỉ là một cá nhân tiến hành.*(7) Về lợi thế so sánh*, trong chiến tranh truyền thống, quốc gia nào ở trình độ phát triển cao hơn sẽ có lợi thế so sánh lớn hơn. Tuy nhiên, chiến tranh mạng mang tính bất đối xứng, quốc gia nào phát triển hơn, ứng dụng công nghệ thông tin sâu rộng hơn càng dễ bị tấn công và bị thiệt hại nặng nề hơn, chỉ một lực lượng rất nhỏ cũng có thể gây thiệt hại rất lớn cho đối thủ. *(8) Về biểu hiện bên ngoài,* chiến tranh truyền thống gắn liền với các hoạt động quân sự, thiệt hại gây ra là thương vong và sự phá hủy, do đó, luôn mang đến ấn tượng nghiêm trọng, tàn bạo và rõ ràng. Trong khi đó, chiến tranh mạng biểu hiện ra bên ngoài ở giai đoạn đầu không rõ ràng, trong nhiều trường hợp rất khó nhận thấy. *(9) Về ảnh hưởng*, chiến tranh truyền thống ảnh hưởng tới nhiều người, nhiều lĩnh vực và gắn với yếu tố địa lý, trong khi chiến tranh mạng ảnh hưởng đến mọi người, mọi lĩnh vực có liên quan đến hệ thống mạng bị tấn công và sự ảnh hưởng này dựa trên yếu tố kết nối mạng và sự tương tác với mạng đó. *(10) Về tính minh bạch và quy kết*, trong chiến tranh truyền thống, chủ thể phát động tấn công tương đối minh bạch, thể hiện bằng các tuyên bố hoặc phê chuẩn, hành động của các lực lượng quân sự chính quy, xuất phát từ những “địa chỉ” tương đối rõ ràng. Điều này hoàn toàn ngược lại trong chiến tranh mạng. Diễn ra trên không gian mạng vốn mang đặc tính nặc danh và không biên giới, chiến tranh mạng mang đặc tính nặc danh và ẩn, đối tượng phát động chiến tranh hoàn toàn có thể giả mạo hoặc lợi dụng hệ thống mạng của một quốc gia trung gian để tấn công quốc gia khác, do đó, việc xác định và quy kết chủ thể phát động chiến tranh mạng sẽ rất khó khăn, trong nhiều trường hợp không thể thực hiện được nếu chỉ với nỗ lực của một quốc gia. Điều này sẽ ảnh hưởng rất lớn đến cách thức và tính pháp lý (theo luật quốc tế) của các phản ứng mà một quốc gia có thể lựa chọn trong chiến tranh mạng.  *(11) Về sự ngăn chặn*, trong chiến tranh truyền thống là khá rõ ràng và sử dụng bạo lực, còn trong chiến tranh mạng thì ngược lại, không rõ ràng và không sử dụng bạo lực. Sự không rõ ràng này xuất phát từ tính không biên giới và nặc danh của chiến tranh mạng, do khó có thể xác định hoặc quy kết được chủ thể phát động tấn công, nguồn phát động tấn công và mục tiêu sẽ bị tấn công nên sự ngăn chặn hay đáp trả trong chiến tranh mạng có bản chất khác với trong chiến tranh truyền thống.*(12) Về sự thống trị và bên chiến thắng*, trong chiến tranh truyền thống, một trong các bên có thể đạt được sự thống trị trong một phạm vi địa lý nhất định và yếu tố thắng - bại tương đối rõ ràng. Ngược lại, trong chiến tranh mạng, khó bên nào có thể đạt được sự thống trị và do đó, khó có thể xác định được bên nào dành phần thắng. |

## 4. Quan điểm, chủ trương, chính sách của Đảng, Nhà nước về việc xây dựng, ban hành Luật An ninh mạng

Quan điểm, tư tưởng chỉ đạo của Đảng, Nhà nước về an ninh mạng đã thể hiện rõ, nhất quán, có hệ thống và phù hợp với từng thời kỳ; trong đó, đã kịp thời điều chỉnh, đưa ra các quan điểm, tư tưởng chỉ đạo về vấn đề an ninh mạng trong tình hình mới. Cụ thể:

- Ngày 16/9/2013, Ban Bí thư Trung ương Đảng ra Chỉ thị số 28-CT/TW về “tăng cường công tác bảo đảm an toàn thông tin mạng”, xác định cụ thể các vấn đề, nhiệm vụ của công tác an ninh mạng;

- Ngày 25/12/2013, Bộ Chính trị ban hành Chỉ thị số 30-CT/TW về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên Internet, chỉ đạo các giải pháp tổng thể trong bảo đảm an ninh thông tin mạng;

- Ngày 17/6/2014, Thủ tướng Chính phủ ban hành Chỉ thị số 15/CT-TTg về “Tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới” đã đưa ra các chỉ đạo cụ thể nhằm tăng cường công tác bảo đảm an ninh mạng, góp phần giữ vững ổn định chính trị, phát triển kinh tế - xã hội của đất nước.

- Nghị quyết số 26/NQ-CP của Chính phủ về việc ban hành Chương trình hành động thực hiện Nghị quyết số 36-NQ/TW ngày 01/7/2014 của Bộ Chính trị Ban Chấp hành Trung ương Đảng Cộng sản Việt Nam về đẩy mạnh ứng dụng, phát triển công nghệ thông tin đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế đã giao nhiệm vụ cho Bộ Công an trong đề xuất, xây dựng Luật An ninh mạng.

- Ngay từ năm 2013, khi Bộ Chính trị, Ban Cán sự đảng Chính phủ giao Đảng ủy Công an Trung ương, Bộ Công an xây dựng Chiến lược an ninh mạng quốc gia, nội dung hoàn thiện hệ thống văn bản pháp luật về an ninh mạng, trong đó có xây dựng, tiến tới ban hành Luật An ninh mạng là một trong những nội dung trọng tâm của Chiến lược.

- Ngày 15/01/2017, Văn phòng Trung ương Đảng đã có thông báo số 26-TB/TW nêu rõ: “*Luật An toàn thông tin mạng hiện nay không đáp ứng được yêu cầu về công tác bảo vệ an ninh quốc gia trong tình hình hiện nay như không đủ hiệu lực để ngăn chặn thông tin xấu độc; phòng, chống tấn công mạng vào hệ thống thông tin quan trọng quốc gia, điển hình là vụ hàng không bị tấn công mạng. Nguy cơ an ninh mạng là rất lớn, tiến tới phải có văn bản pháp quy mới*”.

- Ngày 22/5/2018, Văn phòng Trung ương Đảng có công văn số 6694-CV/VPTW về việc ban hành Nghị quyết của Bộ Chính trị về Chiến lược An ninh mạng quốc gia đã thông báo ý kiến của Bộ Chính trị là “*Cơ bản tán thành với Tờ trình, Đề án và dự thảo Nghị quyết của Bộ Chính trị về Chiến lược An ninh mạng quốc gia do Ban Chỉ đạo chuẩn bị*”. Trong đó, mục 2.II đã nêu rõ một trong những mục tiêu của Chiến lược an ninh mạng quốc gia là “xây dựng, hoàn thiện hệ thống pháp luật, cơ chế, chính sách về an ninh mạng”; mục 2.III đã nêu rõ: “Tổ chức thực hiện hiệu quả Luật An ninh mạng”.

Như vậy, chủ trương, chính sách của Đảng, Nhà nước về an ninh mạng đã có từ rất lâu, thay đổi theo từng thời kỳ để phù hợp với sự phát triển của đất nước, trong đó, Bộ Chính trị, Ban Chấp hành Trung ương, Chính phủ, Thủ tướng Chính phủ, Ban Bí thư đã có nhiều văn bản chỉ đạo về an ninh mạng. Xây dựng, ban hành Luật An ninh mạng là một trong những nhiệm vụ quan trọng được đặt ra trong thời gian qua.

# II. NỘI DUNG CHÍNH CỦA LUẬT AN NINH MẠNG

Luật An ninh mạng được Kỳ họp thứ 5 Quốc hội khóa XIV thông qua với tỷ lệ **86.86%** số đại biểu tán thành, gồm **7** chương, **43** điều, quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức, cá nhân.

Luật An ninh mạng được chuẩn bị công phu, kỹ lưỡng, với sự tham gia đóng góp ý kiến của các bộ, ngành chức năng, hơn 30 doanh nghiệp viễn thông, công nghệ thông tin lớn trong nước như VNPT, FPT, BKAV; nhiều chuyên gia, tập đoàn kinh tế, viễn thông trong và ngoài nước, trong đó có Facebook, Google, Apple, Amazon, Hội đồng kinh doanh Hoa Kỳ - ASEAN, Hiệp hội điện toán đám mây châu Á; các cơ quan đại diện nước ngoài như Mỹ, Canada, Úc, Nhật Bản… và ý kiến rộng rãi của quần chúng nhân dân.

**Chương I quy định về những vấn đề chung:**

***- Xác định phạm vi điều chỉnh.*** Luật này quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

***- Các khái niệm cơ bản về an ninh mạng.***

*An ninh mạng* là sự bảo đảm thông tin, hệ thống thông tin và hoạt động trên không gian mạng không gây phương hại đến sự ổn định, phát triển bền vững của chế độ xã hội chủ nghĩa và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc, an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân. ***(Khoản 3, Điều 3, Luật An ninh mạng)***

Nội hàm an ninh mạng rất rộng, có tính mở.

***An ninh mạng là vấn đề an ninh phi truyền thống,*** bởi: **(1)** Mang tính toàn cầu, một quốc gia đơn lẻ không thể giải quyết được. **(2)** Mang tính phi chính phủ, bởi nhiều nguy cơ đe dọa an ninh mạng không xuất phát từ đường lối, chính sách của quốc gia mà do một nhóm người, một tổ chức nào đó gây ra. **(3)** Mang tính tương đối, không phải hành vi tấn công mạng nào cũng có mục đích xâm phạm an ninh quốc gia. **(4)** Có tính chuyển hóa, có thể từ vấn đề an ninh phi truyền thống trở thành vấn đề an ninh truyền thống khi vũ khí mạng được sử dụng vào các hoạt động vũ trang. **(5)** Mang tính vận động, các mối đe dọa gây ra từ an ninh mạng không cố định mà luôn thay đổi cả nội dung và hình thức. **(6)** Mang tính vô hình và khó xác định, không ai dự đoán được các mối đe dọa an ninh mạng sẽ xảy ra ở đâu, khi nào và hậu quả ra sao.

*An ninh mạng có quan hệ tác động qua lại với các vấn đề an ninh truyền thống là an ninh chính trị và an ninh quân sự.* Biến động chính trị với tên gọi “Mùa xuân ả Rập” tại hàng loạt quốc gia Trung Đông - Bắc Phi; sâu máy tính Stuxnet phá hủy hàng nghìn máy ly tâm tại Nhà máy Hạt nhân Busher và biến thể của nó là tác nhân gây nổ kho chứa tên lửa đạn đạo Sejil-2 của Iran; hàng loạt các bản thiết kế vũ khí tối tân của Mỹ bị tin tặc đánh cắp, hay mới đây là hệ thống tên lửa phòng không Patriot của Đức đặt tại Thổ Nhĩ Kỳ bị tin tặc kiểm soát... là những minh chứng rõ nhất cho thấy an ninh mạng đã tác động tới an ninh chính trị và an ninh quân sự như thế nào. Ở chiều ngược lại, xuất phát từ lợi ích chính trị, quân sự, các quốc gia không chỉ quan tâm bảo đảm an ninh mạng bằng năng lực công nghệ, chính sách, chiến lược mà còn quan tâm đến hoạt động tình báo, gián điệp mạng, “diễn biến hòa bình” trên không gian mạng, dẫn tới nguy cơ chiến tranh mạng.

An ninh mạng có quan hệ tác động qua lại, chồng lấn, chuyển hóa với các vấn đề an ninh phi truyền thống khác, như an ninh kinh tế, an ninh thông tin, an ninh tư tưởng - văn hóa, đấu tranh phòng, chống tội phạm xuyên quốc gia, khủng bố...

An ninh mạng ngày càng có vị trí quan trọng, là bộ phận không thể tách rời của ANQG. Chủ tịch Trung Quốc Tập Cận Bình đã nêu: **“không có an ninh mạng đồng nghĩa không có an ninh quốc gia”.**

Tổng thống Mỹ B. Obama khẳng định: “**Với tư cách là Tổng thống, tôi sẽ biến an ninh mạng trở thành ưu tiên hàng đầu trong thế kỷ XXI**”.

***- Khái niệm cơ bản về không gian mạng.***

**Không gian mạng** là mạng lưới kết nối toàn cầu của các cơ sở hạ tầng công nghệ thông tin, bao gồm Internet, các mạng viễn thông, các hệ thống máy tính, các hệ thống xử lý và điều khiển thông tin, là môi trường đặc biệt mà con người có thể thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

Cùng với sự phát triển không ngừng của các dịch vụ Internet, đặc biệt là sự xuất hiện và phát triển nhanh chóng của các kết nối không dây, Internet 3G, 4G (sắp tới là 5G), các mạng xã hội, các thiết bị di động thông minh và dịch vụ điện toán đám mây, con người tương tác đa chiều hơn, phản ánh sinh động hơn, tức thời hơn mọi mặt đời sống và các mối quan hệ xã hội lên Internet, biến Internet trở thành không gian xã hội, nơi con người có thể thực hiện các hành vi mang bản chất xã hội của mình, như giao tiếp, lao động, sáng tạo, học tập, sản xuất, tiêu dùng, vui chơi, giải trí… Không gian xã hội đó được gọi là không gian mạng.

Do đó, không gian mạng mang **bản chất vật lý** và **bản chất xã hội**.

Không gian mạng có cấu trúc ba lớp: (1) Hạ tầng truyền dẫn vật lý gồm các thiết bị phần cứng công nghệ thông tin kết nối một cách hợp lý với nhau, tạo ra các loại mạng. (2) Hạ tầng dịch vụ lõi và các dịch vụ tạo ra các giao thức để lưu trữ, xử lý, trao đổi thông tin, chủ yếu bao gồm các quy định chuẩn, hệ điều hành, các công nghệ nền tảng, như công nghệ phần mềm, công nghệ mạng, giao diện, phương thức giao tiếp, giao thức, truyền dẫn xử lý thông tin, điều khiển..., phần mềm ứng dụng với việc tạo các thư viện và dịch vụ dùng chung. (3) Hệ thống ứng dụng công nghệ thông tin và cơ sở dữ liệu, các phần mềm ứng dụng để thông tin dưới dạng số được tạo ra, lưu trữ, xử lý, trao đổi nhằm phục vụ nhu cầu cuộc sống và tác động đến nhận thức của con người.

Không gian mạng được xác lập từ 06 thành tố:

**(1)Chính sách, pháp luật** quy định các quy tắc ứng xử cho tổ chức, cá nhân khi tham gia không gian mạng, quy định các mối quan hệ giữa cơ quan quản lý nhà nước với tổ chức, cá nhân; giữa các quốc gia và tổ chức quốc tế, tạo hành lang pháp lý bảo đảm hoạt động an toàn và hiệu quả của không gian mạng, mở đường cho công nghệ phát triển an toàn. Dưới góc độ quốc phòng, an ninh, nếu chính sách, pháp luật không đầy đủ, chặt chẽ thì chủ quyền không gian mạng dễ bị xâm hại hoặc kìm hãm sự phát triển của xã hội; các quyền cơ bản và quyền sở hữu hợp pháp của cơ quan, tổ chức, cá nhân sẽ không được bảo vệ thỏa đáng...

**(2)Năng lực công nghệ** là khả năng sử dụng công nghệ sẵn có và nghiên cứu công nghệ mới tác động đến không gian mạng. Các loại công nghệ nền tảng, như công nghệ mạng (nếu không có công nghệ mạng, thì không có Internet, mạng viễn thông, truyền thông...), công nghệ điện tử, bán dẫn, vi xử lý (nếu không có công nghệ điện tử, bán dẫn, vi xử lý sẽ không có các nền tảng phần cứng), công nghệ phần mềm (nếu không có công nghệ phần mềm thì không có “linh hồn” cho máy tính và mạng máy tính hoạt động). Ngoài ra, còn có các quy định chuẩn công nghệ, các quy trình phương thức giao tiếp, giao diện giữa các tầng kiến trúc của công nghệ... Tất cả những điều đó nói lên khả năng sáng tạo và ứng dụng công nghệ do con người làm chủ, đóng vai trò cốt lõi trong việc tác động vào không gian mạng, năng lực công nghệ đủ mạnh là yếu tố nền tảng để làm chủ các hoạt động trên không gian mạng.

**(3)Nội dung thông tin**được lưu trữ, xử lý và trao đổi trên không gian mạng, làm nảy sinh các yêu cầu nghiệp vụ chuyên ngành hoặc nhu cầu xã hội, được thực hiện trên không gian mạng nhằm phục vụ cho mục đích nhất định. Ví dụ, nghiệp vụ chẩn đoán lâm sàng ngành y tế dùng cho khám chữa bệnh trực tuyến; nghiệp vụ sư phạm phục vụ đào tạo trực tuyến... Trong lĩnh vực bảo vệ an ninh quốc gia, khi thông tin, tài liệu chứa đựng bí mật nhà nước được lưu trữ, xử lý, trao đổi trên không gian mạng sẽ phát sinh các yêu cầu nghiệp vụ, như hoạt động tình báo, gián điệp nhằm chiếm đoạt thông tin và hoạt động bảo vệ thông tin của chủ sở hữu, hay hoạt động phản gián của cơ quan an ninh. Vì vậy, nội dung thông tin sẽ quyết định không gian mạng của một ngành khoa học nào đó được tạo ra như thế nào, việc sử dụng và phát triển ra sao. Đây chính là định hướng cho sự phát triển không gian mạng.

**(4)Nguồn nhân lực** chính là con người được đào tạo bài bản, hoạt động chuyên biệt, hiểu biết pháp luật, nắm vững công nghệ và kiến thức, nghiệp vụ chuyên ngành. Một nguồn nhân lực như vậy sẽ luôn giành thế chủ động trên không gian mạng. Yếu tố nguồn nhân lực đóng vai trò quyết định cho mọi hoạt động của con người trên không gian mạng.

**(5)Tổ chức bộ máy** là hệ thống cơ quan quản lý nhà nước vận hành thông suốt từ khâu hạ tầng kỹ thuật đến dịch vụ ứng dụng, quản lý, bảo vệ và điều tiết chính sách, pháp luật trên không gian mạng. Vai trò của nó là kết nối một cách hiệu quả các yếu tố trên không gian mạng.

**(6)Ý thức của người** trên không gian mạng là sự tôn trọng chính sách, pháp luật, chuẩn công nghệ, quy tắc nghiệp vụ. ý thức con người quyết định tốc độ và xu hướng phát triển của không gian mạng.

***- Chính sách của Nhà nước về an ninh mạng.***

***- Nguyên tắc bảo vệ an ninh mạng.***

*Điều 4. Nguyên tắc bảo vệ an ninh mạng*

1. Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

2. Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.

3. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho các tổ chức, cá nhân hoạt động trên không gian mạng.

4. Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.

5. Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia. Áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

6. Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên giám sát, kiểm tra về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

7. Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

***- Biện pháp bảo vệ an ninh mạng.***

*Điều 5. Biện pháp bảo vệ an ninh mạng*

1. Biện pháp bảo vệ an ninh mạng bao gồm:

a) Thẩm định an ninh mạng;

b) Đánh giá điều kiện an ninh mạng;

c) Kiểm tra an ninh mạng;

d) Giám sát an ninh mạng;

đ) Ứng phó, khắc phục sự cố an ninh mạng;

e) Đấu tranh bảo vệ an ninh mạng;

g) Sử dụng mật mã để bảo vệ thông tin mạng;

h) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật;

i) Yêu cầu xóa bỏ, truy cập, xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

k) Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng;

l) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật;

m) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự;

n) Các biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

2. Chính phủ quy định trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, trừ các biện pháp quy định tại điểm m và điểm n khoản 1 Điều này.

***- Bảo vệ không gian mạng quốc gia.***

 Theo quy định tại [Luật an ninh mạng 2018](https://thukyluat.vn/vb/luat-an-ninh-mang-55cb8.html#dieu_2-4) (Có hiệu lực thi hành từ ngày 01/01/2019) thì thuật ngữ không gian mạng quốc gia được quy định cụ thể như sau:

* Không gian mạng quốc gia là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.
* Luật An ninh mạng 2018 quy định trong quá trình hoạt động bảo vệ an ninh mạng phải đảm bảo các nguyên tắc sau:
* Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.
* Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.
* Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.
* Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.
* Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.
* Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.
* Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

***- Hợp tác quốc tế về an ninh mạng.***

* Theo quy định tại [Luật an ninh mạng 2018](https://thukyluat.vn/vb/luat-an-ninh-mang-55cb8.html#dieu_7) (Có hiệu lực thi hành từ ngày 01/01/2019) thì chính sách hợp tác quốc tế về an ninh mạng được quy định cụ thể như sau:
* Hợp tác quốc tế về an ninh mạng được thực hiện trên cơ sở tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng và cùng có lợi.

- Nội dung hợp tác quốc tế về an ninh mạng bao gồm:

+ Nghiên cứu, phân tích xu hướng an ninh mạng;

+ Xây dựng cơ chế, chính sách nhằm đẩy mạnh hợp tác giữa tổ chức, cá nhân Việt Nam với tổ chức, cá nhân nước ngoài, tổ chức quốc tế hoạt động về an ninh mạng;

+ Chia sẻ thông tin, kinh nghiệm; hỗ trợ đào tạo, trang thiết bị, công nghệ bảo vệ an ninh mạng;

+ Phòng, chống tội phạm mạng, hành vi xâm phạm an ninh mạng; ngăn ngừa các nguy cơ đe dọa an ninh mạng;

+ Tư vấn, đào tạo và phát triển nguồn nhân lực an ninh mạng;

+ Tổ chức hội nghị, hội thảo và diễn đàn quốc tế về an ninh mạng;

+ Ký kết và thực hiện điều ước quốc tế, thỏa thuận quốc tế về an ninh mạng;

+ Thực hiện chương trình, dự án hợp tác quốc tế về an ninh mạng;

+ Hoạt động hợp tác quốc tế khác về an ninh mạng.

* Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện hợp tác quốc tế về an ninh mạng, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.
* Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện hợp tác quốc tế về an ninh mạng trong phạm vi quản lý.
* Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong hoạt động hợp tác quốc tế về an ninh mạng.
* Trường hợp hợp tác quốc tế về an ninh mạng có liên quan đến trách nhiệm của nhiều Bộ, ngành do Chính phủ quyết định.
* Hoạt động hợp tác quốc tế về an ninh mạng của Bộ, ngành khác, của địa phương phải có văn bản tham gia ý kiến của Bộ Công an trước khi triển khai, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng.

***- Các hành vi bị nghiêm cấm về an ninh mạng.***

*Điều 8. Các hành vi bị nghiêm cấm*

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

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

b) Tổ chức, hoạt động, cấu 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;

c) 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;

d) Thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho các 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 tổ chức, cá nhân khác;

đ) 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 cộng đồng;

e) Xúi giục, lôi kéo, kích động người khác phạm tội.

2. 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.

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 máy tính, mạng viễn thông; phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc 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 tổ chức, cá nhân hoặc để trục lợi.

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

***- Xử lý vi phạm pháp luật về an ninh mạng.***

*Điều 9. Xử lý vi phạm pháp luật về an ninh mạng*

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 phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

**Chương II quy định về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.**

Đây là một trong những nội dung đặc biệt quan trọng của Luật An ninh mạng, thể hiện đầy đủ các biện pháp, hoạt động bảo vệ tương xứng với mức độ quan trọng của hệ thống thông tin này, trong đó nêu ra tiêu chí xác định, lĩnh vực liên quan, quy định các biện pháp như thẩm định an ninh mạng, đánh giá điều kiện, kiểm tra, giám sát an ninh mạng và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

***Tham khảo: 08 nguy cơ, thách thức tại hội thảo Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia (Quảng Ninh, năm 2017)***

**Thứ nhất**, nguy cơ gây rối loạn, mất kiểm soát hệ thống thông tin phục vụ quốc phòng an ninh.

Nếu cuộc tấn công mạng vào hệ thống thông tin điều khiển máy bay quân sự, máy bay không người lái, tên lửa hành trình … thì những phương tiện đó sẽ bị chiếm quyền sử dụng, thậm chí quay lại tấn công chính điểm xuất phát hoặc các mục tiêu quan trọng khác của đát nước.

**Thứ hai**, nguy cơ bị tấn công, chiếm đoạt, đánh cắp tài liệu, bí mật nhà nước từ hệ thống cơ sở dữ liệu, hệ thống mạng máy tính nội bộ.

Từ nguy cơ này có thể dẫn đến khả năng thất bại trong cuộc chiến tranh mạng khi đối phương nắm rõ hệ thống phòng thủ, lực lượng, tiềm lực, quân sự, phòng chống tấn công mạng hay thất bại trong các cuộc đàm phán ngoại giao, thương lượng khi mọi chủ trương, quyết sách, sự chuẩn bị bị đối phương kiểm soát.

Hàng năm, cơ quan chức năng phát hiện hàng chục vụ lộ lọt bí mật nhà nước trên mạng internet. Tin tặc có thể thực hiện tấn công mạng theo từng đợt hoặc âm thầm kéo dài nhiều năm mà chủ thể bị tấn công không hay biết.

Ở Việt Nam, thể hiện rõ nhất là đợt tấn công vào hệ thống thông tin của Vietnam Airlines kéo dài từ năm 2012 đến sự kiện nghiêm trọng ngày 29/7/2016.

Thời điểm này, trên màn hình thông tin chuyến bay tại sân bay Nội Bài, Tân Sơn Nhất xuất hiện nhiều thông tin kích động, xúc phạm Việt Nam và Philippines, xuyên tạc các nội dung về Biển Đông. Hệ thống phát thanh của sân bay cũng phát đi những thông điệp tương tự.

Cùng thời điểm, trên website của hãng hàng không Viet Nam cũng bị thay đổi nội dung, đồng thời đăng tải thông tin (họ tên, ngày sinh, địa chỉ, chức vụ, cơ quan công tác, số điện thoại …) của hơn 400.000 tài khoản khách hàng thành viên của Viet nam Airlines.

**Thứ ba**, nguy cơ đình trệ, tê liệt hoạt động của hệ thống cổng thông tin điện tử, trang thông tin của các cơ quan Đảng, Nhà nước.

Tấn công mạng có thể khiến hoạt động quản lý, điều hành của Chính phủ bị tê liệt hoặc làm sai lệch, cung cấp thông tin sai sự thật gây hoang mang, bất bình và hỗn loạn của quần chúng nhân dân mà ví dụ rõ nhất là kết quả một số cuộc bầu cử HĐND các cấp bị làm giả, sai lệch.

Ngoài ra, việc các hạ tầng dịch vụ lõi (router, thiết bị mạng…) dùng trong các cơ quan nhà nước bị tấn công có thể khiến các mệnh lệnh chỉ đạo trong tình huống khẩn cấp bị gián đoạn, vô hiệu hóa.

**Thứ tư**, tấn công mạng kéo theo nguy cơ gây rối loạn các giao dịch tài chính, hoạt động vận hành, điều khiển hành không, điện lưới quốc gia, hệ thống giao thông đường bộ, xử lý hóa chất phục vụ cung cấp nước sinh hoạt, y tế…

Khi đó, nhiều kịch bản thảm họa có thể sẽ hiện hữu như: dịch vụ hải quan bị xâm nhập khiến hành trình của hàng nghìn khách hàng và chuyến bay quốc tế bị ngưng hoạt động, gián đoạn; hệ thống ngân hàng tự động chuyển tiền đến hàng trăm, hàng nghìn tài khoản cuàng lúc; 5 thành phố trực thuộc trung ương đồng loạt mất điện; chất độc hại xuất hiện trong nước sinh hoạt cung cấp cho Hà Nội, Tp.HCM hay các thiết bị y tế mà hệ thống đo lường, cảnh báo bị vô hiệu hóa …

**Thứ năm**, nguy cơ hệ thống điều khiển tự động hóa (SCADA) của các nhà máy lọc dầu, thủy điện, nhiệt điện, đường ống xăng dầu, khí đốt… bị tê liệt, rối loạn, dẫn đến nguy cơ mất an toàn cháy nổ. Ảnh hưởng này gây thiệt hại vô cùng lớn về mặt kinh tế, an ninh trật tự và đời sống dân sinh.

**Thứ sáu**, nguy cơ hệ thống thông tin phục vụ phát thanh, truyền hình, báo chí, xuất bản của nhà nước bị kiểm soát, vô hiệu hóa. Ở cấp độ thấp, đó là những tin đồn thất thiệt, thông tin xuyên tạc sai tự thật gây mất niểm tin của nhân dân.

Cao hơn , đó là hoạt động kích động biểu tình, gây bạo loạn, lật đổ trên cơ quan báo chí chính thống…ảnh hưởng trực tiếp đến sự tồn vong của chế độ XHCN và Nhà nước CHXHCN Việt Nam.

**Thứ bảy**, nguy cơ bị kiểm soát, chiếm đoạt, phá hủy hệ thống thông tin phục vụ cơ sở dữ liệu quốc gia về thủ tục hành chính, dân cư, xuất nhập cảnh, … dẫn tới sự đình trệ hoạt động từ trung ương tới địa phương, sự quá tải của các cơ quan quản lý xuất nhập cảnh và tại các nhà ga, san bay quốc tế.

**Thứ tám**, nguy cơ tấn công mạng nhằm vào hạ tầng truyền dẫn vật lý (cáp truyền dẫn quốc tế, trục tuyến dẫn nội bộ quốc gia …) khiến kết nối internet của Việt nam với quốc tế bị gián đoạn hoặc ngừng. Từ đó, hàng loạt giao dịch về mọi lĩnh vực của Việt nam với thế giới bị ảnh hưởng

Đặc biệt, nguy cơ Việt Nam bị mất chủ quyền trên không gian mạng, kéo theo sự thất bại trong một cuộc chiến tranh mạng mà hậu quả khôn lường.

**Để bảo vệ tối đa quyền và lợi ích hợp pháp của tổ chức, cá nhân, Chương III Luật An ninh mạng quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật.** Bao gồm: (1) Phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; (2) Phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; (3) Phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội; (4) Phòng, chống tấn công mạng; (5) Phòng, chống khủng bố mạng; (6) Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; (7) Đấu tranh bảo vệ an ninh mạng. Đây là hành lang pháp lý vững chắc để người dân có thể yên tâm buôn bán, kinh doanh hay hoạt động trên không gian mạng.

**Chương IV tập trung quy định về triển khai hoạt động bảo vệ an ninh mạng một cách đồng bộ, thống nhất từ Trung ương tới địa phương, trọng tâm là các cơ quan nhà nước và tổ chức chính trị,** quy định rõ các nội dung triển khai, hoạt động kiểm tra an ninh mạng đối với hệ thống thông tin của các cơ quan, tổ chức này. Cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế cũng là một trong những đối tượng được bảo vệ trọng điểm. Với các quy định chặt chẽ, sự tham gia đồng bộ của cơ quan nhà nước, doanh nghiệp và tổ chức, cá nhân, việc sử dụng thông tin để vu khống, làm nhục, xâm phạm danh dự, nhân phẩm, uy tín của người khác sẽ được xử lý nghiêm minh. Các hoạt động nghiên cứu, phát triển an ninh mạng, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng, nâng cao năng lực tự chủ về an ninh mạng và bảo vệ trẻ em trên không gian mạng cũng được quy định chi tiết trong Chương này.

Hiện nay, dữ liệu của người sử dụng Việt Nam trên không gian mạng đã và đang bị sử dụng tràn lan, với mục đích thu lợi nhuận mà Nhà nước chưa có đủ hành lang pháp lý để quản lý, thậm chí là bị sử dụng vào các âm mưu chính trị hoặc vi phạm pháp luật. Để quản lý chặt chẽ, bảo vệ nghiêm ngặt dữ liệu của nước ta trên không gian mạng, Khoản 3 Điều 26 Luật An ninh mạng đã quy định: “*Doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ*”.

Nguồn nhân lực bảo vệ an ninh mạng là một trong những yếu tố quyết định sự thành bại của công tác bảo vệ an ninh mạng. Chương V Luật An ninh mạng đã quy định đầy đủ các nội dung bảo đảm triển khai hoạt động bảo vệ an ninh mạng, xác định lực lượng chuyên trách bảo vệ an ninh mạng, ưu tiên đào tạo nguồn nhân lực an ninh mạng chất lượng cao, chú trọng giáo dục, bồi dưỡng, phổ biến kiến thức về an ninh mạng.

**Trách nhiệm của cơ quan, tổ chức, cá nhân cũng được quy định rõ trong Chương VI, tập trung vào trách nhiệm của lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng.** Theo chức năng, nhiệm vụ được giao, các bộ, ngành chức năng có trách nhiệm thực hiện đồng bộ các biện pháp được phân công để hướng tới một không gian mạng ít nguy cơ, hạn chế tối đa các hành vi vi phạm pháp luật trên không gian mạng.

**Chương VII quy định về Điều khoản thi hành,** theo đó Luật có hiệu lực thi hành từ ngày 01 tháng 01 năm 2019.

# III. MỘT SỐ VẤN ĐỀ THU HÚT SỰ CHÚ Ý CỦA DƯ LUẬN

## 1. Một số vấn đề băn khoăn trong quá trình xây dựng, thảo luận về Luật An ninh mạng

### 1.1. Sự ảnh hưởng, tác động của Luật An ninh mạng đối với các doanh nghiệp hoạt động các lĩnh vực công nghệ, truyền thông và nội dung số?. Luật An ninh mạng có gây cản trở các doanh nghiệp viễn thông, internet và các doanh nghiệp khởi nghiệp Việt Nam, có tạo giấy phép con không?

**Nhiệm vụ của Luật An ninh mạng. Luật An ninh mạng sẽ tập trung giải quyết tổng thể các vấn đề sau:**

- Quy định và hướng dẫn các tổ chức, cá nhân thực hiện biện pháp đảm bảo an ninh mạng.

- Quy định về việc kiểm tra, giám sát hệ thống mạng, tiến hành các hoạt động phòng ngừa, phát hiện và đấu tranh với hoạt động sử dụng dịch vụ Viễn thông, Internet và thông tin trên mạng gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

- Bảo vệ thông tin thuộc bí mật nhà nước không bị chiếm đoạt, lộ, lọt trên Internet.

- Bảo vệ an toàn các cổng thông tin điện tử, báo điện tử, trang thông tin điện tử của cơ trọng yếu, các hệ thống cơ sở dữ liệu trọng yếu của quốc gia; bảo vệ an toàn cơ sở hạ tầng thông tin quan trọng liên quan đến an ninh quốc gia.

- Sử dụng các biện pháp nghiệp vụ, kỹ thuật được pháp luật quy định để phòng ngừa, đấu tranh ngăn chặn âm mưu, hoạt động sử dụng dịch vụ Internet và thông tin trên mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

- Phối hợp với các cơ quan hữu quan thực hiện quản lý nhà nước về an ninh mạng đối với hoạt động cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng; thanh tra, kiểm tra việc chấp hành các quy định về đảm bảo an ninh mạng.

- Tuyên truyền nâng cao ý thức tự giác chấp hành các quy định về công tác bảo đảm an ninh mạng cho người sử dụng.

- Điều chỉnh toàn diện và bao quát về an ninh mạng, đặc biệt là các vấn đề tình báo mạng, gián điệp mạng, chiến tranh mạng, khủng bố mạng; đảm bảo sự thống nhất, tương thích, tham chiếu với các văn bản liên quan an toàn thông tin.

- Phân định rõ các hành vi cần sự điều chỉnh và tuân thủ của pháp luật về an ninh mạng, đáp ứng sự phát triển nhanh chóng của công nghệ thông tin và truyền thông, đáp ứng xu thế hội tụ công nghệ và xu thế hội nhập kinh tế quốc tế. Xác định rõ các hành vi vi phạm an ninh mạng có thể dẫn đến vi phạm an ninh thông tin cấu thành tội phạm.

- Làm rõ quyền hạn, trách nhiệm pháp lý của các cá nhân, tổ chức, doanh nghiệp, nhà nước trong việc áp dụng, thực thi các biện pháp, chương trình bảo vệ thông tin và đảm bảo an ninh mạng; đảm bảo quyền lợi hợp pháp của các đối tượng trong hoạt động đảm bảo an ninh mạng.

- Làm rõ các quy định về đầu tư vào an ninh mạng và kinh doanh trong lĩnh vực an ninh mạng. Định hướng phát triển cho doanh nghiệp và thị trường công nghệ thông tin. Xác định rõ yêu cầu đảm bảo an ninh mạng trong công tác đầu tư, phát triển mạng và các dịch vụ. Xác lập cơ chế, chính sách trong các hoạt động công ích về an ninh mạng, phát huy mọi nguồn lực xã hội vào các hoạt động công ích đảm bảo an ninh mạng.

**Mục tiêu của việc ban hành Luật An ninh mạng**

Xuất phát từ yêu cầu thực tiễn nêu trên, việc xây dựng Luật an ninh mạng là cần thiết nhằm đạt các mục tiêu chủ yếu sau đây:

(1) Ban hành văn bản Luật đầu tiên về an ninh mạng theo hướng đảm bảo tính thống nhất, đồng bộ, khả thi của các quy định trong lĩnh vực này.

(2) Phát huy các nguồn lực của đất nước để phát triển ngành an ninh mạng đáp ứng cho phát triển kinh tế - xã hội, quốc phòng, an ninh, góp phần nâng cao chất lượng cuộc sống của nhân dân, bảo đảm quốc phòng, an ninh, giữ gìn trật tự an toàn xã hội.

(3) Tôn trọng, bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động an ninh mạng; ngăn chặn những hành vi lợi dụng mạng thông tin gây ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội.

(4) Đẩy mạnh công tác bảo vệ an ninh quốc gia trên không gian mạng, bảo vệ hệ thống mạng thông tin trọng yếu quốc gia. Chỉ định cơ quan quản lý an ninh mạng để đảm bảo hiệu quả công tác thực thi quản lý nhà nhà nước trong lĩnh vực này.

(5) Mở rộng hợp tác quốc tế về an ninh mạng trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với pháp luật Việt Nam và điều ước quốc tế mà Việt Nam ký kết hoặc tham gia.

**Luật An ninh mạng có thể tác động ở một số mặt như sau:**

***+ Trên lĩnh vực bảo vệ an ninh quốc gia, giữ gìn trật tự an toàn xã hội:***

• Bảo vệ an ninh, chủ quyền quốc gia trên không gian mạng, đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia có hiệu quả hơn khi có những quy định rõ ràng, đồng bộ, thống nhất trong lĩnh vực an ninh mạng.

• Tăng cường hiệu quả công tác đấu tranh với các hoạt động tội phạm sử dụng không gian mạng xâm phạm trật tự an toàn xã hội.

• Tạo khung pháp lý cho việc điều tra, xác minh, củng cố chứng cứ, nhất là nguồn chứng cứ điện tử.

***+ Tác động về hiệu quả quản lý nhà nước:***

• Tăng cường công tác quản lý nhà nước về an ninh thông tin, an ninh mạng, hạn chế những tồn tại bất cập trong quản lý nhà nước về an ninh mạng hiện nay như: việc xem nhẹ vấn đề bảo đảm an ninh thông tin, an ninh mạng, vi phạm các nguyên tắc bảo đảm an ninh thông tin, an ninh mạng; có sự định hướng về nguồn nhân lực, đội ngũ cán bộ làm công tác quản lý nhà nước về an ninh mạng; hạn chế những nguy cơ mất an ninh thông tin, an ninh mạng khi sử dụng các thiết bị nhập khẩu từ nước ngoài; chưa có tiêu chuẩn thống nhất về an ninh thông tin, an ninh mạng; hạn chế lộ lọt bí mật nhà nước.

• Tăng cường bảo vệ thông tin nhạy cảm, bí mật nhà nước không bị chiếm đoạt, lộ, lọt trên mạng Internet; bảo đảm an ninh thông tin cho các Cổng thông tin điện tử, báo điện tử, trang thông tin điện tử của cơ quan trọng yếu, các hệ thống cơ sở dữ liệu trọng yếu của quốc gia; bảo vệ an toàn cơ sở hạ tầng thông tin quan trọng liên quan đến an ninh quốc gia.

• Quy định rõ ràng, thống nhất việc sử dụng các biện pháp nghiệp vụ, kỹ thuật được pháp luật quy định để phòng ngừa, đấu tranh ngăn chặn âm mưu, hoạt động sử dụng dịch vụ Internet và thông tin trên mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

• Nâng cao trách nhiệm của các cơ quan hữu quan thực hiện quản lý nhà nước về viễn thông, Internet đối với hoạt động cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng.

• Tổ chức triển khai thực thi công tác đảm bảo an ninh mạng có hiệu quả hơn khi môi trường pháp lý hoàn thiện, đồng bộ, thể chế hóa kịp thời bằng các văn bản pháp luật tạo hành lang pháp lý cho hoạt động đảm bảo an ninh mạng.

• Tạo được sự bình đẳng và cân bằng về mặt pháp lý trong việc điều chỉnh tổ chức và hoạt động của các tổ chức hoạt động trên lĩnh vực an ninh mạng phù hợp với tình hình phát triển nền kinh tế thị trường, yêu cầu hội nhập quốc tế hiện nay.

• Tạo cơ chế, chính sách, biện pháp thúc đẩy phát triển các hoạt động đảm bảo an ninh mạng thông thoáng, phù hợp với tình hình mới.

• Tổ chức quản lý có hiệu quả hơn khi phân định rõ trách nhiệm của các Bộ, ngành, địa phương; quy định rõ trách nhiệm của chủ thể trong công tác quản lý nhà nước.

***+ Tác động về kinh tế:***

Theo kết quả nghiên cứu của các hãng bảo mật Việt Nam và thế giới, trên 40% website của Việt Nam hiện nay đang tồn tại lỗ hổng bảo mật, mỗi năm Việt Nam thiệt hại hơn 8.000 tỷ đồng từ các cuộc tấn công mạng. Việc ban hành Luật An ninh mạng sẽ tăng cường bảo đảm an ninh thông tin cho hệ thống mạng thông tin Việt Nam, tạo cơ sở vững chắc cho các thành phần kinh tế có hoạt động trên không gian mạng phát triển, hạn chế thiệt hại về kinh tế có thể xảy ra.

***+ Cải thiện mối quan hệ giữa Nhà nước và công dân:***

• Nâng cao ý thức tự giác chấp hành các quy định về công tác bảo đảm an ninh mạng cho người sử dụng.

• Phân định rõ các hành vi cần sự điều chỉnh và tuân thủ của pháp luật về an ninh mạng, đáp ứng sự phát triển nhanh chóng của công nghệ thông tin và truyền thông, đáp ứng xu thế hội tụ công nghệ và xu thế hội nhập kinh tế quốc tế. Xác định rõ các hành vi vi phạm an ninh mạng có thể dẫn đến vi phạm an ninh thông tin cấu thành tội phạm.

• Làm rõ quyền hạn, trách nhiệm pháp lý của các cá nhân, tổ chức, doanh nghiệp, nhà nước trong việc áp dụng, thực thi các biện pháp, chương trình bảo vệ thông tin và đảm bảo an ninh mạng; đảm bảo quyền lợi hợp pháp của các đối tượng trong hoạt động đảm bảo an ninh mạng.

• Làm rõ các quy định về đầu tư vào an ninh mạng và kinh doanh trong lĩnh vực an ninh mạng. Xác định rõ yêu cầu đảm bảo an ninh mạng trong công tác đầu tư, phát triển mạng và các dịch vụ. Xác lập cơ chế, chính sách trong các hoạt động công ích về an ninh mạng, phát huy mọi nguồn lực xã hội vào các hoạt động công ích đảm bảo an ninh mạng.

**- Trong Luật An ninh mạng không có quy định nào kiểm soát, quản lý, hạn chế hay gây cản trở hoạt động kinh doanh của doanh nghiệp, cũng như hoạt động khởi nghiệp.**

**Không có quy định nào trong Luật An ninh mạng có nội dung cấp giấy phép con.**

Luật An ninh mạng chỉ quy định trách nhiệm phối hợp của doanh nghiệp trong bảo vệ an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng, phòng chống các hành vi vi phạm pháp luật về an ninh mạng được quy định tại Chương III.

Luật An ninh mạng còn có những quy định mang tính hướng dẫn các doanh nghiệp, tổ chức, cá nhân áp dụng các biện pháp để tự bảo vệ mình trước những mối đe dọa từ không gian mạng.

### 1.2. Phạm vi điều chỉnh và một số nội dung trong Luật An ninh mạng tồn tại sự trùng dẫm với Luật An toàn thông tin mạng

Đây là ý kiến được nêu ra bởi Bộ Thông tin và Truyền thông, Hiệp hội An toàn thông tin số (thuộc Bộ Thông tin và Truyền thông), ý kiến của một số đại biểu Quốc hội cho rằng, Luật An toàn thông tin mạng đã quy định về trật tự an toàn xã hội, hệ thống thông tin quan trọng quốc gia, kiểm tra an toàn thông tin mạng, nếu Luật An ninh mạng tiếp tục quy định sẽ gây trùng dẫm, chồng chéo.

Thực tế:

- Phạm vi Luật An toàn thông tin mạng tập trung bảo đảm 3 thuộc tính nguyên vẹn, bảo mật và khả dụng của thông tin mạng; trong khi đó, phạm vi Luật An ninh mạng tập trung bảo đảm hoạt động sử dụng không gian mạng không gây phương hại đến an ninh quốc gia (*bao gồm chế độ và nhà nước CHXHCN Việt Nam, độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc, bí mật nhà nước*), trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

- Luật An toàn thông tin mạng tập trung quy định các hoạt động quản lý hành chính nhà nước, còn Luật An ninh mạng quy định các nội dung, biện pháp, hình thức nhằm phòng ngừa, ngăn chặn, đấu tranh, xử lý các hành vi vi phạm pháp luật trên không gian mạng.

Khi so sánh, đối chiếu và thẩm tra nội dung dự thảo Luật An ninh mạng, Ủy ban Quốc phòng và An ninh, Ủy ban Pháp luật của Quốc hội đã nhận thấy rằng, do sự khác nhau về khách thể, đối tượng, mục tiêu, phương pháp nên nội dung và các hoạt động triển khai nhằm bảo vệ an ninh mạng không trùng dẫm với Luật An toàn thông tin mạng.

Như vậy, sự khác biệt cơ bản giữa Luật An toàn thông tin mạng và Luật An ninh mạng đã được thể hiện rõ ngay từ sự cấp thiết ban hành và phạm vi điều chỉnh của Luật An ninh mạng. Luật An toàn thông tin mạng chủ yếu quy phạm các loại trạng thái có khả năng gây hại về kỹ thuật và những vấn đề chung đặt ra trong quản lý nhà nước về an toàn thông tin. Luật An ninh mạng tập trung điều chỉnh các hành vi có khả năng gây hại cho an ninh quốc gia, trật tự an toàn xã hội, quy định các biện pháp phòng ngừa, phát hiện, đấu tranh, xử lý để loại bỏ các mối nguy hại với an ninh quốc gia, trật tự an toàn xã hội.

### 1.3. Nguyên tắc bảo vệ an ninh mạng

* Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.
* Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nồng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.
* Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.
* Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.
* Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.
* Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.
* Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

 ***Cơ sở hạ tầng và an ninh mạng***

 Năm ngoái, British Airways đã hủy hơn 400 chuyến bay và khiến 75.000 hành khách bị mắc kẹt vì gặp phải lỗi công nghệ thông tin do một kỹ sư đã ngắt kết nối nguồn điện tại trung tâm dữ liệu gần sân bay Heathrow của Luân Đôn. Khi nói đến các trung tâm dữ liệu và mạng lưới, ngay cả những lỗi nhỏ của con người cũng có thể có tác động cực kỳ lớn đến các doanh nghiệp và khách hàng của họ.

 Với chi phí cắt cổ và nguồn nhân lực cần thiết để duy trì hệ thống tại chỗ, các tổ chức nên tìm đến các công ty cung cấp dịch vụ điện toán đám mây công cộng có các nguồn lực cần thiết để quản lý và bảo mật các trung tâm dữ liệu của họ một cách chính xác.

 Các công ty điện toán đám mây công cộng đầu tư vốn và chuyên môn vào hệ thống. Cơ sở hạ tầng vật lý và trung tâm dữ liệu của họ được bảo vệ tốt hơn nhiều so với những gì mà hầu hết các công ty có thể tự mình thực hiện. Ví dụ: Google tập trung vào bảo mật và bảo vệ dữ liệu được ăn sâu trong các giải pháp công nghệ và văn hóa của công ty họ. Với ý nghĩ đó, nó là tiêu chí thiết kế chính khi họ xây dựng trung tâm dữ liệu.

 Google sử dụng mô hình bảo mật lớp bao gồm các biện pháp bảo vệ như thẻ truy cập điện tử được thiết kế tùy chỉnh, cảnh báo, rào cản truy cập xe, hàng rào chu vi, máy dò kim loại, sinh trắc học và phát hiện xâm nhập chùm tia laser trên tầng trung tâm dữ liệu. Các trung tâm dữ liệu cũng được giám sát 24/7 bằng camera với độ phân giải cao có thể phát hiện và theo dõi những kẻ xâm nhập. Các bản ghi truy cập, hồ sơ hoạt động và cảnh quay của camera luôn có sẵn trong trường hợp xảy ra sự cố. Hơn nữa, nó chỉ có thể truy cập vào tầng trung tâm dữ liệu bằng cách sử dụng một hành lang an ninh có tính năng kiểm soát truy cập đa yếu tố đòi hỏi một mã tổng hợp bảo mật và xác nhận sinh trắc học. Chỉ những nhân viên được cho phép và có vai trò cụ thể mới được cung cấp thông tin đăng nhập cần thiết để truy cập.

 ***Bảo mật mạng***

 Nếu bạn nghĩ rằng tường lửa của bạn được an toàn, hãy suy nghĩ lại. Bảo mật vật lý là quan trọng nhưng bảo mật mạng của bạn cũng quan trọng. Nó giống như một cuộc chạy đua vũ trang giữa tường lửa phòng thủ và hệ thống an ninh và tin tặc. Gần một nửa (48%) các tổ chức bị một cuộc tấn công mạng xác định nguyên nhân gốc rễ của việc vi phạm dữ liệu của họ là từ một cuộc tấn công nguy hiểm.

 Không chỉ tường lửa được xây dựng bên trong thường bị quản lý kém và dễ bị tấn công hơn, chúng cũng không thể cung cấp cho các tổ chức các cảnh báo nguy cơ cần thiết. Các công ty duy nhất thực sự có đủ nhân viên được đào tạo bài bản, đúng chuyên môn và các nguồn lực cần thiết để luôn đứng đầu về an ninh mạng là các công ty cung cấp dịch vụ điện toán đám mây công cộng.

 Với rất nhiều lỗ hổng trên mạng, ví dụ như năm backdoors mà Cisco phát hiện năm nay với con sâu Conficker USB khét tiếng, bạn cần sự bảo vệ tốt nhất. Nếu không được bảo trì thường xuyên, tin tặc có thể và sẽ vượt qua tường lửa của bạn và các phần mềm bảo mật có sẵn khác. Chỉ có tường lửa là không đủ để đảm bảo rằng dữ liệu được đặt trong mạng bảo mật của công ty bạn là an toàn. Tuy nhiên, việc kiểm tra, bảo trì và nâng cấp liên tục là quá khắt khe đối với nhiều doanh nghiệp đang cố gắng tự thực hiện.

 Mặt khác, một số công ty điện toán đám mây hàng đầu sử dụng hàng trăm chuyên gia bảo mật và quyền riêng tư trong các bộ phận kỹ thuật và hoạt động phần mềm của họ. Nhân viên của các công ty điện toán đám mây công cộng bao gồm một số chuyên gia hàng đầu thế giới về bảo mật dữ liệu, ứng dụng và an ninh mạng - xuất bản hàng trăm nghiên cứu về bảo mật thông tin và mật mã hàng năm. Đội ngũ chuyên môn cao của họ được chia thành các bộ phận nhanh nhẹn hơn dành riêng cho các lĩnh vực bao gồm bảo mật, quyền riêng tư, kiểm toán nội bộ và tuân thủ, và an ninh hoạt động. Mức chuyên môn này đảm bảo rằng nhu cầu bảo mật của khách hàng sẽ nhận được sự chú ý nhiều hơn nữa.

 ***Nâng cấp phần mềm***

 Nhiều lỗ hổng mạng được mô tả trong phần trước đã nhanh chóng được các nhà cung cấp cố định sau khi chúng được phát hiênh, nhưng điều này là không đủ. Các công ty cũng cần phải cập nhật hệ điều hành, cơ sở dữ liệu và máy chủ web của họ để các bản vá được áp dụng. Nhiều người bỏ qua trách nhiệm này. Khi phần mềm không được cập nhật đúng cách để bảo vệ chống lại các mối đe dọa trên mạng mới nhất, toàn bộ công ty sẽ gặp rủi ro.

 Khi nói đến việc bảo trì phần mềm, có nhiều điều hơn là nâng cấp và chi phí lắp đặt. Khả năng cập nhật ngăn xếp phần mềm của công ty cũng phụ thuộc vào khả năng của nhóm CNTT của công ty và từng cá nhân nhân viên sử dụng thiết bị cá nhân do công ty phát hành hoặc thiết bị cá nhân cho công việc. Việc cập nhật hệ thống và thiết bị mà không bị gián đoạn dịch vụ cũng là một thách thức. Nhiều phòng CNTT sẽ trì hoãn việc triển khai các bản cập nhật quan trọng để giảm thiểu tác động của gián đoạn.

 Đây là một cạm bẫy phổ biến của các tổ chức sử dụng phần mềm ngoài ngày kết thúc chính thức của ngày hỗ trợ. Điều này đặt các tổ chức như vậy ở một nguy cơ rất lớn, đó là không thể vá lỗ hổng nghiêm trọng. Ví dụ, như trường hợp với WannaCry. Các bản vá lỗi cho phần mềm cũ không có sẵn khi kết thúc ngày hỗ trợ là vào năm 2014.

 Các tác động của lỗ hổng phần mềm có thể nghiêm trọng như bất kỳ vi phạm bảo mật CNTT nào khác. Ví dụ, IHG phát hành dữ liệu cho thấy rằng tiền mặt đăng ký tại hơn 1.000 tài sản của nó đã bị tổn hại bởi phần mềm độc hại được thiết kế để hút dữ liệu thẻ ghi nợ và thẻ tín dụng của khách hàng.

 Sử dụng quản lý lỗ hổng chuyên dụng, bằng cách phòng chống phần mềm độc hại và các nhóm giám sát, Google cung cấp cho khách hàng của mình một nền tảng kinh doanh an toàn. Chiến lược phòng chống phần mềm độc hại của Google sử dụng máy quét thủ công và tự động để quét chỉ mục tìm kiếm của họ cho các tên miền có thể là phương tiện cho phần mềm độc hại hoặc mưu đồ lừa đảo. Google cũng sử dụng nhiều công cụ chống vi-rút trong Gmail và Drive cũng như trên máy chủ và máy trạm của họ để giúp xác định phần mềm độc hại có thể bị các chương trình chống vi-rút khác bỏ qua.

 ***Xác thực người dùng***

 Yêu cầu về xác thực người dùng phải đi một chặng đường dài để đảm bảo an ninh phù hợp cho tổ chức. Điều quan trọng là phải đảm bảo rằng những người đang truy cập dữ liệu của bạn là những người mà họ cho phép. Điều này có thể đạt được bằng mật khẩu mạnh, xác thực đa yếu tố và các khóa bảo mật vật lý; là tất cả những thứ mà các công ty điện toán đám mây công cộng đang đầu tư rất nhiều.

 Ví dụ: Khóa bảo mật Titan của Google sử dụng xác thực đa yếu tố để bảo vệ người dùng khỏi các cuộc tấn công. Tin tặc có thể lấy cắp mật khẩu của bạn trong thế giới kỹ thuật số nhưng chúng sẽ gặp khó khăn hơn nhiều khi ăn cắp một khóa bảo mật vật lý. Với thực hành xác thực nhiều lớp, các tổ chức giảm nguy cơ giả mạo của người không được phép muốn thay thế thông tin của người dùng thực.

 Chỉ cần nhìn vào những gì đã xảy ra vào năm 2017 đối với Deloitte, một khi được Gartner đặt tên là “nhà tư vấn bảo mật không dây tốt nhất trên thế giới”, đã thất bại trong việc sử dụng xác thực đa yếu tố. Tin tặc đã có thể truy cập mạng của Deloitte sau khi bẻ khóa mật khẩu của tài khoản quản trị viên không yêu cầu xác thực đa yếu tố. Điều này đã khiến cho các tội phạm mạng không bị giới hạn truy cập vào email và tệp đính kèm trong email của công ty. Bây giờ, Deloitte đã sử dụng xác thực đa yếu tố, tin tặc sẽ không có số nhận dạng phụ mà chúng cần để đăng nhập và chủ tài khoản sẽ được cảnh báo về việc sử dụng trái phép tài khoản của họ - những thứ có khả năng ngăn chặn vi phạm .

 Tuy nhiên, nó không chỉ là về mật khẩu. Đó cũng là về việc có chính sách và thủ tục phù hợp. Giải pháp dịch vụ điện toán đám mây công khai cung cấp quyền tùy chỉnh và quy trình công việc tích hợp giúp cải thiện bảo mật và tăng năng suất. Các tổ chức có thể theo dõi ai đang cố gắng truy cập vào mạng của họ và chủ động chặn các thiết bị không xác định kết nối.

### 1.4. Các biện pháp bảo vệ an ninh mạng:

*Một là,* thống nhất và nâng cao nhận thức về an toàn thông tin trong thời kỳ kỹ thuật số. Xác định công tác bảo đảm an ninh, ATTT, phòng, chống vi phạm và tội phạm mạng là một bộ phận trọng yếu của cuộc đấu tranh bảo vệ an ninh quốc gia, giữ gìn trật tự, an toàn xã hội là nhiệm vụ của cả hệ thống chính trị dưới sự lãnh đạo của Đảng, sự quản lý của Nhà nước là trách nhiệm của các cấp, các ngành, trong đó có lực lượng công an giữ vai trò nòng cốt.

*Hai là* coi trọng việc đẩy mạnh xây dựng nguồn nhân lực ANTT Việt Nam cả số lượng lẫn chất lượng. Đào tạo thêm nhiều kỹ sư thuộc các chuyên ngành an ninh mạng, đảm bảo nhu cầu khác nhân lực hiện nay. Không chỉ đảm bảo về mặt số lượng, cần phải nâng cao chất lượng trong ngành bằng việc đào tạo đội ngũ giảng dạy có phương pháp và quy trình chuẩn.

*Ba là* tăng cường năng lực và nâng cao một bước hiệu quả quản lý nhà nước về công nghệ thông tin và truyền thông, về ANTT, an ninh mạng. Tiếp tục xây dựng, hoàn thiện hệ thống pháp luật về an ninh mạng, ANTT, quy chuần về ANTT. Kiện toàn tổ chức bộ máy thực thi quản lý nhà nước về an ninh, an toàn mạng thông tin quốc gia, hệ thống các đơn vị chuyên trách về ANTT, công nghệ thông tin. Hoàn thiện hệ thống quản lý theo pháp luật, đảm bảo.

*Bốn là* đẩy mạnh các phương án hợp tác phối hợp giữa các cơ quan, ban ngành, địa phương trong đảm bảo an ninh , ANTT.  Cần thiết phải xây dựng mô hình và các biện pháp xây dựng lòng tin giữa các quốc gia trong việc sản xuất, phát triển và sử dụng công nghệ thông tin phù hợp với luật pháp quốc tế, trên cơ sở tôn trọng quyền tự do và những quyền cơ bản khác của con người, đồng thời không can thiệp công việc nội bộ lẫn nhau; phản đối mọi hình thức lợi dụng vấn đề “tự do thông tin”, “nhân quyền”, “dân chủ” trên không gian mạng để xâm hại lợi ích của các quốc gia, quyền và lợi ích hợp pháp của các công dân.

*Năm là* chủ động có phương án, chiến lược phòng chống các cuộc tấn công mạng. Lập kế hoạch triển khai khi có sự cố sảy ra để không bị động trước những tấn công bất thường.

### 1.5. Những hành vi sử dụng không gian mạng bị nghiêm cấm?. Luật An ninh mạng có cấm người sử dụng internet truy cập Facebook, Google, Youtube không?

### 1.5.1. Những hành vi sử dụng không gian mạng bị nghiêm cấm?

 Điều 8 Luật An ninh mạng quy định các hành vi bị nghiêm cấm về không gian mạng như sau:

1. Sử dụng không gian mạng để thực hiện các hành vi sau:
* 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 Công 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 cộng đồng;
* Xúi giục, lôi kéo, kích động người khác phạm tội.
1. 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.
2. 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.
3. 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.
4. 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.
5. Hành vi khác vi phạm quy định của Luật này.

### 1.5.2. Luật An ninh mạng có cấm người sử dụng internet truy cập Facebook, Google, Youtube không?

**KHÔNG!** Luật An ninh mạng không cấm người dân truy cập Facebook, Google, Youtube. Người dân Việt Nam vẫn được tự do truy cập vào các trang mạng của Facebook, Google, Youtube hay bất kỳ trang mạng xã hội nào khác ở trong và ngoài nước.

Ngược lại, Luật An ninh mạng quy định các biện pháp bảo vệ về an ninh mạng cho người dân khi tham gia hoạt động trên các trang mạng xã hội như Facebook, Google...

Tuy nhiên, người nào sử dụng những mạng xã hội trên hoặc bất kỳ mạng xã hội nào khác để thực hiện hành vi vi phạm pháp luật đều bị xử lý nghiêm theo quy định của pháp luật.

### 1.6. Vấn đề một số doanh nghiệp nước ngoài phải lưu trữ một số loại dữ liệu và đặt văn phòng đại diện tại Việt Nam

 Đây là vấn đề thu hút nhiều sự chú ý của dư luận xã hội, khi cho rằng, với việc quy định một số doanh nghiệp nước ngoài phải lưu trữ một số loại dữ liệu và đặt văn phòng đại diện tại Việt Nam sẽ khiến cho các doanh nghiệp như Google, Facebook rút khỏi Việt Nam, khiến tăng trưởng kinh tế của Việt Nam suy giảm, trái với thông lệ quốc tế, không phù hợp với các quy định của WTO, CPTPP.

 Trong quá trình xây dựng dự thảo, Ban Soạn thảo đã lắng nghe, tiếp thu các ý kiến góp ý, theo đó không quy định phải đặt máy chủ tại Việt Nam, mà tùy tình hình thực tế và yêu cầu đặt ra, Chính phủ sẽ có quy định một số doanh nghiệp phải lưu trữ một số loại dữ liệu và đặt văn phòng đại diện tại Việt Nam. Theo đó, Khoản 3 Điều 26 Luật An ninh mạng quy định: “*Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam*”. Như vậy, quy định trên chỉ áp dụng đối với một số doanh nghiệp, một số loại hình dữ liệu chứ không áp dụng toàn bộ đối với các doanh nghiệp nước ngoài có hoạt động trên không gian mạng tại Việt Nam.

Việc quy định như trên là hoàn toàn phù hợp với thông lệ quốc tế, hệ thống háp luật trong nước, không vi phạm các cam kết quốc tế mà Việt Nam đã tham gia, vì: **(1)** Đã có hơn 18 quốc gia trên thế giới có văn bản luật quy định yêu cầu các doanh nghiệp nước ngoài phải lưu trữ dữ liệu quan trọng ở trong phạm vi lãnh thổ quốc gia[[10]](#footnote-10). **(2)** Phù hợp với khả năng của doanh nghiệp vì Google đã đặt khoảng 70 văn phòng đại diện, Facebook khoảng 80 văn phòng đại diện tại các quốc gia trên thế giới; tại khu vực Đông Nam Á, Google, Facebook đã mở văn phòng đại diện Singapore, Malaysia, Indonesia. **(3)** Theo pháp luật nước ta, trong đó có Luật thương mại năm 2005, Luật Quản lý ngoại thương năm 2017 và các văn bản hướng dẫn thi hành, quy định các tổ chức xúc tiến thương mại nước ngoài phải lập văn phòng đại diện tại Việt Nam[[11]](#footnote-11), dự thảo Luật quản lý thuế (sửa đổi), Bộ Tài chính cũng đề nghị nhà cung cấp dịch vụ nước ngoài (như Google, Facebook...) phải mở văn phòng đại diện chính thức tại Việt Nam. **(4)** Không trái với các cam kết quốc tế, bao gồm các điều ước liên quan WTO (gồm Hiệp định chung về thuế quan và thương mại - GATT 1994, Hiệp định chung về thương mại dịch vụ - GATS, Hiệp định về các khía cạnh liên quan đến thương mại của quyền sở hữu trí tuệ - TRIPS) và **Hiệp định Đối tác toàn diện và tiến bộ xuyên Thái Bình Dương (CPTPP)**[[12]](#footnote-12)**. (5)** Đảm bảo tính khả thi bởi, Google và Facebook đã đặt gần 2000 máy chủ ở trong nước mà không khai báo với cơ quan quản lý[[13]](#footnote-13).

Thời gian qua, có một số thông tin sai lệch, ngụy tạo nhằm tạo dư luận xấu về Luật An ninh mạng khi cho rằng, Luật An ninh mạng sẽ khiến GDP sụt giảm 1.7%, đầu tư nước ngoài giảm 3.1%. Thực chất, đây là tài liệu được đưa ra bởi Trung tâm Nghiên cứu kinh tế chính trị Châu Âu (ECIPE) từ 04 năm trước (năm 2014), dựa trên các kịch bản tiêu cực nhất, đánh giá các nền kinh tế là Liên minh Châu Âu, Trung Quốc, Ấn Độ, Hàn Quốc, Indonesia, Brazil và Việt Nam (khi đó nước ta mới ban hành Nghị định 72/2013/NĐ-CP) sẽ sụt giảm GDP và đầu tư nước ngoài khi quản lý chặt các doanh nghiệp nước ngoài sử dụng dữ liệu người dùng. Tuy nhiên, không quốc gia nào ảnh hưởng bởi dự đoán trên.

###  1.7. Vấn đề bảo vệ quyền con người trong Luật An ninh mạng

Luật An ninh mạng bảo về quyền con người khi tham gia hoạt động trên không gian mạng.

Nội dung Luật An ninh mạng phù hợp với tinh thần của Hiến chương Liên hợp quốc, Tuyên ngôn về quyền con người của Đại hội đồng Liên hợp quốc (1948) và các văn bản khác có liên quan, phù hợp với Hiến pháp nước CHXHCN Việt Nam, Bộ luật Hình sự, Bộ luật Dân sự Việt Nam.

Luật An ninh mạng trực tiếp bảo vệ 05 quyền con người sau đây:

(1) Quyền sống, quyền tự do và an ninh cá nhân; quyền bình đẳng trước pháp luật và được pháp luật bảo vệ;

(2) Quyền không bị can thiệp vào đời tư, gia đình, chỗ ở hoặc thư tín;

 (3) Quyền không bị xâm hại danh dự hay uy tín cá nhân;

 (4) Quyền tự do tư tưởng, tín ngưỡng và tôn giáo của công dân;

 (5) Quyền tự do ngôn luận, tự do biểu đạt của công dân.

 Luật An ninh mạng còn giúp phòng ngừa, xử lý các hành vi sử dụng không gian mạng xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân.

 Cụ thể:

 Công dân có quyền tự do bày tỏ quan điểm, tự do chính kiến của mình trên không gian mạng, ngoại trừ những hành vi bị pháp luật nghiêm cấm.

 Điều 8 Luật An ninh mạng đã quy định cụ thể 06 nhóm hành vi bị nghiêm cấm, có tác dụng bảo vệ quyền con người trước các nguy cơ, hành vi vi phạm pháp luật có thể xâm phạm tới quyền, lợi ích hợp pháp của tổ chức, cá nhân. Qua đó, bảo vệ quyền con người của công dân trên không gian mạng.

Điều 17 Luật An ninh mạng quy định cụ thể về bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng. Đây là quy định cụ thể hóa Khoản 1 Điều 14 Hiến pháp năm 2013, theo đó, “các quyền con người, quyền công dân về chính trị, dân sự, kinh tế, văn hóa, xã hội được công nhận, tôn trọng, bảo vệ, bảo đảm theo Hiến pháp và pháp luật”.

Điểm a Khoản 2 Điều 26 Luật An ninh mạng cũng quy định các doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm bảo mật thông tin, tài khoản của người dùng”. Đây là quy định cụ thể nhằm hạn chế, ngăn chặn việc bán thông tin người dùng cho các doanh nghiệp cung cấp dịch vụ hoặc bên thứ 3 mà chưa có sự đồng ý của người dùng

Luật An ninh mạng cũng quy định cụ thể trường hợp lực lượng chuyên trách bảo vệ an ninh mạng được tiếp cận thông tin người dùng là khi phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng. Quy định này phù hợp với nội dung Khoản 2 Điều 14 Hiến pháp năm 2013: “*Quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng*”.

### 1.8. Vấn đề cung cấp thông tin cá nhân để phục vụ điều tra, xử lý hành vi vi phạm pháp luật

Thông tin cá nhân là một trong những loại dữ liệu điện tử, chứng cứ điện tử, có tác dụng quan trọng trong điều tra, xử lý các hành vi phạm pháp luật. Tất cả các cơ quan thực thi pháp luật trên thế giới đều được quyền áp dụng các biện pháp cần thiết, trong phạm vi pháp luật cho phép để thực hiện nhiệm vụ của mình, ngăn ngừa tội phạm phát sinh.

Điều 17 Luật An ninh mạng quy định cụ thể về bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng. Đây là quy định tiến bộ, cụ thể hóa Khoản 1 Điều 14 Hiến pháp năm 2013, theo đó, “các quyền con người, quyền công dân về chính trị, dân sự, kinh tế, văn hóa, xã hội được công nhận, tôn trọng, bảo vệ, bảo đảm theo Hiến pháp và pháp luật”. Đồng thời, bảo vệ thông tin cá nhân trước các hoạt động mua bán, sử dụng, lạm dụng trái phép như hiện nay.

Điểm a, khoản 2 Điều 26 dự thảo Luật An ninh mạng quy định: “*Doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng*”.

Như vậy, chỉ khi nào có yêu cầu phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an mới được pháp luật cho phép yêu cầu cung cấp thông tin người dùng có liên quan tới hành vi vi phạm pháp luật đã nêu trên.

Hiện nay, có nhiều thông tin trên không gian mạng cho rằng, Luật An ninh mạng cho phép cơ quan chức năng tùy tiện yêu cầu doanh nghiệp cung cấp toàn bộ thông tin người dùng như thông tin cá nhân, thông tin riêng tư là không chính xác. Luật An ninh mạng đã quy định rõ ràng, chỉ trong trường hợp phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng mới được quyền yêu cầu cung cấp thông tin người dùng. Các quy định trong Bộ luật Tố tụng Hình sự và các văn bản có liên quan đã quy định rõ về việc quản lý, sử dụng thông tin được cung cấp để phục vụ điều tra, xử lý các hành vi vi phạm pháp luật.

Hàng năm, chính phủ các nước đã yêu cầu Facebook cung cấp thông tin về tài khoản người dùng liên quan đến các vụ việc pháp lý, trong đó Mỹ và Ấn Độ thường đứng trong top đầu danh sách với khoảng 30 ngàn lượt yêu cầu mỗi năm, trong khi đó Việt Nam mới chỉ yêu cầu Facebook cung cấp một vài vụ việc.

### 1.9. Quy định về đặt chi nhánh hoặc văn phòng đại diện của doanh nghiệp nước ngoài cung cấp dịch vụ tại Việt Nam?.

 ***- Trong quá trình xây dựng Luật An ninh mạng, các cơ quan đại diện nước ngoài như Đại sứ quán Mỹ, Nhật Bản, Anh, Úc, Canada, Liên minh Châu Âu*** đã có hoạt động tác động chính sách đối với Luật An ninh mạng khi gửi thư kiến nghị tới Chủ tịch Quốc hội, Văn phòng Chính phủ, Bộ Công an, Bộ Ngoại giao, Bộ Công thương, Bộ Thông tin và Truyền thông về một số vấn đề trong dự thảo Luật; một số cơ quan đại diện như Nhật Bản đã có đề nghị làm việc trực tiếp với đơn vị chức năng của Bộ Công an để nghe ý kiến về nội dung dự thảo Luật. Các cơ quan đại diện nước ngoài nêu trên cho rằng:

**(1)** Một số quy định trong hành vi bị nghiêm cấm (Điều 8) và phòng ngừa xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống (Điều 16), được quy chiếu theo nội dung Bộ luật Hình sự là chung chung, chưa rõ ràng, làm hình sự hóa các hình thức bày tỏ hòa bình mà không phải là mối đe dọa đến an ninh mạng hoặc an ninh quốc gia.

**(2)** Quan ngại về một số nội dung có liên quan tới quyền cơ bản của con người, đề nghị giữ các cam kết quốc tế đối với tiêu chuẩn nhân quyền quốc tế bằng việc không hạn chế nội dung được phổ biến trên mạng internet.

**(3)** Một số nội dung trong Luật An ninh mạng làm ảnh hưởng đến nền kinh tế số đang phát triển và sự tăng trưởng kinh tế nói chung, làm gia tăng chi phí kinh doanh, gia tăng rào cản thương mại khi có những quy định thiếu thực tế đối với các hoạt động kinh doanh và các nhà cung cấp dịch vụ như thiết lập văn phòng đại diện và đặt hệ thống lưu trữ dữ liệu tại Việt Nam.

- Trong quá trình sửa đổi Hiệp định Đối tác xuyên Thái Bình Dương (TPP) khi Mỹ rút lui, một số quốc gia đã có ý kiến cho rằng, nội dung Luật An ninh mạng vi phạm quy định tại Điều 14.11 (Chuyển giao thông tin xuyên biên giới bằng phương tiện điện tử), Điều 14.13 (Địa điểm của các hạ tầng công nghệ thông tin).

- Trong các phiên họp của Ủy ban Hàng rào kỹ thuật (TBT) thuộc WTO, một số quốc gia thành viên là Nhật Bản, Liên minh Châu Âu, Mỹ đã nêu quan ngại với dự thảo Luật An ninh mạng của Việt Nam, cho rằng dự luật chưa được xây dựng trên tiêu chuẩn quốc tế và đề nghị tham khảo Cơ chế Thừa nhận Tiêu chí chung (CCRA) trong quá trình xây dựng, chỉnh sửa; một số điều khoản gây cản trở thương mại trên mức cần thiết.

Trước hoạt động tác động chính sách của các cơ quan đại diện nước ngoài, một số nội dung Chính phủ đã giao Bộ Công an phối hợp với các bộ, ngành chức năng trong giải trình, tiếp thu ý kiến cũng như đấu tranh với các hoạt động tác động chính sách của cơ quan đại diện nước ngoài, kết quả đạt được là tích cực:

**(1)** Bộ Công an đã chỉ đạo Cục An ninh mạng và các cơ quan chức năng liên quan làm việc trực tiếp tới một số cơ quan đại diện nước ngoài như Nhật Bản để làm rõ một số vấn đề liên quan, tạo được đồng thuận của Công sứ kinh tế Nhật Bản.

**(2)** Bộ Công an cũng phối hợp với Ủy ban Đối ngoại, Ủy ban Quốc phòng và An ninh của Quốc hội làm việc với các cơ quan đại diện nước ngoài để nghe ý kiến, giải thích một số nội dung và đấu tranh với luận điệu không đúng, kết quả buổi làm việc là tích cực khi ta đề nghị họ cung cấp một số giải pháp pháp lý của nước họ để Việt Nam tham khảo (*khi họ cũng có quy định tương tự, thậm chí là chặt chẽ hơn*), chỉ rõ quy định lưu trữ dữ liệu vi phạm cam kết quốc tế nào thì họ không chỉ ra được.

**(3)** Đối với Hiệp định TPP, nội dung Hiệp định mới (***Hiệp định Đối tác toàn diện và tiến bộ xuyên Thái Bình Dương - CPTPP*)** đã có những quy định riêng đối với một số quốc gia, trong đó có Việt Nam được tạm hoãn 05 năm đối với 02 nghĩa vụ trong chương Thương mại điện tử có liên quan tới an ninh mạng.

**(4)** Cung cấp thông tin cho Bộ Ngoại giao, Bộ Công thương để kiên trì quan điểm trong các phiên họp của Ủy ban Hàng rào kỹ thuật (TBT) thuộc WTO, khẳng định nội dung Luật An ninh mạng không tạo hàng rào kỹ thuật đối với các doanh nghiệp nước ngoài, không vi phạm các cam kết của WTO.

*- Các doanh nghiệp nước ngoài Facebook, Google, Amazon...* đã triển khai nhiều hoạt động nhằm tác động tới nội dung Luật An ninh mạng như: (1) Đề nghị làm việc trực tiếp với Ban Soạn thảo, Tổ Biên tập để tìm hiểu nội dung Luật An ninh mạng và đưa kiến nghị. (2) Vận động, phối hợp các hiệp hội, tập đoàn nước ngoài gửi ý kiến tới Ban Soạn thảo, Tổ Biên tập và các cơ quan chức năng của Việt Nam[[14]](#footnote-14). (3) Tổ chức thảo luận, tọa đàm về quy định liên quan tới an ninh mạng của một số quốc gia Đông Nam Á, trong đó có Việt Nam nhằm tìm kiếm sự đồng thuận và dư luận xã hội. (4) Tài trợ kinh phí cho các doanh nghiệp, hiệp hội trong nước thảo luận, tọa đàm về dự thảo Luật An ninh mạng[[15]](#footnote-15), qua đó “núp bóng” các doanh nghiệp trong nước để đưa ra các nhận định bất lợi, thiếu thực tế đối với dự thảo Luật An ninh mạng, cung cấp thông tin cho cơ quan truyền thông, báo chí khai thác, đưa tin, tạo “hiệu ứng ngược” ủng hộ hoạt động kinh doanh chưa được pháp luật Việt Nam cho phép của các doanh nghiệp nước ngoài.

Nội dung các doanh nghiệp này kiến nghị khá tương đồng với nội dung các cơ quan đại diện nước ngoài gửi cơ quan chức năng của nước ta, cho rằng dự thảo Luật An ninh mạng có nguy cơ trở thành rào cản đối với nền kinh tế số của nước ta, làm tăng chi phí cho các hoạt động kinh doanh tại Việt Nam, không nhất quán với các cam kết của WTO, áp dụng trách nhiệm hình sự đối với một số nội dung chưa rõ ràng, chưa phù hợp với tiêu chuẩn toàn cầu, quy định địa phương hóa dữ liệu gây tổn hại đến nền kinh tế và người tiêu dùng.

Trong tình hình đó, Bộ Công an đã chỉ đạo đơn vị chức năng là Cục An ninh mạng phối hợp với các đơn vị có liên quan gặp gỡ, làm việc trực tiếp với các doanh nghiệp như Facebook, Google, Amazon; các hiệp hội như Hội đồng kinh doanh Hoa Kỳ - ASEAN, Phòng Thương mại Mỹ (AmCham), Liên minh Internet Châu Á, Tập đoàn VISA và Mastercard, Hiệp hội điện toán đám mây Châu Á (ACCA) để cung cấp thông tin chính xác, đưa ra các nội dung cũng như các vấn đề cần giải đáp, bác bỏ một số thông tin, dư luận không chính xác về nội dung dự thảo.

Với thái độ cầu thị, Ban Soạn thảo cũng đã nghiên cứu, tiếp thu một số kiến nghị của các doanh nghiệp nêu trên, như kiến nghị về phân loại dữ liệu theo kiến nghị của Amazon, chính sách xử lý thông tin theo kiến nghị của Google, Facebook, hoàn thiện dự thảo Luật. Qua đó, nội dung tại Khoản 4 Điều 34 cũ (yêu cầu đặt máy chủ lưu trữ dữ liệu người dùng Việt Nam) được lược bỏ, thay vào đó Khoản 3 Điều 26 chỉ quy định một số “*doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam”.*

### Quy định lưu trữ dữ liệu có gây cản trở và khiến Facebook, Google rút khỏi Việt Nam không?

**KHÔNG!** Quy định trên không cản trở hoạt động của Facebook, Google, bởi các lý do sau:

(1) Google, Facebook đều đã thuê máy chủ tại nước ta. Theo thống kê sơ bộ, Google thuê khoảng 1781 máy chủ, Facebook thuê khoảng 441 máy chủ tại 8 doanh nghiệp cung cấp dịch vụ trong nước.

(2) Việc lưu trữ dữ liệu người sử dụng dịch vụ tại Việt Nam giúp các doanh nghiệp này tiết kiệm chi phí kinh doanh, tăng mức tốc độ truy cập và nâng cao chất lượng dịch vụ; giúp các nhà mạng trong nước tiết kiệm kinh phí khi phải mua băng thông quốc tế.

(3) Về kỹ thuật, việc lưu trữ dữ liệu trong nước được tiến hành dễ dàng khi công nghệ cho phép, nhất là áp dụng công nghệ điện toán đám mây và các doanh nghiệp này đã có sẵn kinh nghiệm và thiết bị do áp dụng tương tự ở nhiều quốc gia khác.

Hiện có gần 50 triệu người Việt Nam sử dụng Facebook và trên 60 triệu người Việt Nam sử dụng Google. Có thể thấy, Việt Nam là một trong những thị trường quan trọng và các doanh nghiệp này đã thu lợi nhuận hàng trăm triệu đô la mỗi năm từ người dùng Việt Nam, vì vậy, không có lý gì mà họ lại rời bỏ thị trường Việt Nam. Cũng chưa có thông tin chính thức nào về việc này.

### 1.10. Việc ban hành Luật An ninh mạng có tạo đặc lợi cho quốc gia khác hay không?

**KHÔNG!** Đây là luận điệu xuyên tạc nhằm mục đích chống phá, bôi xấu Luật An ninh mạng.Luật An ninh mạng là nội luật của Việt Nam. Luật An ninh mạng được ban hành nhằm bảo vệ ANQG, TTATXH của Việt Nam; đồng thời, bảo vệ quyền, lợi ích hợp pháp của các tổ chức, cá nhân của Việt Nam trên không gian mạng; vì lợi ích của cơ quan, doanh nghiệp, tổ chức, cá nhân Việt Nam.

**1.11. Hình thức, biện pháp xử lý khi phát hiện vi phạm.**

* Tại Khoản 1 Điều 2 Luật An ninh mạng 2018 có quy định về khái niệm an ninh mạng như sau:
* “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”.

***=> Như vậy, theo khái niệm này thì có thể thấy được hành vi vi phạm pháp luật về an ninh mạng là những hành vi trên không gian mạng nhằm 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.***

* Theo đó, tại Điều 9 Luật này có quy định về việc xử lý vi phạm pháp luật về an ninh mạng như sau:

***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 trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.***

# IV. VIỆC TRIỂN KHAI THI HÀNH LUẬT AN NINH MẠNG

Kế hoạch triển khai thi hành Luật An ninh mạng trên địa bàn tỉnh xác định rõ trách nhiệm và phân công nhiệm vụ cụ thể cho các sở, ban, ngành, UBND huyện, thành phố trong triển khai thi hành Luật An ninh mạng đảm bảo kịp thời, đồng bộ, thống nhất, hiệu quả. Huy động sự tham gia có trách nhiệm, sự phối hợp chặt chẽ giữa các cơ quan, đơn vị liên quan trong quá trình triển khai Luật An ninh mạng trên địa bàn toàn tỉnh.
 Theo đó, Kế hoạch được thực hiện với các nội dung: tổ chức quán triệt, tuyên truyền, phổ biến Luật An ninh mạng và các văn bản hướng dẫn thi hành; Rà soát các văn bản quy phạm pháp luật có liên quan đến Luật An ninh mạng; Tham gia xây dựng văn bản thi hành Luật An ninh mạng; Tập huấn chuyên sâu, bồi dưỡng nghiệp vụ an ninh mạng.
 UBND tỉnh yêu cầu Công an tỉnh tổ chức hội nghị triển khai thi hành Luật An ninh mạng và các văn bản hướng dẫn thi hành. Có trách nhiệm chủ trì tham mưu tổ chức các hội nghị quán triệt, tuyên truyền, phổ biến nội dung Luật An ninh mạng, các văn bản hướng dẫn thi hành cho cán bộ, chiến sĩ trong lực lượng Công an toàn tỉnh, cán bộ, công chức doanh nghiệp và nhân dân trên địa bàn với quy mô, phạm vi phù hợp. Chủ trì tổ chức tham gia ý kiến vào dự thảo các văn bản hướng dẫn thi hành Luật An ninh mạng theo chỉ đạo hoặc yêu cầu của Bộ Công an.
 Công an tỉnh chủ trì, phối hợp với các đơn vị chức năng có liên quan triển khai tuyên truyền, phổ biến Luật An ninh mạng và các văn bản hướng dẫn thi hành. Tổ chức tuyên truyền, phổ biến Luật An ninh mạng và các văn bản hướng dẫn thi hành cho từng đối tượng cụ thể nhằm nâng cao nhận thức, hiểu biến của cán bộ, nhân dân, nhất là người đứng đầu cơ quan, tổ chức và chủ quản hệ thống thông tin quan trọng. Sở Thông tin và Truyền thông chỉ đạo các cơ quan báo chí, truyền thông, phối hợp với Công an tỉnh đăng tải, tuyên truyền sâu rộng nội dung Luật An ninh mạng và các văn bản hướng dẫn thi hành trên các phương tiện thông tin đại chúng, trên Cổng thông tin điện tử tỉnh, nhất là những nội dung được dư luận quan tâm; đồng thời có tin, bài phản ánh kịp thời về tình hình triển khai thi hành, phản bác các quan điểm có nội dung xuyên tạc đường lối, chủ trương, chính sách của Đảng, pháp luật của Nhà nước về an ninh mạng. Giám đốc các sở, ban, ngành; Chủ tịch UBND các huyện, thành phố chỉ đạo cơ quan chuyên môn tăng cường công tác tuyên truyền, phổ biến nội dung của Luật An ninh mạng, cùng các văn bản hướng dẫn thi hành đến cán bộ, công chức, viên chức, học sinh và quần chúng nhân dân trên địa bàn, góp phần nâng cao nhận thức, tạo sự động thuận nhất trí cao trong quá trình thực hiện.
 Sở Tư pháp chủ trì, phối hợp với các đơn vị chức năng rà soát các văn bản quy phạm pháp luật có liên quan đến Luật An ninh mạng để tham mưu UBND tỉnh đề xuất Quốc hội, Chính phủ sửa đổi, bổ sung, thay thế, bãi bỏ hoặc ban hành mới theo đúng quy định hiện hành.
 Công an tỉnh chủ trì phối hợp với các đơn vị liên quan tổ chức tập huấn chuyên sâu, bồi dưỡng nghiệp vụ an ninh mạng cho cán bộ lãnh đạo, lực lượng  bảo vệ an ninh mạng được bố trí tại các sở, ban, ngành, UBND các huyện, thành phố. Bộ Chỉ huy quân sự tỉnh tổ chức tập huấn chuyên sâu, bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc phạm  vi quản lý.

Tình hình an ninh mạng trong thời gian tới sẽ tiếp tục diễn biến phức tạp khi tình hình chính trị thế giới tiếp tục có những diễn biến khó lường, xung đột địa chính trị vẫn diễn ra, xu thế hình thành thế giới đa cực ngày càng rõ nét, sự phát triển của khoa học công nghệ mang tới cho nhân loại nhiều thời cơ đột phá nhưng cũng đồng thời đặt các quốc gia trước những nguy cơ, thách thức nghiêm trọng. Khả năng tác động tới an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức cá nhân bởi các hành vi vi phạm pháp luật trên không gian mạng ngày một nguy hiểm và thường trực hơn. Mục đích nhằm tổ chức việc tuyên truyền, phổ biến Luật An ninh mạng và các văn bản hướng dẫn thi hành đến các tầng lớp nhân dân, cán bộ, công chức, viên chức và lực lượng vũ trang; làm tốt công tác tập huấn nghiệp vụ an ninh mạng cho lực lượng làm công tác bảo vệ an ninh mạng. Đồng thời xác định nội dung công việc, thời hạn, tiến độ hoàn thành và trách nhiệm cũng như cơ chế phối hợp của các sở, ban, ngành cấp tỉnh và UBND các huyện, thị xã, thành phố nhằm bảo đảm triển khai thi hành Luật kịp thời, đồng bộ, thống nhất và hiệu quả. Các sở, ban, ngành cấp tỉnh; UBND các huyện, thị xã, thành phố được giao nhiệm vụ chủ trì hoặc tham gia phối hợp thực hiện phải tích cực, chủ động triển khai thực hiện Kế hoạch theo đúng nội dung, tiến độ, bảo đảm chất lượng, hiệu quả. Vì vậy, việc triển khai thi hành Luật An ninh mạng có vai trò và ý nghĩa quan trọng trong bảo đảm an ninh mạng, đấu tranh phòng chống tội phạm mạng, trong đó cần tậm trung thực hiện một số nhiệm vụ trọng tâm sau:

## 1. Xây dựng các văn bản quy định chi tiết và hướng dẫn thi hành Luật An ninh mạng

Ngày 11/4/2019, Văn phòng Chính phủ ra Công văn số 2965/VPCP-PL về trình ban hành văn bản quy định chi tiết thi hành luật, pháp lệnh. Công văn này truyền đạt yêu cầu của Thủ tướng Chính phủ Nguyễn Xuân Phúc và các Bộ trưởng phải trực tiếp chỉ đạo việc soạn thảo, khẩn trương hoàn thiện, trình Chính phủ, Thủ tướng ban hành trước ngày 15/4/2019 đối với các văn bản hướng dẫn Luật An ninh mạng cụ thể, như sau:

+ Nghị định của Chính phủ quy định chi tiết về trình tự, thủ tục áp dụng một số biện pháp bảo vệ an ninh mạng (Khoản 2 Điều 5)

+ Nghị định của Chính phủ quy định chi tiết một số điều trong Luật An ninh mạng (Khoản 4 Điều 10; Khoản 5 Điều 12; Khoản 1 Điều 23; Khoản 7 Điều 24; Khoản 4 Điều 26; Khoản 5 Điều 36)

+ Riêng Quyết định của Thủ tướng Chính phủ ban hành Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (Khoản 3 Điều 10; Khoản 3 Điều 43) được lùi sang Quý II/2019

Sau khi Luật An ninh mạng được thông qua, Bộ Công an có trách nhiệm chủ trì, phối hợp với các bộ, ngành liên quan xây dựng trình Chính phủ, Thủ tướng Chính phủ các văn bản quy định chi tiết và hướng dẫn thi hành Luật An ninh mạng. Trước mắt, tập trung xây dựng 03 Nghị định và 02 Quyết định sau: Nghị định của Chính phủ hướng dẫn một số điều trong Luật An ninh mạng; Nghị định của Chính phủ quy định xử lý vi phạm hành chính về an ninh mạng; Nghị định của Chính phủ quy định chi tiết về trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng; Quyết định của Thủ tướng Chính phủ về Danh mục hệ thống thông tin quan trọng về an ninh quốc gia; Quyết định của Thủ tướng Chính phủ về việc lưu trữ dữ liệu và đặt văn phòng đại diện tại Việt Nam.

## 2. Tuyên truyền, phổ biến Luật An ninh mạng

- Tổ chức tập huấn chuyên sâu Luật An ninh mạng trong CAND, lực lượng chuyên trách bảo vệ an ninh mạng và các lực lượng có liên quan.

- Tổ chức Hội nghị phổ biến nội dung Luật An ninh mạng tại các khu vực trọng điểm, cho các doanh nghiệp, tổ chức, cá nhân có liên quan.

- Phổ biến rộng rãi nội dung Luật An ninh mạng trên các phương tiện thông tin đại chúng.

- Rà soát, bổ sung nội dung an ninh mạng vào hệ thống giáo trình, tài liệu giảng dạy của các trường trong CAND, cơ sở giáo dục quốc phòng, an ninh.

- Luật An ninh mạng năm 2018 có hiệu lực ngày 01/01/2019 có 8 nội dung nổi bật cần lưu ý:

 ***Nghiêm cấm thông tin sai sự thật gây hoang mang trên mạng:***

Điều 8 của Luật này quy định nhiều hành vi bị nghiêm cấm trên môi trường mạng. Trong đó, nghiêm cấm việc sử dụng không gian mạng để thực hiện các hành vi như: Tổ chức, hoạt động, câu kết, xúi giục mua chuộc lừa gạt, lôi kéo người chống phá Nhà nước; Xuyên tạc lịch sử; Thông tin sai sự thật gây hoang mang; Hoạt động mại dâm, tệ nạn xã hội; Sản xuất, đưa vào sử dụng phần mềm gây rối loạn hoạt động của mạng viễn thông, mạng Internet…

***Doanh nghiệp nước ngoài phải lưu trữ dữ liệu người dùng tại Việt Nam:***

Khoản 3 Điều 26 của Luật yêu cầu doanh nghiệp trong nước và nước ngoài cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Riêng doanh nghiệp phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

***Ngừng cung cấp dịch vụ mạng khi có yêu cầu của cơ quan chức năng:***

Ngoài yêu cầu phải lưu trữ dữ liệu người dùng tại Việt Nam, các doanh nghiệp trong và ngoài nước không được cung cấp hoặc phải ngừng cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên mạng thông tin bị nghiêm cấm nêu trên, khi có yêu cầu của lực lượng bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông.

***Doanh nghiệp phải cung cấp thông tin người dùng để phục vụ điều tra:***

Các doanh nghiệp nêu trên cũng phải có trách nhiệm xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng. Đặc biệt, phải cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng.

***Thông tin vi phạm trên mạng bị xóa bỏ trong vòng 24 giờ:***

Khi người dùng chia sẻ những thông tin bị nghiêm cấm, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam phải ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin vi phạm chậm nhất là 24 giờ, kể từ thời điểm có yêu cầu của lực lượng bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan của Bộ Thông tin và Truyền thông. Đồng thời, doanh nghiệp phải lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian quy định.

***Bảo vệ trẻ em trên không gian mạng:***

Đây là một quy định rất nhân văn của Luật An ninh mạng 2018. Theo đó, Điều 29 quy định: Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia trên không gian mạng. Các doanh nghiệp phải đảm bảo kiểm soát nội dung để không gây nguy hại cho trẻ em; đồng thời, xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em…

**“Nghe lén” các cuộc đàm thoại được coi là hành vi gián điệp mạng:**

Các hành vi gián điệp mạng; xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng được liệt kê tại Khoản 1 Điều 17 Luật An ninh mạng 2018, trong đó có:

- Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật;

- Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại;

- Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền va lợi ích hợp pháp của cơ quan, tổ chức, cá nhân…

***Khuyến khích cá nhân, tổ chức tham gia phổ biến kiến thức an ninh mạng:***

Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan Nhà nước phối hợp với tổ chức cá nhân, cá nhân thực hiện chương trình giáo dục và nâng cao nhận thức về an ninh mạng. Bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức trong Bộ, ngành, cơ quan, tổ chức. UBND cấp tỉnh có trách nhiệm phổ biến kiến thức cho cơ quan, tổ chức, cá nhân của địa phương.

## 3. Đẩy mạnh phối hợp với Ban Tuyên giáo Trung ương trong triển khai, thi hành Luật An ninh mạng, trọng tâm là công tác bảo đảm an ninh thông tin mạng

Hoạt động tuyên truyền chống Đảng, Nhà nước trên không gian mạng của các thế lực thù địch đã tác động tiêu cực tới tư tưởng, nhận thức, quan điểm của một bộ phận cán bộ, đảng viên và quần chúng nhân dân, gây tâm lý hoang mang, hoài nghi và làm suy giảm lòng tin của quần chúng đối với Đảng, chế độ, các đồng chí lãnh đạo cấp cao và lực lượng Công an. Thời gian qua, Bộ Công an đã phối hợp chặt chẽ với Ban Tuyên giáo Trung ương trong công tác bảo đảm an ninh thông tin mạng, xử lý các thông tin chống Đảng, Nhà nước. Sau khi Luật An ninh mạng có hiệu lực, công tác phối hợp cần đẩy mạnh và chặt chẽ hơn trước đây.

Điều 16 Luật An ninh mạng đã quy định cụ thể các biện pháp phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống. Điều 26 Luật An ninh mạng đã quy định đầy đủ các nội dung của công tác bảo đảm an ninh thông tin trên không gian mạng. Như vậy, lực lượng chức năng của Bộ Công an, Ban Tuyên giáo Trung ương đã có cơ sở pháp lý đủ mạnh, vững chắc trong phòng ngừa, phát hiện, đấu tranh, xử lý thông tin và hành vi tuyên truyền chống Đảng, Nhà nước trên không gian mạng. Công tác phối hợp đó được thể hiện qua các vấn đề sau đây:

- Kịp thời đưa thông tin chính thống đến quần chúng nhân dân, cán bộ, đảng viên qua không gian mạng, nhất là khi diễn ra các sự kiện “nóng”, sự kiện thu hút sự quan tâm của dư luận, không để các thế lực thù địch lợi dụng tình trạng thiếu thông tin để tuyên truyền xuyên tạc, có biện pháp chấn chỉnh hoạt động đưa tin của báo chí trong nước.

- Tăng cường, nâng cao nhận thức, cảnh giác trước những luận điệu tuyên truyền phản động của các thế lực thù địch trên không gian mạng; tuyên truyền nội dung, kết quả của công tác đấu tranh chống tham nhũng, tiêu cực, thuần khiết nội bộ; đẩy mạnh công tác điều tra, nghiên cứu dư luận xã hội làm cơ sở cho việc ban hành và đưa các chủ trương, chính sách, pháp luật của Đảng, Nhà nước thực sự đi vào cuộc sống, tạo sự đồng thuận cao trong xã hội; không để nảy sinh tâm lý bức xúc, bất mãn và bày tỏ tiêu cực trên mạng của quần chúng nhân dân.

- Tăng cường công tác quản lý nhà nước đối với các dịch vụ viễn thông, Internet, các doanh nghiệp cung cấp, quản lý dịch vụ Internet và thông tin điện tử trên mạng, thuê bao di động trả trước, thuê bao 3G, dịch vụ OTT...; sớm hình thành và thực thi có hiệu quả Bộ Quy tắc ứng xử trên không gian mạng.

- Chủ động phối hợp trong ngăn chặn triệt để các trang web, blog có nội dung tuyên truyền chống Đảng, Nhà nước, đáp ứng yêu cầu công tác an ninh đặt ra trong tình hình mới.

**4. Giải pháp nâng cao hiệu quả công tác quản lý nhà nước đối với vấn đề an ninh mạng trong tình hình hiện nay**

**4.1. Tham mưu cho lãnh đạo Đảng, Nhà nước, các bộ, ngành liên quan triển khai đồng bộ các mặt công tác nhằm nâng cao nhận thức người sử dụng không gian mạng**

Việc tăng cường tuyên truyền nâng cao nhận thức về âm mưu và hoạt động sử dụng Internet, không gian mạng xâm phạm ANQG của các TLTĐ có ý nghĩa quan trọng, là liều thuốc phòng ngừa cần thiết để người sử dụng có sức đề kháng đối với hoạt động tuyên truyền phá hoại tư tưởng, móc nối phát triển lực lượng, thu thập tin tức bí mật nhà nước qua không gian mạng của địch, đồng thời phát hiện, tố giác hoạt động sử dụng không gian mạng xâm phạm ANQG của các TLTĐ. Để thực hiện tốt việc này, cần tham mưu cho Đảng, Nhà nước và phối hợp với các cơ quan hữu quan các tổ chức đoàn thể quần chúng... thực hiện tốt công tác tuyên truyền nâng cao bản lĩnh chính trị, ý thức cảnh giác cho cán bộ, đảng viên và quần chúng; nâng cao ý thức trách nhiệm, nhận thức của cán bộ các ban ngành có liên quan về tính chất nguy hiểm; phương thức, thủ đoạn sử dụng không gian mạng xâm phạm ANQG của các TLTĐ. Để thực hiện tốt việc này, cần sử dụng tổng hợp các hình thức, biện pháp khác nhau, trong đó cần chú ý:

- Tổ chức quán triệt, thực hiện nghiêm túc các nghị quyết, chỉ thị của Trung ương Đảng, Quốc hội, Chính phủ về công tác đảm bảo an ninh, an toàn thông tin, nhất là Chỉ thị số 28-CT/TW ngày 16/9/2013 của Ban Bí thư Trung ương Đảng (Khóa XI) về tăng cường công tác đảm bảo an toàn thông tin mạng; Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng. Tăng cường tuyên truyền, giáo dục, phổ biến kiến thức, làm cho cán bộ, đảng viên và nhân dân nhận thức rõ tầm quan trọng của công tác đảm bảo an ninh, an toàn mạng thông tin quốc gia, coi đây là nhiệm vụ cấp bách, thường xuyên.

- Tham mưu, phối hợp với Ban Tuyên giáo Trung ương, Bộ TT&TT, các cơ quan thông tấn, báo chí nâng cao bản lĩnh chính trị, kịp thời đưa những thông tin chính thống về các sự kiện đang thu hút sự chú ý của dư luận tới đông đảo quần chúng nhân dân; chủ động đấu tranh, phản bác luận điệu phản tuyên truyền của các TLTĐ, vạch trần các hoạt động chống Đảng, Nhà nước của các cá nhân, tổ chức phản động; đưa các nội dung này vào nội dung sinh hoạt chi bộ; chỉ đạo báo, đài tăng cường phổ biến tình hình an ninh mạng trong và ngoài nước, kiến thức về công nghệ thông tin và bảo đảm an ninh, an toàn thông tin giúp quần chúng nhân dân có nhận thức đúng đắn. Qua đó nâng cao cảnh giác, định hướng tư tưởng cho cán bộ, đảng viên và nhân dân tự đề kháng trước những luận điệu tuyên truyền phá hoại của các TLTĐ.

- Tham mưu, phối hợp với Bộ Giáo dục và Đào tạo, Trung ương Đoàn thanh niên Cộng sản Hồ Chí Minh và Trung ương Hội thanh niên Việt Nam tăng cường công tác giáo dục chính trị, tư tưởng cho học sinh, sinh viên, thường xuyên cập nhật những thông tin chính thống về các sự kiện đang thu hút sự chú ý của dư luận để học sinh, sinh viên có nhận thức đúng đắn, không bị tác động bởi những thông tin xấu, không để các đối tượng phản động móc nối, lôi kéo học sinh, sinh viên vào các hoạt động chống phá Nhà nước.

- Bộ Công an đẩy mạnh phong trào “Toàn dân bảo vệ an ninh Tổ quốc”; phối hợp với các cơ quan chức năng thông báo các thông tin liên quan đến âm mưu, thủ đoạn hoạt động của các TLTĐ sử dụng không gian mạng tuyên truyền, phá hoại tư tưởng, để cán bộ, đảng viên, cơ quan chủ quản nắm được thông tin, nâng cao ý thức cảnh giác, chủ động phòng ngừa, bảo vệ lợi ích của chính mình và của Nhà nước.

Có thể thấy, không gian mạng có khả năng lan truyền thông tin rất nhanh chóng, có ảnh hưởng ngày càng sâu sắc tới mọi mặt của đời sống xã hội, đặc biệt là tới cách thức giao tiếp, liên lạc của con người. Do đó, cần phải đẩy mạnh công tác tuyên truyền định hướng dư luận thông qua việc tạo lập, khuyến khích phát triển các dịch vụ tiện ích cũng như các diễn đàn trên mạng Internet, các dịch vụ tìm kiếm của Việt Nam đồng thời tạo điều kiện để trở thành công cụ tìm kiếm thu hút được người dùng tại Việt Nam tiến tới có vị thế áp đảo so với các dịch vụ và công cụ tìm kiếm nước ngoài. Những công cụ tìm kiếm này cần có cơ chế quản lý đặc biệt dưới sự chỉ đạo của Nhà nước, cho phép tạo nội dung đa dạng, được cộng đồng mạng ưa thích, tin cậy; có những chính sách khuyến khích phát triển những dịch vụ hấp dẫn lớp trẻ một cách hợp lý như các dịch vụ trò chơi trực tuyến, dịch vụ âm nhạc, các dịch vụ nhắn tin, gọi điện, hội thoại… để thu hút người dùng Internet đến với các dịch vụ của Việt Nam cung cấp, tránh sự lệ thuộc quá vào các dịch vụ của các doanh nghiệp nước ngoài, như vậy sẽ tạo ra được một lực lượng truyền thông xã hội trên mạng và tạo môi trường thông tin trên mạng lành mạnh, vừa kiểm soát được thông tin, định hướng dư luận vừa có thể nhanh chóng tấn công chế áp, đẩy lùi những thông tin xấu, độc hại, xâm phạm ANQG và TTATXH.

**4.2. Tham mưu cho các bộ, ngành và đơn vị hữu quan thực hiện tốt chức năng quản lý nhà nước về an ninh quốc gia đối với hoạt động của các nhà cung cấp dịch vụ mạng ở Việt Nam**

Trong thời gian qua, bên cạnh những việc đã làm được thìcông tác quản lý nhà nước đối với các dịch vụ Internet cũng bộc lộ một số bất cập cần sớm khắc phục như: chưa quy định rõ trách nhiệm và cơ chế phối hợp của các Bộ, ngành, các đơn vị có liên quan dẫn tới sự quản lý chồng chéo giữa các cơ quan, đơn vị cũng như bỏ sót một số nội dung không có đơn vị nào thực hiện; sự phối hợp giữa cơ quan quản lý nhà nước về an ninh, trật tự và cơ quan quản lý nhà nước về kinh tế xã hội và cơ quan có liên quan khác chưa chặt chẽ, đồng bộ; thiếu những khuôn khổ pháp lý và những biện pháp cần thiết để bảo vệ người sử dụng khỏi những thông tin và ứng dụng độc hại từ Internet. Do đó, để tăng cường hiệu lực quản lý nhà nước về ANQG trên lĩnh vực an ninh, an toàn thông tin thời gian tới CQAN cần tham mưu cho làm tốt vấn đề sau:

*Một là, hoàn thiện các quy định của pháp luật làm cơ sở pháp lý cho các hoạt động bảo vệ an ninh, an toàn mạng thông tin quốc gia.*

Đây là yêu cầu có tính khách quan của quản lý nhà nước bằng pháp luật. Chỉ có xây dựng, bổ sung, hoàn thiện những quy định pháp luật thì chúng ta mới tạo ra được môi trường pháp lý đáp ứng yêu cầu của công tác đảm bảo an toàn cơ sở hạ tầng và an ninh thông tin; đồng thời, tạo chỗ dựa vững chắc cho CQAN trong đấu tranh chống các hoạt động vi phạm pháp luật, xâm phạm ANQG trên lĩnh vực này.

Từ thực tiễn cho thấy cần tham mưu cho Đảng, Nhà nước bổ sung, sửa đổi, ban hành các văn bản liên quan đến công tác đảm bảo an ninh, an toàn mạng thông tin quốc gia trong đó có đấu tranh với hoạt động sử dụng MXH xâm phạm ANQG cho phù hợp với yêu cầu thực tiễn. Trong đó cần nhanh chóng xây dựng Luật An ninh thông tin, ban hành Nghị định về công tác quản lý nhà nước trên lĩnh vực Internet; đồng thời quy định rõ trách nhiệm của các cơ quan, ban, ngành, tổ chức trong đấu tranh với hoạt động sử dụng không gian mạng làm công cụ tuyên truyền, phá hoại tư tưởng, chia rẽ nội bộ, kích động biểu tình, bạo loạn cũng như sử dụng những tài liệu có nội dung xấu trên không gian mạng để gây chia rẽ nội bộ.

*Hai là, nâng cao hiệu quả quản lý các loại hình dịch vụ trên mạng Internet.*

Cần chủ động tham mưu cho các cấp ủy, chính quyền nâng cao hiệu lực, hiệu quả quản lý nhà nước đối với các loại hình thông tin trên mạng. Rà soát, hoàn thiện hệ thống văn bản quy phạm pháp luật để thống nhất chỉ đạo, có chế tài xử lý các vi phạm, trong đó tập trung xây dựng và hoàn thiện dự thảo Chỉ thị của Thủ tướng Chính phủ về “Tăng cường công tác bảo đảm an ninh, an toàn thông tin trong tình hình mới”; các văn bản hướng dẫn thi hành Nghị định 72/2013/NĐ-CP ngày 15/7/2013 về “Quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng”.

Đẩy mạnh hoạt động thanh tra, kiểm tra, đôn đốc, hướng dẫn các doanh nghiệp, các điểm giao dịch, các đại lý, người sử dụng dịch vụ tuân thủ các quy định của pháp luật liên quan đến sử dụng mạng Internet. Từ đó đề xuất các biện pháp, hình thức xử lý phù hợp đối với những hành vi vi phạm nhằm nâng cao ý thức trách nhiệm của họ trong việc đảm bảo ANQG, phòng ngừa các đối tượng sử dụng các loại hình này để xâm phạm ANQG.

*Ba là, tăng cường quản lý các mặt hoạt động của các doanh nghiệp nước ngoài khi cung cấp dịch vụ xuyên biên giới vào Việt Nam*

Với đặc thù là một môi trường mở, hình thức cung cấp dịch vụ xuyên biên giới vào Việt Nam khá đa dạng với nhiều loại hình dịch vụ và thông tin như các MXH trực tuyến (Facebook, Twitter,...) dịch vụ thư điện tử (yahoo, mail, Gmail,...), dịch vụ điện thoại Internet (skype), dịch vụ quảng cáo,... đang thu hút hàng triệu người Việt Nam sử dụng Internet. Các văn bản pháp luật hiện tại chưa quy định trách nhiệm của các doanh nghiệp nước ngoài khi cung cấp dịch vụ xuyên biên giới vào Việt Nam, dẫn tới việc quản lý gặp nhiều khó khăn, đặc biệt là khi xử lý các vụ việc vi phạm pháp luật có liên quan đến nội dung thông tin. Do đó, cần tham mưu, phối hợp với các cơ quan chức năng nâng cao hiệu quả quản lý hoạt động của các doanh nghiệp, góp phần loại bỏ những sơ hở, thiếu sót mà các TLTĐ, các loại tội phạm có thể sử dụng hoạt động xâm phạm ANQG và TTATXH. Cụ thể là các tổ chức, doanh nghiệp nước ngoài cung cấp dịch vụ xuyên biên giới vào Việt Nam phải thực hiện các yêu cầu như:

- Tạo môi trường bình đẳng giữa doanh nghiệp trong nước và nước ngoài trong việc cung cấp dịch vụ viễn thông cho người Việt Nam và việc thực thi pháp luật Việt Nam;

- Có cam kết bằng văn bản tuân thủ các quy định về nội dung thông tin và hợp tác với các cơ quan chức năng của Việt Nam trong việc xử lý nghiêm những thông tin có nội dung trái với quy định pháp luật của Việt Nam. Trường hợp thông tin vi phạm do tổ chức, cá nhân khác cung cấp, khi có yêu cầu của các cơ quan quản lý nhà nước của Việt Nam phải phối hợp, loại bỏ các thông tin vi phạm;

- Cung cấp thông tin về người sử dụng có liên quan phục vụ việc phòng chống khủng bố, điều tra tội phạm khi có yêu cầu của cơ quan quản lý nhà nước của Việt Nam;

- Có văn phòng đại diện hoặc chỉ định tổ chức, cá nhân đại diện hợp pháp tại Việt Nam để thay mặt giải quyết các vấn đề liên quan và phối hợp với cơ quan chức năng của Việt Nam ngăn chặn, loại bỏ các thông tin vi phạm.

*Hoạt động được thực hiện với sự hỗ trợ kinh phí của Chương trình hỗ trợ pháp lý liên ngành dành cho doanh nghiệp giai đoạn 2015 - 2020 – Bộ Tư pháp./.*

1. Mỹ coi không gian mạng là một miền quan trọng trong chiến lược phát triển quốc gia trong tương lai, ban hành hàng loạt Chiến lược an ninh mạng với phạm vi bao trùm toàn thế giới hoặc các đạo luật riêng về từng lĩnh vực cụ thể, như: Chiến lược không gian mạng quốc tế, Chỉ thị của Tổng thống về an ninh mạng quốc gia, Luật tăng cường năng lực bảo vệ an ninh mạng, nghiên cứu phát triển an ninh mạng, lồng ghép các nội dung an ninh mạng vào các đạo luật cơ bản như Luật về an ninh quốc gia, Quốc phòng. [↑](#footnote-ref-1)
2. Trung Quốc ban hành Chiến lược An ninh mạng, Luật An ninh mạng, các văn bản pháp luật quản lý chặt chẽ thông tin, truyền thông; đồng thời, sử dụng báo chí, truyền hình, 35 trang/cổng TTĐT trọng điểm và hàng trăm tài khoản trên các diễn đàn, mạng xã hội, mở rộng mạng lưới tuyên truyền “ẩn thân” gồm 33 đài phát thanh trên 14 quốc gia thường xuyên đăng tải thông tin tuyên truyền phô trương sức mạnh TQ. [↑](#footnote-ref-2)
3. Nước ta chưa có nền công nghiệp an ninh mạng đủ mạnh để sản xuất được các thiết bị an ninh mạng, thiết bị viễn thông, thông tin, đặt ra nhiều vấn đề về năng lực tự chủ trên không gian mạng, khả năng bị kiểm soát, giám sát. Nguồn nhân lực an ninh mạng chất lượng cao chưa đáp ứng được yêu cầu thực tiễn. Nhận thức, kiến thức về an ninh mạng còn hạn chế, khả năng nhận diện các nguy cơ trên không gian mạng thấp, đa phần không đánh giá đúng, đầy đủ được các nguy cơ trên không gian mạng. Sự đầu tư cho an ninh mạng còn hạn chế. [↑](#footnote-ref-3)
4. Trong 6 tháng đầu năm 2018, phát hiện 2.769 trang/cổng TTĐT tên miền quốc gia, trong đó có 35 trang/cổng TTĐT thuộc quản lý của các cơ quan Đảng, Nhà nước bị tấn công, thay đổi giao diện, chiếm quyền điều khiển, chỉnh sửa nội dung. [↑](#footnote-ref-4)
5. Trong vụ lộ thông tin cá nhân người dùng Facebook vừa qua, có 427.446 tài khoản người dùng Việt Nam (*đứng thứ 9 trên thế giới*) bị lộ; thông tin cá nhân được cho là của khoảng 24.853.850 tài khoản Zing ID của Công ty cổ phần VNG được rao bán trên diễn đàn Raidforums. [↑](#footnote-ref-5)
6. Đầu năm 2018, máy chủ thư điện tử của Tập đoàn Dầu khí quốc gia Việt Nam (PVN) tồn tại lỗ hổng bảo mật nghiêm trọng, bị cài cắm loại mã độc tin tặc TQ thường hay sử dụng để duy trì kiểm soát, điều khiển máy chủ từ xa, chiếm đoạt thông tin, tài liệu; ngày 22/01/2018, hệ thống giao dịch tại Sở Giao dịch chứng khoán Tp. Hồ Chí Minh (HOSE) đã gặp sự cố không thể thực hiện khớp lệnh trong đợt giao dịch định kỳ xác định giá đóng cửa; ngày 28/01/2018, hệ thống check-in của Hãng hàng không Vietjet Air bị tấn công khiến nhiều chuyến bay phải tạm hoãn. [↑](#footnote-ref-6)
7. Trong 6 tháng đầu năm 2018, phát hiện và xử lý 47 vụ đăng tải tài liệu bí mật nhà nước trên mạng Internet, , xuất hiện nhiều tài liệu “Tuyệt mật”, “Tối mật” được đăng tải trên các trang mạng, mạng xã hội. [↑](#footnote-ref-7)
8. Hệ thống trang thiết bị phục vụ hạ tầng mạng Việt Nam đa phần nhập từ nước ngoài, chủ yếu có nguồn gốc xuất xứ từ Trung Quốc [↑](#footnote-ref-8)
9. Trước khi Luật An ninh mạng được ban hành, chưa có văn bản luật nào quy định về vấn đề an ninh mạng. Các quy định hiện hành về an ninh quốc gia, hình sự, dân sự, an toàn thông tin mạng chưa đáp ứng được yêu cầu bảo vệ an ninh mạng trong tình hình mới. [↑](#footnote-ref-9)
10. Mỹ, Canada, Liên bang Nga, Đức, Trung Quốc, Indonesia, Hi Lạp, Bulgaria, Đan Mạch, Phần Lan, Thụy Điển, Thổ Nhĩ Kỳ, Venezuela, Colombia, Argentina, Brazil [↑](#footnote-ref-10)
11. Các doanh nghiệp cung cấp dịch vụ qua biên giới như Google, Facebook đang có hoạt động kinh doanh sinh lợi tại Việt Nam thuộc sự điều chỉnh của các văn bản này [↑](#footnote-ref-11)
12. Các văn bản này không quy định việc lưu trữ một số loại hình dữ liệu có liên quan tới an ninh quốc gia là trái cam kết, đồng thời **có điều khoản ngoại lệ về an ninh, tôn trọng và đề cao an ninh quốc gia trong bất cứ hoạt động thương mại nào được đề cập trong các cam kết đó** [↑](#footnote-ref-12)
13. Việc lưu trữ dữ liệu trong nước còn giúp các doanh nghiệp này tiết kiệm chi phí kinh doanh, tăng mức tốc độ truy cập và nâng cao chất lượng dịch vụ; giúp các nhà mạng trong nước tiết kiệm kinh phí khi phải mua băng thông quốc tế. Về kỹ thuật, việc lưu trữ dữ liệu trong nước được tiến hành dễ dàng khi công nghệ cho phép, nhất là áp dụng công nghệ điện toán đám mây và các doanh nghiệp này đã có sẵn kinh nghiệm và thiết bị do áp dụng tương tự ở nhiều quốc gia khác. [↑](#footnote-ref-13)
14. như: Hội đồng kinh doanh Hoa Kỳ - ASEAN, Phòng Thương mại Mỹ (AmCham), Liên minh Internet Châu Á, Tập đoàn VISA và Mastercard, Hiệp hội điện toán đám mây Châu Á (ACCA)... [↑](#footnote-ref-14)
15. như Phòng Thương mại công nghiệp Việt Nam (VCCI), Hiệp hội truyền thông số Việt Nam (VDCA) [↑](#footnote-ref-15)