TS. NGUYỄN VIỆT LÂM (Chủ biên)

CHÍNH SÁCH AN NINH MẠNG

TRONG QUAN HỆ QUỐC TẾ HIỆN NAY VÀ ĐỐI SÁCH CỦA VIỆT NAM

(Sách tham khảo)

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

Chịu trách nhiệm xuất bản:
Q. GIÁM ĐỐC - TỔNG BIÊN TẬP
PHẠM CHÍ THÀNH

Chịu trách nhiệm nội dung:
PHÓ GIÁM ĐỐC - PHÓ TỔNG BIÊN TẬP
TS. ĐỖ QUANG DŨNG

Biên tập nội dung:	ThS. CÙ THỊ THÚY LAN
	TS. HOÀNG MẠNH THẮNG
	NGUYỄN MINH HÀ
	ThS. NGUYỄN VIỆT HÀ
Trình bày bìa:	PHẠM THÚY LIỄU
Chế bản vi tính:	LÂM THỊ HƯƠNG
Đọc sách mẫu:	MINH HÀ
	BÍCH LIỄU

Số đăng ký kế hoạch xuất bản: 892-2020/CXBIPH/8-295/CTQG.
Số quyết định xuất bản: 4873-QĐ/NXBCTQG, ngày 16/04/2020.
Nộp lưu chiểu: tháng 5 năm 2020.
Mã ISBN: 978-604-57-5550-1.

CHÍNH SÁCH AN NINH MẠNG

TRONG QUAN HỆ QUỐC TẾ HIỆN NAY VÀ ĐỐI SÁCH CỦA VIỆT NAM

Biên mục trên xuất bản phẩm
của Thư viện Quốc gia Việt Nam

Nguyễn Việt Lâm
Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam / Nguyễn Việt Lâm ch.b. - H. : Chính trị Quốc gia, 2019. - 220tr. ; 21cm

1. An ninh mạng 2. Hợp tác quốc tế 3. Chính sách 4. Việt Nam
005.8 - dc23

CTM0327p-CIP

TS. NGUYỄN VIỆT LÂM (Chủ biên)

CHÍNH SÁCH AN NINH MẠNG

TRONG QUAN HỆ QUỐC TẾ HIỆN NAY VÀ ĐỐI SÁCH CỦA VIỆT NAM

(Sách tham khảo)

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT
Hà Nội - 2019

TẬP THỂ TÁC GIẢ

TS. NGUYỄN VIỆT LÂM (Chủ biên)
ThS. ĐẶNG BẢO CHÂU
ThS. PHẠM BÁ VIỆT
ThS. NGUYỄN ĐÌNH SÁCH
ThS. NGUYỄN DUY QUÝ

LỜI NHÀ XUẤT BẢN

Từ khi ra đời, những lợi ích mà Internet mang lại cho con người là không thể phủ nhận. Internet là kho dữ liệu khổng lồ với rất nhiều thông tin/ứng dụng để con người có thể tra cứu, trao đổi công việc, học tập, mua bán, giao dịch ngân hàng,... một cách nhanh chóng và hiệu quả. Tuy nhiên, tính ưu việt, sự phát triển của Internet lại đang bị một số đối tượng lợi dụng với mục đích xấu, dẫn tới sự gia tăng các cuộc tấn công trên mạng với quy mô và mức độ ngày càng lớn, phức tạp. Điều này không chỉ gây thiệt hại về kinh tế mà còn gây bất ổn về mọi mặt và đe dọa đến nền an ninh của các quốc gia,... Cho đến nay, vấn đề an ninh mạng không còn là vấn đề của một cá nhân hay quốc gia đơn lẻ nữa mà đã và đang trở thành vấn đề toàn cầu của cả thế giới.

Việt Nam đang trên đà phát triển và hội nhập sâu rộng với thế giới. Bên cạnh đó, sự bùng nổ của cuộc Cách mạng công nghiệp 4.0 trên mọi lĩnh vực của đời sống, trong đó Internet có đóng vai trò rất lớn. Do vậy, Việt Nam cũng không tránh khỏi việc trở thành "nạn nhân" của rất nhiều vụ tấn công trên không gian mạng, gây ảnh hưởng đến ổn định xã hội, phát triển kinh tế, chính trị, đối nội, đối ngoại của đất nước. Hiện nay, thực trạng an toàn thông tin/an ninh mạng ở Việt Nam đang diễn biến khá phức tạp và nguy hiểm. Các cuộc tấn công mạng có quy mô, mức độ ngày càng tinh vi và được

chuẩn bị kỹ lưỡng. Mục tiêu tấn công không chỉ nhằm vào các cá nhân mà còn chuyển sang các mục tiêu lớn hơn là các tập đoàn kinh tế hay các hệ thống thông tin quan trọng của quốc gia. Chẳng hạn, năm 2017, khi mã độc tống tiền WannaCry được phát tán gây ảnh hưởng cho hơn 70 quốc gia thì tại Việt Nam, có khoảng 1.000 máy tính cá nhân và công ty bị nhiễm mã độc này. Việt Nam là một trong 20 nước bị thiệt hại nặng nề nhất. Theo Hiệp hội An toàn thông tin Việt Nam (VNISA), có tới hơn 50% cơ quan, doanh nghiệp không phát hiện được mình bị tấn công và chưa đến 30% đơn vị được cảnh báo có khả năng xử lý sự cố. Mức độ thiệt hại do các cuộc tấn công mạng ngày càng cao. Dựa trên thống kê của hệ thống giám sát virus của Bkav thì chỉ trong năm 2018, ở Việt Nam, hơn 1,6 triệu lượt máy tính bị mất dữ liệu; 77% USB bị nhiễm mã độc ít nhất một lần trong năm. Trong hai năm 2017-2018, số lượng lỗ hổng an ninh trong các phần mềm, ứng dụng là hơn 75.000 lỗ hổng, cao hơn gấp nhiều lần so với các năm trước,... Những con số này cho thấy tình hình an ninh mạng ở Việt Nam đang ở mức báo động. Chính phủ Việt Nam cùng các cơ quan, tổ chức có liên quan cần hành động kịp thời và thiết thực để xử lý tình trạng trên.

Các chuyên gia, học giả của Mỹ, Trung Quốc, châu Âu, Nga và ASEAN đánh giá, trong 10 năm nữa, an ninh mạng sẽ là chủ đề then chốt trên chính trường quốc tế. Quá trình số hoá đang diễn ra mạnh mẽ trên thế giới cùng với các mối đe dọa phức tạp trên không gian mạng với nhiều hình thức đa dạng hơn, tinh vi hơn buộc các quốc gia sẽ phải hợp tác cùng ứng phó. Nhưng làm sao để có được những thỏa thuận, khung pháp lý về an ninh mạng phù hợp với tình hình của mỗi quốc gia mà vẫn hài hòa các mối quan hệ quốc tế là vấn đề đang được đặt ra và cần tích cực giải quyết. Để bạn đọc hiểu

hơn về thực trạng an ninh mạng của nhiều nước trên thế giới, tác động của an ninh mạng đến quan hệ quốc tế và đối sách của Việt Nam về vấn đề này, Nhà xuất bản Chính trị quốc gia Sự thật xuất bản cuốn sách ***Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam*** của TS. Nguyễn Việt Lâm (Chủ biên). Cuốn sách sẽ là nguồn tài liệu bổ ích cho bạn đọc tham khảo.

Xin giới thiệu cuốn sách cùng bạn đọc.

Tháng 9 năm 2019

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

LỜI NÓI ĐẦU

Không gian mạng từ lâu đã là một vấn đề phức tạp đối với an ninh của các quốc gia và trong quan hệ quốc tế. Cách đây gần hai thập kỷ, tác giả Cobb (năm 1999) nghiên cứu và đã chỉ ra rằng, các cuộc xung đột xuất phát từ không gian mạng là những mối đe dọa nguy hiểm nhất đối với an ninh quốc gia kể từ khi thế giới phát triển vũ khí hạt nhân trong những năm 1940. Việc bảo vệ không gian mạng hiện nay đang là mối quan tâm hàng đầu của chính phủ nhiều nước trên thế giới. Không gian mạng trở thành "không gian chiến lược mới", vùng "lãnh thổ đặc biệt", gắn kết chặt chẽ với các môi trường tự nhiên (đất liền, biển đảo, trên không, vũ trụ) để các quốc gia khai thác, phát triển kinh tế, chính trị - xã hội, bảo vệ chủ quyền, lợi ích và an ninh quốc gia. Trên không gian mạng hiện có bốn mối đe dọa đến an ninh quốc gia là chiến tranh không gian mạng, gián điệp kinh tế, tội phạm mạng và khủng bố trên không gian mạng, mỗi loại có khung thời gian khác nhau và trên nguyên tắc là sẽ có các giải pháp xử lý khác nhau. Không gian mạng là một mặt trận để tiến hành các cuộc chiến

tranh thông tin, chiến tranh không gian mạng và các phương thức tác chiến không gian mạng độc lập hoặc kết hợp với phương thức tác chiến trên các môi trường tự nhiên trong chiến tranh cục bộ, xung đột vũ trang, tranh chấp tài nguyên, chủ quyền lãnh thổ, biển, đảo, xung đột sắc tộc, tôn giáo, hoạt động can thiệp, lật đổ, ly khai và khủng bố. Hiện nay, hoạt động gián điệp và tội phạm mạng gây ra nhiều thiệt hại lớn về kinh tế (thiệt hại do gián điệp mạng gây ra cho kinh tế Mỹ có thể từ 0,5% đến GDP 1%, hay 25 tỷ đến 100 tỷ USD)[1], nhưng hai loại hình đe dọa còn lại có thể trở thành mối đe dọa lớn hơn trong thập niên tới.

Khi các chủ thể trong không gian mạng hình thành liên minh và phát triển chiến thuật, các loại hình đe dọa an ninh mạng nói trên có thể ngày càng chồng chéo nhau. Tổng thống Mỹ Barack Obama (nhiệm kỳ 2009-2017) từng phát biểu: "Đe dọa về an ninh mạng trở thành một trong những thách thức về kinh tế và an ninh quốc gia nguy hiểm nhất đối với nước Mỹ". Trên thực tế, từ năm 2013 nước Mỹ đã xác định: "Các mối đe dọa từ không gian mạng là đe dọa chiến lược số 1, xếp trên mối đe dọa về khủng bố". Ngày 11/5/2017, Tổng Thống Mỹ Donald Trump đã ký ban hành

---

1. Thiên Minh: "Gián điệp mạng Trung Quốc tác động xấu đến lợi ích kinh tế Mỹ", *An ninh thế giới Online,* http://antg.cand.com.vn/Ho-so-mat/Gian-diep-mang-Trung-Quoc-tac-dong-xau-den-loi-ich-kinh-te-My-308673/, truy cập ngày 05/5/2019.

sắc lệnh về an ninh mạng, thể hiện sự quan tâm tiếp nối của Mỹ với vấn đề này. Còn Chủ tịch Trung Quốc Tập Cận Bình thì khẳng định: "Không có an ninh mạng đồng nghĩa không có an ninh quốc gia". Internet và an ninh thông tin đã trở thành thách thức mới đối với Trung Quốc, vì cả hai đều gắn liền với an ninh quốc gia và ổn định xã hội.

An ninh mạng không chỉ được các nước phát triển quan tâm mà trở thành vấn đề được quan tâm của các nước trên thế giới.

Tại Việt Nam, mặc dù có quá trình hội nhập nhanh, độ mở của nền kinh tế lớn và lượng người dùng mạng Internet tăng nhanh ở khu vực châu Á Thái Bình Dương, nhưng do năng lực an ninh mạng (bao gồm cơ sở hạ tầng cứng và mềm) còn yếu, hạn chế nên các biện pháp phòng vệ trước các mối đe dọa an ninh mạng chưa thực sự hiệu quả. Ngoài ra, Việt Nam hiện đã và đang trở thành mục tiêu và đối tượng của nhiều thế lực có ý đồ xấu (cả về địa chiến lược và các lý do khác,...) nên nguy cơ bị tấn công mạng luôn thường trực. Điển hình, cuộc tấn công bằng mã độc WannaCry năm 2017 đã khiến hơn 1.000 máy tính của các công ty và các cá nhân ở Việt Nam bị ảnh hưởng. Giới chuyên gia đánh giá Việt Nam nằm trong top 20 quốc gia, vùng lãnh thổ bị ảnh hưởng nhất, bên cạnh Ucraina, Ấn Độ, Trung Quốc, Đài Loan (Trung Quốc),... Vụ việc Hãng hàng không quốc gia Việt Nam Vietnam Airlines bị hacker tấn công ngày 29/7/2016 là cảnh báo mạnh mẽ về nguy cơ

các cuộc tấn công có chủ đích (APT) tại Việt Nam sẽ còn tiếp tục trong thời gian tới. Từ năm 2012, hệ thống quan sát của các cơ quan chức năng đã phát hiện mạng lưới phần mềm gián điệp tấn công có chủ đích (APT) xuất hiện tại nhiều cơ quan, doanh nghiệp.

Ở Việt Nam, các sự cố, sự việc liên quan đến tình hình an ninh trên không gian mạng cũng diễn biến vô cùng phức tạp. Trong năm 2015, nhiều cổng thông tin điện tử của Việt Nam bị tin tặc nước ngoài sử dụng virus gián điệp để xâm nhập hệ thống, có khoảng 10.060 trang tin, cổng thông tin điện tử của Việt Nam bị tin tặc tấn công, chiếm quyền quản trị, chỉnh sửa nội dung; trong nửa đầu năm 2016, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) ghi nhận 127.630 sự cố an ninh mạng, tăng gấp bốn lần so với năm 2015 và gấp 6,5 lần so với năm 2014. Tháng 12/2017, VNCERT cho biết đã phát hiện hơn 420.000 tài khoản sử dụng thư điện tử ở Việt Nam (trong đó có 930 tài khoản sử dụng hòm thư của cơ quan nhà nước có đuôi "gov.vn" để đăng nhập và rất nhiều tài khoản sử dụng thư điện tử của các tập đoàn, doanh nghiệp quan trọng của Việt Nam) bị xâm nhập và lấy thông tin, mật khẩu[1].

---

1. Xem Công văn số 442/VNCERT-ĐPƯC ngày 26/12/2017 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam về việc lộ 1,4 tỷ tài khoản và mật khẩu từ các trang mạng xã hội, dịch vụ trực tuyến.

Tại cuộc hội thảo quốc tế về an ninh mạng (Xingapo, từ ngày 20 đến 21/9/2017), nhiều học giả của Mỹ, Trung Quốc, châu Âu, Nga và ASEAN đánh giá rằng, trong 10 năm nữa, an minh mạng sẽ là chủ đề then chốt trong chính trị quốc tế. Quá trình số hóa đang diễn ra mạnh mẽ trên thế giới cùng với các mối đe dọa hiếu chiến trong không gian mạng với nhiều hình thức khác nhau sẽ ngày càng tăng. Để xử lý các mối nguy hại từ an ninh mạng do các chính phủ tài trợ trên thế giới, các quốc gia có một số lựa chọn chính sách. Trong đó có ba biện pháp được thảo luận rộng rãi hiện nay là: phòng vệ *(defence),* răn đe *(deterrence)* và ngoại giao *(diplomacy)*. Tại hội thảo quốc tế về an ninh mạng trong khuôn khổ Hội nghị Cấp cao ASEAN - Ôxtrâylia năm 2018 (Sydney, Ôxtrâylia), các nhà nghiên cứu, học giả của các nước ASEAN, Ôxtrâylia, Mỹ và Nga đều thống nhất rằng, cần nghiên cứu, thúc đẩy hợp tác quốc tế về an ninh mạng và đặc biệt sớm xây dựng bộ Quy tắc ứng xử về an ninh mạng trong quan hệ quốc tế trong bối cảnh tình hình khu vực và thế giới thời gian qua có nhiều biến động khó lường.

Chính sách phòng vệ và răn đe có thể mang lại các giải pháp tốt trong ngắn hạn nhưng câu hỏi đặt ra là liệu hai chính sách này có giúp tạo ổn định và bảo đảm an ninh mạng quốc tế trong dài hạn hay không. Thực tế cho thấy cả hai biện pháp này đã góp phần tạo ra và thúc đẩy nguy cơ chạy đua vũ trang không gian mạng và chu kỳ leo thang

giữa các đối thủ (có thể là các quốc gia, cá nhân và nhóm hacker quốc tế) tiềm ẩn trong không gian mạng. Các biện pháp ngoại giao khó có thể mang lại kết quả ngay trong ngắn hạn nhưng sẽ là một lựa chọn tối ưu trong dài hạn. Về lâu dài, sự hợp tác giữa các quốc gia nhằm thiết lập lòng tin và các quy tắc quốc tế về hành vi ứng xử trong không gian mạng là biện pháp hữu hiệu cho sự ổn định và an ninh mạng của các quốc gia trong quan hệ quốc tế. Thực tế, sự hợp tác giữa các quốc gia đã có những bước tiến, nhưng chưa đi vào thực chất và chưa trở thành xu thế chủ đạo, trong khi sự đối đầu vẫn rất gay gắt. Một cuộc chạy đua vũ trang thật sự trên không gian mạng và chiến tranh mạng đang trở thành hình thái chiến tranh mới. Nguy cơ về một cuộc chiến tranh "không khói súng, không chiến tuyến, không biên giới lãnh thổ và cũng không loại trừ bất cứ quốc gia nào" đang hiện hữu hơn bao giờ hết. Tại Việt Nam, việc hợp tác quốc tế về an minh mạng đang được đẩy mạnh giữa Bộ Công an, Bộ Thông tin và Truyền thông với các đối tác nước ngoài trong việc bảo đảm không gian mạng tại Việt Nam an toàn, lành mạnh, cởi mở và góp phần thúc đẩy cho sự phát triển của đất nước.

Do vậy, cuốn sách ***Chính sách an ninh mạng trong quan hệ quốc tế hiện nay và đối sách của Việt Nam*** đi sâu phân tích tình hình an ninh mạng trong quan hệ quốc tế hiện nay, chính sách an ninh mạng của các cường quốc, trung tâm lớn, các nước mạnh về không gian mạng, các

nước sát sườn với lợi ích của Việt Nam. Trên cơ sở đó, nhóm tác giả đưa ra một số khuyến nghị về chính sách an ninh mạng từ khía cạnh đối ngoại.

Cuốn sách gồm ba chương:

Chương 1: An ninh mạng và thực trạng: tập trung phân tích các khía cạnh cơ bản của vấn đề an ninh mạng (khái niệm, những thách thức về an ninh mạng, vai trò của vấn đề an ninh mạng trong tổng thể an ninh quốc gia, vai trò của vấn đề an ninh mạng đối với sự phát triển kinh tế - xã hội,...); vấn đề an ninh mạng trong cuộc Cách mạng Công nghiệp lần thứ tư (gọi tắt là cuộc Cách mạng công nghệ 4.0), qua đó nêu thách thức, rủi ro về an ninh mạng, phản ánh thực tế hợp tác và đấu tranh giữa các chủ thể chính là các nước lớn trong quan hệ quốc tế hiện nay về an ninh mạng.

Chương 2: Chính sách an ninh mạng và tình hình hợp tác về an ninh mạng của một số quốc gia trên thế giới: giới thiệu và phân tích chính sách an ninh mạng/an ninh thông tin của một số nước lớn và khu vực trên thế giới như Mỹ, Nga, Trung Quốc, EU; các nước có trình độ khoa học -kỹ thuật phát triển cao trong lĩnh vực an ninh mạng; các nước láng giềng của Việt Nam; và các nước trong khu vực Đông Nam Á.

Chương 3: Kiến nghị, đề xuất chính sách về an ninh mạng cho Việt Nam: phân tích thực tế vấn đề an ninh mạng của Việt Nam, trong đó chú ý đến các yếu tố về pháp luật,

chính sách; các thành tựu và hạn chế trong việc bảo đảm an ninh mạng. Trên cơ sở đó đưa ra kiến nghị, đề xuất chính sách về an ninh mạng của Việt Nam nói chung và từ góc độ chính sách đối ngoại nói riêng.

Chương 1

AN NINH MẠNG VÀ THỰC TRẠNG

1. Về an ninh mạng

1.1. Khái niệm

Theo Bách khoa toàn thư Anh (năm 2015), an ninh mạng được hiểu theo nghĩa hẹp là một hệ thống các kỹ thuật, thủ tục và biện pháp được thiết kế nhằm bảo vệ sự toàn vẹn của mạng, máy tính, chương trình và dữ liệu khỏi các cuộc tấn công, phá hoại hoặc xâm nhập trái phép. Theo Phát kiến quốc gia về sự nghiệp và nghiên cứu an ninh mạng của Mỹ (NICCS), an ninh mạng được định nghĩa là "hoạt động hoặc quá trình, khả năng, hay trạng thái mà theo đó thông tin, hệ thống thông tin liên lạc và thông tin chứa trong đó được bảo vệ khỏi và/hoặc bảo vệ chống lại thiệt hại, sự sử dụng trái phép hoặc sửa đổi, khai thác"[1]. Như vậy, chức năng cơ bản của an ninh mạng là bảo vệ thông tin và hệ thống từ các mối đe dọa mạng dưới nhiều hình thức, từ tấn công chương trình, malware, ransomware,

---

1. Xem thêm tại https://niccs.us-cert.gov/about-niccs/glossary.

phishing, tấn công từ chối dịch vụ, cho đến những truy cập trái phép, sử dụng sai mục đích, sửa đổi, hủy hoại hoặc tiết lộ không đúng thông tin nhằm bảo đảm mọi thông tin, dữ liệu trong tình trạng an toàn nhất. Tấn công mạng ở hình thái cao nhất bao gồm các hình thức khủng bố mạng, chiến tranh mạng hay gián điệp mạng. Theo Tạp chí *Forbes,* thị trường an ninh mạng toàn cầu hiện ở mức 77 tỷ USD và sẽ đạt 170 tỷ USD vào năm 2020. Sự tăng trưởng mạnh mẽ của thị trường này được hỗ trợ bởi một loạt xu hướng công nghệ mới như Internet vạn vật (IoT) hay "mang thiết bị cá nhân đi làm" (BYOD), việc sử dụng ngày càng rộng rãi các ứng dụng dựa trên đám mây, việc mở rộng nhu cầu an ninh ra ngoài các phạm vi dữ liệu truyền thống và việc các nước áp dụng tiêu chuẩn bảo mật ngày càng chặt chẽ, chẳng hạn như Quy định chung về bảo vệ dữ liệu của EU (GDPR) hay Khuôn khổ an ninh mạng của Viện quốc gia về tiêu chuẩn và công nghệ (NIST).

Tuy nhiên, ở cấp độ quốc gia, khái niệm an ninh mạng được hiểu theo nghĩa rộng hơn, là một phần trong khái niệm an ninh thông tin với mục tiêu bảo vệ thông tin kỹ thuật số khỏi các mối đe dọa đến sự toàn vẹn và bất khả xâm phạm của thông tin. Luật Trung Quốc định nghĩa an ninh mạng là "sử dụng các biện pháp cần thiết để phòng, chống lại các sự cố tấn công, xâm nhập, quấy rối, phá hoại, sử dụng phi pháp và sự cố bất ngờ, bảo đảm cho mạng vận hành ổn định và bảo vệ tính bí mật, tính nguyên vẹn, khả

năng sử dụng số liệu mạng"[1]. Luật Ixraen định nghĩa an ninh mạng là "các đường lối, chính sách, hoạt động, cơ chế tự vệ, quản lý rủi ro và phương tiện kỹ thuật nhằm bảo vệ không gian mạng, là một khu vực hữu hình và vô hình, bao gồm các hệ thống máy tính, mạng lưới máy tính và truyền thông, thông tin điện tử và nội dung được truyền giữa các máy tính, phương tiện truyền thông, cơ sở dữ liệu và người sử dụng". Luật Nhật Bản định nghĩa an ninh mạng là "những biện pháp cần thiết được thực hiện nhằm quản lý thông tin một cách an toàn, chẳng hạn như ngăn ngừa sự lộ, lọt, biến mất hoặc hư hại thông tin được lưu trữ, gửi đi, chuyển đi hoặc tiếp nhận bởi các phương tiện điện tử, từ tính hoặc các phương tiện khác không được tiếp nhận một cách tự nhiên; và bảo đảm tính an toàn, đáng tin cậy của hệ thống thông tin và mạng lưới viễn thông".

Tại Việt Nam, Luật An ninh mạng năm 2018 định nghĩa "*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"[2]. An ninh mạng quốc gia là một bộ phận không thể tách rời của an ninh quốc gia; bao gồm sự bất khả xâm phạm về chủ quyền quốc gia trên không gian

---

1. Understand China's Cybersecurity Law, https://www.mfat.govt.nz/assets/China/Understanding-Chinas-cybersecurity-law.pdf.

2. Luật An ninh mạng, Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2019, tr.7.

mạng, bảo đảm mọi 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, trật tự, an toàn xã hội.

Như vậy, có sự khác biệt khá rõ trong khái niệm về an ninh mạng của Việt Nam với các nước tư bản phương Tây. Đối với phương Tây, an ninh mạng chỉ giới hạn ở phạm vi điều chỉnh các biện pháp kỹ thuật nhằm ngăn chặn và đối phó với những hoạt động truy cập trái phép và các cuộc tấn công mạng. Trong khi đó, Việt Nam và Trung Quốc lại coi an ninh mạng là một bộ phận không thể tách rời của an ninh quốc gia.

1.2. An ninh mạng trong thời kỳ Cách mạng công nghiệp lần thứ tư

1.2.1. Cách mạng công nghiệp lần thứ tư

"Cách mạng công nghiệp lần thứ tư" với tên gọi ban đầu là "Công nghiệp 4.0" (Industrie 4.0) là thuật ngữ có nguồn gốc từ một dự án công nghệ cao của Chính phủ Đức nghiên cứu và thử nghiệm từ năm 2006 đến 2013 nhằm nâng cao vai trò của công nghệ vi tính trong sản xuất. Đến năm 2014, nhiều công ty bên ngoài nước Đức đã bắt đầu áp dụng.

Trước khi xuất hiện "Công nghiệp 4.0", công nghiệp sản xuất của loài người đã trải qua ba cuộc cách mạng. Cuộc Cách mạng công nghiệp lần thứ nhất trong khoảng

thế kỷ XVIII - XIX, bắt nguồn từ phát minh động cơ hơi nước và các công trình đường sắt ở châu Âu và châu Mỹ. Cuộc Cách mạng công nghiệp lần thứ hai bắt đầu từ cuối thế kỷ XIX đến đầu thế kỷ XX đã cho phép sản xuất hàng loạt với những phát minh về điện, chuỗi lắp ráp, điện thoại, động cơ đốt trong. Cuộc Cách mạng công nghiệp lần thứ ba diễn ra vào những năm 1960 và được ví như một cuộc cách mạng công nghệ số do cuộc cách mạng này được thúc đẩy bởi các phát minh công nghệ bán dẫn, máy tính lớn, máy tính cá nhân, internet và công nghệ thông tin liên lạc.

Cuộc Cách mạng công nghiệp lần thứ tư (Cách mạng công nghiệp 4.0) được xem như sự kế thừa của cuộc cách mạng lần thứ ba. Áp dụng những thành tựu khoa học - công nghệ của Cách mạng công nghiệp lần thứ ba, Cách mạng công nghiệp 4.0 đã tạo ra những đột phá công nghệ trong hầu như tất cả các lĩnh vực sản xuất, dịch vụ với những phát minh như trí thông minh nhân tạo, công nghệ nano, máy tính lượng tử, công nghệ sinh học, Internet vạn vật, xe tự động,... và sự phát triển khiến cho những công nghệ vốn có trở nên hiện đại, giá thành thấp và dễ tiếp cận hơn. Điểm khác biệt lớn nhất giữa cuộc Cách mạng công nghiệp lần thứ tư và cuộc Cách mạng công nghiệp lần thứ ba là sự kết nối mạng và kiểm soát số đã tích hợp sâu với các công cụ đời thực.

1.2.2. An ninh mạng trong thời kỳ Cách mạng công nghiệp 4.0

Có thể nói, với những tiến bộ vượt bậc, cuộc Cách mạng công nghiệp 4.0 đã tác động mạnh tới đời sống xã hội loài

người. Số lượng người sử dụng mạng Internet tăng lên nhanh chóng, các cá nhân và các chính phủ ngày càng phụ thuộc vào mạng truyền thông cho các hoạt động thông tin, giao dịch.

Việc mạng lưới Internet được sử dụng phổ biến đã làm thay đổi cách thức cung ứng các tiện ích xã hội. Hiện nay, ước tính có gần 2 tỷ người sử dụng mạng Internet; người sử dụng dành phần lớn thời gian trong ngày trên môi trường mạng. Trên cơ sở đó, những công ty sử dụng nền tảng Internet để cung cấp sản phẩm, dịch vụ đang ngày càng phổ biến, từ dịch vụ tài chính với các giao dịch ngân hàng điện tử (e-banking), mặt hàng tiêu dùng được mua qua mạng thông qua kênh bán hàng là các tập đoàn lớn trên thế giới như Amazon hay Alibaba, dịch vụ vận chuyển hàng hóa bằng phương tiện không người lái (drone), các khóa học trực tuyến, cho tới dịch vụ thuê khách sạn Airbnb hay taxi Uber, Grab,... tạo ra sự tiện lợi chưa từng có đối với người tiêu dùng và một thị trường toàn cầu cho các nhà cung cấp.

Sự ra đời của các mạng xã hội cũng đã làm thay đổi cách thức con người tương tác với nhau và cập nhật thông tin, tin tức. Có đến 30% dân số thế giới đang sử dụng mạng xã hội để cập nhật, theo dõi các sự kiện trên thế giới. Nhiều sự kiện (như thông tin cập nhật trực tiếp về vụ đánh bom ở Boston và diễn biến truy bắt tội phạm trong vụ việc này)

được người sử dụng cập nhật trực tiếp và thậm chí còn nhanh hơn tin tức từ báo chí, truyền thông.

Với sự bùng nổ của cuộc Cách mạng công nghiệp 4.0, Internet ngày càng trở thành một tiện ích không thể thiếu. Điều này khiến cho các hoạt động gây ảnh hưởng tới an ninh mạng và tội phạm mạng cũng gia tăng một cách đáng ngại. Từ chính những tiện ích của sự kết nối toàn cầu, các tổ chức tội phạm có thể dễ dàng chia sẻ cách thức phạm tội, truyền bá tư tưởng cực đoan, tuyển dụng thành viên, tổ chức các hoạt động phạm tội,... Cuộc Cách mạng công nghiệp 4.0 đã tạo ra một xã hội kết nối, các dịch vụ từ đời sống thường nhật cho đến các hoạt động của chính phủ đều phụ thuộc vào môi trường mạng; bên cạnh đó, một trong những nhược điểm lớn nhất của môi trường mạng luôn kết nối là rất dễ sử dụng nhưng rất khó bảo đảm an ninh vì:

- *Thứ nhất*, môi trường không gian mạng được tạo ra bởi hệ thống các phần mềm được cấu tạo bởi hàng triệu các dòng lệnh; trong số những dòng lệnh đó không thể bảo đảm sẽ không xảy ra lỗi để các tin tặc lợi dụng tấn công vào hệ thống. Do đó, việc bảo đảm an ninh mạng bằng cách củng cố, sửa chữa những lỗi phần mềm chỉ mang tính tương đối và theo các chuyên gia nhận định, không thể bảo đảm các phần mềm sẽ không chứa bất kỳ lỗ hổng an ninh nào và ta buộc phải chấp nhận thực tế này.

- *Thứ hai*, tội phạm trên môi trường mạng có tính nặc danh với rất nhiều thủ thuật kỹ thuật (sử dụng các dịch vụ

địa chỉ mạng ảo như VPN, Tor...). Những tội phạm này có thể ẩn tung tích của mình và rất khó để các cơ quan chức năng có thể tìm ra được ngay cả khi có thể xác định được vị trí địa lý của tin tặc thì trong nhiều trường hợp tin tặc lại ở ngoài vùng tài phán của quốc gia chịu ảnh hưởng từ cuộc tấn công mạng đó. Hơn nữa, đối với những vụ tấn công mạng mà chính phủ quốc gia được cho là đứng đằng sau thì rất khó để có thể truy cứu trách nhiệm của đối tượng tấn công, khi mà vụ tấn công xảy ra đối với nạn nhân ở một nước, kẻ thực hiện lại ở một nước khác, sử dụng công nghệ được cung cấp bởi một nước khác, và kẻ chủ mưu lại ở một nước khác nữa. Các cuộc tấn công nhằm vào môi trường mạng phát triển nhanh chóng về cả hình thức và quy mô, có tính chất xuyên biên giới, gây ảnh hưởng nghiêm trọng tới sự ổn định kinh tế - chính trị của các nước. Từ chỗ chỉ là những cuộc tấn công tự phát do các cá nhân thực hiện nhằm đánh cắp thông tin, trục lợi bất chính từ những lỗ hổng an ninh của các phần mềm, đến nay tội phạm mạng đã được thực hiện bởi các nhóm tin tặc có tổ chức, thậm chí có sự hậu thuẫn của chính phủ một số nước...

Ở Việt Nam, các sự cố, sự việc liên quan đến an ninh mạng cũng diễn ra vô cùng phức tạp. Từ năm 2010 đến nay, đã phát hiện nhiều trang tin điện tử và mạng xã hội trong nước có hành vi vi phạm, đăng tải thông tin có nội dung chính trị phản động; nhiều cổng thông tin điện tử của

Việt Nam bị tin tặc nước ngoài sử dụng virus gián điệp để xâm nhập hệ thống.

1.3. Tác động của các dịch chuyển trong không gian mạng

1.3.1. Tác động trong lĩnh vực kinh tế

Đánh giá về vai trò của thông tin trên không gian mạng, học giả Nandan Nilekani (Chủ tịch công ty Infosys, Chủ tịch đầu tiên của Cơ quan quản lý thông tin của Ấn Độ - ngang cấp bộ trưởng) cho rằng, ngày nay dữ liệu có thể được coi là một loại dầu hỏa mới (*new oil*), có thể được mua, bán và là một nguồn tài nguyên chiến lược của đất nước[1]. Lý do là vì dữ liệu cũng có thể được "chiết suất" và sử dụng bởi bên thứ ba (điển hình như việc Facebook cho phép Cambridge Analytica thu thập và sử dụng dữ liệu người dùng Facebook để phục vụ chiến dịch tranh cử Tổng thống Mỹ). Do đó, có thể nói các tài nguyên số ngày nay có giá trị hơn các tài sản hữu hình. Ví dụ, Uber là công ty taxi công nghệ lớn nhất thế giới nhưng không sở hữu bất kỳ một phương tiện nào. Facebook là công ty truyền thông lớn nhất thế giới nhưng không tạo ra nội dung nào. Alibaba là hãng bán lẻ có giá trị nhất nhưng không có nhà kho. Airbnb là nhà cung cấp dịch vụ cho thuê phòng lớn nhất thế giới nhưng không có cơ sở lưu trú nào.

---

1. Nandan Nilekani: "Data to the People: India's Inclusive Internet", *Foreign Affair*, 97(5), 19 (2018).

Học giả Viktor Mayer-Schonberger (Giáo sư ngành quản trị và quản lý Internet, Đại học Oxford, Anh) và Thomas Ramge (Phóng viên chuyên ngành công nghệ, Tạp chí *Economist,* Anh) cho rằng, sự phát triển nhanh chóng của lĩnh vực dịch vụ trên không gian mạng cũng đang dẫn đến các chuyển dịch về mặt kinh tế[1]. Về quy mô, năm 2006, 3 trong tổng số 6 công ty có giá trị lớn nhất thế giới là các công ty dầu lửa, chỉ một trong số đó là công ty công nghệ. Vào năm 2016, chỉ còn một công ty dầu lửa nằm trong nhóm này, còn lại là các công ty công nghệ. Về thị trường, Trung Quốc và Ấn Độ hiện nay là hai thị trường số lớn nhất thế giới với 722 triệu và 281 triệu người sử dụng. Chỉ trong khoảng 5 năm trở lại đây, tổng giá trị giao dịch thanh toán di động ở Trung Quốc là 9 nghìn tỷ USD, trong khi con số này ở Mỹ chỉ là 49 tỷ USD[2].

Về cơ cấu thị trường, sự phát triển nhanh chóng của một vài công ty công nghệ lớn dẫn đến sự tập trung về dữ liệu cũng như thị phần quá lớn, từ đó dẫn đến nguy cơ về độc quyền và các hệ lụy cho nền kinh tế. Hiện nay, Facebook có hơn 2 tỷ người sử dụng. Google và Facebook chiếm hơn một nửa thị trường quảng cáo số. Apple đang

---

1. Viktor Mayer - Schonberger and Thomas Ramge: "A Big Choice for Big Tech: Share Data or Suffer the Consequences", *Foreign Affair*, 97 (5) 48 (2018).

2. Nandan Nikekani: "Data to the People: India's Inclusive Internet", *Foreign Affair,* 97(5), 19 (2018).

duy trì thị trường các phần mềm di động lớn nhất thế giới về mặt doanh số. Amazon gần như chiếm lĩnh hoàn toàn thị trường Mỹ với khả năng sinh lợi khổng lồ.

Sự thành công của các hãng này đem lại lợi ích to lớn cho người tiêu dùng nhưng cũng đem lại nhiều nguy cơ cho xã hội và nền kinh tế. *Thứ nhất*, việc chiếm thị phần quá lớn làm suy yếu tính cạnh tranh của thị trường. Lịch sử cho thấy tình trạng độc quyền luôn tiềm tàng tính dễ tổn thương cho toàn bộ nền kinh tế. *Thứ hai*, việc các công ty độc quyền này thu thập và lưu trữ một lượng khổng lồ thông tin người sử dụng cũng khiến các công ty này trở thành mục tiêu của các nhóm tấn công mạng (hacker), dẫn đến các lo ngại về việc bảo mật thông tin cá nhân. *Thứ ba*, nguy cơ lớn nhất là việc gây ra các thách thức mang tính hệ thống, làm tổn hại tính đàn hồi (*resilience*) của nền kinh tế. Theo đó, việc nắm được các thông tin về sở thích, nhu cầu cá nhân, lịch sử các giao dịch của người tiêu dùng sẽ dẫn đến việc tác động và dẫn dắt (bởi một nhóm nhỏ các công ty thông qua tác động vào kết quả tìm kiếm và hiển thị quảng cáo trên mạng) việc mua sắm, giao dịch của người tiêu dùng nhằm phục vụ mục tiêu lợi nhuận của các công ty công nghệ. Thực tế này gần giống với hệ thống kinh tế tập trung (*Centrally planned system*). Bất cứ một lỗi nào xảy ra trong hệ thống cũng có thể tác động đến tất cả những người tham gia khác trên thị trường.

Về mặt thể chế, cũng theo các học giả Viktor Mayer-Schonberger và Thomas Ramge, luật chống độc quyền hiện

nay đã không đáp ứng được việc ứng phó với các nguy cơ nói trên[1]. Hiện nay, việc một công ty thành công trong lĩnh vực dịch vụ mạng hay không phụ thuộc rất lớn vào việc tiếp cận với dữ liệu và thông tin. Trong khi đó, một lượng lớn dữ liệu lại chủ yếu nằm trong tay một nhóm nhỏ các công ty siêu lớn. Một giải pháp cho vấn đề hiện nay là chia nhỏ các hãng khổng lồ này, tương tự như trường hợp Mỹ đã làm với Standard Oil (một công ty dầu mỏ lớn của Mỹ) và AT&T (một công ty viễn thông đa quốc gia có trụ sở tại Texas, Mỹ). Chính sách này có thể gây tổn thương đối với các hãng công nghệ lớn nhưng lại tạo điều kiện cho các hãng mới ra đời và phát triển. Tuy nhiên, học giả Viktor cho rằng, cách làm tốt hơn là việc yêu cầu chia sẻ một phần dữ liệu mà các hãng lớn đã tích lũy được để duy trì sự tồn tại của các hãng này, đồng thời thúc đẩy tính sáng tạo, cạnh tranh và giảm thiểu tính dễ bị tổn thương trước các cú sốc bất ngờ.

Quy định về việc chia sẻ dữ liệu đã được áp dụng tại một số quốc gia. Tại Mỹ, chính quyền liên bang đã từng yêu cầu các hãng chia sẻ dữ liệu trong các vụ sáp nhập công ty. Đức quy định các công ty bảo hiểm lớn phải chia sẻ thông tin cho các công ty bảo hiểm nhỏ. Tại EU, yêu cầu về chia

---

1. Viktor Mayer-Schonberger; Thomas Ramge: "A Big Choice for Big Tech: Share Data or Suffer the Consequences", *Foreign Affair*, 97 (5), 48 (2018).

sẻ thông tin đã được quy định trong Quy định về bảo vệ dữ liệu (*General Data Protection Regulation* - QDPR).

1.3.2. Tác động đối với vận động chính trị - xã hội

Học giả Helen Dixon (Chuyên gia bảo vệ dữ liệu của Ailen) cho rằng, thế giới ngày nay đang được định hình bởi sự bất cân xứng về công nghệ giữa một bên là các tập đoàn và chính phủ mạnh về công nghệ với người dân ít kiến thức hơn[1]. Điều này dẫn đến việc người dùng Internet đang trở nên dễ bị tổn thương khi các thông tin cá nhân dễ dàng bị các công ty, chính phủ thu thập, lưu trữ, xử lý; từ đó, các thông tin này được sử dụng để tác động đến các lựa chọn, tâm lý của người dân (về tin tức, thông tin giải trí, mua sắm hàng hóa) thông qua các thuật toán. Các nhóm tuyên truyền, cực đoan cũng có thể lợi dụng các mạng xã hội thông qua tài trợ cho các chiến dịch quảng cáo, đưa các thông tin sai lệch trên mạng xã hội, từ đó tác động đến hiểu biết và suy nghĩ của người sử dụng. Internet được coi là nguyên nhân gây ra làn sóng Mùa xuân Arập đã lan tràn ở hầu khắp các nước Arập năm 2011.

Ở góc độ xã hội, mặc dù tính mở của Internet đã góp phần thúc đẩy sáng tạo, tinh thần doanh nghiệp, gia tăng sức mạnh cho người tiêu dùng và các tổ chức chính trị, tuy nhiên, theo học giả Karen Kornbluh (nghiên cứu viên cao cấp về chính sách số, Hội đồng đối ngoại Mỹ, cựu đại sứ

---

1. Helen Dixon: "Regulate to Liberate Can Europe Save the Internet", *Foreign Affair*, 97 (5), 28 (2018).

Mỹ tại Tổ chức Hợp tác và phát triển kinh tế - OECD), tính mở này đang ngày càng bị hạn chế[1]. Một báo cáo năm 2017 của Freedom House cho thấy tự do Internet đã giảm trên toàn cầu trong 7 năm liên tục do các quốc gia như Trung Quốc, Nga, các nước vùng vịnh triển khai các công cụ nhằm hạn chế các tiếp cận đối với thông tin và công cụ truyền thông trên mạng. Tại Philíppin, Tổng thống Duterte thậm chí còn thành lập một lực lượng nhằm định hướng tâm lý người sử dụng mạng xã hội cũng như làm giảm chỉ trích đối với cá nhân tổng thống. Sau sự kiện đảo chính bất thành, Thổ Nhĩ Kỳ đã yêu cầu Facebook loại bỏ các thông tin liên quan, Wikipedia phải dừng hoạt động do không chỉnh sửa cũng như gỡ bỏ thông tin.

Nhà nghiên cứu Karen cũng cho rằng, Internet còn được sử dụng để làm suy yếu các nền dân chủ. Ví dụ gần đây nhất là việc Nga bị cáo buộc can thiệp vào cuộc bầu cử tại Mỹ. Theo đó, Nga đã tạo tài khoản Twitter giả (TEN_GOP) nhằm đánh lừa dư luận rằng đây là tài khoản của Đảng Cộng hòa tại bang Tennnessee và đăng tải các nội dung ủng hộ ứng cử viên Donald Trump[2]; đồng thời lập trang Facebook *Blacktivist* nhằm tác động đến tâm lý của nhóm

---

1. Karen Kornbluh: "The Internet's Lost Promise: And How American Can Restore It", *Foreign Affair*, 97 (5), 33 (2018).

2. Luke O'Brien: "Twitter ignored this Russia - Controlled Account during the election. Team Trump did not", https://www.huffpost.com/entry/twitter-ignored-this-russia-controlled-account-during-the-election_n_59f9bdcbe4b046017fb010b0.

cử tri gốc Phi, từ đó làm giảm sự ủng hộ cho ứng cử viên Hilary Clinton[1]. Hai tài khoản mạng xã hội này đã tiến hành các hoạt động thu thập thông tin của người sử dụng, phân tích các thông tin này qua các thuật toán để phân loại cử tri, từ đó sắp đặt sự hiển thị các thông tin, quảng cáo, tài khoản theo ý muốn nhằm tác động để tâm lý cử tri.

Thực tế là người dân và cử tri ngày càng dễ bị tác động và dẫn dắt bởi các thông tin đã được lọc và định hướng bởi các nhà cung cấp dịch vụ mạng. Thông tin và dữ liệu cá nhân của người dân đang được thu thập bởi các công ty công nghệ lớn nhằm chiếm lĩnh và thu lợi nhuận khổng lồ. Điều này cũng đặt ra nguy cơ lớn về việc các thông tin này được sử dụng vào các mục đích chính trị - xã hội khác mà người dân không hề hay biết. Các thể chế độc tài thường tận dụng vai trò của công nghệ để kiểm duyệt thông tin và đàm áp các lực lượng đối lập. Học giả Karen kết luận rằng, giới hoạch định chính sách đã không theo và quản lý kịp các tác động của sự phát triển trong không gian mạng.

2. Thực trạng an ninh mạng trong quan hệ quốc tế hiện nay

2.1. Cơ hội

Vấn đề an ninh mạng đem lại cơ hội hợp tác giữa các chủ thể chính trong quan hệ quốc tế cũng như cơ hội trong

---

1. Donie O' Sullivan và Dylan Byes: "Fake black activist accounts linked to Russian government", https://money.cnn.com/2017/09/28/media/bkacktivist_russia_facebook_twitter/index.html.

việc xây dựng hệ thống pháp luật, quy định, tập quán quốc tế trong lĩnh vực an ninh mạng.

Do không gian mạng bao trùm trên phạm vi toàn cầu, cộng đồng quốc tế cần có tầm nhìn chung để ứng phó với các vấn đề trên không gian mạng. Thông qua thúc đẩy hợp tác, các quốc gia có thể giải quyết vấn đề liên quan đến tính xuyên biên giới của tội phạm mạng. Điều này đóng vai trò như chất xúc tác thúc đẩy hợp tác giữa các quốc gia. Tuy nhiên, điều quan trọng là cộng đồng quốc tế phải thiết lập một cơ chế ứng phó toàn diện với các thách thức an ninh mạng bằng việc hoàn thiện hệ thống pháp lý, đặc biệt là các hiệp định quốc tế.

Thực trạng và nhu cầu xây dựng hệ thống pháp luật quốc tế

Sự phát triển nhanh chóng của công nghệ thông tin và các dịch vụ mạng đặt ra vấn đề về an ninh mạng cho các chính phủ. Tội phạm trên không gian mạng tạo ra thách thức ngày càng trực tiếp đối với an ninh của cơ sở hạ tầng mạng và cơ sở hạ tầng công nghệ thông tin.

Hầu hết các quốc gia đều nhận thức được tính dễ tổn thương của công nghệ thông tin, việc lạm dụng các dữ liệu công cộng từ Internet và tầm quan trọng trong việc bảo vệ các cơ sở hạ tầng quan trọng. Các quốc gia đã và đang áp dụng các chiến lược và chính sách của riêng mình để đối phó với nguy cơ tấn công mạng có tác động lớn. Các nhà hoạch định chính sách ở các quốc gia đang xem xét các

chiến lược ngăn chặn để hỗ trợ việc bảo đảm an ninh mạng. Nhưng rất khó để chống lại mối đe dọa này bằng các chiến lược và chính sách quốc gia trong bối cảnh không gian mạng trải rộng khắp toàn cầu và các cuộc tấn công mạng có thể được thực hiện từ bất kỳ nơi nào trên thế giới.

Không chỉ hợp tác để bảo đảm vấn đề an ninh, an toàn mạng, các quốc gia cũng cần hợp tác để ứng phó với vấn đề tội phạm mạng vì hiện nay, tội phạm mạng không phân biệt ranh giới, thẩm quyền hay quốc gia. Sự phát triển của Internet cũng kéo theo sự hợp tác chưa từng có giữa các nhóm tội phạm.

Trong số các thách thức từ tội phạm mạng, khủng bố hoặc cyber warfare (chiến tranh mạng) đang gia tăng nhanh chóng cùng với sự phát triển của công nghệ thông tin và truyền thông. Trong khi đó, luật pháp quốc tế trong lĩnh vực tội phạm mạng đang chậm thích ứng. Công ước quốc tế về tội phạm mạng năm 2001 của Hội đồng châu Âu (Công ước Budapest) là công ước quốc tế đầu tiên về giải quyết vấn đề tội phạm trên Internet và máy tính, đặc biệt là các vi phạm bản quyền, gian lận liên quan đến máy tính, vi phạm an ninh mạng thông qua các biện pháp thúc đẩy các sáng kiến lập pháp ở cấp quốc gia và tăng cường hợp tác quốc tế.

Sự thiếu hiệu quả của hệ thống luật pháp quốc tế hiện có liên quan đến không gian mạng nằm ở việc hầu như chưa có các điều khoản thi hành. Việc trừng phạt tội phạm

mạng bên ngoài khuôn khổ Luật nhân quyền quốc tế (IHRL) hoặc Luật nhân đạo quốc tế (IHL) hầu như chưa có. Mặt khác, các vấn đề liên quan đến không gian mạng là đa chiều và quá phức tạp, khó xác định việc áp dụng luật nào. Điều này tạo ra các quan điểm khác nhau trong việc coi tội phạm mạng là một loại tội phạm đơn thuần hay tội phạm liên quan đến an ninh quốc gia. Cho đến khi có một văn kiện khả thi về mặt chính trị thì điều quan trọng là phải xem xét các hệ thống luật pháp hiện tại có thể thực hiện ở mức nào để ứng phó với những thách thức trong an ninh mạng như tội phạm mạng, khủng bố không gian mạng hoặc chiến tranh mạng,... đang gia tăng. Không chỉ các quốc gia cần hợp tác với nhau mà tất cả các chủ thể liên quan như doanh nghiệp, cá nhân, tổ chức cũng cần hỗ trợ lẫn nhau. Một trong những nhu cầu cấp bách nhất của cộng đồng quốc tế là thiết lập một cơ chế bao trùm để điều chỉnh không gian mạng. Cách tốt nhất để bảo đảm an ninh trên mạng quốc tế là tạo ra một khung pháp lý phù hợp với mọi quốc gia.

Với tư cách là tổ chức quốc tế bao trùm nhất, có phạm vi hoạt động rộng nhất, Liên hợp quốc có thể đứng ra chủ trì việc xem xét và thảo luận về một khuôn khổ pháp lý đa phương trong việc ứng phó với các vấn đề trong không gian mạng. Các tổ chức quốc tế khác, đặc biệt là NATO, Liên minh châu Âu, Hội đồng châu Âu, Nhóm 8 quốc gia có nền công nghiệp hàng đầu thế giới (G-8), Tổ chức Hợp tác và

phát triển kinh tế (OECD) có thể đóng vai trò đi đầu trong việc thúc đẩy hợp tác quốc tế trong lĩnh vực an ninh mạng.

Thực trạng và nhu cầu hình thành tập quán quốc tế về vấn đề an ninh mạng

Một vài quốc gia và các chủ thể phi nhà nước khác cho rằng, do tính chất không xác định của Internet nên rất khó để có thể tìm ra thủ phạm tiến hành các cuộc tấn công mạng. Trong khi đó, Mỹ và Anh đã đạt được kết quả quan trọng trong việc phá hủy các mạng lưới tấn công mạng giấu mặt. Điều này cho thấy, mặc dù việc hợp tác và định danh thủ phạm các cuộc tấn công mạng là khó khăn và phức tạp nhưng không phải là không thể làm được.

Việc hợp tác giữa các chủ thể trong không gian mạng, bao gồm cả chủ thể nhà nước và các chủ thể phi nhà nước rất khó có thể làm được nếu như thiếu các quy chuẩn và quy định.

Theo trang mạng Carnegie.ru, ý tưởng về việc đưa ra một bộ quy tắc hành xử trên không gian mạng lần đầu tiên đã được Nga đề nghị từ mùa thu năm 2011. Nga đã đề xuất Liên hợp quốc xây dựng công ước về bảo đảm an ninh thông tin quốc tế, trong đó đề cập các tiêu chuẩn điều phối hoạt động trên Internet có tính đến những thách thức của chủ nghĩa khủng bố, hình sự, chính trị và quân sự[1]. Ngoài việc

---

1. Xem thêm tại https://tuoitre.vn/nga-my-va-cuoc-chien-tranh-lanh-tren-khong-gian-mang-1216756.htm.

cấm sử dụng mạng để can thiệp vào công việc nội bộ các nước và lật đổ các chế độ, Nga đề nghị trao cho các chính phủ quyền tự do rộng rãi để hành động bên trong "phân khúc quốc gia" của Internet. Văn kiện này cũng đề nghị cấm quân sự hóa không gian điều khiển và không được phép "sử dụng công nghệ thông tin vào những hành động thù địch".

Tuy nhiên, sáng kiến này của Nga đã không được thúc đẩy. Mỹ và các nước đồng minh cho rằng, đề nghị cấm các nước phát triển công nghệ tấn công không gian điều khiển là "thiếu thực tiễn" vì những thỏa thuận truyền thống (như Hiệp ước không phổ biến vũ khí hạt nhân) sẽ khó có hiệu lực trên không gian mạng. Còn yêu cầu không can thiệp vào công việc nội bộ các nước trên Internet cũng như trao cho các chính phủ có nhiều quyền hạn hơn để đối phó thì bị cho là "nhằm áp đặt kiểm duyệt và kiểm soát nhà nước trên mạng".

Việc xây dựng các quy chuẩn cho vấn đề an ninh mạng đã bắt đầu bằng các diễn đàn trong khuôn khổ Liên hợp quốc và đơn vị trực thuộc Liên hợp quốc là Liên minh viễn thông quốc tế (*International Telecommunications Union* - ITU). Song song với các diễn đàn này, Mỹ đang cố gắng dẫn dắt các sáng kiến an ninh mạng toàn cầu trong các khuôn khổ khác. Lý do khiến Mỹ đi đầu trong nỗ lực thiết lập các quy chuẩn trong không gian mạng là vì theo Mỹ, các công cụ mềm là lựa chọn phù hợp nhất trong lĩnh vực

không gian mạng. *Thứ nhất*, Mỹ và các quốc gia đều phải đối mặt các nguy cơ bị tấn công mạng, các cuộc tấn công này khó có thể giải quyết bằng các công cụ quân sự thông thường. *Thứ hai*, rất khó để bảo đảm rằng hệ thống thông tin phức tạp được bảo vệ đầy đủ do các hạn chế hiện nay về mặt kỹ thuật. *Thứ ba*, cách tiếp cận, ngăn chặn không dễ thực hiện khi việc xác định kẻ chủ mưu và thời điểm tấn công mạng là vô cùng khó. *Thứ tư*, các hiệp ước quốc tế rất khó thực hiện do khó xác định việc tuân thủ chúng trên không gian mạng.

Hiệp ước song phương Nga - Mỹ năm 2013 và thỏa thuận trong khuôn khổ Nhóm làm việc của Liên hợp quốc về lĩnh vực công nghệ thông tin năm 2015 đều yêu cầu thiết lập các quy tắc có thể áp dụng cho các nước. Tuy nhiên, các quy chuẩn đều ở dạng tuyên bố, mang tính tự nguyện và thiếu cơ chế thực hiện. Các thỏa thuận quốc tế về các nguyên tắc chung như hiện nay là chưa đủ. Do đó, một thỏa thuận mang tính chính thức và ràng buộc về mặt pháp lý sẽ có tính hiệu quả hơn là luật mềm (*soft law*) và tập quán.

Nỗ lực để đạt được một thỏa thuận quốc tế về một bộ quy tắc ứng xử trên không gian mạng tiếp tục được đưa ra vào năm 2015 khi Nhóm chuyên gia chính phủ của Liên hợp quốc về an ninh mạng (UN GGE) đã đi đến thỏa thuận với 4 nguyên tắc về việc sử dụng hòa bình không gian mạng do Mỹ đưa ra bao gồm: các quốc gia không được can thiệp vào các cơ sở hạ tầng trọng yếu của nhau, không được tấn

công vào các biệt đội phản ứng an ninh mạng khẩn cấp của nhau, hỗ trợ lẫn nhau trong điều tra các vụ tấn công mạng, chịu trách nhiệm cho các hành động tấn công xuất phát trong phạm vi lãnh thổ của mình. Song, thỏa thuận này vẫn không có giá trị pháp lý ràng buộc.

Nga và Trung Quốc lại có cách tiếp cận khác đối với việc xây dựng quy chuẩn chung[1]. Trung Quốc không muốn áp dụng luật quốc tế vào không gian mạng với việc nước này liên tục nhấn mạnh vai trò của Hiến chương Liên hợp quốc và tầm quan trọng của chủ quyền quốc gia mà không nhắc đến các luật pháp quốc tế khác. Trong cuộc họp của Nhóm chuyên gia chính phủ của Liên hợp quốc về an ninh mạng (UN GGE) năm 2015, Trung Quốc đã đề xuất loại bỏ tất cả việc dẫn chiếu đến luật quốc tế trong báo cáo làm việc của nhóm. Tương tự, sau vụ tấn công tin tặc vào Ủy ban Đảng Dân chủ toàn quốc (DNC) của Mỹ được cho là có liên quan đến Chính phủ Nga năm 2016, Nga phủ nhận và không ủng hộ các cuộc thảo luận liên quan đến các biện pháp đáp trả từ Mỹ, trong đó bao gồm các hành động của Mỹ đối với các nhóm tấn công mạng.

Có thể nói, do tính phức tạp về mặt kỹ thuật và tính chất bao trùm toàn cầu của vấn đề không gian mạng, các quốc gia đều nhận thấy nhu cầu hợp tác trong việc cùng

---

1. https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

nhau ứng phó với các thách thức chung ở lĩnh vực không gian mạng. Các quốc gia không chỉ hợp tác song phương mà còn tham gia hợp tác đa phương trong các khuôn khổ hợp tác khu vực như ASEAN, NATO,... hay ở cấp toàn cầu như Liên hợp quốc. Tuy nhiên, việc đạt được thỏa thuận về các quy chuẩn chung trong lĩnh vực không gian mạng còn gặp trở ngại do quan điểm khác biệt cũng như những diễn biến phức tạp trong lĩnh vực an ninh mạng trong quan hệ song phương/đa phương giữa các nước lớn.

2.2. Thách thức

2.2.1. Thiếu cơ sở pháp lý, cơ chế hợp tác

a) Hạn chế trong việc thực thi Công ước quốc tế về vấn đề an ninh mạng

Các quốc gia vẫn chưa thống nhất các bước cần thực hiện để áp dụng luật pháp quốc tế trên không gian mạng. Nguyên nhân chủ yếu là do các nước có cách tiếp cận khác nhau đối với vấn đề an ninh mạng, thực tiễn chưa đủ đồng bộ để có các quy phạm chung và việc xây dựng một công ước quốc tế về an ninh mạng sẽ tốn thời gian và nguồn lực, sẽ bị lạc hậu so với những phát triển của khoa học công nghệ. Hiện nay, Công ước Budapest năm 2001 của Liên minh châu Âu về tội phạm mạng được coi là công ước quốc tế duy nhất có hiệu quả nhằm thiết lập khuôn khổ pháp lý chung cho công tác phòng, chống tội phạm mạng thông qua việc các quốc gia nội luật hóa những trình tự, thủ tục

tịch thu, khám xét, khai thác dữ liệu máy tính,...; hợp tác thông qua tương trợ tư pháp (dẫn độ, hỗ trợ điều tra, cung cấp dữ liệu thông tin). Công ước được đàm phán, xây dựng bởi các quốc gia châu Âu và được mở cho các quốc gia ngoài khu vực cùng tham gia. Đến nay đã có 54 quốc gia thành viên, trong đó có 22 quốc gia ngoài khu vực (các nước châu Á có Nhật Bản và Philíppin) tham gia Công ước. Đây là thành công bước đầu của cộng đồng quốc tế nhằm giải quyết các vấn đề liên quan đến tội phạm mạng nói riêng và an ninh mạng nói chung. Hiện nay, nhiều nước kêu gọi sự gia nhập rộng rãi hơn vào cơ chế của công ước, tuy nhiên vẫn còn nhiều ý kiến trái chiều - một số nước bày tỏ quan ngại do không được tham gia vào quá trình đàm phán công ước nên những lợi ích của quốc gia mình không được phản ánh và cho rằng cần phải xây dựng một công ước mới mang tính phổ cập hơn.

Trong khi đó các quốc gia thành viên Công ước Budapest lại cho rằng, không cần thiết phải xây dựng một công ước mới về tội phạm mạng. Công ước Budapest được đàm phán và tham gia bởi nhiều quốc gia trên thế giới, các quy định pháp lý chặt chẽ, có tính ứng dụng và linh hoạt cao, cơ chế hợp tác hiệu quả, cơ chế thành viên rộng mở cho mọi quốc gia. Hơn nữa, việc đàm phán, ký kết một công ước quốc tế mới về tội phạm mạng sẽ tốn rất nhiều thời gian và nguồn lực hiện tại. Trong bối cảnh Liên hợp quốc đang cạn kiệt nguồn lực, các nước nên tập trung

nguồn lực để đối phó hiệu quả với tội phạm mạng thông qua thúc đẩy hợp tác quốc tế, hỗ trợ kỹ thuật,...

Mặc dù Nga, Trung Quốc, Braxin cho rằng Công ước Budapest có những giá trị nhất định nhưng không thể được coi là công ước toàn cầu về tội phạm mạng. Trung Quốc lập luận cụ thể như sau: (i) Công ước Budapest xuất phát điểm là điều ước quốc tế khu vực, dựa trên những đặc thù của khu vực, tập trung xử lý những vấn đề của khu vực, không phản ánh điều kiện và nhu cầu của tất cả các quốc gia và khu vực khác trên thế giới; (ii) Trung Quốc và nhiều nước không tham gia quá trình đàm phán công ước nên các quan điểm và lợi ích quốc gia không được thể hiện; (iii) Quy trình gia nhập rất phức tạp, quốc gia muốn gia nhập phải được mời và chấp thuận bởi tất cả quốc gia thành viên; (iv) Điều 32b của Công ước về thu thập chứng cứ xuyên biên giới (cho phép một quốc gia thành viên truy cập dữ liệu lưu trữ tại quốc gia khác thành viên khác) vi phạm chủ quyền quốc gia, nhân quyền và pháp luật quốc gia nơi có dữ liệu.

b) Thiếu đồng thuận trong việc áp dụng luật pháp quốc tế

Các tổ chức quốc tế như Liên hợp quốc và NATO đã thông qua những văn kiện khuyến nghị về những nguyên tắc của luật pháp quốc tế áp dụng trong không gian mạng như Nghị quyết số 56/121 của Đại hội đồng Liên hợp quốc về đấu tranh chống hành vi sử dụng trái phép công nghệ thông tin (năm 2002); Nghị quyết số 58/199 của Đại hội

đồng Liên hợp quốc về việc xây dựng văn hóa toàn cầu về an ninh mạng và bảo vệ cơ sở hạ tầng dữ liệu thiết yếu (năm 2004); Báo cáo số A/65/201 (năm 2010) và A/68/98 (năm 2013) của UN GGE; Hướng dẫn Tallin 2.0 của NATO (năm 2017)[1]. Những văn kiện này kêu gọi các quốc gia trong quá trình xây dựng pháp luật quốc gia về vấn đề an ninh mạng cần phải bảo đảm tôn trọng quyền con người, quyền công dân, hợp tác quốc tế trong việc trao đổi thông tin, cũng như truy cứu, xét xử những hành vi vi phạm an ninh mạng, áp dụng các nguyên tắc cơ bản của luật pháp quốc tế đối với không gian mạng.

Nhóm chuyên gia Chính phủ của Liên hợp quốc được thành lập nhằm thảo luận và nghiên cứu về khả năng áp dụng luật pháp quốc tế trong môi trường mạng. Tuy nhóm hoạt động độc lập nhưng các chuyên gia có sự hậu thuẫn lớn từ chính phủ các nước. Thảo luận của nhóm diễn ra trong suốt 8 năm và qua hai báo cáo nêu trên, nhóm đã khẳng định, luật pháp quốc tế được áp dụng trong môi trường mạng. Tương tự như vậy, Hướng dẫn Tallinn của NATO cũng chỉ ra rằng, các nguyên tắc của luật pháp quốc tế về xung đột vũ trang cũng được áp dụng trên môi trường mạng.

---

1. Hướng dẫn Tallinn 2.0 đưa ra cách thức áp dụng luật quốc tế cho các hoạt động mạng trong thời bình và trong các cuộc xung đột chiến tranh, cung cấp những phân tích pháp lý về những sự cố mạng phổ biến mà các quốc gia phải đối mặt hằng ngày và những sự cố này rơi vào ngưỡng dưới của sử dụng vũ lực hoặc xung đột vũ trang (TG).

Tuy nhiên, những tài liệu nêu trên mới chỉ nêu được những nguyên tắc chung, việc áp dụng cụ thể những nguyên tắc đó còn nhiều điểm chưa rõ ràng. Chẳng hạn như, trong xung đột vũ trang cần bảo đảm nguyên tắc về tính tương xứng (*propotionality*) - quy mô, hình thức tấn công phải tương xứng với quy mô của mối đe dọa - để đạt được ưu thế về quân sự; trên môi trường mạng, việc này sẽ rất khó xác định.

c) Bất đồng về quan điểm, cách thức hợp tác

Hiện nay, các nước có nhiều quan điểm khác nhau về vấn đề chủ quyền quốc gia trên không gian mạng. Nhìn chung, các nước cho rằng, các nguyên tắc về chủ quyền lãnh thổ quốc gia là cơ sở pháp lý hiệu quả để xây dựng các quy phạm về an ninh mạng; theo đó quốc gia hoàn toàn có quyền quản lý và áp dụng luật pháp quốc gia về không gian mạng trong giới hạn lãnh thổ quốc gia mình. Tương tự như trong các lĩnh vực khác, chủ quyền quốc gia trên không gian mạng cần được thực thi một cách phù hợp với luật pháp quốc tế. Điểm khác biệt giữa các quốc gia nằm ở cách thức để bảo đảm chủ quyền đối với không gian mạng: một số nước cho rằng, để có thể quản lý một cách hiệu quả không gian mạng trong phạm vi lãnh thổ quốc gia, các công ty, tập đoàn cung cấp dịch vụ trên không gian mạng cần phải đặt hệ thống cơ sở hạ tầng, máy chủ trong quốc gia mình để chính phủ có thể thực thi quyền quản lý; một số nước khác lại cho rằng, yêu cầu như vậy sẽ không hiệu quả

về mặt kinh tế và làm mất đi tính tiện ích toàn cầu của các dịch vụ viễn thông, công nghệ thông tin.

Về vấn đề luật pháp quốc tế áp dụng cho không gian mạng, có ý kiến đề xuất về khả năng áp dụng những nguyên tắc hiện có của luật pháp quốc tế đối với môi trường mạng. Về vấn đề chiến tranh mạng, theo Hướng dẫn Tallinn 2.0 và các Công ước Geneva (năm 1949), Luật nhân đạo quốc tế hiện hành đã quy định đầy đủ về việc bảo vệ thường dân và cơ sở hạ tầng dân sự trong tình trạng chiến tranh; với chiến tranh mạng, việc bảo vệ các đối tượng trên càng trở nên cấp thiết do các cuộc tấn công mạng phần lớn đều nhằm vào vào các hệ thống dân sự như ngân hàng, bệnh viện,... Hiện còn nhiều cách hiểu khác nhau về khái niệm chiến tranh mạng nhưng nhìn chung các nước đều thừa nhận các cuộc tấn công trên không gian mạng là những hành vi của các nhóm "hacker" xâm nhập mạng lưới mạng nhằm gây hại các dữ liệu có giá trị, làm suy yếu hệ thống thông tin truyền thông, các dịch vụ cơ sở hạ tầng như vận chuyển và các dịch vụ y tế hoặc làm gián đoạn thương mại.

Một vấn đề khác cũng gây khó khăn cho việc bảo đảm an ninh mạng trên thực tế là việc quy kết trách nhiệm hành vi thực hiện các cuộc tấn công mạng. Về vấn đề này, có ý kiến đề xuất áp dụng các nguyên tắc về trách nhiệm quốc gia đối với các hành vi sai phạm quốc tế, trong đó có các quy định về những hành vi của cá nhân, cơ quan, tổ chức có thể được quy kết cho quốc gia, cũng như các quy định về

các biện pháp trả đũa (*countermeasures*) mà quốc gia là nạn nhân của sự vi phạm có thể được thực hiện.

2.2.2. Năng lực các quốc gia

Nỗ lực của các quốc gia trong việc ứng phó, phòng, chống các cuộc tấn công mạng luôn gặp khó khăn do hạn chế về năng lực, cơ sở hạ tầng công nghệ thông tin; quá trình ban hành các văn bản pháp luật quy định về biện pháp, chế tài thường mất nhiều thời gian và một khi những văn bản đó được ban hành thì lại trở nên lạc hậu so với những thủ đoạn mới của tin tặc; thiếu chặt chẽ trong sự điều phối giữa các cơ quan chức năng có liên quan (công an, quốc phòng, thông tin - truyền thông). Một thực tế không thể phủ nhận rằng, một trong những thách thức đối với việc bảo đảm an ninh mạng trên toàn thế giới là sự không đồng đều về năng lực giữa các quốc gia phát triển và các quốc gia đang phát triển, thậm chí là giữa các khu vực khác nhau trong cùng một quốc gia (như ở Trung Quốc hay Ấn Độ).

*

* *

Có thể nói, vấn đề an ninh mạng đang nổi lên và trở thành mối quan tâm hàng đầu của các quốc gia, tổ chức trên thế giới. Sự phát triển trong không gian mạng đang được thúc đẩy bởi Cuộc Cách mạng công nghiệp lần thứ tư với tác động nhiều chiều, ngày càng sâu rộng trên mọi mặt của đời sống kinh tế - xã hội.

An ninh mạng có thể được hiểu là các hoạt động hoặc quá trình, khả năng, hay trạng thái mà theo đó thông tin, hệ thống thông tin liên lạc và thông tin chứa trong đó được bảo vệ khỏi và/hoặc bảo vệ chống lại thiệt hại, sự sử dụng trái phép hoặc sửa đổi, khai thác. Như vậy, chức năng cơ bản của an ninh mạng là bảo vệ thông tin và hệ thống từ các mối đe dọa mạng dưới nhiều hình thức, từ tấn công chương trình, tấn công từ chối dịch vụ, cho đến những truy cập trái phép, sử dụng sai mục đích, sửa đổi, hủy hoại hoặc tiết lộ không đúng thông tin nhằm bảo đảm mọi thông tin, dữ liệu trong tình trạng an toàn nhất.

Vấn đề an ninh mạng đem lại các cơ hội hợp tác giữa các chủ thể chính trong quan hệ quốc tế cũng như cơ hội trong việc xây dựng hệ thống pháp luật, quy định, tập quán quốc tế trong lĩnh vực an ninh mạng. Tuy nhiên, bên cạnh đó, trong lĩnh vực an ninh mạng, các quốc gia cũng đang phải đối mặt với một số thách thức như: (i) thiếu cơ sở pháp lý, cơ chế hợp tác; (ii) thiếu đồng thuận về áp dụng luật pháp quốc tế; (iii) bất đồng về quan điểm, cách thức hợp tác; và (iv) năng lực của các quốc gia còn khác nhau trong lĩnh vực bảo đảm an ninh mạng.

Chương 2

CHÍNH SÁCH AN NINH MẠNG VÀ TÌNH HÌNH HỢP TÁC VỀ AN NINH MẠNG CỦA MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI

I. CHÍNH SÁCH AN NINH MẠNG CỦA MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI

1. Mỹ

Lịch sử chính sách an ninh mạng của Mỹ

Chính sách thông tin đã trở thành một yếu tố cơ bản trong chính sách đối nội của Mỹ kể từ thời của cựu Tổng thống Bill Clinton. Tại thời điểm đó, Nhà Trắng cho rằng sự đi đầu của Mỹ trong lĩnh vực thông tin sẽ đạt được thông qua việc phát triển công nghệ thông tin và tốc độ tăng trưởng kinh tế nhanh chóng của nước này. Chính quyền Clinton đã tìm cách tạo ra môi trường thuận lợi nhất cho sự phát triển của công nghệ thông tin thương mại để kích thích nền kinh tế. Sự phát triển tích cực của công nghệ thông tin ở Mỹ dẫn đến lượng truy cập các thông tin từ cộng đồng doanh nghiệp và công chúng lớn chưa từng có.

Chính phủ đã cung cấp các ưu đãi về thuế, nhờ đó việc sử dụng máy tính và Internet ngày càng phổ biến trên cả nước. Công nghệ thông tin đã trở thành yếu tố kích thích và dẫn dắt sự tăng trưởng kinh tế ở Mỹ vào thập niên 1990. Để tăng doanh thu từ sản xuất và bán công nghệ thông tin, cải cách hệ thống kiểm soát xuất khẩu trong lĩnh vực công nghệ cao được áp dụng. Các máy tính, phần mềm và cấu trúc Internet của Mỹ được áp đặt như một tiêu chuẩn cho người dùng không gian mạng toàn cầu.

Đến thời Tổng thống George W. Bush, chính sách an ninh mạng đã được thúc đẩy bởi các mối đe dọa an ninh sau cuộc tấn công khủng bố ngày 11/9/2001. Chính quyền Bush đã cố gắng thiết lập sự kiểm soát thông tin không chỉ ở cấp quốc gia mà còn trên toàn cầu. Điều này đã góp phần hình thành các quyết định về chính sách đối ngoại của Mỹ về hợp tác quốc tế trong lĩnh vực phát triển công nghệ thông tin và bảo đảm an ninh mạng.

Chính sách của Mỹ trong lĩnh vực an ninh mạng nhằm giữ cân bằng giữa hỗ trợ doanh nghiệp và thực hiện các bước cần thiết để bảo đảm an ninh mạng. Qua các thử nghiệm chính sách, giới chính trị Mỹ kết luận rằng, việc bảo đảm an ninh mạng đòi hỏi sự hợp tác chặt chẽ giữa các cơ quan nhà nước, lợi ích doanh nghiệp, xã hội dân sự và cộng đồng quốc tế.

Đến lượt mình, Chính quyền Barack Obama xác định ưu tiên trong lĩnh vực an ninh thông tin thông qua Chiến lược

quốc tế về không gian mạng. Chiến lược này bao gồm hai tài liệu học thuyết: (i) Thịnh vượng, an ninh và sự cởi mở trong thế giới mạng và (ii) Chiến lược của Bộ Quốc phòng về hoạt động trong không gian mạng. Các văn bản này thể hiện quan điểm của Chính phủ Mỹ về an ninh thông tin, sự phát triển chiến lược của không gian mạng toàn cầu và vai trò của quân đội trong việc bảo đảm an ninh mạng.

Trong các tài liệu chính sách này, Mỹ xác định sẵn sàng sử dụng bất kỳ phương tiện cần thiết nào để ứng phó với các cuộc tấn công không gian mạng. Do đó, các biện pháp ngoại giao, kinh tế hoặc quân sự đều được cân nhắc. Cơ sở của quan điểm là việc áp dụng tất cả các biện pháp có thể để hạn chế các thách thức an ninh mạng. Việc áp dụng trên thực tế chỉ có thể được thực hiện nếu Mỹ sở hữu các loại vũ khí tấn công trên không gian mạng (*offensive cyberweapons*). Tuy nhiên, thông tin về vũ khí tấn công trên không gian mạng hiện vẫn được coi là thông tin mật/hạn chế và được coi là một phần của chiến lược quân sự về không gian mạng

Trong khi đó, một số nguồn thông tin cho thấy cộng đồng tình báo Mỹ xem xét các mối đe dọa an ninh mạng một cách rất nghiêm túc. Năm 2009, Giám đốc Tình báo quốc gia Mỹ, ông Dennis Blair đặc biệt nhấn mạnh mối đe dọa của các cuộc tấn công khủng bố đối với khu vực tài chính của nền kinh tế Mỹ. Ngoài ra, báo cáo tình báo về khả năng kỹ thuật của Nga và Trung Quốc nhằm phá hoại cơ sở hạ tầng thông tin của Mỹ và thu thập thông tin tình

báo lần đầu tiên xuất hiện trong buổi điều trần tại Quốc hội năm 2009. Ông Blair tuyên bố rằng, cần có một sự hợp tác quốc tế để ứng phó với mối đe dọa này. Năm 2012, Giám đốc Tình báo quốc gia, ông James Clapper đã gọi mối đe dọa an ninh mạng là quan tâm chiến lược mới đối với giới chính trị Mỹ. Những ưu tiên trong chính sách đối ngoại của Mỹ được lồng ghép vào vấn đề an ninh mạng do nhu cầu cấp thiết trong việc bảo vệ cơ sở hạ tầng mạng. Mặc dù Mỹ khá chủ động trong hợp tác quốc tế về vấn đề an ninh mạng nhưng lại không coi Nga là đồng minh chiến lược trong lĩnh vực này. Nga và Trung Quốc được coi là những nguồn tấn công chính đối với hệ thống máy tính và ăn cắp thông tin sở hữu trí tuệ Mỹ.

Chính sách an ninh mạng của Mỹ hiện nay

Mục tiêu chính sách của Mỹ trong vấn đề an ninh mạng là thúc đẩy một không gian mạng mở, đáng tin cậy và an toàn nhằm tăng cường tính hiệu quả, sáng tạo, giao lưu và thịnh vượng kinh tế đồng thời tôn trọng quyền riêng tư và chống lại sự gián đoạn các dịch vụ mạng, gian lận và trộm cắp trên không gian mạng. Bên cạnh đó, Mỹ cũng đẩy mạnh phát triển nguồn nhân lực trong lĩnh vực không gian mạng[1].

---

1. Xem thêm "Sắc lệnh mới về An ninh mạng của Mỹ ngày 11/5/2017", http://www.whitehouse.gov/president-action/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

Bộ An ninh nội địa Mỹ, một trong số các cơ quan phụ trách vấn đề an ninh mạng, cho rằng không gian mạng và các cơ sở hạ tầng mạng dễ bị tổn hại trước các nguy cơ từ chính không gian mạng hay cơ sở hạ tầng mạng. Các chủ thể khác nhau, trong đó có chủ thể nhà nước, có thể sử dụng tính dễ bị tổn hại này để đánh cắp thông tin cũng như tiền bạc. Các chủ thể trong không gian mạng đang phát triển năng lực trong việc làm gián đoạn, phá hủy cũng như đe dọa các dịch vụ mạng. Các loại tội phạm truyền thống nay cũng đã xuất hiện cả trên không gian mạng, như việc sản xuất và phát tán các hình ảnh khiêu dâm trẻ vị thành niên, âm mưu lợi dụng trẻ em và các loại tội phạm khác. Các hình thức tội phạm này đều gây ra những hậu quả nghiêm trọng cho xã hội[1].

Để ứng phó với các thách thức an ninh mạng, Mỹ tiếp cận theo hai cách chính. *Thứ nhất*, cách tiếp cận đa thành phần (*multi-stakeholders*) bảo đảm việc ứng phó với các thách thức an ninh mạng phải có sự tham gia đầy đủ của các bên có liên quan, trong đó có các cơ quan nhà nước, doanh nghiệp, chuyên gia/học giả và người dân. *Thứ hai*, cách tiếp cận toàn diện (*whole of government approach*) bảo đảm tất cả các bộ, ngành cùng tham gia giải quyết các vấn đề về an ninh mạng, trong đó Bộ Ngoại giao đóng vai trò tích cực trong việc làm cầu nối với chính phủ các nước

1. Xem thêm https://www.dhs.gov/cybersecurity-overview.

và mời các chuyên gia. Bản thân các bộ, ngành đều có đơn vị hoặc đội ngũ riêng về vấn đề an ninh mạng.

Điểm mấu chốt của cách tiếp cận toàn diện là việc thiết kế một khuôn khổ rõ ràng trong việc phối hợp và phân rõ trách nhiệm của từng cơ quan nhà nước. Tại Mỹ, ba cơ quan chính chịu trách nhiệm giải quyết các vấn đề an ninh mạng là Bộ Tư pháp, Bộ An ninh nội địa và Văn phòng Tình báo quốc gia. Chức năng, nhiệm vụ của các cơ quan này trong lĩnh vực an ninh mạng được quy định tại Chỉ thị của Tổng thống số DIRECTIVE/PPD-41 ngày 26/7/2016[1]. Theo đó, Bộ Tư pháp, thông qua Cục Điều tra liên bang (FBI) và Lực lượng đặc nhiệm chung điều tra mạng quốc gia (NCIJTF) có vai trò ngăn chặn những nguy cơ an ninh mạng trước khi vụ việc xảy ra. Bộ An ninh nội địa đảm nhiệm các vấn đề về kỹ thuật khi có sự cố, đồng thời đóng vai trò phối hợp liên ngành. Văn phòng Tình báo quốc gia cung cấp thông tin về các mối đe dọa an ninh mạng. Việc phân chia như vậy sẽ giúp tránh tình trạng chồng chéo chức năng, giúp giải quyết khủng hoảng nhanh hơn, ít nhầm lẫn hơn và nâng cao nhận thức liên ngành hơn.

Hệ thống khung pháp lý của Mỹ trong lĩnh vực an ninh mạng bao gồm 54 sắc lệnh hành pháp (*executive orders*), chiến lược an ninh mạng ban hành thời Tổng thống Obama

---

1. Xem thêm https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

(năm 2011), kế hoạch phản ứng an ninh mạng (thông qua vào tháng 12/2015),... Sắc lệnh hành pháp mới nhất được Tổng thống Donald Trump ký thông qua ngày 11/5/2017[1]. Trong đó, chiến lược quốc tế về không gian mạng năm 2011 nhấn mạnh tầm quan trọng của phát triển, ngoại giao và bảo vệ trong hợp tác ứng phó với các thách thức an ninh mạng.

Ở cấp độ quốc gia, các hoạt động của Chính phủ Mỹ trong việc nâng cao năng lực ứng phó với các thách thức an ninh mạng bao gồm tiến hành các chiến dịch nâng cao nhận thức của công chức, viên chức và người dân về các vấn đề an ninh mạng, cung cấp các gói phần mềm có bản quyền giảm giá để sử dụng tại nhà nhằm tránh việc bị tấn công trên các máy tính cá nhân và do đó ảnh hưởng đến hệ thống mạng (cơ quan, công ty,...),...

Ở cấp độ tiểu bang, chính quyền từng bang cũng có bộ phận riêng phụ trách các vấn đề an ninh mạng, tuy nhiên cách tiếp cận, cơ cấu tổ chức và cách thức hoạt động ở từng bang là khác nhau và các bộ phận này không chịu trách nhiệm báo cáo lên chính quyền liên bang. Việc mà chính quyền liên bang làm là thúc đẩy chính quyền các bang hợp tác với chính quyền liên bang và hợp tác giữa các bang để cùng ứng phó với các thách thức an ninh mạng.

Các cuộc tấn công mạng diễn ra ở cả khu vực tư nhân và điều này cần đến sự vào cuộc của cả chính quyền. Đối

---

1. Xem thêm https://www.dhs.gov/cybersecurity-overview.

với lĩnh vực tài chính, vấn đề an ninh mạng đóng vai trò đặc biệt quan trọng do các giao dịch và dịch vụ tài chính hiện nay được tiến hành chủ yếu trên không gian mạng. Do đó, chính quyền Mỹ đề ra các tiêu chí mà các định chế tài chính phải đạt được trong lĩnh vực an ninh mạng. Chính quyền sẽ cấp giấy chứng nhận cho các định chế đáp ứng được các tiêu chí này. Hằng năm, chính quyền sẽ làm việc với các nhà lãnh đạo trong lĩnh vực tài chính để cập nhật thêm các tiêu chí nhằm đáp ứng tình hình thực tế.

Về hợp tác quốc tế trong lĩnh vực không gian mạng, Mỹ cho rằng trong thế giới kết nối hiện nay, nước Mỹ đang phụ thuộc rất nhiều vào sự an toàn và phát triển mang tính toàn cầu của Internet. Theo đánh giá của Chính phủ Mỹ, môi trường an ninh mạng trong khu vực hiện nay có nhiều thay đổi, các hoạt động tấn công mạng về thương mại ngày càng gia tăng; các chủ thể thực hiện các vụ tấn công này rất đa dạng, bao gồm cả chính phủ và cá nhân; hình thức tấn công phổ biến không chỉ là đánh cắp thông tin đơn thuần như trước mà còn biến đổi thông tin (*manipulation*), làm thay đổi hành vi của đối tượng trên mạng hay sử dụng thông tin để tống tiền (*ransomware*). Công cụ phổ biến để tội phạm mạng đánh cắp thông tin hiện nay là các đường dẫn gửi kèm trong thư, tin nhắn điện tử và gửi đi cho hàng loạt người dùng.

Về các đối tượng quốc gia, Mỹ tập trung vào Nga, Trung Quốc và Cộng hòa Dân chủ nhân dân Triều Tiên. Chính

phủ Mỹ cho rằng, Nga là quốc gia có khả năng thực hiện tấn công an ninh mạng cao nhất và không ngần ngại làm việc đó. Ví dụ, Nga được cho là đứng sau vụ tấn công mang vào Ucraina hồi tháng 6/2017, tung ra các "tin giả" (*fake news*) trong đợt bầu cử Mỹ, Pháp và Hà Lan,... Đối với Trung Quốc, Bộ Chỉ huy không gian mạng của Mỹ (*Cyber Command*) năm 2016 đã đưa ra báo cáo khẳng định việc Trung Quốc vẫn tiếp tục các hoạt động gián điệp mạnh mẽ nhằm vào các công ty của Mỹ. Quân đội Trung Quốc sử dụng các biện pháp ngăn chặn thông tin nhằm chống tiếp cận (*anti-access*). Tuy nhiên, Mỹ và Trung Quốc đã đạt được Biên bản ghi nhớ (MOU) về an ninh mạng trong lĩnh vực thương mại. Đối với Cộng hòa Dân chủ nhân dân Triều Tiên, đây là mối quan tâm an ninh ưu tiên của chính quyền Trump. Mặc dù Mỹ đánh giá Cộng hòa Dân chủ nhân dân Triều Tiên không có năng lực về không gian mạng cao như Nga hay Trung Quốc nhưng việc công ty Sony bị tấn công cho thấy đây là nhân tố không thể xem nhẹ. Ngoài ra, Mỹ cũng chú trọng vào các nhóm khủng bố sử dụng không gian mạng để tuyển mộ thành viên và tuyên truyền, tấn công vào các trang mạng của chính phủ.

Do đó, Mỹ phải làm việc với các đồng minh và đối tác nhằm bảo đảm mục tiêu về an ninh mạng. Theo đó, ba mục tiêu của Mỹ trong việc tham gia vào các thể chế quốc tế về an ninh mạng bao gồm (i) đạt được nhận thức chung về các vấn đề an ninh mạng (hành vi nào được coi là hợp pháp

hoặc không hợp pháp trên không gian mạng); (ii) nâng cao nhận thức cho các đối tác về an ninh mạng; và (iii) nâng cao năng lực phản ứng và bảo vệ của các đối tác trước các rủi ro an ninh mạng. Các mục tiêu này nằm trong định hướng chung của Mỹ là tăng cường quan hệ đối tác với không chỉ các đồng minh mà cả các đối tác mới. Hợp tác quốc tế của Mỹ trong bảo đảm an ninh mạng diễn ra ở cả kênh song phương và đa phương. Ở kênh song phương, Mỹ ký hiệp định về hợp tác an ninh mạng với các đối tác chính như Nga, Trung Quốc, Ôxtrâylia,... nhưng mức độ hợp tác và tính hiệu quả chưa cao. Ở kênh đa phương, Mỹ cùng các nước hợp tác trong khuôn khổ NATO, Khối Hiệp ước An ninh quân sự Ôxtrâylia - Niu Dilân - Mỹ (ANZUS),...

2. Nga

Nga coi vấn đề an ninh mạng là một ưu tiên trong chính sách an ninh quốc gia bên cạnh các lĩnh vực ưu tiên khác như quốc phòng, đối ngoại, kinh tế, truyền thông... và được đề cập trong nhiều văn kiện lớn như Chiến lược An ninh quốc gia 2009-2020, Thuyết Quốc phòng Liên bang Nga năm 2010, Chính sách Đối ngoại Liên bang Nga năm 2013, Chính sách Quốc phòng Liên bang Nga năm 2014, Chính sách An ninh quốc gia Liên bang Nga năm 2015,... cũng như các văn kiện cụ thể về vấn đề an ninh mạng như Chiến lược nhà nước Liên bang Nga trong lĩnh vực an ninh thông tin quốc tế cho giai đoạn 2009-2020, Thuyết An ninh thông

tin Liên bang Nga năm 2016[1],... Có thể thấy, khác với nhiều nước trên thế giới, Nga không coi môi trường mạng như một mặt trận riêng lẻ mà đã được lồng ghép trong các chính sách, chiến lược của nước này về lĩnh vực thông tin.

Nga bắt đầu xem xét việc xây dựng chiến lược an ninh thông tin từ đầu năm 2000 sau khi có đánh giá cho thấy sự gia tăng các nguy cơ tội phạm và khủng bố trên môi trường mạng. Đặc biệt, sau vụ khủng bố nhằm vào nước Mỹ ngày 11/9/2001, các phương thức mà các phần tử khủng bố sử dụng đã có sự thay đổi rõ rệt, buộc chính phủ Nga phải có các biện pháp an ninh mới để ứng phó. Bên cạnh đó, sự kiện Mùa xuân Arập cũng cho thấy sức mạnh của mạng xã hội khi được sử dụng nhằm tổ chức và điều phối các hoạt động chống lại chính phủ. Đặc biệt, sau sự kiện Mỹ và Ixraen tấn công các cơ sở hạt nhân của Iran trong Operation Stuxnet[2] năm 2010, Nga đã có cách nhìn hoàn toàn khác về an ninh mạng. Với Nga, nguy cơ đến từ không

---

1. "Doctrine of Information Security of the Russian Federation" thông qua ngày 5/12/2016, xem tại http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

2. Stuxnet là tên gọi của một sâu máy tính được phát hiện tháng 6/2010. Stuxnet đã tấn công một cơ sở hạt nhân của Iran gây sự cố cho hàng loạt máy ly tâm trong chương trình làm giàu Urani của nước này (*BT*).

gian mạng cũng tương tự nguy cơ tới từ phương Tây trong lĩnh vực chính trị, đặc biệt là khi không gian mạng bị sử dụng như vũ khí nhằm vào nhà nước, khủng bố mạng và tội phạm mạng. Bên cạnh đó, Nga cho rằng cũng tồn tại nguy cơ đến từ việc sử dụng mạng Internet nhằm mục đích can thiệp các vấn đề nội bộ, tuyên truyền chống phá nhà nước gây ảnh hưởng đến sự ổn định về kinh tế, chính trị, xã hội,... trong nước, tạo ra hận thù dân tộc,... Theo Nga, sự phát triển nhanh chóng của mạng xã hội và các " microblog"[1] đã góp phần lan rộng tư tưởng khủng bố trên mạng. Đồng thời, số lượng tội phạm mạng đang ngày một tăng, đặc biệt là tội phạm đánh cắp danh tính cá nhân trên mạng và truy cập trái phép vào các hệ thống thanh toán. Chính sách An ninh mạng năm 2016 của Nga là một phần trong Chiến lược Chính sách nhà nước Liên bang Nga trong lĩnh vực an ninh thông tin cho giai đoạn 2009-2020[2] được ban hành cuối năm 2015 do Hội đồng An ninh, Bộ Ngoại giao, Bộ Quốc phòng, Bộ Thông tin và Truyền thông và Bộ Tư pháp Nga xây dựng. Chiến lược trên xác định 07 trọng tâm lợi ích quốc gia, gồm: (1) đẩy mạnh và bảo vệ quyền hợp hiến và tự do cá nhân, công dân về quyền riêng tư trên mạng; (2) hỗ

---

1. Microblog là Tiểu Blog hay blog vi mô là một dạng blog có các bài đăng với nội dung thu gọn như một câu nói ngắn, hình ảnh riêng hoặc một liên kết đến video (*BT*).

2. Sắc lệnh Tổng thống Nga số 646, dựa trên Chính sách an ninh thông tin năm 2014.

trợ các thể chế dân chủ, nhà nước và cơ chế tương tác của xã hội dân sự; (3) bảo tồn giá trị văn hóa, lịch sử, tinh thần và đạo đức của dân tộc đa sắc tộc Nga; (4) bảo đảm sự vận hành bền vững và không bị gián đoạn của cơ sở hạ tầng thông tin quốc gia quan trọng trong thời bình và thời chiến chống lại hành vi xâm lược nước ngoài; (5) phát triển lĩnh vực công nghệ thông tin; (6) thúc đẩy chính sách quốc gia và quốc tế của Nga về an ninh và quốc phòng trên mạng; (7) thúc đẩy an ninh mạng quốc tế. Với Thuyết An ninh thông tin Liên bang Nga năm 2016, Chính phủ Nga đã bắt đầu có những bước đi cụ thể nhằm đấu tranh chống tội phạm mạng[1] và bảo đảm an ninh thông tin. Mục tiêu chủ

---

1. Có một số thông tin cho rằng, chính phủ Nga thờ ơ với những hoạt động tội phạm mạng nhằm vào các đối tượng nước ngoài, khiến cho công tác quốc tế nhằm trừng phạt các nghi phạm của Nga trở nên khó khăn; thậm chí còn có sự cấu kết giữa nhà nước và các tổ chức tội phạm hoạt động nhân danh nhà nước. Trong số các nhóm tội phạm trong nước, nổi bật nhất là nhóm Mạng lưới Doanh nghiệp Nga (Russian Bussiness Network - RBN) cung cấp dịch vụ và truy cập Internet cho các hoạt động tội phạm, các cá nhân tham gia nhóm này có thu nhập lên tới 100 triệu bảng Anh/năm. Công ty này không đăng ký kinh doanh, máy chủ được đăng ký với các địa chỉ ẩn danh; chủ doanh nghiệp chỉ được biết đến thông qua các biệt danh; các giao dịch điện tử không thể bị theo dõi. RBN được biết đến như một tổ chức tội phạm mạng đa ngành, chuyên đánh cắp danh tính để trục lợi. Từ RBN đã phát sinh ra các mã độc như Mpack và Storm Botnet. Một hoạt động điển hình của RBN là sử dụng các phần mềm chống virus giả mạo để xâm nhập hệ thống máy tính và đánh cắp danh tính.

đạo trong các chiến lược an ninh mạng của Nga là bảo vệ các nguồn tài nguyên mạng và hoạt động trên Internet khỏi các cuộc tấn công bởi tin tặc, khủng bố mạng và gián điệp mạng nước ngoài với trọng tâm là bảo vệ các mạng lưới công cộng và tài sản nhà nước trên mạng. Do đó, các cuộc tấn công mạng nhằm vào các trang mạng và tài nguyên mạng được xem là nhằm kiểm soát quyền lực và bị coi là hành vi phạm tội.

Nga có quan điểm khác các nước phương Tây về đối tượng và hành vi cấu thành các nguy cơ đến từ không gian mạng, về sự cân bằng giữa bảo đảm quyền tự do cá nhân và lợi ích của quốc gia trên không gian mạng. Với Nga, mối quan ngại lớn nhất đến từ nội dung đăng tải trên không gian mạng. Chủ quyền trên mạng - khả năng của Nhà nước kiểm soát không gian thông tin, là một khái niệm căn bản ở Nga. Vấn đề không can thiệp vào không gian mạng cũng là một vấn đề quan trọng khi mà Nga đang thúc đẩy xây dựng các cơ chế quốc tế mới. Nga đề cao nguyên tắc về chủ quyền lãnh thổ trên không gian mạng, trong khi theo các nước phương Tây, thông tin phải được truyền tải một cách tự do. Nga đã thiết lập các cơ chế, công cụ để thu thập chứng cứ trên mạng, nắm quyền vận hành, đóng cửa các tài nguyên mạng mà không cần phải có quyết định của tòa án. Các công ty an ninh tư nhân ở Nga hợp tác chặt chẽ với cơ quan an ninh của Nga, trong đó 30-40% hoạt động của các công ty như Group IB là do cơ quan an ninh Nga yêu cầu.

Quyền tự do ngôn luận nhìn chung được chấp nhận trên môi trường mạng ở Nga; tuy nhiên trong một số trường hợp cần thiết, cơ quan có thẩm quyền của Nga vẫn có thể đóng cửa toàn bộ các trang mạng được cho là có thông tin, nội dung không phù hợp. Nga cũng tránh sử dụng các biện pháp quá mạnh khi kiểm soát không gian mạng. Khác với các nước như Trung Quốc, Nga không chặn các mạng xã hội, nhưng đồng thời lại đầu tư vào các phần mềm theo dõi.

Về hệ thống cơ quan bảo đảm an ninh thông tin, Cơ quan An ninh liên bang Nga có vai trò đứng đầu trong việc điều phối các công tác an ninh trên mạng, trong đó có điều phối chiến dịch truyền bá thông tin. Cơ quan này cũng là cơ quan chủ quản của hệ thống các biện pháp tìm kiếm hoạt động (System of Operative - search Measures - SORM) và phụ trách theo dõi thông tin truyền thông, công nghệ thông tin và Truyền thông đại chúng kiểm soát các danh sách đen về thông tin và quản lý truyền thông. Bộ Nội vụ Nga phụ trách về tội phạm mạng. Bộ Quốc phòng phụ trách các vấn đề về an ninh quốc phòng và chiến tranh thông tin. Ngoài ra, các cơ quan bảo vệ liên bang và cơ quan tình báo nước ngoài của Nga cũng cấu thành hệ thống bảo đảm an ninh thông tin cho nước này.

Để nâng cao tính an toàn cho cơ sở hạ tầng dữ liệu thiết yếu chống lại các hoạt động tội phạm mạng và vi phạm quyền cá nhân trên mạng, Nga đã ban hành Luật Liên bang

số 187-FZ về bảo vệ quyền sở hữu trí tuệ trong mạng lưới thông tin liên lạc Liên bang Nga sẽ có hiệu lực từ ngày 01/01/2018[1]. Luật này yêu cầu các tổ chức, cá nhân của Nga có sở hữu hoặc cho thuê, thuê sử dụng các thiết bị cơ sở hạ tầng dữ liệu thiết yếu trong một trong các lĩnh vực: y tế, khoa học, giao thông, thông tin truyền thông, năng lượng, ngân hàng và thị trường tài chính, dầu khí, hạt nhân, quốc phòng, tên lửa và vũ trụ, khai thác mỏ, kim loại, và công nghiệp hóa chất phải: (1) đánh giá tầm quan trọng của cơ sở hạ tầng để xác định cơ sở hạ tầng đó có được xếp là thông tin quan trọng hay không và mức độ quan trọng; tiêu chí xếp loại bao gồm: (i) về mặt xã hội: khả năng gây hại tới đời sống của người dân hoặc gây ra sự ngừng hoặc lỗi hoạt động đối với các thiết bị cơ sở hạ tầng hỗ trợ đời sống, cơ sở hạ tầng giao thông hoặc các mạng lưới thông tin truyền thông hoặc ngừng cung cấp dịch vụ công quá thời

---

1. Federal Law No. 187-FZ of July 2, 2013, on Amendments to Certain Laws of the Russian Federation Concerning the Protection of Intellectual Rights in Information and Telecommunication Networks, xem tại http://www.wipo.int/wipolex/en/text.jsp?file_id=334516. Luật này định nghĩa "cơ sở hạ tầng dữ liệu thiết yếu" là các thiết bị và mạng lưới thông tin truyền thông sử dụng cho sự tương tác giữa các thiết bị đó; định nghĩa "tấn công mạng" là cuộc tấn công có chủ đích thông qua việc sử dụng phần mềm và/hoặc chương trình cơ sở (firmware) nhằm vào các thiết bị cơ sở hạ tầng dữ liệu thiết yếu hoặc các mạng lưới thông tin truyền thông gây vô hiệu và/hoặc tạo ra mối đe dọa đối với an ninh của dữ liệu được xử lý bởi các thiết bị thông tin.

gian cho phép; (ii) về mặt chính trị: khả năng gây hại tới lợi ích của Nga trong các vấn đề liên quan đến chính sách đối nội, đối ngoại; (iii) về mặt kinh tế: khả năng gây hại trực tiếp hoặc gián tiếp tới các nhà vận hành cơ sở hạ tầng dữ liệu thiết yếu và/hoặc ngân sách của Nga; (iv) tác động đến môi trường; (v) tác động đến quốc phòng, trật tự xã hội và luật pháp. (2) lập tức thông báo cơ quan liên bang và cơ quan liên quan về vụ việc tấn công mạng. (3) hợp tác với cơ quan liên bang trong việc phát hiện, ngăn chặn và khắc phục hậu quả từ các cuộc tấn công mạng; xác định nguyên nhân và tình huống dẫn đến các sự cố mạng.

Về quốc phòng, Thuyết An ninh thông tin Liên bang Nga đã chỉ ra những mối đe dọa tới lợi ích và an ninh quốc gia trên không gian mạng và những ưu tiên để ứng phó với những mối đe dọa đó; đặc biệt văn kiện này còn kêu gọi chính phủ cần phải xây dựng một hệ thống quản lý Internet thuộc chủ quyền của Nga. Bên cạnh những nguy cơ đến từ khủng bố, gián điệp và tội phạm mạng, văn kiện cũng cho rằng, lãnh đạo các nước đã gây ảnh hưởng về thông tin và tâm lý với các nước khác nhằm gây bất ổn tình hình chính trị của Nga. Theo văn kiện này, một yếu tố mới được bổ sung vào danh sách những nguy cơ đối với an ninh quốc phòng và kinh tế của Nga trên không gian mạng là sự phương hại tới giá trị đạo đức truyền thống - "sự gia tăng cơ hội để các nước gây ảnh hưởng tới cơ sở hạ tầng thông tin

của Nga vì mục đích quân sự"[1]. Văn kiện trên đặc biệt nhấn mạnh tới hoạt động của truyền thông đại chúng nước ngoài và tác động to lớn của các hoạt động này đối với Nga, đặc biệt là giới trẻ. Mục tiêu của việc gây ảnh hưởng này là gây hại tới các nguyên tắc đạo đức, nền tảng lịch sử và lòng yêu nước của nhân dân Nga. Trong văn kiện này, Nga đặc biệt quan tâm tới việc đấu tranh chống lại "cuộc cách mạng Twitter" để ngăn chặn những sự kiện tương tự sự kiện Mùa xuân Arập, cho rằng qua sự kiện này, các dịch vụ như Facebook, Twitter hay các dịch vụ tin nhắn cho phép những thông tin gây bất ổn đến tình hình chính trị và xã hội được phát tán.

Ngoài chiến lược tự vệ trong chiến tranh mạng, Nga cũng chú trọng phát triển khả năng tấn công trên mạng, như được nêu trong Thuyết Quốc phòng Liên bang Nga năm 2010: một trong những đặc tính của xung đột vũ trang hiện đại là áp dụng sớm các biện pháp chiến tranh thông tin để đạt được các mục tiêu chính trị mà không phải dùng đến lực lượng quân sự và tạo ra phản ứng tích cực từ cộng đồng quốc tế, từ đó có thể sử dụng lực lượng

---

1. "Doctrine of Information Security of the Russian Federation" ("Thuyết An ninh thông tin Liên bang Nga" năm 2016), xem tại http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

quân sự[1]. Năng lực tấn công trên môi trường mạng giữ vai trò hỗ trợ quan trọng trong việc giúp quốc gia đạt được ưu thế về thông tin trong mọi giai đoạn của cuộc xung đột. Hơn nữa, Nga không coi các chiến dịch trên môi trường mạng như những sự kiện riêng rẽ, cụ thể mà có tính chiến lược và lâu dài. Ngoài ra, từ những cuộc xung đột giữa Nga với Extônia (năm 2007), Grudia (năm 2008) và Ucraina (năm 2013).

Chiến lược an ninh mạng của Nga được thực hiện ở cấp quốc gia và quốc tế. Ở tầm quốc tế, Chính phủ Nga muốn hợp tác với các nước đồng minh, đặc biệt là các nước thành viên của Tổ chức Hợp tác Thượng Hải, Tổ chức Hiệp ước an ninh tập thể và các nước thuộc nhóm BRICS. Bên cạnh đó, Nga cũng thúc đẩy các sáng kiến an ninh thông tin trên diễn đàn Liên hợp quốc, đặc biệt là việc xây dựng một công ước quốc tế về bảo đảm an ninh thông tin, xây dựng chuẩn mực ứng xử trên môi trường mạng, quốc tế hóa hệ thống quản trị mạng và thiết lập thể chế pháp lý quốc tế về không phổ biến vũ khí thông tin. Quan điểm không can thiệp về chủ quyền trên mạng của Nga đã nhận được sự ủng hộ của

---

1. The Military Doctrine of the Russian Federation , approved by Russian Federation presidential edict on February 5, 2010 (translated). Accessed at http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

các nước thành viên của các tổ chức nêu trên, trong đó có Trung Quốc, Tátgikixtan, Udơbêkixtan,...

Đối với vấn đề xây dựng công ước quốc tế về bảo đảm an ninh thông tin, Nga không đồng tình với việc áp dụng Công ước Budapest, thay vào đó Nga xây dựng dự thảo Công ước về chống tội phạm thông tin. Dự thảo này được Nga giới thiệu tại Khóa họp lần thứ 26 của Ủy ban về phòng, chống tội phạm và tư pháp hình sự năm 2017 (CCPCJ) thuộc Văn phòng Liên hợp quốc về chống ma túy và tội phạm (UNODC). Ngoài ra, Nga đã và đang vận động các nước cùng tham gia xây dựng dự thảo bằng nhiều hình thức như tổ chức hội thảo giữa cơ quan an ninh của Nga và các nước, đề nghị lồng ghép nội dung về an ninh thông tin vào các tuyên bố chung[1], ký thỏa thuận với các nước như Bắc Ailen nhằm ngăn chặn sự leo thang của các vụ việc trên mạng thành xung đột quốc tế... Trong thỏa thuận quốc tế với Bắc Ailen, Nga đề xuất xây dựng cơ chế hợp tác an ninh thông tin trên cơ sở các trung tâm quốc gia thiết lập ở hai nước, thông báo cho nhau về các cuộc tấn công và cơ sở hạ tầng quan trọng của hai nước. Bên cạnh đó, hai kênh đặc

---

1. Với Việt Nam, Nga cho biết đã có 25 nước ủng hộ xây dựng công ước mới và tham gia cùng xây dựng dự thảo công ước, đề nghị đưa ra Tuyên bố chung giữa Tổng thống Nga và Chủ tịch nước Việt Nam về vấn đề an ninh mạng, trong đó nêu lên sự cần thiết xây dựng văn kiện trong khuôn khổ Liên hợp quốc về an ninh mạng - thông tin từ Vụ châu Âu, Bộ Ngoại giao.

biệt được thiết lập để trao đổi thông tin về các sự cố máy tính và tội phạm mạng. Kênh thứ nhất được sử dụng để liên lạc giữa các cơ quan an ninh quốc gia về nội dung an ninh thông tin; kênh thứ hai là kênh khẩn cấp cho các sự cố máy tính, tập trung vào việc theo dõi các hoạt động gây hại trên Internet. Chính phủ Nga đang đẩy nhanh đàm phán với các nước NATO trong tương lai gần để xây dựng các thỏa thuận tương tự.

3. Trung Quốc

Trung Quốc là một trong những nước đi đầu trong việc áp dụng công nghệ thông tin trong các hoạt động của đời sống kinh tế - xã hội và đang ngày càng phụ thuộc vào công nghệ. Hiện nay có khoảng 721 triệu người Trung Quốc sử dụng mạng Internet[1]. Điều này khiến mạng Internet và thông tin truyền thông trở thành mối quan tâm hàng đầu của các nhà lãnh đạo Trung Quốc. Vào tháng 11/2013 tại Hội nghị Trung ương 3 khóa XVIII, Trung Quốc đã thành lập Tiểu ban lãnh đạo trung ương về An ninh Internet và thông tin thuộc Ban Chấp hành Trung ương Đảng Cộng sản Trung Quốc do Tổng Bí thư, Chủ tịch nước Tập Cận Bình làm trưởng tiểu ban. Ông cho rằng, Trung Quốc cần phải bắt kịp phương Tây trong đổi mới và rằng không có an toàn

---

1. Xem thêm Internet Live Stats Internet Live Stats, 2016. Accessed 18 Aug, 2016. http://www.internetlivestats.com/ internet- users/china/.

Internet thì sẽ không có an ninh quốc gia và không quản lý thông tin thì không có hiện đại hóa[1]. Tiểu ban này có nhiệm vụ tập trung vào các vấn đề liên quan đến công nghệ thông tin trong các lĩnh vực kinh tế, chính trị, xã hội và quân sự; điều phối các hoạt động của chính phủ về an ninh mạng và quản lý thông tin.

Năm 2016, Trung Quốc đã ban hành Luật an ninh mạng quốc gia gồm 7 chương và 79 điều. Về phạm vi áp dụng, Luật này áp dụng cho các cơ sở hạ tầng thông tin thiết yếu ở Trung Quốc, các nhà vận hành mạng và doanh nghiệp trong các ngành liên quan đến cơ sở hạ tầng thông tin thiết yếu. Tương tự như Nga và nhiều nước trên thế giới, cơ sở hạ tầng thông tin thiết yếu của Trung Quốc bao gồm nhiều lĩnh vực như thông tin liên lạc, mạng lưới phát thanh, năng lượng, tài chính, giao thông, giáo dục, nghiên cứu khoa học, sản xuất công nghiệp, y tế, dịch vụ công,... Luật này yêu cầu các nhà vận hành mạng hợp tác với Chính phủ Trung Quốc trong việc điều tra về tội phạm, cho phép truy cập đối với các dữ liệu, hỗ trợ kỹ thuật khi cơ quan có thẩm quyền yêu cầu. Luật này cũng quy định bắt buộc phải có sự kiểm định và chứng nhận các thiết bị máy tính đối với các nhà vận hành mạng trong lĩnh vực thông tin thiết yếu.

---

1. Zhu, Ningzhu: Xi Jinping Leads Internet Security Group, Xinhuanet, 27 Feb. 2014. Accessed 22 Aug, 2016. <http://news.xinhuanet.com/english/china/201402/27/c_133148273.htm>.

Điều 21 của Luật này quy định các nhà vận hành mạng phải thiết lập hệ thống quản lý an ninh nội bộ và bảo vệ an ninh mạng; áp dụng các biện pháp kỹ thuật để ngăn chặn virus máy tính hay các hình thức tấn công mạng khác; áp dụng các biện pháp kỹ thuật để theo dõi và lưu trữ thông tin về an toàn mạng; phân loại dữ liệu, mã hóa và lưu trữ những dữ liệu quan trọng. Những biện pháp an ninh này tương tự như ở các nước khác và trên thực tế đã được áp dụng như những khuyến nghị đối với các doanh nghiệp trong việc bảo vệ dữ liệu thông tin của mình. Ngoài ra, Điều 37 của Luật còn yêu cầu các nhà vận hành mạng trong lĩnh vực thông tin thiết yếu phải lưu trữ trong lãnh thổ Trung Quốc những dữ liệu do nhà vận hành mạng đó tạo ra hay thu thập được ở Trung Quốc. Luật cũng yêu cầu thông tin, dữ liệu về công dân Trung Quốc phải được lưu trữ trong các máy chủ nội địa và không được truyền ra ngoài nếu không được phép. Luật cũng cấm xuất khẩu dữ liệu về kinh tế, kỹ thuật, khoa học có khả năng đe dọa đến an ninh quốc gia hay lợi ích công cộng.

Đến tháng 12/2016, Trung Quốc ban hành chính sách an ninh mạng đầu tiên của mình, coi an ninh mạng tương đương với an ninh quốc gia, với mục tiêu hàng đầu là xây dựng Trung Quốc trở thành một cường quốc về môi trường mạng, đồng thời thúc đẩy phát triển môi trường mạng có trật tự, an ninh và mở, bảo đảm chủ quyền quốc gia. Chính sách này coi an ninh mạng như một vùng lãnh thổ mới của

chủ quyền quốc gia, đánh dấu bước đi mới trong việc đồng bộ hóa quyền kiểm soát của nhà nước trên môi trường mạng. Những nhiệm vụ chủ yếu được nêu trong chính sách gồm: (1) bảo vệ chủ quyền trên không gian mạng; (2) bảo vệ an ninh quốc gia; (3) bảo vệ cơ sở hạ tầng thông tin thiết yếu; (4) xây dựng văn hóa trực tuyến lành mạnh; (5) đấu tranh chống tội phạm mạng, gián điệp mạng và khủng bố; (6) cải thiện quản trị mạng; (7) nâng cao chuẩn an ninh mạng; (8) tăng cường năng lực quốc phòng trên không gian mạng; (9) tăng cường hợp tác quốc tế. Theo chính sách này, sự ảnh hưởng đến từ bên ngoài qua môi trường mạng là mối đe dọa hàng đầu tới an ninh và ổn định quốc gia của Trung Quốc. Chính vì vậy, chính sách cho phép Chính phủ Trung Quốc sử dụng mọi biện pháp cần thiết như khoa học - kỹ thuật, pháp lý, ngoại giao, quân sự để bảo đảm chủ quyền trên mạng. Việc Trung Quốc muốn kiểm soát chặt chẽ thông tin trên mạng trong lãnh thổ nước mình cũng đồng nghĩa với việc những thông tin có nội dung được xem là trái với lợi ích của Trung Quốc sẽ bị cấm đăng tải trên môi trường mạng của Trung Quốc. Các nhà vận hành mạng nước ngoài - những tập đoàn lớn như Google hay Facebook, Twitter có quan điểm trái ngược, cho rằng thông tin phải được truyền một cách tự do, và việc phải đặt máy chủ của mình ở Trung Quốc để lưu trữ thông tin và chịu sự theo dõi, điều chỉnh của Chính phủ Trung Quốc không những là trái với quyền tự do thông tin mà còn gây

tốn kém, không hiệu quả về kinh tế. Do đó, phần lớn những tập đoàn nước ngoài trong lĩnh vực thông tin, đặc biệt là các mạng xã hội, đã không đạt được thỏa thuận để vận hành trong lãnh thổ Trung Quốc.

Về mặt quân sự, năm 2015 trong loạt bài nghiên cứu khoa học chiến lược quân sự, Trung Quốc đã nhấn mạnh nguy cơ bị xâm nhập và lật đổ bởi phương Tây và sự cần thiết phải chống lại sự suy tàn văn hóa[1], để làm được điều này cần phải đấu tranh trên mặt trận không gian mạng. Bài nghiên cứu cũng cho rằng cần phải đẩy nhanh xây dựng lực lượng trên không gian mạng và tăng cường khả năng phòng thủ trên mạng[2]. Đây là văn kiện đầu tiên chính thức công nhận việc Trung Quốc nỗ lực xây dựng lực lượng trên không gian mạng với khả năng tấn công mạng. Từ đó, Trung Quốc đã tiến hành cải tổ hệ thống quốc phòng với sự ra đời của Lực lượng hỗ trợ chiến lược (SSF) thuộc Quân Giải phóng nhân dân Trung Quốc (PLA) với nhiệm vụ tác chiến điện tử, không gian và chiến tranh mạng. Lực lượng này được hợp nhất từ các cơ quan trước đây của quân đội phụ trách hỗ trợ về thông tin, không gian, tình báo, theo dõi, trinh sát, có vị trí tương đương với không quân, hải quân. Sự thành lập Lực lượng hỗ trợ chiến lược cho thấy

---

1. "China's Military Strategy", *USNI News*, May 26, 2015, https://news.usni.org/2015/05/26/document-chinas-military-strategy.

2. "China's Military Strategy", *Ministry of National Defense,* May 26, 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm

Quân Giải phóng nhân dân Trung Quốc coi ưu thế về thông tin và môi trường mạng không chỉ là để bổ trợ hay hỗ trợ cho khả năng chiến đấu của quân đội mà còn là một phần không thể thiếu của toàn bộ lực lượng quân đội. Ngoài ra, các lực lượng khác thuộc Bộ Quốc phòng cũng tập trung giám sát các mạng lưới thông tin công cộng, bảo vệ chủ quyền trên môi trường mạng, thực hiện gián điệp mạng. Công tác này cho thấy nỗ lực của Trung Quốc trong việc phát triển năng lực trên mạng ở cả thời bình và thời chiến.

Đáng chú ý, vào năm 2014, một báo cáo của Công ty Mandiant - một công ty chuyên về an ninh máy tính cho thấy Đơn vị 61398 thuộc Quân Giải phóng nhân dân Trung Quốc (thường được biết đến với cái tên APT1 – Advanced Persistent Threat 1) đã thực hiện tấn công các tập đoàn và chính phủ nước ngoài trên khắp thế giới từ năm 2006. APT1 được cho là có bốn mạng lưới lớn ở Thượng Hải và là một trong hơn 20 nhóm APT đến từ Trung Quốc. Vụ số 3 và Vụ số 4 thuộc Quân Giải phóng nhân dân Trung Quốc phụ trách về chiến tranh điện tử được cho là chịu trách nhiệm chính trong việc xâm nhập và chiếm quyền điều khiển các mạng lưới máy tính. Trước năm 2013, Chính phủ Trung Quốc luôn giữ thái độ phủ nhận các cáo buộc về tấn công mạng; tuy nhiên vào năm 2013, Trung Quốc đã thay đổi quan điểm và công khai thừa nhận về sự tồn tại của các đơn vị chiến tranh mạng bí mật trong quân đội và bộ phận dân sự của Chính phủ nhưng không nêu thông tin cụ thể.

Trên phương diện hợp tác quốc tế trong vấn đề an ninh mạng, Trung Quốc có cùng quan điểm với Nga. Tại các diễn đàn quốc tế, Trung Quốc kêu gọi xây dựng cộng đồng mạng quốc tế chung vận mệnh và thúc đẩy các nguyên tắc về tôn trọng chủ quyền trên mạng, bảo đảm an ninh mạng, khuyến khích không gian mạng mở và thiết lập trật tự trên mạng, xây dựng một hệ thống quản trị mạng đa phương[1].

Thực tế triển khai chính sách an ninh mạng và sự vươn lên của Trung Quốc trong không gian mạng

Với việc coi trọng và thúc đẩy mạnh mẽ việc áp dụng công nghệ thông tin trong các hoạt động kinh tế - xã hội, tiềm lực khoa học - công nghệ của Trung Quốc trong lĩnh vực không gian mạng đang được gia tăng một cách đáng kể, dần trở thành cường quốc trong lĩnh vực không gian mạng. Nhà nghiên cứu Adam Segal (Chủ tịch Chương trình Nghiên cứu về các công nghệ mới nổi và an ninh quốc gia, Hội đồng Đối ngoại Mỹ) cho rằng, Mỹ đang dần để mất vai trò đi đầu của mình trong lĩnh vực không gian mạng vào tay Trung Quốc[2]. Trung Quốc đã nỗ lực để trở thành siêu cường trong không gian mạng. Nước này hiện đã đặt các cơ quan quản lý Internet dưới sự lãnh đạo thống nhất của

---

1. "Infographic: Achievements of the 2nd WIC", *China Daily,* 21 Dec, 2015. Accessed 23 Aug, 2016; http://www.chinadaily.com.cn/business/tech/2015-12/21/content_22761073.htm.

2. Adam Segal: "When China Rules the Web: Technology in Service of the State", 97 *Foreign Affair*, 97(5), 10 (2018).

Tổng Bí thư, Chủ tịch nước Tập Cận Bình nhằm đạt được bốn mục tiêu: (i) bảo đảm tính hài hòa của Internet, (ii) giảm sự phụ thuộc vào các nhà cung cấp dịch vụ và công nghệ nước ngoài, (iii) thúc đẩy sự phát triển của các lực lượng tác chiến không gian mạng và bảo vệ hệ thống mạng của Trung Quốc và (iv) thúc đẩy khái niệm chủ quyền không gian mạng (*cyber sovereignty*) trở thành một nguyên tắc cơ bản trong quản trị Internet. Việc thực hiện các mục tiêu nói trên đòi hỏi Trung Quốc phải thực hiện một cách quyết liệt việc quản lý không gian mạng ở trong nước cũng như thúc đẩy cách tiếp cận của mình ở cấp độ toàn cầu.

Thực tế, trong năm 2017, Trung Quốc đã phạt các công ty Tencent, Baidu, Weibo (đều là các công ty cung cấp dịch vụ mạng của Trung Quốc) vì đã vi phạm Luật an ninh mạng khi đăng các nội dung không phù hợp liên quan đến Đại hội Đảng lần thứ XIX của nước này. Trung Quốc cũng yêu cầu các công ty dịch vụ mạng nước ngoài (như Apple) phải dỡ bỏ phần mềm VPNS (giúp người dùng mạng có thể truy cập Facebook và các trang mạng xã hội nước ngoài) khỏi nước này. Việc Chính phủ Trung Quốc đưa ra các quy định chặt chẽ về quản lý không gian mạng khiến các nhà đầu tư nước ngoài lo ngại về việc nước này có thể lợi dụng các quy định luật pháp để đánh cắp thông tin, bí mật kinh doanh, công nghệ.

Ở cấp độ trong nước, để đảm bảo an ninh, an toàn trên không gian mạng, Trung Quốc đã tìm cách tự chủ về năng

lực công nghệ với việc đầu tư mạnh vào nghiên cứu và phát triển (R&D). Từ năm 1999, đầu tư trong lĩnh vực này của Trung Quốc tăng liên tục 20%/năm và hiện nay đã đạt 233 tỷ USD, chiếm 20% tổng đầu tư cho R&D toàn thế giới[1]. Trung Quốc cũng là quốc gia có lượng sinh viên tốt nghiệp ngành khoa học và kỹ sư cao nhất thế giới và đã vượt Mỹ về số lượng các xuất bản phẩm, các bài nghiên cứu trong lĩnh vực khoa học - công nghệ. Cựu Chủ tịch Google, ông Eric Schmidt dự báo đến năm 2020, Trung Quốc sẽ đuổi kịp Mỹ trong lĩnh vực trí tuệ nhân tạo, đến năm 2025 sẽ vượt Mỹ và đến năm 2030, Trung Quốc sẽ hoàn toàn thống trị trong lĩnh vực này. Ngoài ra, Trung Quốc còn thúc đẩy việc áp dụng trí tuệ nhân tạo trong lĩnh vực quốc phòng, ngăn chặn tấn công mạng, kiểm soát mạng xã hội.

Ở cấp độ quốc tế, Trung Quốc nhấn mạnh vai trò của Liên hợp quốc trong việc thúc đẩy cách tiếp cận đa phương trong quản trị không gian mạng (trong khi Mỹ và các nước phương Tây áp dụng mô hình quản lý phi tập trung - *distributed model*, Trung Quốc lại áp dụng mô hình nhà nước quản lý - *state-centric*) nhằm thu hút sự ủng hộ của các nước có cùng mong muốn quản lý chặt không gian mạng như Trung Quốc. Trung Quốc đã phản đối mạnh mẽ các nỗ lực của Mỹ trong việc áp dụng luật quốc tế, đặc biệt

---

1. Adam Segal: "When China Rules the Web: Technology in Service of the State", *Foreign Affair*, 97(5), 10 (2018).

là xung đột vũ trang có nguyên nhân từ không gian mạng. Nhóm chuyên gia chính phủ của Liên hợp quốc về an ninh mạng (UN GGE) hiện đang bế tắc trong việc thúc đẩy xây dựng các quy chuẩn chung (norms) về ứng xử trong không gian mạng, một phần do Trung Quốc và Nga có quan điểm khác với Mỹ và các nước phương Tây. Trong bối cảnh đó, Trung Quốc đã phổ biến các khuôn khổ quốc tế của riêng mình nhằm gia tăng ảnh hưởng của Trung Quốc trong quản lý không gian mạng như tổ chức Hội nghị Internet thế giới hàng năm tại Wuzhen (Ô Trấn, Thượng Hải). Đại diện Apple đã tham dự và bày tỏ ủng hộ cách tiếp cận của Trung Quốc về việc phát triển nền kinh tế số mở và vì lợi ích chung.

Trung Quốc cũng ngày càng gia tăng tiếng nói của mình trong việc quản trị Internet thông qua thương mại và đầu tư. Trong khuôn khổ sáng kiến "Vành đai, con đường", ngoài việc đầu tư kết nối cơ sở hạ tầng, Trung Quốc cũng đang xây dựng một con đường tơ lụa số qua việc thiết lập hệ thống cáp quang, mạng di động, các trạm vệ tinh, trung tâm dữ liệu và mạng lưới các thành phố thông minh. Kế hoạch này được thực hiện thông qua các dự án, các công ty công nghệ, dịch vụ mạng Trung Quốc, từ đó chính phủ nước này có thể kiểm soát, thu thập thông tin, dữ liệu. Điều này khiến các quốc gia khác lo ngại. Thực tế, Ôxtrâylia đang xem xét việc cấm công ty Huawei cung cấp các thiết bị để triển khai mạng 5G tại Ôxtrâylia; Mỹ đang tìm cách

hạn chế Trung Quốc đầu tư vào các công ty công nghệ Mỹ (chặn các ứng dụng của công ty China Mobile tại thị trường Mỹ, cấm điện thoại thông minh của Huawei và ZTE tại các căn cứ quân sự của Mỹ và hiện nay là cấm các công ty Mỹ cung cấp dịch vụ cho Huawei. Mỹ cũng cấm các công ty truyền thông Mỹ sử dụng các thiết bị và dịch vụ quan trọng từ Trung Quốc).

Về mặt quản lý xã hội, Trung Quốc hiện đã thiết lập một hệ thống chặt chẽ để quản lý không gian mạng, đồng thời đầu tư mạnh cho các hoạt động nghiên cứu và phát triển nhằm đạt được sự tự chủ và đi đầu về công nghệ mạng. Nước này cũng đã đã xây dựng bộ chỉ số xã hội (*social credit*) nhằm đánh giá các thông tin công khai và thông tin cá nhân của người sử dụng mạng xã hội, lấy đó làm cơ sở đối với việc tuyển dụng, giáo dục, nhà ở và đi lại[1].

4. Canađa

Canađa được xếp hạng là một trong 10 quốc gia đứng đầu về hành động và nhận thức về an ninh mạng. Còn theo Chỉ số an toàn thông tin mạng toàn cầu năm 2017 của Liên minh Viễn thông quốc tế (ITU), Canađa đứng thứ chín trên

---

1. An Hồng: "Hệ thống chấm điểm công dân Trung Quốc hoạt động thế nào?", 2019, Báo điện tử *Vnexpress*, https://vnexpress.net/the-gioi/he-thong-cham-diem-cong-dan-trung-quoc-hoat-dong-the-nao-3903327.html.

thế giới. Thứ hạng này được bình chọn dựa trên việc chấm điểm nhiều tiêu chí khác như: hệ thống quy định pháp lý, yếu tố công nghệ, kỹ thuật, khả năng giáo dục, nghiên cứu và sự hợp tác của quốc gia này trong các mạng chia sẻ thông tin với các đối tác. Mỗi năm, có hàng ngàn cuộc tấn công nhắm vào các doanh nghiệp Canađa, chính phủ và các cá nhân, gây thiệt hại hàng tỷ USD mỗi năm[1]. Một số ví dụ điển hình cho thấy mức độ nghiêm trọng của tội phạm mạng ở Canađa: Năm 2011, Bộ Tài chính, Ban Thư ký Hội đồng tài chính và Nghiên cứu quốc phòng Canađa đã buộc phải tạm ngưng các dịch vụ sau khi tin tặc có được quyền truy cập dữ liệu thông tin cá nhân. Gần đây nhất, Cơ quan Doanh thu Canađa và Hội đồng Nghiên cứu quốc gia (NRC) đều bị xâm nhập hệ thống bất hợp pháp, khoảng 900 số bảo hiểm xã hội cũng như dữ liệu nghiên cứu và phát triển có giá trị đã bị đánh cắp,...

Theo nhiều đánh giá, trong đó có một báo cáo năm 2012 của Tổng Kiểm toán Canađa, Chính phủ Canađa chỉ đơn thuần là chưa có sự chuẩn bị cần thiết để bảo vệ mình khỏi các mối đe dọa, các cuộc tấn công kỹ thuật số ngày càng tinh vi hơn. Nhiều doanh nghiệp Canađa cũng không ngoại lệ. Theo một nghiên cứu của Liên minh Bảo vệ an ninh mạng quốc tế tại Anh cho thấy, 69% các công ty

---

1. Symantec: "2013 Norton Report", http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.en_ca.pdf.

Canađa đã bị xâm nhập hệ thống trong năm 2014[1]. Các cuộc tấn công này bao gồm từ phần mềm độc hại và virus đến lừa đảo và truy cập trái phép vào tài sản của công ty. Trong nhiều trường hợp, thông tin khách hàng có giá trị đã bị xâm phạm, gây thiệt hại hàng triệu USD và làm giảm hoặc mất uy tín. Trong khi Chính phủ và các doanh nghiệp cam kết đầu tư lớn để giải quyết những mối đe dọa này, thì người dân Canađa vẫn trong nguy cơ bị tấn công trực tuyến ngày càng nhiều.

Do vậy, Chính phủ Canađa đã phát động chiến lược an ninh mạng đầu tiên vào ngày 03/10/2010. Chiến lược được thiết kế nhằm hướng tới một không gian mạng an toàn hơn cho tất cả mọi người dân Canađa với ba mục tiêu chính: (i) Một hệ thống chính phủ an ninh; (ii) Hợp tác để bảo đảm các hệ thống mạng quan trọng của các công ty, tập đoàn phi chính phủ; (iii) Bảo vệ người dân khi truy cập và sự dụng các dịch vụ trực tuyến.

Về vấn đề nâng cao nhận thức cho cộng đồng, Chính phủ Canađa đã đưa ra các chiến lược quảng cáo thông qua các trang web, các mạng xã hội, các phương tiện truyền thông và tổ chức các buổi triển lãm, sự kiện đặc biệt để phổ

---

1. International Cyber Security Protection Alliance, 2014, "Study of the Impact of Cyber Crime on Businesses in Canada: Fighting Cybercrime Together", https://www.icspa.org/wp-content/uploads/2014/12/ICSPA-Canada-Cyber-Crime-Study-Report.pdf.

biến về an ninh thông tin. Song song với những chiến dịch đó, Chính phủ Canađa còn thường xuyên cập nhật, đưa ra các bảng thống kê đánh giá mức độ nhận thức về an toàn thông tin cho người dân để đưa ra các biện pháp xử lý kịp thời. Với một tham vong xa hơn, Canađa còn xây dựng quan hệ đối tác với các tổ chức liên bang khác và các bên có liên quan trong cộng đồng quốc tế, mở rộng phạm vi, gia tăng tần suất và tác động của việc tuyên truyền này.

Về tội phạm trên không gian mạng, Chính phủ Canađa đã đưa ra những kế hoạch hành động, trong đó bước đầu tiên là thành lập một trung tâm chuyên nghiên cứu các tình huống và phân tích các xu hướng tội phạm mạng. Kèm theo đó là Đạo luật Bill C-12 về bảo vệ thông tin cá nhân của người dân Canađa ("*Safeguarding Canadian's Personal Information Act*") dựa trên Đạo luật về bảo vệ thông tin cá nhân và các tài liệu điện tử ("*Personal Information Protection and Electronic Documents Act*" - PIPEDA) bao gồm cả biện pháp phòng, chống rò rỉ dữ liệu. Bill C-28 - Đạo luật về chống thư rác ("*Canada's Anti-spam Legislation*") giúp bảo vệ người dân Canađa khỏi thư rác trong khi vẫn bảo đảm các doanh nghiệp có thể tiếp tục cạnh tranh trên thị trường toàn cầu[1].

---

1. "Action plan 2010 - 2015 for Canada's Cyber Security Strategy", https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx.

Chính sách Quốc phòng của Canađa năm 2017

Ngày 03/11/2017, Canađa ban hành Chính sách Quốc phòng dài hạn "Mạnh mẽ, an ninh, gắn kết ("*Strong, Secure, Engaged*"), trong đó cam kết nhiều điều khoản nhằm tăng cường phòng thủ trên mạng và tiến hành các hoạt động trên mạng để chống lại kẻ thù tiềm năng khi các nhiệm vụ quân sự được chính phủ ủy quyền. Các hoạt động trên mạng sẽ phải tuân thủ tất cả các điều luật hiện hành trong nước, luật pháp quốc tế, các quy tắc để tham gia, đánh giá mục tiêu và đánh giá những thiệt hại ngoài dự kiến. Chính phủ Canađa sẵn sàng cung cấp 4,6 tỷ USD trong 20 năm cho những dự án liên kết (joint capabilities), trong đó có việc cải thiện khả năng mã hóa, khả năng điều hành dữ liệu và những yếu tố quan trọng của mạng bao gồm an ninh mạng; nhận dạng và phản hồi những mối đe dọa trên mạng; sự phát triển của các hoạt động thông tin quân sự và các hoạt động mang tính chất đáp trả như nhắm mục tiêu, khai thác, tấn công và làm ảnh hưởng để hỗ trợ cho các hoạt động quân sự.

Tình báo quốc phòng của Canađa cũng là vấn đề được coi trọng. Để giải quyết nhu cầu về tình báo quốc phòng nội bộ, trong Chính phủ Canađa và các nước đồng minh. Theo đó, Bộ Quốc phòng Canađa sẽ xây dựng và nâng cấp lực lượng tình báo Canađa có khả năng cung cấp những phương thức tình báo tinh vi hơn để hỗ trợ cho các hoạt động gồm hoạt động nâng cao dự báo các điểm chớp

nhoáng và các mối đe dọa mới nổi; hoạt động hỗ trợ các nền tảng, hạ tầng mới, đồng thời nắm bắt được xu thế phát triển nhanh chóng trong không gian, mạng và các lĩnh vực mới nổi khác. Để tận dụng tốt hơn những tính năng của mạng trong việc hỗ trợ các hoạt động quân sự, Bộ Quốc phòng sẽ phát triển, tăng cường một đội mới cho Cyber Operator (Cơ quan quản lý hoạt động mạng) của Lực lượng vũ trang Canađa bằng cách thu hút những tài năng tốt nhất, sáng giá nhất của Canađa và gia tăng đáng kể số lượng nhân viên quân sự trong lĩnh vực mạng. Nhân viên của Cyber Operator có nhiệm vụ bảo vệ hệ thống mạng máy tính và liên lạc với các đồng minh của Canađa để nâng cao hiệu quả trong việc cung cấp một môi trường mạng an toàn cho Bộ Quốc phòng và Lực lượng vũ trang Canađa[1]. Đồng thời bảo vệ các hệ thống mạng, thiết bị quân sự chủ chốt trước các cuộc tấn công có chủ định và phát triển một mạng lưới linh hoạt để hỗ trợ các nhiệm vụ quân sự chống lại những kẻ thù tiềm năng[2].

Chiến lược An ninh mạng quốc gia Canađa năm 2018

Mục tiêu cốt lõi của chiến lược được phản ánh trong các khoản đầu tư đáng kể mà Chính phủ Canađa dành cho vấn

---

1. Cyber Operator Occupation, http://dgpaapp.forces.gc.ca/en/canada-defence-policy/themes/canada-vision-defence/cyber-operator.asp.

2. "Strong, Secure, Engaged" Canada's Defence policy, http://publications.gc.ca/collections/collection_2017/mdn-dnd/D2-386-2017-eng.pdf.

đề an ninh mạng trong năm 2018 với mức đầu tư hơn 500 triệu USD trong 5 năm. Đây là khoản đầu tư lớn nhất của Canađa từ trước tới nay cho vấn đề này, điều này thể hiện sự cam kết về an toàn và bảo mật thông tin của Canađa trong kỷ nguyên số. Khoản đầu tư này được sử dụng trong:

- Tài trợ các trung tâm an ninh mạng mới để hỗ trợ các nhà lãnh đạo và tiến hành hợp tác ở cấp chính phủ và các đối tác quốc tế, đồng thời cung cấp nguồn lực rõ ràng và đáng tin cậy cho công dân và doanh nghiệp Canađa.

- Thành lập đơn vị điều phối tội phạm quốc gia để mở rộng khả năng của Royal Canadian Mounted Police trong việc điều tra tội phạm mạng, thiết lập một trung tâm điều phối cho cả đối tác trong nước và quốc tế.

- Tài trợ để thúc đẩy đổi mới và tăng trưởng kinh tế và sự phát triển của tài năng mạng Canađa.

5. Liên minh châu Âu (EU)

Chính sách an ninh mạng chung của EU nhằm tạo các quy định phù hợp cho các doanh nghiệp hoạt động tại các quốc gia thành viên. Ba thành tố tạo nên chính sách an ninh mạng của EU bao gồm Cơ quan về An ninh mạng và An ninh thông tin (ENISA), Chỉ thị về An ninh mạng và An ninh thông tin (NIS) và Tiêu chuẩn bảo vệ dữ liệu chung của EU (GDPR). Vào thời điểm hiện nay, sau sự kiện Brexit, vấn đề đặt ra trong thực thi chính sách an ninh mạng của EU là làm thế nào để Vương Quốc Anh

cũng tuân thủ các các quy định hiện hành của EU về an ninh mạng.

Cơ quan về An ninh mạng và An ninh thông tin (ENISA)

ENISA là cơ quan về an ninh mạng và an ninh thông tin của Liên minh châu Âu và là cơ quan quản lý được thành lập bởi các văn bản: Quy định số 460/2004 của Nghị viện châu Âu và Hội đồng Liên minh châu Âu vào ngày 10/3/2004 với mục đích nâng cao an ninh mạng và an ninh thông tin, chỉ thị về an ninh mạng và an ninh thông tin (NIS). Hiện nay, ENISA hoạt động theo Quy định (EU) số 526/2013. ENISA làm việc tích cực với tất cả các nước thành viên của Liên minh châu Âu trong việc cung cấp một loạt các dịch vụ thuộc lĩnh vực không gian mạng, trong đó tập trung vào ba yếu tố chính: (i) Khuyến nghị các nước thành viên về các hành động đối vi phạm an ninh mạng; (ii) Xây dựng chính sách và hỗ trợ việc thực hiện các quy định về an ninh mạng cho tất cả các thành viên EU; (iii) Hỗ trợ trực tiếp (theo đó, ENISA trực tiếp làm việc với các đội, nhóm hoạt động trong lĩnh vực không gian mạng của EU).

ENISA đã phát hành các ấn phẩm khác nhau về tất cả các vấn đề quan trọng liên quan đến an ninh mạng. ENISA đã đưa ra nhiều sáng kiến, bao gồm: Chiến lược điện toán đám mây EU, Các tiêu chuẩn mở trong công nghệ truyền thông - thông tin, Chiến lược An ninh mạng của EU và một

nhóm điều phối An ninh mạng. ENISA cũng bắt tay hợp tác với các tổ chức tiêu chuẩn quốc tế như ISO và ITU.

Chỉ thị về An ninh mạng và An ninh thông tin (NIS)

Ngày 6/7/2016, Nghị viện châu Âu ra Chỉ thị về an ninh mạng và An ninh thông tin (NIS). Chỉ thị này có hiệu lực vào tháng 8/2016 và tất cả các quốc gia thành viên của EU có 21 tháng để tích hợp các luật lệ trong chỉ thị này vào luật quốc gia. Mục đích của Chỉ thị NIS là tạo ra mức độ an ninh mạng tổng thể cao hơn trong EU. Chỉ thị này có ảnh hưởng đáng kể đến các nhà cung cấp dịch vụ kỹ thuật số, các công nghệ xử lý tín hiệu số (DSP) và các nhà khai thác dịch vụ thiết yếu (OES). Các nhà khai thác dịch vụ thiết yếu bao gồm bất kỳ tổ chức nào mà hoạt động bị ảnh hưởng rất lớn trong trường hợp có lỗ hổng an ninh. Cả DSP và OES hiện đang chịu trách nhiệm trong việc báo cáo các sự cố an ninh cho các đội phản ứng nhanh sự cố an ninh máy tính (CSIRTs). Trong khi DSP không phải chịu những quy định ngặt nghèo như các nhà khai thác dịch vụ thiết yếu, DSP không được thiết lập trong EU nhưng các hoạt động trong EU vẫn phải tuân thủ các các quy định của khối. Ngay cả khi DSP và OES thuê ngoài việc duy trì các hệ thống thông tin từ bên thứ ba, Chỉ thị NIS vẫn được áp dụng nhằm bảo đảm bên chịu trách nhiệm trong trường hợp xảy ra sự cố.

Các quốc gia thành viên của EU được yêu cầu phải có chiến lược thực thi Chỉ thị NIS, bao gồm việc thành lập các đội CSIRTs, các cơ quan về tội phạm quốc gia của từng nước

(The National Crime Agency - NCAs)[1] và các cơ quan điều phối (SPOCs). Các đơn vị này có trách nhiệm xử lý các vi phạm về an ninh mạng để giảm thiểu ảnh hưởng của các vi phạm này. Ngoài ra, tất cả các quốc gia thành viên EU được khuyến khích chia sẻ thông tin về an ninh mạng.

Những yêu cầu bảo mật của Chỉ thị NIS bao gồm các biện pháp kỹ thuật quản lý rủi ro của hành vi vi phạm an ninh mạng bằng cách phòng ngừa. Bên cạnh đó, cả DSP và OES phải cung cấp thông tin cho phép đánh giá chuyên sâu hệ thống thông tin và chính sách bảo mật. Tất cả các sự cố quan trọng phải được thông báo cho các đội CSIRTs. Độ nghiêm trọng của sự cố an ninh mạng được xác định bởi số lượng người sử dụng sẽ bị ảnh hưởng bởi cuộc tấn công mạng cũng như khoảng thời gian xảy ra các sự cố và phạm vi địa lý của vụ việc.

Quy định về bảo vệ dữ liệu chung của EU (GDPR)

Quy định về bảo vệ dữ liệu chung của EU (GDPR), ra đời ngày 14/4/2016 và có hiệu lực ngày 25/5/2018. Các quy định chung này nhằm thiết lập các tiêu chuẩn thống nhất để bảo vệ dữ liệu giữa tất cả các nước thành viên trong EU. Với việc thông qua GDPR, EU đã đi đầu trong việc áp dụng các quy định nhằm cân bằng giữa việc bảo vệ thông tin cá nhân và các lợi ích kinh doanh của chính phủ và doanh nghiệp. GDPR quy định rõ trách nhiệm của các công

1. NCAs là các cơ quan thực thi pháp luật quốc gia ở mỗi nước (*BT*).

ty, tổ chức một cách rõ ràng trong việc thu thập và xử lý thông tin một cách hợp pháp, trách nhiệm hợp tác với cơ quan chính phủ trong trường hợp xảy ra sự cố thông tin, đồng thời mở rộng quyền cho người sử dụng trong việc quản lý thông tin cá nhân đã được thu thập. Để bảo đảm việc thực thi, GDPR cũng quy định chặt chẽ các công cụ thực hiện, trong đó có việc cho phép áp dụng các mức phạt cao trong trường hợp xảy ra vi phạm.

Quy định không chỉ áp dụng cho các tổ chức hoạt động trong EU mà còn áp dụng cho các tổ chức xử lý dữ liệu của bất kỳ cư dân nào của EU. Bất kể nơi nào dữ liệu được xử lý, nếu là dữ liệu của một công dân EU, các tổ chức phải tuân theo quy định này. Quy định cũng đưa ra mức phạt nặng và tổng cộng có thể lên tới 20 triệu euro hay 4% doanh thu hằng năm. Ngoài ra, tương tự như những quy định trước đây, tất cả các hành vi vi phạm dữ liệu ảnh hưởng tới các quyền và tự do của những cá nhân cư trú tại EU phải được công bố trong vòng 72 giờ. Ban Bảo vệ dữ liệu của EU (EDP) phải chịu trách nhiệm về tất cả các giám sát theo quy định của GDPR.

Sự đồng thuận đóng một vai trò quan trọng trong các quy định của GDPR. Các công ty nắm giữ dữ liệu liên quan đến công dân EU phải bảo đảm cho các công dân quyền được từ chối chia sẻ dữ liệu dễ dàng như việc người dân đồng ý chia sẻ chúng. Ngoài ra, người dân cũng có thể hạn chế việc xử lý các dữ liệu được lưu trữ về họ. Công dân EU

có thể chọn lựa để cho phép các công ty lưu trữ dữ liệu của họ nhưng không xử lý dữ liệu đó, điều này tạo ra một sự khác biệt rõ ràng. Khác với các quy định trước đây, GDPR cũng hạn chế việc chuyển giao dữ liệu của một công dân ra bên ngoài EU hoặc cho một bên thứ ba mà không có sự đồng ý trước của công dân đó.

Các vấn đề liên quan tới Brexit

Với việc Anh quyết định rút khỏi EU, các quy định hiện nay được áp dụng tại Anh chỉ bao gồm ENISA và Chỉ thị NIS.

Tuy nhiên, hiện vẫn còn một số ý kiến cho rằng, GDPR vẫn được áp dụng tại Anh dù ngày thực thi của GDPR là vào thời điểm nào thì GDPR được ký kết và có hiệu lực khi Anh vẫn là một phần của Liên minh châu Âu.

6. Ixraen

Tuy là nước nhỏ, Ixraen là một trong những nước có năng lực mạnh nhất thế giới về công nghệ thông tin nói chung và an ninh mạng nói riêng. Ixraen hiện đang là một trong những quốc gia dẫn đầu về ứng dụng và phát triển công nghệ thông tin nói chung và an toàn thông tin nói riêng, đặc biệt là các giải pháp, công cụ cốt lõi trong ngành an ninh nội địa bảo vệ cơ sở hạ tầng trọng yếu và an ninh mạng.

Chính sách tự lực, tự cường về an ninh mạng của Ixraen xuất phát từ nhiều lý do, trong đó quan trọng nhất là bảo vệ đất nước khỏi sự tấn công của các thế lực thù địch. Ngay

từ khi được thành lập năm 1948, Nhà nước Ixraen đã phải đối mặt với nhiều vấn đề trong chính sách đối ngoại khi bị các nước Arập tẩy chay. Đến nay, trong số 192 quốc gia thành viên Liên hợp quốc vẫn có 31 nước không công nhận hoặc không thiết lập quan hệ ngoại giao với Ixraen. Ixraen cũng đã trải qua bốn cuộc chiến tranh và hàng trăm cuộc xung đột lớn nhỏ với các nước láng giềng. Song song với những mối nguy cơ từ không gian thực, Ixraen còn phải đối mặt hằng ngày với những mối đe dọa từ không gian ảo. Riêng trong năm 2017, Ixraen đã hứng chịu 1.400 cuộc tấn công mạng có tổ chức, trong đó 35% các cuộc tấn công này nhằm vào các cơ quan công lập, 25% nhằm vào các doanh nghiệp công nghệ, 10% nhằm vào các cơ sở tài chính. Theo Giám đốc Bộ An ninh (Shin Bet) Nadav Argaman, Ixraen không chỉ bị tấn công từ các quốc gia như Iran (với hai cánh quân chính là Lực lượng Quds và Bộ Tình báo) mà còn từ Trung Quốc và Nga, những nước có quan hệ hữu hảo với Ixraen. Thời gian qua, Shin Bet đã ngăn chặn nhiều vụ sáp nhập, tham gia thầu của các công ty Trung Quốc liên quan đến các dự án hạ tầng thông tin, viễn thông quan trọng của Ixraen. Một số cơ quan trọng yếu của Ixraen đã cấm nhân viên sử dụng điện thoại Trung Quốc[1]. Ngoài các nguy cơ đến từ lực lượng quốc gia hoặc do quốc gia hậu thuẫn, Ixraen còn phải đối phó với các cuộc tấn công mạng

1. Https://www.ynetnews.com/articles/0,7340,L-5320392,00.html.

kiểu "con sói đơn độc". Riêng trong năm 2017, các cơ quan an ninh mạng Ixraen đã ngăn chặn được hơn 2.000 cuộc tấn công do các hacker gây ra.

Về phần mình, Bộ Ngoại giao Ixraen cũng rất coi trọng vai trò của hợp tác về an ninh mạng. Vị trí Điều phối viên an ninh mạng (Cyber Security Coordinator) là một vị trí quan trọng trong Vụ các vấn đề chiến lược của Bộ Ngoại giao Ixraen, hiện do một viên chức ngoại giao cao cấp, nguyên Trợ lý Tổng giám đốc (hàm Vụ trưởng), Phó Đại sứ Ixraen tại Bắc Kinh đảm trách. Phòng Hợp tác an ninh mạng trong Bộ Ngoại giao có nhiệm vụ xây dựng và điều phối chính sách liên quan đến hợp tác quốc tế trong lĩnh vực an ninh mạng[1].

Chính sách an ninh mạng của Ixraen

Tháng 6/2018, Ixraen đã giới thiệu dự thảo lần thứ nhất Luật an ninh mạng gây nhiều tranh cãi, trong đó quy định về việc Cục An ninh mạng quốc gia có quyền yêu cầu các cơ quan, tổ chức - bao gồm cơ quan công quyền, cơ sở hạ tầng quan trọng, các thực thể dân sự - cung cấp thông tin và tịch thu trang thiết bị công nghệ thông tin của họ mà không cần lệnh của tòa án. Tuy nhiên, cơ quan dự thảo luật khẳng định yêu cầu này là cần thiết nhằm đối phó với những nguy cơ từ mạng chưa từng có và ngày càng gia tăng. Dự kiến Luật An ninh mạng sẽ phải

1. Https://cyberweek.tau.ac.il/2016/speakers/113-iddo-moed.

trải qua nhiều lần chỉnh sửa trước khi trình Quốc hội thông qua trong năm 2020[1].

Các quy định, quy tắc về an ninh mạng được đề cập trong nhiều đạo luật và văn bản dưới luật của Ixraen. Luật về quyền riêng tư (năm 1981) quy định các biện pháp bảo vệ dữ liệu an ninh và dữ liệu riêng tư trên mạng; Luật máy tính (năm 1995) về phòng chống tội phạm mạng, máy tính (Luật này đã được sửa đổi năm 2012 cho phù hợp với Công ước Budapest về tội phạm mạng, mặc dù đến năm 2016 Ixraen mới tham gia phê chuẩn Công ước này); Pháp lệnh về sở hữu dữ liệu (năm 1986) quy định các thủ tục, trình tự trong việc sở hữu, bảo vệ và chuyển dữ liệu giữa các cơ quan nhà nước; Pháp lệnh về chuyển dữ liệu (năm 2001) quy định các thủ tục, trình tự trong việc sở hữu, bảo vệ và chuyển dữ liệu ra ngoài lãnh thổ Ixraen[2]; Pháp lệnh về an ninh thông tin (năm 2012) quy định các nghĩa vụ về an ninh thông tin và an ninh mạng đối với các tổ chức và cá nhân của Ixraen; Thông tư số 2016-9-14 của Bộ Tài chính và các thông tư số 361, 357 của Ngân hàng Trung ương Ixraen về kiểm soát an ninh thông tin tài chính, ngân hàng trên môi trường mạng. Ngoài ra, các quy định về an ninh

---

1. Https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law.

2. Đáng chú ý, dự thảo Pháp lệnh các quy định dữ liệu quan trọng, nhạy cảm phải được cơ quan chuyên môn kiểm định trước khi chuyển ra ngoài lãnh thổ Ixraen, nhưng đến khi ban hành thì quy định này đã bị bỏ.

mạng của Ixraen còn nằm rải rác ở các đạo luật khác như Luật về tự do và phẩm giá của con người (năm 1992), Luật chữ ký điện tử (năm 2001), Luật kiểm soát xuất khẩu quốc phòng (năm 2007), Luật nghe lén thiết bị điện tử (năm 1979, sửa đổi năm 2013), Nghị quyết số 2443 về các tiêu chuẩn ISO đối với thiết bị an ninh mạng,...

Theo Nghị quyết số 3611, Ixraen định nghĩa an ninh mạng là "các đường lối, chính sách, hoạt động, cơ chế tự vệ, quản lý rủi ro và phương tiện kỹ thuật nhằm bảo vệ không gian mạng"; trong khi không gian mạng được định nghĩa là "khu vực hữu hình và vô hình, bao gồm các hệ thống máy tính, mạng lưới máy tính và truyền thông, thông tin điện tử và nội dung được truyền giữa các máy tính, phương tiện truyền thông, cơ sở dữ liệu và người sử dụng".

Một số quy định cụ thể của Ixraen về an ninh mạng

- Bảo đảm sự toàn vẹn và bất khả xâm phạm của dữ liệu: Luật về quyền riêng tư (năm 1981) quy định các biện pháp bảo đảm và bảo vệ dữ liệu khỏi việc sử dụng hoặc sao chép bất hợp pháp. Pháp lệnh về sở hữu dữ liệu (năm 1986) quy định rõ các biện pháp vật lý, hành chính hoặc kỹ thuật để bảo đảm sự toàn vẹn của dữ liệu (ví dụ như quy định công chức quản lý những dữ liệu mật, nhạy cảm của chính phủ phải đổi mật khẩu 6 tháng một lần). Để đáp ứng nhu cầu bảo vệ dữ liệu ngày càng tăng trong bối cảnh khoa học - công nghệ phát triển vượt bậc, Quốc hội Ixraen đã giới thiệu Pháp lệnh về an ninh thông tin (ban hành tháng 3

năm 2017, có hiệu lực từ tháng 3 năm 2018), trong đó quy định người quản lý dữ liệu mật, nhạy cảm phải thực thi nhiều biện pháp như: xây dựng danh mục và bản đồ (mapping) dữ liệu; dữ liệu phải đặt ở nơi an toàn; phân công chuyên viên chuyên trách bảo vệ an ninh dữ liệu; xây dựng quy trình an ninh dữ liệu; phân cấp, phân quyền cụ thể trên cơ sở trách nhiệm và công việc; tách hệ thống có dữ liệu mật ra khỏi hệ thống có dữ liệu thông thường, dữ liệu mật và nhạy cảm truyền trên Internet phải được mã hóa (*encrypted*), nếu thuê ngoài (*outsourcing*) thì phải thẩm tra kỹ lưỡng nhân thân của các tổ chức, cá nhân được thuê; đánh giá định kỳ về mức độ an toàn của dữ liệu và tập huấn cho chuyên viên, có hệ thống sao lưu và khôi phục dữ liệu, có hệ thống cảnh báo tự động tới các cơ quan có liên quan trong trường hợp dữ liệu bị xâm phạm,... Ngoài ra, đối với các dữ liệu tối mật, có độ rủi ro cao, người quản lý phải có đánh giá nguy cơ (*risk assessment*) định kỳ 18 tháng, kiểm tra mức độ thâm nhập (*penetration test*) định kỳ 18 tháng, hàng quý rà soát lại các sự kiện về an ninh (*security incidents*), trên cơ sở đó sửa đổi, bổ sung quy trình an ninh dữ liệu. Pháp lệnh này được giới chuyên gia đánh giá là văn bản toàn diện và có hệ thống nhất cho đến nay của Ixraen trong lĩnh vực bảo vệ dữ liệu[1].

---

1. Haim Ravia & Dotan Hammer: *Dramatic Overhaul of Israeli Data Security Regulations,* Huntons & William, 5/2017.

- Bảo vệ an ninh mạng đối với các cơ sở hạ tầng quan trọng: Luật an ninh đối với các cơ quan công (năm 2002) liệt kê danh sách các cơ quan công quyền và cơ sở hạ tầng quan trọng (như điện lực, đường sắt, sân bay, viễn thông), theo đó NCB có nghĩa vụ ban hành quy trình và văn bản hướng dẫn bảo vệ an ninh mạng đối với hệ thống mạng của các cơ sở trên.

- Phòng chống tội phạm mạng: Luật máy tính quy định cụ thể các biện pháp phòng, chống đột nhập máy tính phi pháp (*hacking*), tấn công từ chối dịch vụ (DoS), gian lận email (*phishing*), tấn công mã độc (*malware*), ăn cắp dữ liệu cá nhân (*identity theft*), ăn cắp điện tử (*electronic theft*). Người vi phạm các tội trên có thể bị phạt tù 3 - 5 năm và phạt tiền tới 226.000 NIS (tương đương khoảng 65.000 USD).

Theo đánh giá của các chuyên gia, tuy chưa có luật riêng về an ninh mạng, nhưng các quy định của Ixraen về an ninh mạng hiện đạt mức trung bình khá so với thế giới[1]. Các quy định về quyền riêng tư có tiêu chuẩn ở mức cao, trong khi các quy định về bảo vệ dữ liệu còn lỗi thời và thiếu cập nhật (cho đến khi Pháp lệnh về an ninh thông tin năm 2017 ra đời). Ngoài các quy định, luật lệ hiện hành về an ninh mạng, Viện Tiêu chuẩn Ixraen cũng ban hành một số tiêu chuẩn về an ninh (không bắt buộc, nhưng khuyến khích áp

---

1. Alan Charles Raul: *The Privacy, Data Protection and Cyber Security Law Review* (2nd Edition), Law Business Research, 11/2015.

dụng, nhất là đối với các cơ quan công quyền), bao gồm SI ISO 27001, SI ISO 27799, SI ISO 15408 và SII 1495.

Bộ máy thực thi an ninh mạng của Ixraen

Chính phủ Ixraen với sự tham mưu của các cơ quan chức năng chịu trách nhiệm ban hành chính sách, chiến lược và bảo đảm an ninh mạng quốc gia; thu hút các tập đoàn quốc tế trong lĩnh vực an ninh mạng đầu tư, xây dựng các trung tâm, cơ sở nghiên cứu an ninh mạng tại Ixraen nhằm mục đích đưa quốc gia này trở thành một trong 5 nước dẫn đầu thế giới về lĩnh vực an ninh mạng. Các cơ quan chịu trách nhiệm chính trong quản lý nhà nước về an ninh mạng của Ixraen gồm:

(i) Cơ quan An ninh thông tin quốc gia (*National Information Security Agency* - NISA) thuộc Bộ An ninh (Shin Bet) được thành lập năm 2002: Là cơ quan trụ cột của Ixraen trong vấn đề an ninh mạng, có vai trò hoạch định, tham mưu và đề xuất chính sách an ninh mạng, cũng như giám sát việc thực thi chính sách ở các cơ quan trọng yếu của Chính phủ, các cơ quan quốc phòng, an ninh, cơ sở hạ tầng trọng yếu như điện lực, giao thông.

(ii) Cục An ninh mạng quốc gia (*National Cyber Bureau* - NCB) được thành lập năm 2011, trực thuộc Văn phòng Thủ tướng: Là cơ quan chủ trì, chịu trách nhiệm trước Chính phủ về việc thực hiện nhiệm vụ có tính chiến lược trong quản lý nhà nước về an ninh mạng; tham mưu cho Thủ tướng ban hành chính sách an ninh mạng quốc gia, đặc biệt trong lĩnh vực phòng thủ mạng và xây dựng sức mạnh

quốc gia trong lĩnh vực không gian mạng; làm đầu mối phối hợp với các bộ, ngành, doanh nghiệp, viện nghiên cứu trong lĩnh vực an ninh mạng nhằm tăng cường bảo vệ các cơ sở hạ tầng quốc gia từ tấn công mạng và khuyến khích sự tiến bộ của các chủ thể trong các lĩnh vực công nghiệp số, hướng tới đưa Ixraen trở thành quốc gia dẫn đầu trong lĩnh vực không gian mạng. Các nhiệm vụ cụ thể của NCB:

- Tham mưu cho thủ tướng, Chính phủ và các ủy ban nhà nước về những vấn đề liên quan đến không gian mạng.

- Củng cố, tăng cường công tác bảo đảm an ninh mạng hệ thống máy tính của Chính phủ và các ủy ban nhà nước; theo dõi việc thực hiện các quyết định về an ninh mạng của Chính phủ.

- Bảo đảm an ninh mạng đối với hệ thống thông tin của các cơ sở hạ tầng trọng yếu.

- Thúc đẩy sự phối hợp và hợp tác giữa các cơ quan chính phủ, cộng đồng quốc phòng, các viện nghiên cứu, các doanh nghiệp và các cơ quan khác có liên quan đến lĩnh vực mạng.

- Thúc đẩy pháp luật và các quy định về an ninh mạng.

- Thúc đẩy và nâng cao nhận thức của công chúng về các mối đe dọa trong không gian mạng; cảnh báo và xây dựng cơ chế, giải pháp đối phó.

- Thúc đẩy nghiên cứu và phát triển trong lĩnh vực an ninh mạng.

- Thực hiện hợp tác quốc tế về an ninh mạng.

Hiện NCB có khoảng hơn 100 nhân viên, ngân sách hằng năm tuy không công bố, nhưng ước tính tương đương khoảng 40 triệu USD. Những năm vừa qua, NCB đã tham mưu cho Chính phủ Ixraen đầu tư và thu hút đầu tư nước ngoài cho lĩnh vực an ninh mạng với quyết tâm trở thành một trong 5 cường quốc hàng đầu về không gian mạng. Theo đó, số vốn đầu tư liên doanh cho lĩnh vực này đã tăng gấp 4 lần từ năm 2010[1].

(iii) Cơ quan Phòng vệ mạng quốc gia (*National Cyber Defense Authority* - NCDA hay còn gọi là *National Cyber Security Authority* - NCSA) được thành lập năm 2015, trực thuộc Văn phòng Thủ tướng. Đây là cơ quan chuyên trách trong lĩnh vực bảo vệ không gian mạng dân sự, bao gồm bảo vệ an ninh mạng đối với các dịch vụ công ích, công trình công cộng cũng như các thực thể dân sự với mục đích nâng cao sức mạnh của không gian mạng dân sự Ixraen.

Đơn vị mạnh nhất của NCDA là Đội ứng cứu khẩn cấp máy tính Ixraen (*Ixraen National Cyber Event Readiness Team* - IL-CERT), có nhiệm vụ quản lý các sự kiện an ninh mạng quốc gia, chia sẻ thông tin tình báo về an ninh mạng với các đối tác, phát triển các hành vi an ninh mạng tối ưu, thúc đẩy nhận thức về an ninh mạng trong các tổ chức, cá nhân, và là đầu mối duy nhất của Ixraen trong việc tiếp

---

1. Daniel Shkedi: "The Cybersecurity Sector in Israel", Embassy of India in Israel, 2015.

nhận các thông báo, đe dọa về an ninh mạng từ các tổ chức trong nước và quốc tế, các công ty an ninh mạng và các đội ứng cứu khẩn cấp máy tính ở các quốc gia khác. IL-CERT hiện là thành viên của Diễn đàn các đội an ninh và ứng cứu khẩn cấp (FIRST), tổ chức lớn nhất thế giới trong lĩnh vực chia sẻ thông tin, đánh giá rủi ro và ứng cứu khẩn cấp về an ninh mạng[1].

(iv) Cơ quan Luật pháp, Thông tin và Kỹ thuật Ixraen (*The Israel Law, Information and Technology Authority* - ILITA) trực thuộc Bộ Tư pháp là cơ quan đầu mối chịu trách nhiệm bảo vệ an ninh mạng trong công tác hộ tịch, tín dụng, chữ ký điện tử.

(v) Lực lượng An ninh mạng của quân đội: Về mặt chính thức, Quân đội Ixraen (*Ixraen Defense Forces* - IDF) không có trung tâm chỉ huy hay đơn vị chuyên trách an ninh mạng cấp cục/vụ trực thuộc. Mảng phản gián an ninh mạng, xây dựng và bảo vệ mạng máy tính thuộc về Cục Viễn thông (D4I), trong khi các mảng an ninh, tình báo mạng khác thuộc trách nhiệm của Cục Tình báo. Tháng 12/2016, Tổng Tham mưu trưởng IDF công bố kế hoạch thành lập một trung tâm tác chiến mạng với mục tiêu thống nhất các đơn vị chiến tranh mạng, bao gồm tấn công và phòng thủ, trong hai năm tới nhằm đối phó với những

---

1. FIRST hiện có 396 thành viên, riêng Ixraen có tới ba tổ chức là thành viên, trong khi Việt Nam không có thành viên nào.

thách thức nghiêm trọng mà IDF gặp phải trong không gian mạng[1]. Tuy nhiên, đến nay tiến độ triển khai kế hoạch trên vẫn chưa được tiết lộ.

Tuy IDF không có trung tâm chỉ huy về an ninh mạng, nhưng nghiên cứu của Trung tâm Hợp tác phòng thủ mạng NATO (CCDCOE) và một số tổ chức khác cho thấy, trong biên chế của IDF có nhiều đơn vị tác chiến rất mạnh về chiến tranh và phòng thủ mạng. Nổi tiếng nhất trong số đó là Đơn vị 8200, lực lượng lớn nhất trong số các đơn vị của IDF với hàng nghìn binh sĩ và được đánh giá là một trong những cơ quan tình báo mạng xuất sắc nhất thế giới, cùng với Cơ quan An ninh quốc gia Mỹ (NSA) và Sở chỉ huy thông tin của Chính phủ Anh (GCHQ)[2]. Nhiệm vụ bề nổi của Đơn vị 8200 là mã thám và thu thập thông tin tình báo mạng (theo giới chuyên gia, số lượng tin tức tình báo của Đơn vị 8200 chiếm tới hơn một nửa thông tin của cộng đồng tình báo Ixraen). Tuy nhiên, trên thực tế, Đơn vị 8200 còn là đại bản doanh của một trong những đội quân hacker tinh nhuệ nhất thế giới. Năm 2011, Đơn vị 8200 đã phối hợp với NSA sử dụng mã độc Stuxnet tấn công hệ thống điều khiển, gây đình trệ hoạt động, phá hủy hàng nghìn

---

1. Anna Ahronheim: "IDF decides not to have a cyber command department", *The Jerusalem Post,* 01/01/2017.

2. John Reed: "Unit 8200: Israel's cyber spy agency, Former insiders and whistle-blowers provide a view of the formidable military intelligence outfit", *Financial Times,* 10/7/2015.

máy làm giàu uranium của Nhà máy điện hạt nhân Busher tại Iran, 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 ngày 12/11/2011 làm 17 chuyên gia, trong đó có thiếu tướng Hassan Moghaddam, thiệt mạng.

Mối quan hệ giữa an ninh mạng với hệ sinh thái khởi nghiệp

Ixraen là quốc gia có hệ sinh thái khởi nghiệp phát triển nhất thế giới, xuất phát từ nhiều nguyên nhân đặc thù: tinh thần dân tộc rất cao, môi trường quân ngũ tạo sự gắn bó mọi công dân, giáo dục khuyến khích sáng tạo, sự hậu thuẫn to lớn của cộng đồng Do Thái trên thế giới, chính phủ khuyến khích sự khởi nghiệp trong khu vực tư nhân,... Nhiều người đánh giá Ixraen là "Quốc gia khởi nghiệp" và mặc dù có diện tích nhỏ hơn cả bang New Jersey và dân số ít hơn thành phố New York của Mỹ, song Ixraen là "nhà" của nhiều công ty có chân trên sàn giao dịch chứng khoán Mỹ NASDAQ hơn bất cứ quốc gia nào, ngoại trừ Mỹ và Trung Quốc.

Một đặc điểm quan trọng trong sự phát triển ngành công nghiệp an ninh mạng Ixraen là sự hợp tác công tư chặt chẽ với ba thành tố cơ bản của hệ sinh thái khởi nghiệp: chính phủ, doanh nghiệp và cơ sở giáo dục đào tạo. Chính phủ Ixraen rất quan tâm việc phát triển các giải pháp an

ninh mạng từ các công ty tư nhân. Chính phủ đã triển khai chương trình KIDMA 1.0 (năm 2012) và KIDMA 2.0 (năm 2015) để cấp kinh phí cho các công ty mạng của Ixraen trong việc xây dựng giải pháp toàn diện hỗ trợ tích hợp, bảo đảm những nhu cầu của khách hàng về an ninh mạng với tổng số vốn lên tới hơn 50 triệu USD. CNB đang triển khai kế hoạch giúp bốn thành phố lớn nhất của Ixraen trở thành các thành phố mạng; kết hợp các đơn vị quân đội với các doanh nghiệp để nghiên cứu và phát triển giải pháp an ninh mạng; tài trợ cho nhiều doanh nghiệp áp dụng giải pháp server (máy chủ), tiến hành xây dựng hệ sinh thái server hiệu quả.

Ngày 26/6/2017, phát biểu tại Cyber Week - hội nghị về an ninh mạng hàng đầu thế giới với sự tham dự của khoảng 7.000 đại biểu đến từ hơn 50 nước, Thủ tướng Ixraen Benjamin Netanyahu khẳng định: an ninh mạng "vừa là nguy cơ, vừa là ngành kinh doanh nghiêm túc đối với Ixraen". Ixraen là một trong 10 nước hứng chịu nhiều cuộc tấn công mạng nhất thế giới, nhưng vấn đề an ninh mạng cũng giúp nhiều doanh nghiệp công nghệ thông tin phát triển mạnh. Ngành công nghiệp an ninh mạng Ixraen chiếm tới 10% thị phần toàn cầu với doanh thu đạt 77 tỷ USD năm 2017 và 13% ngân sách hoạt động R&D trong lĩnh vực này. Ixraen hiện có khoảng 600-700 startup (công ty khởi nghiệp) về an ninh mạng; thu hút khoảng 20% trong tổng đầu tư tư nhân vào an ninh mạng trên phạm vi toàn

cầu. Ông Netanyahu đánh giá khối doanh nghiệp tư nhân là một trong những yếu tố giúp đưa Ixraen lên vị trí một trong 5 quốc gia hàng đầu thế giới trong lĩnh vực an ninh mạng[1].

Thành tố thứ hai trong hệ sinh thái khởi nghiệp Ixraen là sức mạnh của cộng đồng doanh nghiệp. Có đến 36 công ty Ixraen nằm trong danh sách 500 công ty an ninh mạng nóng nhất và sáng tạo nhất thế giới của Cybersecurity Ventures, với nhiều tên tuổi nổi tiếng trong ngành công nghiệp an ninh mạng như CyberArc (xếp thứ 12), Check Point (xếp thứ 35), Checkmarx (xếp thứ 37). Trong số 65 startups mới được thành lập vào năm 2016, 25 startup trong số đó đã thành công trong vòng huy động vốn Series A hoặc vòng đầu tư hạt giống, với mức đầu tư trung bình là 1,6 triệu USD. Nhiều công ty an ninh mạng của Ixraen được niêm yết trên sàn chứng khoán NASDAQ. Ixraen có trên 20 trung tâm R&D quốc tế tập trung vào lĩnh vực an ninh mạng. Nổi tiếng là nước xuất khẩu công nghệ an ninh mạng lớn thứ hai trên thế giới chỉ sau Mỹ, Ixraen đóng vai trò then chốt trong ngành công nghiệp này. Xuất phát từ nhu cầu liên quan đến quốc phòng và định hướng xuất khẩu, các giải pháp an ninh mạng của Ixraen nổi bật và khác biệt so với các đối thủ cạnh tranh trên thị trường.

---

1. Toàn văn phát biểu của Thủ tướng Ixraen Netanyahu có thể tham khảo tại Website chính thức của Cyber Week tại https://cyberweek.tau.ac.il.

Tuy nhiên, thành tố quan trọng nhất của hệ sinh thái khởi nghiệp trong lĩnh vực an ninh mạng của Ixraen lại không phải là Chính phủ hay cộng đồng doanh nghiệp, mà là cơ sở giáo dục đào tạo. Ixraen rất chú trọng vấn đề công nghệ thông tin nói chung và an ninh mạng nói riêng từ các cấp học phổ thông. Trong số các môn thi tự chọn, học sinh bậc trung học phổ thông được khuyến khích chọn thi về an ninh mạng. Một số trường đại học thành lập chuyên khoa hoặc trung tâm nghiên cứu an ninh mạng và nhiều trường khác nghiên cứu, giảng dạy những lĩnh vực liên quan an minh mạng ở nhiều khoa khác nhau. IDF luôn quan tâm tới việc thu hút nhân tài máy tính ngay từ cấp phổ thông và đưa ra những gói hợp đồng hấp dẫn để đón nhân tài về IDF ngay sau khi rời trường. Từ năm 2011, IDF khởi động chương trình Magshimim nhằm thu hút hàng nghìn học sinh phổ thông tham gia vào các đơn vị an ninh và tình báo mạng quân đội, chủ yếu là Đơn vị 8200.

Đã có nhiều quốc gia tuyển dụng nhân tài máy tính trực tiếp từ nhà trường vào quân đội, nhưng Ixraen là một trong những nước có chương trình đào tạo, tuyển dụng lớn và tập trung nhất. Một phần của việc đầu tư này là do đất nước Ixraen luôn nằm trong tình trạng bị đe dọa bởi chiến tranh, cả trên chiến trường thực tế lẫn chiến trường ảo. Chương trình Magshimim được giới lãnh đạo Ixraen ủng hộ do liên quan chặt chẽ đến an ninh quốc gia cũng như giúp thúc đẩy năng lực của các công ty an ninh mạng. Theo luật Ixraen,

thanh niên 18 tuổi phải thi hành nghĩa vụ quân sự bốn năm với Đơn vị 8200 và sau khi rời khỏi tổ chức thì họ có được kinh nghiệm về an ninh mạng nhiều hơn người cùng tuổi tại các quốc gia khác. Theo đánh giá của FORBES (Mỹ), hơn 1.000 công ty được thành lập bởi các cựu quân nhân từ Đơn vị 8200 - từ Waze đến Check Point và Mirabilis, công ty mẹ của ICQ. Điều này lý giải cho việc những tập đoàn công nghệ khổng lồ mong muốn mua lại những công ty xuất thân từ Đơn vị 8200. Trong hai năm 2015-2016, Microsoft đã mua Adallom (Công ty quản lý an ninh dữ liệu cá nhân) với giá 320 triệu USD; Facebook mua lại Công ty phân tích di động Onavo với khoảng 150 triệu USD; và PayPal thôn tính CyActive (Công ty dự đoán hoạt động xâm nhập máy tính trái phép) với khoảng 60 triệu USD. Ý tưởng khuyến khích giới trẻ gia nhập thế giới tình báo và sau đó rời khỏi đó để thành lập công ty an ninh riêng của Ixraen đã được một số nước học tập, nhưng chưa thành công do hệ sinh thái khởi nghiệp đặc trưng của Ixraen không dễ bắt chước. Thêm vào đó, Ixraen là nơi tập trung đông đảo các công ty khởi nghiệp, nhà khoa học tài giỏi và chuyên gia công nghệ dày dạn kinh nghiệm hơn bất cứ quốc gia nào khác trên thế giới.

7. Các nước Đông Nam Á

Khu vực Đông Nam Á là khu vực có số lượng người sử dụng Internet đông thứ tư thế giới cùng với số lượng người

sử dụng điện thoại thông minh cũng tăng nhanh chóng[1]. Tuy nhiên hệ thống luật bảo vệ dữ liệu chưa phát triển và chưa áp dụng triệt để các kinh nghiệm hữu ích trên thế giới khiến khu vực Đông Nam Á trở nên dễ bị tổn thương trước các cuộc tấn công mạng.

Trong những năm qua, nhận thức của các nước Đông Nam Á về không gian mạng cũng như nhu cầu bảo đảm an ninh mạng không ngừng gia tăng, từ việc công nhận vai trò của không gian mạng đến việc triển khai các kế hoạch và sáng kiến hành động cụ thể. Sự chuyển biến này bắt nguồn từ thực tế Internet đang ngày càng phát triển và đóng vai trò quan trọng trong sự phát triển kinh tế, xã hội của từng quốc gia trong khu vực.

Inđônêxia

Inđônêxia là quốc gia có số lượng người dùng Internet lớn nhất khu vực Đông Nam Á và cũng là quốc gia chưa có nhiều quy định pháp lý về an ninh mạng và không gian mạng. Hiện nay, Inđônêxia có Luật giao dịch điện tử và thông tin (năm 2016). Luật bảo vệ dữ liệu cá nhân đang được xây dựng và dự kiến sẽ được thảo luận thông qua tại Quốc hội trong năm 2019. Ngoài ra, Bộ Thông tin và Truyền thông của Inđônêxia đang là cơ quan chịu trách nhiệm quản lý, xử lý đối với những tin tức độc hại, tin giả

---

1. Https://www.huffingtonpost.com/asiatoday/southeast-asia-begins-to_b_14334812.html.

liên quan đến vấn đề chính trị, bạo lực cực đoan. Ngoài ra, Tổng thống Inđônêxia mới ban hành văn bản về việc thành lập Cơ quan quốc gia về an ninh mạng và mã hóa (BSSN).

Lào

Năm 2015, Lào thông qua Luật phòng chống tội phạm mạng, theo đó áp dụng, thắt chặt các biện pháp quản lý Internet. Luật này cấm việc đăng và truyền tải những nội dung không phù hợp/tin giả chống lại Đảng Nhân dân Cách mạng Lào, phá hoại hòa bình và sự độc lập, chủ quyền, sự thống nhất và thịnh vượng của Lào. Luật này cũng quản lý, ngăn chặn các thông tin độc hại có nội dung khuyến khích người dân Lào tham gia khủng bố, giết người và các hoạt động bạo động xã hội. Năm 2017, Lào cũng thông qua Luật bảo vệ dữ liệu nhằm bảo đảm an toàn cho dữ liệu điện tử của người dùng một cách toàn diện.

Malaixia

Malaixia là một trong những nước đầu tiên xây dựng chính sách quản lý việc sử dụng Internet bao gồm các chính sách về an ninh mạng. Năm 1997, Malaixia ban hành Luật tội phạm máy tính và đến năm 1998, nước này ban hành Luật truyền thông và đa phương tiện. Năm 2010, Malaixia ban hành Luật bảo vệ dự liệu cá nhân. Tuy nhiên, luật này lại chỉ áp dụng đối với khu vực tư nhân trong thu thập dữ liệu. Năm 2016, Malaixia ban hành Chính sách An ninh mạng quốc gia, theo đó đưa ra nội hàm/định nghĩa về Hạ tầng thông tin chủ chốt quốc gia (CNII). Năm 2017,

Malaixia xây dựng Luật an ninh mạng, cơ sở pháp lý cho hoạt động của Cơ quan quốc gia về an ninh mạng của (NCSA). Malaixia cũng là nước đầu tiên trong ASEAN xây dựng quy định quản lý mạng xã hội thông qua việc ban hành Luật chống tin giả năm 2018. Tuy nhiên, Chính phủ mới của nước này đã bãi bỏ luật này do có nội dung hạn chế quyền tự do ngôn luận của người dân.

Brunây - Campuchia - Mianma - Timo Lexte

Brunây: hiện vẫn áp dụng các luật đã có từ trước như Luật cấm nói xấu Hoàng gia được thông qua năm 1948 (sửa đổi năm 2005). Luật này hiện được áp dụng trong việc quản lý lĩnh vực truyền thông và Internet. Năm 2014, Hoàng gia Brunây ban hành Hướng dẫn về bảo vệ dữ liệu cá nhân.

Campuchia: Hiện nay, Campuchia không có các quy định về bảo vệ dữ liệu cá nhân mặc dù năm 2016, Chính phủ nước này thông báo sẽ xây dựng dự luật về vấn đề này. Tương tự Brunây, Campuchia vẫn áp dụng Luật cấm nói xấu, bình luận không hay về Hoàng gia và Chính phủ trong quản lý sử dụng Internet. Năm 2015, Chính phủ nước này đã trình Quốc hội Dự thảo Luật an ninh mạng nhưng đến nay vẫn chưa được thông qua.

Mianma: hiện đang trong quá trình xây dựng cơ sở hạ tầng viễn thông. Năm 2017, Mianma cải tổ Luật Thông tin truyền thông năm 2013 nhằm quản lý Internet và ban hành Luật bảo vệ quyền riêng tư và an ninh của người dân (tháng 5/2017).

Timo Lexte: hiện đang trong quá trình xây dựng cơ sở hạ tầng viễn thông và chỉ có duy nhất Luật Thông tin truyền thông năm 2012 là liên quan đến quản lý Internet.

Philíppin

Luật về thương mại (*Republic Act 8972*) được ban hành năm 2000 nhằm đối phó với mối đe dọa tội phạm mạng, là quy định đầu tiên của Philíppin trong việc quản lý Internet. Năm 2012, Philíppin ban hành Luật phòng, chống tội phạm mạng (Republic Act 10175). Tuy nhiên, Tòa án tối cao nước này đã ban hành lệnh bãi bỏ thực thi luật này do có những nội dung đi ngược lại với việc bảo đảm quyền tự do ngôn luận, phát biểu ý kiến. Cũng trong năm 2012, Philíppin ban hành Luật dữ liệu riêng tư (Republic Act 101073/2012). Năm 2017, Philíppin ban hành Kế hoạch An ninh mạng quốc gia đến năm 2022, theo đó đưa ra phạm vi, định nghĩa về hạ tầng thông tin chủ chốt (CII). Tuy nhiên, kế hoạch này hiện chưa được Quốc hội và Chính phủ Philíppin thông qua. Ngoài ra, Philíppin cũng đang thảo luận về Dự luật quản lý mạng xã hội, theo đó các công ty mạng xã hội bắt buộc phải xác thực người dùng trước khi cung cấp tài khoản đăng ký. Điều này sẽ giúp ngăn chặn việc tạo các tài khoản giả và phổ biến thông tin giả.

Xingapo

Xingapo là nước đi đầu trong khu vực về an ninh mạng. Xingapo có đầy đủ hệ thống pháp lý về an ninh mạng. Cụ thể như Luật quản lý và phát triển thông tin truyền thông năm 2016, Luật phát sóng, Luật giao dịch điện tử, Luật

thông tin và xuất bản báo chí, Luật dịch vụ bưu diện và Luật thông tin truyền thông. Ngoài ra, Xingapo cũng ban hành Luật kiểm soát thư rác và Luật bảo vệ dữ liệu cá nhân. Tháng 2 năm 2018, Xingapo ban hành Luật an ninh mạng, chính thức có định nghĩa và phạm vi về hạ tầng thông tin chủ chốt (CII). Trước đó, năm 2016, Xingapo khởi động Chiến lược an ninh quốc gia về an ninh mạng, kéo theo việc ra đời Cơ quan chuyên trách về an ninh mạng (CSA) của nước này.

Thái Lan

Giống như các nước ASEAN, Thái Lan vẫn áp dụng quy định của mình vào việc quản lý người dùng Internet, đặc biệt đối với những bình luận không chuẩn mực liên quan đến Hoàng gia. Năm 2007, Thái Lan ban hành Luật tội phạm máy tính (Computer Crime Act) và luật này sau đó được sửa đổi, bổ sung thành Luật tội phạm mạng (Cyber Crime Law) vào năm 2016. Luật này trao quyền lớn hơn cho Chính phủ trong việc giới hạn quyền tự do ngôn luận và có quyền can thiệp vào quyền riêng tư của những người dùng Internet.

Năm 2018, Chính phủ Thái Lan đã đệ trình lên Quốc hội bốn dự luật liên quan đến không gian mạng bao gồm Luật an ninh mạng, Luật bảo vệ dữ liệu, Luật giao dịch điện tử và việc thành lập Cơ quan Phát triển giao dịch điện tử (ETDA). Ngày 29/02/2019, Hội đồng Lập pháp quốc gia Thái Lan (NLA) thông báo, cơ quan này đã thông qua Luật

an ninh mạng với 133 phiếu thuận và 16 phiếu trắng[1]. Theo đó, Luật này cho phép các cơ quan chức năng của Thái Lan bỏ qua các lệnh của tòa án trong các tình huống quan trọng va thành lập Ủy ban An ninh mạng quốc gia, do Thủ tướng Chính phủ chủ trì, để soạn thảo chính sách và kế hoạch hành động nhằm củng cố an ninh mạng. Ngoài ra, Thái Lan sẽ thành lập Ủy ban Giám sát an ninh mạng, do Bộ trưởng phụ trách kinh tế kỹ thuật số và xã hội điều hành. Người đứng đầu Ủy ban An ninh mạng quốc gia được phép tìm kiếm, tịch thu hệ thống máy tính mà không cần lệnh của tòa án để đối phó với các mối đe dọa về an ninh mạng. Tòa án và các bên liên quan sau đó có thể sẽ được thông báo về những hành động như vậy.

Bên cạnh các dự luật nêu trên, Thái Lan còn đang trong quá trình xây dựng Chiến lược an ninh quốc gia về an ninh mạng, bao gồm việc thành lập Cơ quan chuyên trách về an ninh mạng.

II. TÌNH HÌNH HỢP TÁC VỀ AN NINH MẠNG GIỮA CÁC QUỐC GIA TRÊN THẾ GIỚI

1. Hợp tác Mỹ - Trung Quốc

Hợp tác Mỹ - Trung Quốc trong lĩnh vực không gian

---

1. "Thái Lan thông qua Luật An ninh mạng", xem https://www.nhandan.com.vn/thegioi/tin-tuc/item/39345202-thai-lan-thong-qua-luat-an-ninh-mang.html.

mạng nằm trong tổng thể của quan hệ Mỹ - Trung Quốc, do vậy mức độ và phạm vi hợp tác trong lĩnh vực này cũng nằm trong tổng thể xu hướng phát triển của quan hệ Mỹ - Trung Quốc. Hiện nay, quan hệ Mỹ - Trung Quốc vẫn đang tiếp tục xu hướng vừa hợp tác vừa đấu tranh với việc thiết lập hàng loạt các cơ chế làm việc ở các cấp trong các lĩnh vực khác nhau của quan hệ song phương. Đối với vấn đề an ninh mạng, nền tảng cho hợp tác giữa hai nước là việc ký kết Hiệp định An ninh mạng năm 2015. Theo đó, hai nước cam kết sẽ không tiến hành hoạt động gián điệp kinh tế do chính phủ tài trợ trong không gian mạng nhằm ngăn chặn gián điệp mạng giữa hai quốc gia, đặc biệt là việc đánh cắp quyền sở hữu trí tuệ và bí mật thương mại.

Hiệp định về an ninh mạng giữa Mỹ và Trung Quốc nhằm xoa dịu căng thẳng giữa hai bên sau vụ Snowden và các cáo buộc về gián điệp mạng. Đặc biệt, vụ Snowden đã khiến quan hệ Mỹ - Trung trở nên căng thẳng. Các tài liệu do Snowden cung cấp cho thấy Mỹ đã tấn công mạng Trung Quốc và Hồng Kông từ năm 2009.

Theo hiệp định, Mỹ và Trung Quốc "sẽ hành động kịp thời trong trường hợp cần thông tin và hỗ trợ liên quan đến các hoạt động không gian mạng, không tiến hành hoặc hỗ trợ các hành vi đánh cắp thông tin trên mạng, tiến hành các biện pháp nhằm xác định và thúc đẩy các chuẩn mực phù hợp về hành vi của nhà nước trong không gian mạng và thiết lập cơ chế đối thoại cấp cao về chống lại tội phạm mạng và các vấn đề liên quan".

Việc triển khai hiệp định này diễn ra tương đối chậm, thậm chí việc thiết lập các địa chỉ email tạm thời phải mất vài tháng sau khi hai nước ký hiệp định. Chính phủ đồng ý sẽ không tiến hành hoặc hỗ trợ hoạt động gián điệp qua mạng có động cơ kinh tế và tăng cường trao đổi, hợp tác trong việc chống lại tội phạm mạng.

Các kết quả đã đạt được

Mặc dù còn nhiều nghi ngại, nhưng hiệp định đã góp phần tuyên truyền về vấn đề gián điệp mạng. Mỹ và Trung Quốc đã thiết lập "đường dây nóng" tiếp xúc trong trường hợp khẩn cấp và sẽ tổ chức cuộc họp quan chức cấp cao hai nước sáu tháng một lần để thảo luận về tình hình triển khai hợp tác trên không gian mạng. Trong khi việc triển khai đường dây nóng không mấy hiệu quả thì trọng tâm kinh tế của hiệp định đã tạo nền tảng chung để tiến hành hợp tác. Hai bên cũng đã tổ chức các cuộc họp chung về an toàn hệ thống mạng và việc lạm dụng công nghệ để tiến hành các hoạt động khủng bố.

Một số thống kê cho thấy các vụ việc hacker Trung Quốc tấn công mạng của các công ty Mỹ đã giảm hơn 90% trong hơn một năm rưỡi kể từ khi hiệp định được ký kết, góp phần làm giảm các vụ ăn cắp quyền sở hữu trí tuệ và bí mật thương mại. Tuy nhiên, hoạt động gián điệp nhằm vào các mục tiêu của Chính phủ Mỹ vẫn tiếp tục. Điều này được giải thích là do hiệp định chủ yếu tập trung hạn chế hoạt động gián điệp qua mạng trong lĩnh vực kinh tế. Việc giảm số lượng các vụ ăn cắp bản quyền và các bí mật kinh

doanh giúp giảm bớt căng thẳng giữa hai nước liên quan đến gián điệp kinh tế.

Một số hạn chế trong hiệp định giữa Mỹ và Trung Quốc về vấn đề an ninh mạng

Hiện rất khó đánh giá hiệp định này ảnh hưởng như thế nào đến quan hệ Mỹ - Trung Quốc, đặc biệt trong việc cung cấp nền tảng để thảo luận và giải quyết các khác biệt về chính sách. Hiệp định này cũng không loại trừ nhu cầu tăng cường các nỗ lực an ninh mạng của Mỹ vì bất kỳ sự hiểu lầm nào cũng có thể đe dọa quan hệ song phương. Cho nên, còn quá sớm để nói liệu hiệp định có ảnh hưởng lớn đến quan hệ Mỹ - Trung Quốc hay không.

Một câu hỏi đặt ra là các cuộc tấn công mạng đã thực sự giảm xuống hay chúng đã trở nên tinh vi và khó nắm bắt hơn. Tấn công mạng dường như đang gia tăng tại các quốc gia khác và trong khi số lượng các cuộc tấn công mạng từ Trung Quốc đã giảm, các cuộc tấn công này có thể được tiến hành từ bên ngoài lãnh thổ Trung Quốc. Do khó có thể chứng minh được đối tượng đứng đằng sau các cuộc tấn công này nên đây sẽ là một thách thức mới trong việc ứng phó với vấn đề tấn công mạng.

Việc các hiệp định liên quan đến an ninh mạng giữa Mỹ và Trung Quốc được ký kết cho thấy cơ hội giải quyết các vấn đề trong quan hệ song phương, tuy nhiên hai bên vẫn cần tiếp tục nỗ lực hơn do còn tồn tại nhiều vấn đề trong quan hệ hai nước.

Trong khi chính quyền mới của Mỹ còn chậm đưa ra các chính sách nhằm ứng phó với vấn đề an ninh không gian mạng thì thỏa thuận an ninh mạng gần đây giữa Trung Quốc và Ôxtrâylia rất đáng chú ý. Thỏa thuận này gần giống với hiệp định về an ninh mạng giữa Mỹ - Trung Quốc và tập trung vào việc chính phủ hai nước cam kết không hỗ trợ hành vi trộm cắp thông tin qua mạng và quyền sở hữu trí tuệ, đồng thời đồng ý thiết lập các cơ chế để thảo luận về vấn đề tội phạm mạng. Trung Quốc và Ôxtrâylia cũng đồng ý ứng xử phù hợp với các quy chuẩn được đưa ra bởi UN GGE.

Hiệp định về an ninh mạng giữa Mỹ và Trung Quốc, nếu được duy trì, có thể là một mô hình cho các hiệp định thỏa thuận song phương khác nhằm giảm thiểu hoạt động gián điệp kinh tế và các vấn đề liên quan đến không gian mạng khác. Điều này mở ra khả năng ký kết các hiệp định song phương trong tương lai nếu có một mô hình mẫu để xem xét và áp dụng.

Cạnh tranh trong quan hệ Mỹ - Trung Quốc về lĩnh vực an ninh mạng kể từ nửa cuối năm 2018

Như đã được đề cập, hợp tác trong lĩnh vực an ninh mạng giữa Mỹ và Trung Quốc nằm trong tổng thể của cặp quan hệ này. Khi quan hệ hai nước tốt đẹp, các hoạt động hợp tác cũng được duy trì. Tuy nhiên, kể từ khi quan hệ hai nước gặp trắc trở, lĩnh vực an ninh mạng cũng trở thành chủ đề gây bàn cãi. Đặc biệt, do tính chất chiến lược của

vấn đề, an ninh mạng hay rộng hơn là vấn đề công nghệ trên không gian mạng ngày càng trở thành tâm điểm của cạnh tranh Mỹ - Trung Quốc. Sự cọ xát trong quan hệ hai nước kể từ nửa cuối năm 2018 khi chiến tranh thương mại Mỹ - Trung bùng phát là bằng chứng rõ ràng cho thấy yếu tố chiến lược của vấn đề an ninh mạng và công nghệ đang trở thành trọng tâm của cạnh tranh hoặc hợp tác trong quan hệ Mỹ - Trung Quốc.

Dấu hiệu về sự gia tăng căng thẳng trong quan hệ Mỹ - Trung Quốc liên quan đến vấn đề an ninh mạng được đánh dấu bằng việc quân đội Mỹ cấm các binh sĩ và nhân viên sử dụng điện thoại do hãng Huawei và ZTE của Trung Quốc sản xuất với lo ngại điện thoại có thể trở thành mối đe dọa an ninh cho các nhân viên, cũng như lộ, lọt thông tin quốc gia quan trọng. Các modem để kết nối Internet do hai công ty này cung cấp cũng bị Chính phủ Mỹ cấm sử dụng tại các cơ sở quân sự do nghi ngờ có thể là mối nguy hiểm an ninh, tuy nhiên, các binh sĩ Mỹ vẫn được sử dụng điện thoại của Huawei hoặc ZTE cho mục đích cá nhân bên ngoài công việc[1]. Trước đó, vào tháng 4/2018, Bộ Thương mại Mỹ cũng đã áp đặt lệnh cấm kéo dài 7 năm đối với ZTE. Theo đó, Mỹ không cho phép các công ty công nghệ của nước

---

1. Nguyễn Nguyễn: "Mỹ "cấm tiệt" điện thoại Huawei, ZTE tại căn cứ quân sự", Báo điện tử *Dân trí*, 2018; https://dantri.com.vn/suc-manh-so/my-cam-tiet-dien-thoai-huawei-zte-tai-can-cu-quan-su-20180504073105651.htm.

này bán thiết bị phần cứng và phần mềm cho thương hiệu này. Người đứng đầu CIA, FBI và NSA cũng đưa ra cảnh báo người dùng không nên mua điện thoại của Huawei.

Vụ việc đầu tiên gây căng thẳng trong quan hệ Mỹ - Trung Quốc liên quan đến công ty Huawei là việc bà Mạnh Vãn Chu, Giám đốc Tài chính của Huawei bị bắt ở Canađa theo đề nghị của Mỹ tháng 12/2018 vì bị tình nghi vi phạm lệnh trừng phạt của Washington nhằm vào Iran. Huawei là một trong những công ty hàng đầu của ngành công nghiệp công nghệ Trung Quốc. Sản phẩm điện thoại thông minh của Huawei được sử dụng rộng rãi trên toàn thế giới. Công ty này hiện đang trở thành nhân tố chính trong việc phát triển cơ sở hạ tầng di động, đặc biệt là công nghệ 5G. Trong tháng 5/2019, Nhà sáng lập, Chủ tịch của Huawei, Nhậm Chính Phi đã phát biểu rằng, hãng này đang đi đầu về công nghệ 5G và ít nhất trong 2 năm tới, các quốc gia khác cũng không theo kịp Huawei về công nghệ này. Đáng chú ý, tính đến tháng 8/2018, Huawei vượt qua Apple, trở thành nhà sản xuất điện thoại thông minh lớn thứ hai thế giới và lên kế hoạch để trở thành nhà sản xuất hàng đầu thế giới về sản phẩm này (vượt qua Samsung).

Ngoài các cáo buộc đe dọa an ninh, vi phạm lệnh cấm vận đối với Iran, Mỹ cũng cáo buộc Huawei ăn cắp bí mật công nghệ của hãng T-mobile. Đến tháng 4/2019, CIA cáo buộc Huawei nhận hỗ trợ từ Ủy ban An ninh quốc gia và từ quân đội Trung Quốc, các thiết bị Huawei có thể được sử

dụng để làm gián điệp[1]. Trên cơ sở các báo buộc và lo ngại đó, Mỹ đã đề nghị các quốc gia châu Âu không sử dụng thiết bị của Huawei trong triển khai công nghệ 5G, đồng thời gửi thông báo về các lo ngại an ninh gây ra bởi Huawei tới nhóm Five Eyes, bao gồm Mỹ, Anh, Ôxtrâylia, Canađa và Niu Dilân. Đây là nhóm các quốc gia duy trì việc chia sẻ thông tin tình báo.

Đỉnh điểm trong căng thẳng quan hệ Mỹ - Trung Quốc về an ninh mạng đến nửa đầu năm 2019 là việc ngày 15/5/2019, Tổng thống Mỹ Trump ký sắc lệnh hành pháp tuyên bố tình trạng khẩn cấp quốc gia, cấm các công ty sử dụng các thiết bị viễn thông do các công ty có thể có mối đe dọa đối với an ninh quốc gia Mỹ. Bộ Thương mại Mỹ đưa Huawei và 68 chi nhánh vào danh sách đen thương mại, theo đó Huawei bị cấm mua các linh kiện và thành phần khác từ công ty Mỹ nếu không có sự chấp thuận từ Chính phủ Mỹ. Thực hiện sắc lệnh này, Google đã ngừng cấp phép sử dụng Android cho Huawei, các hãng công nghệ lớn khác của Mỹ như Intel, Qualcomm, Broadcom, Xilinx ngừng cung cấp linh kiện cho Huawei cho đến khi có thông báo mới. Trước các lệnh trừng phạt của Mỹ, Huawei

---

1. *Microsoft News*, https://www.msn.com/vi-vn/news/world/ t%C3%ACnh-b%C3%A1o-m%E1%BB%B9-c%C3%A1o-bu%E1%BB%99c-huawei-nh%E1%BA%ADn-t%C3%A0i-tr%E1%BB%A3-t%E1%BB%AB-an-ninh-trung-qu%E1%BB%91c/ar-BBW9Vj7?li=BBr8Mkl&ocid=iehp&index=7.

đã phải xem xét lại mục tiêu trở thành nhà sản xuất điện thoại thông tin lớn nhất thế giới[1].

Đáp trả lại các lệnh trừng phạt của Mỹ đối với Huawei, Chính phủ Trung Quốc liên tục đưa ra phát ngôn phản đối hành động của Mỹ, cho rằng việc ngăn cản Huawei kinh doanh tại Mỹ sẽ không khiến Mỹ an toàn hay mạnh hơn, thay vào đó, điều này sẽ chỉ khiến người Mỹ phải dựa nhiều hơn vào những thiết bị thay thế đắt tiền và tụt hậu trong cuộc đua triển khai mạng 5G[2]. Trong một diễn biến khác, người phát ngôn Bộ Ngoại giao Trung Quốc cho biết, nước này đang chuẩn bị một danh sách các công ty, tổ chức và cá nhân nước ngoài "không đáng tin cậy", được coi là đã làm tổn hại lợi ích của các công ty Trung Quốc bằng cách vi phạm nghĩa vụ hợp đồng, quy tắc thị trường hoặc tham gia "các biện pháp phân biệt đối xử"[3]. Phát ngôn này ám chỉ việc Trung Quốc có khả năng đưa các công ty công nghệ Mỹ có làm ăn với Trung Quốc vào danh sách "không đáng

---

1. Tuấn Hưng: "Huawei 'xem xét lại' mục tiêu chiếm ngôi số một từ Samsung", Báo điện tử *Vnexpress*, 2019; https://vnexpress.net/so-hoa/huawei-xem-xet-lai-muc-tieu-chiem-ngoi-so-mot-tu-samsung-3932623.html.

2. Thanh Hà: "Trung Quốc lên tiếng phản đối lệnh trừng phạt của Mỹ đối với Huawei", Báo điện tử *Vnexpress*, 2019; https://baomoi.com/trung-quoc-len-tieng-phan-doi-lenh-trung-phat-cua-my-doi-voi-huawei/c/30738728.epi.

3. Kiến Văn: "Trung Quốc lập danh sách công ty nước ngoài 'không đáng tin cậy", Báo điện tử *Vnexpress*, 2019; https://thanhnien.vn/cong-nghe/trung-quoc-lap-danh-sach-cong-ty-nuoc-ngoai-khong-dang-tin-cay-1088655.html.

tin cậy", từ đó Trung Quốc sẽ triển khai các biện pháp hạn chế sản xuất kinh doanh của các công ty này.

Cạnh tranh Mỹ - Trung Quốc trong vấn đề Huawei còn được thể hiện qua việc Mỹ lôi kéo các đồng minh ngăn chặn việc sử dụng công nghệ và trang thiết bị của Huawei trong triển khai mạng 5G[1]. Tuy nhiên, phản ứng của các đồng minh của Mỹ khá trái chiều. Trong khi Ôxtrâylia và Niu Dilân nhanh chóng hưởng ứng kêu gọi này của Mỹ thì Anh vẫn cho phép sử dụng các cấu phần không quan trọng từ Huawei. Đáng chú ý, hai đồng minh quan trọng của Mỹ tại châu Âu là Đức và Pháp lại tuyên bố sẽ không loại bỏ Huawei khỏi việc triển khai mạng 5G. Tương tự, Bỉ và Hà Lan cũng cho rằng, cần phải đánh giá xem xét liệu Huawei có thực sự gây ra các mối đe dọa về an ninh thông tin, an ninh quốc gia hay không[2]. Dù vậy, chính quyền của Tổng thống Mỹ D.Trump hiện rất cương quyết trong việc áp đặt các biện pháp cứng rắn với Huawei và đe dọa các nước đồng minh nếu không ngừng sử dụng các thiết bị của hãng

---

1. Robin Emmott: "U.S. warns European allies not to use Chinese gear for 5G networks", Reuters, 2019; https://www.reuters.com/article/us-usa-china-huawei-tech-eu/u-s-warns-european-allies-not-to-use-chinese-gear-for-5g-networks-idUSKCN1PU1TG.

2. "How other countries are responding to Trump's Huawei threat"; *The Guardian;* https://www.theguardian.com/business/2019/may/16/how-other-countries-are-responding-to-trump-huawei-threat.

này thì Mỹ sẽ hạn chế việc chia sẻ các thông tin tình báo với các nước này[1].

Việc "cọ xát" Mỹ - Trung Quốc liên quan đến việc sử dụng trang thiết bị 5G của Huawei ngày càng gia tăng cho thấy mặt cạnh tranh trong quan hệ Mỹ - Trung Quốc về lĩnh vực an ninh mạng đang ngày càng gay gắt. Sự nổi lên của mặt cạnh tranh này có thể là bởi hai lý do chính. *Thứ nhất*, quan hệ Mỹ - Trung Quốc bước vào giai đoạn "cọ xát", cạnh tranh căng thẳng khiến cho các vấn đề trong quan hệ hai nước trở thành công cụ trong quan hệ song phương (như vấn đề thương mại, công nghệ 5G). *Thứ hai*, vấn đề an ninh mạng, công nghệ trong không gian mạng ngày càng nổi lên và trở thành vấn đề mang tính quyết định đối với sự phát triển và sức mạnh của các cường quốc. Việc Huawei vươn lên và đi đầu trong công nghệ 5G hiện nay cho thấy Mỹ đang đi sau Trung Quốc trong lĩnh vực này. Do đó, Mỹ cần có biện pháp để không có đối thủ nào có thể vượt mình.

2. Hợp tác Mỹ - Nga

Hợp tác Mỹ - Nga trong lĩnh vực an ninh mạng được thể hiện qua nhiều cơ chế. Trong đó, cơ chế bao trùm nhất là

---

1. "How other countries are responding to Trump's Huawei threat"; *The Guardian;* https://www.theguardian.com/business/2019/may/16/how-other-countries-are-responding-to-trump-huawei-threat.

Ủy ban Tổng thống song phương (*Bilateral Presidential Commission*) nhằm điều phối tổng thể quan hệ hai nước. Ủy ban này do Tổng thống Obama và Tổng thống Medvedev thành lập ngày 06/7/2009, do tổng thống hai nước làm đồng chủ tịch và ngoại trưởng hai nước phụ trách việc điều phối hoạt động ở mỗi nước. Trong khuôn khổ của ủy ban này, các nhóm làm việc được thành lập thuộc nhiều lĩnh vực trong quan hệ song phương, trong đó có nhóm làm việc về các mối đe dọa đối với việc sử dụng thông tin và truyền thông. Nhóm làm việc này bắt đầu cuộc họp đầu tiên từ ngày 21 - 22/11/2013.

Nhóm làm việc thảo luận về hàng loạt vấn đề liên quan đến lợi ích chung của hai nước trong việc sử dụng thông tin - truyền thông dưới góc độ an ninh quốc tế, trong đó phần chính là thảo luận việc thực hiện các biện pháp xây dựng lòng tin được tổng thống hai nước thông qua từ tháng 6/2013. Các biện pháp xây dựng lòng tin này nhằm tăng cường tính minh bạch và ổn định chiến lược thông qua việc giảm thiểu căng thẳng gây ra bởi các mối đe dọa từ việc sử dụng thông tin và truyền thông. Các cuộc thảo luận trong khuôn khổ nhóm làm việc cũng đề cập các biện pháp tăng cường lòng tin ở cấp độ khu vực thông qua các diễn đàn như Tổ chức An ninh và Hợp tác châu Âu (OSCE) và Diễn đàn khu vực ASEAN (ARF). Ngoài ra, nhóm làm việc cũng thảo luận các vấn đề chính sách như quy chuẩn về hành xử của các nhà nước, hợp tác chống lại tội phạm trong lĩnh vực

thông tin - truyền thông và vấn đề quốc phòng trong lĩnh vực thông tin - truyền thông

Tuy nhiên, tiếp nối căng thẳng ngoại giao Nga - Mỹ do sự kiện Nga sáp nhập Crưm năm 2014, nhóm làm việc liên quan đến các mối đe dọa về thông tin - truyền thông đã bị tạm dừng. Tuy vậy, hai nước vẫn xác định lợi ích chung trong việc hợp tác an ninh mạng song phương. Một trong số các biện pháp xây dựng lòng tin là việc thiết lập đường dây nóng để quan chức hai nước thảo luận phương hướng xử lý tình hình trong trường hợp xảy ra khủng khoảng an ninh mạng. Biện pháp này góp phần giải quyết quan ngại về một cuộc tấn công mạng có vẻ như được tiến hành từ lãnh thổ của nước kia có thể dẫn đến một cuộc đối đầu thật giữa hai nước. Do vậy, cho dù nhóm làm việc bị tạm dừng nhưng đường dây nóng giữa hai nước vẫn được duy trì.

Tháng 3/2016, Mỹ - Nga đã quyết định nối lại các cuộc thảo luận về hợp tác an ninh mạng nhằm tăng cường việc thực hiện thỏa thuận đã đạt được năm 2013. Tháng 4/2016, Nga đã tìm kiếm sự giúp đỡ từ Mỹ trong việc chống lại tội phạm trên mạng[1]. Tuy nhiên, những nỗ lực hợp tác an ninh mạng hai nước đang bị phủ bóng đen bởi cáo buộc Nga can thiệp vào cuộc bầu cử tại Mỹ. Gần đây, Tổng thống Mỹ đề xuất việc thiết lập một đơn vị chung với

---

1. Xem thêm tại Https://www.lookingglasscyber.com/blog/threat-intelligence-insights/the-u-s-and-russia-re-engage-in-cyber-cooperation/.

Nga trong lĩnh vực an ninh mạng nhưng bị dư luận Mỹ chỉ trích gay gắt trong bối cảnh các cáo buộc Nga tấn công mạng Đảng Dân chủ trước bầu cử. Trong khi đó, Nga cũng chủ động đề xuất nối lại các hoạt động hợp tác nhưng phía Mỹ chưa có động thái phản hồi.

3. Hợp tác Nga - Trung Quốc

Kể từ khi thành lập Tổ chức Hợp tác Thượng Hải năm 2009, Nga và Trung Quốc đã tiến hành các cuộc đối thoại thường xuyên về các sáng kiến an ninh mạng. Trên cơ sở đó, hai nước đã thể chế hóa hợp tác thông qua việc ký kết một thỏa thuận về an ninh mạng ngày 08/5/2015. Thỏa thuận này được ký nhân chuyến thăm Nga của Chủ tịch Trung Quốc Tập Cận Bình trong dịp kỷ niệm ngày kết thúc Chiến tranh thế giới thứ hai. Điểm mấu chốt trong thỏa thuận này là hai nước cam kết không tấn công mạng lẫn nhau[1]. Thỏa thuận nêu rõ "mục đích là nhằm hạn chế việc sử dụng công nghệ thông tin để can thiệp nội bộ, làm suy yếu chủ quyền quốc gia, phá hoại ổn định về kinh tế, chính trị, xã hội cũng như làm xáo trộn trật tự công".

Việc nhấn mạnh vào khía cạnh chủ quyền kỹ thuật số vẫn là nguyên tắc cơ bản của chính sách an ninh mạng mỗi nước. Tuy nhiên, yếu tố không xâm phạm lẫn nhau trong

---

1. Xem thêm tại Http://vnreview.vn/tin-tuc-an-ninh-mang/-/view_content/content/1545180/nga-trung-hua-khong-hack-lan-nhau.

thỏa thuận năm 2015 được triển khai còn lúng túng, một phần do việc sử dụng ngôn ngữ không rõ ràng trong thỏa thuận nhưng nguyên nhân chủ yếu là do sự tiếp diễn của các hoạt động gián điệp mạng Trung Quốc. Các hoạt động này đã gia tăng đến mức độ chưa từng có trong năm 2016 với việc Công ty Kaspersky Labs của Nga phát hiện 194 vụ tấn công mạng chỉ trong vòng 7 tháng đầu năm 2016, so với 72 vụ trong năm 2015. Các vụ tấn công nhắm vào các cơ quan chính phủ của Nga, các ngành quốc phòng và hàng không, các công ty công nghệ hạt nhân,... Theo Kaspersky Labs, các vụ tấn công này đã không được báo cáo một cách đầy đủ do chỉ có khoảng 10% khách hàng cung cấp dữ liệu liên quan đến các cuộc tấn công này.

Mặc dù các cuộc tấn công vẫn đang tiếp diễn, Nga và Trung Quốc vẫn tăng cường việc hợp tác về không gian mạng. Tháng 4/2015, Diễn đàn Nga - Trung Quốc về an ninh Internet lần đầu tiên được tổ chức ở Moscow và diễn đàn truyền thông được tổ chức vài tháng sau đó. Tuy nhiên, các diễn đàn này không đưa ra được các hiệp định thực chất và cụ thể nào.

Có thể thấy quan hệ Nga - Trung Quốc trong vấn đề không gian mạng không đơn thuần là để trao đổi quan điểm. Thực tế, quan hệ này cho thấy cách tiếp cận tương tự nhau của hai nước đối với việc quản lý không gian mạng, theo đó cả hai bên đều muốn kiểm soát chặt Internet, trái ngược lại so với cách tiếp cận quản trị mạng của Mỹ.

Trong nỗ lực xích lại gần nhau về vấn đề an ninh mạng, Nga - Trung Quốc đã đồng ý trao đổi tin tức liên quan đến công nghệ mới, các mối đe dọa an ninh mạng cùng với việc trao đổi thông tin giữa các cơ quan thực thi luật pháp. Hợp tác thực tế Nga - Trung Quốc trong lĩnh vực công nghệ thông tin - truyền thông (ICT) cũng tăng mạnh. Tháng 5/2014, Hãng viễn thông quốc gia Nga Rostelecom đã thỏa thuận với Công ty Huawei (Trung Quốc) về việc xây dựng tuyến cáp ngầm Magadan - Sakhalin - Kamchatka trị giá 2,5 tỷ rúp.

Trong tháng 8/2014, cuộc gặp giữa Bộ trưởng Bộ Liên lạc và Thông tin đại chúng Nga Nikolai Nikiforov và Bộ trưởng Bộ Công nghiệp và Thông tin Trung Quốc Miêu Vu, hai bên đã thỏa thuận việc tăng cường xuất khẩu phần mềm của Nga sang Trung Quốc và cung cấp sản phẩm của Nhà sản xuất máy chủ lớn nhất Trung Quốc Inspur Group sang Nga. Các máy chủ này sẽ được cung cấp cho Viện nghiên cứu Voskhod, nơi đang phát triển các hệ thống tự động Vybory, Pravosudyie và Zakonotvorchestvo và hệ thống hộ chiếu, visa sinh học thế hệ mới.

Có thể thấy hợp tác Nga và Trung Quốc trong lĩnh vực an ninh mạng phản ánh sự tương đồng trong quan điểm của mỗi nước về ưu tiên trong lĩnh vực này, đó là sự ổn định của chế độ. Chính phủ Nga đặc biệt chú ý đến khả năng của Trung Quốc trong việc kiểm soát toàn bộ không gian mạng. Các quan chức Nga cho rằng, Nga có thể xem xét

các biện pháp có hiệu quả mà Trung Quốc đã sử dụng để vượt qua các nỗ lực mã hóa, ví dụ như các cuộc tấn công trung gian.

Một số quan chức trong lĩnh vực an ninh mạng của Nga cho rằng, trong khi Nga đang nỗ lực tăng cường khả năng kiểm soát không gian mạng thì việc thiết lập một hệ thống giống với tường lửa (Great Firewall) ở Trung Quốc sẽ rất tốn kém và gây ra các mối quan ngại về chính trị và tài chính. Theo Aleksei Os'kin, Giám đốc hỗ trợ kỹ thuật của ESET (một công ty an ninh mạng có trụ sở tại Séc), cho rằng mặc dù ông ủng hộ việc tăng cường giám sát và kiểm duyệt nhưng lại không hoàn toàn ủng hộ mô hình của Trung Quốc. Ông cho rằng, "Nga đang đi theo hướng gần giống như Trung Quốc", nhưng theo ông, Nga "không sao chép phiên bản tường lửa của Trung Quốc", làm như vậy sẽ rất tốn kém và khó khăn về mặt kỹ thuật. Chặn các địa chỉ của một trang web chỉ là một mặt của vấn đề, vấn đề khác là làm sao để lọc và phân tích các dữ liệu được truyền đi.

4. Hợp tác giữa các nước Đông Nam Á trong khuôn khổ ASEAN

Trên cơ sở phân tích về chính sách, hệ thống pháp lý về an ninh mạng của các nước ASEAN, có thể thấy đến nay, ASEAN vẫn chưa có một hiệp định quốc tế chính thức nào về an ninh mạng ngoài khuôn khổ ARF. Khu vực vẫn chưa đạt được nhận thức chung về vấn đề an ninh mạng giữa các

nước thành viên do sự khác biệt về trình độ kỹ thuật, khoảng cách số cũng như nguồn lực. Hiện nay, Malaixia và Xingapo được đánh giá là nằm trong nhóm 20 quốc gia chuẩn bị tốt nhất để ứng phó với các cuộc tấn công mạng.

Hiện nay, các quốc gia Đông Bắc Á đã có những bước tiến nhanh chóng trong việc ứng phó với các thách thức an ninh mạng thông qua việc xây dựng và thực hiện một cách chủ động các chương trình và chiến lược an ninh mạng cũng như thành lập các cơ quan đảm trách việc bảo vệ cơ sở hạ tầng mạng. Trong khi đó, các quốc gia ASEAN vẫn đang bị cản trở bởi sự khác biệt về trình độ kỹ thuật, hạn chế về nguồn nhân lực và năng lực tài chính cũng như các ưu tiên khác nhau trong bảo đảm an ninh mạng. Tuy nhiên, các quốc gia có trình độ phát triển thấp hơn ở khu vực cũng đã bắt đầu thành lập các đội phản ứng nhanh sự cố máy tính (CERTs) hoặc đội phản ứng các sự cố an ninh máy tính (CIRTs) nhằm ứng phó với các cuộc tấn công mạng.

Việc thành lập các đội CERTs/CIRTs trong các nước ASEAN là do sự cấp thiết trong việc bảo đảm môi trường an toàn và ổn định cho hoạt động thương mại điện tử cũng như chống lại các loại tội phạm trên không gian mạng. Ngoài ra, các nước ASEAN cũng tiến hành diễn tập về ứng cứu sự cố an ninh mạng trên quy mô khu vực Đông Nam Á với sự tham dự của các CERT của các nước trong khu vực. Đây là cơ hội cho các CERT tương tác, rèn luyện thực hành và tinh chỉnh cả về quy trình, thủ tục và kỹ năng xử lý, giải

quyết các sự cố an toàn thông tin mạng. Cuộc diễn tập năm 2017 ngoài sự tham dự của các nước ASEAN còn có sự tham gia của các nước như Ôxtrâylia, Trung Quốc, Ấn Độ, Nhật Bản và Hàn Quốc[1]. Tại cuộc diễn tập này, các đội tham gia được yêu cầu điều tra chứng cứ liên quan đến sự cố; phân tích, xác định hành vi của đối tượng tấn công; đề xuất các biện pháp cảnh báo, khắc phục, giảm thiểu tác động; khôi phục hoạt động của hệ thống và các biện pháp phòng ngừa, ngăn chặn sự lây nhiễm, lan rộng của sự cố,...

Các nước ASEAN ngày càng phụ thuộc vào Internet và phụ thuộc lẫn nhau trong một cộng đồng thông qua việc chia sẻ chung băng tần Internet cũng như có cách tiếp cận giống nhau đối với nhu cầu bảo đảm an ninh mạng thông qua sự phối hợp tổng thể chứ không riêng lẻ trong từng lĩnh vực như thương mại, kinh tế hay tội phạm xuyên quốc gia. Tuy nhiên, cách tiếp cận khác nhau đối với vấn đề an ninh mạng sẽ dẫn đến việc các quốc gia có chính sách khác nhau. Ví dụ, đối với các nội dung được truyền tải trên mạng, các quốc gia như Việt Nam và Mianma có xu hướng kiểm soát chặt chẽ nhằm ngăn ngừa các nội dung xấu, độc hại; còn các quốc gia khác như Thái Lan, Philíppin lại nới lỏng việc kiểm soát các thông tin trên mạng.

---

1. Xem thêm Http://www.sggp.org.vn/dien-tap-ung-cuu-su-co-an-ninh-mang-khu-vuc-asean-467220.html.

ASEAN đã thành lập kế hoạch hành động thông qua Diễn đàn an ninh khu vực ARF nhằm thúc đẩy môi trường không gian mạng hòa bình, an toàn, mở và mang tính hợp tác, đồng thời tránh xung đột, khủng hoảng thông qua việc xây dựng lòng tin giữa các quốc gia. Một số nước trong ASEAN (Xingapo, Malaixia, Thái Lan), với tiềm năng về công nghệ và trong lĩnh vực không gian mạng, đang thúc đẩy hợp tác nội khối và thể hiện vai trò đi đầu của mình tại khu vực trong thúc đẩy hợp tác an ninh mạng. Ngày 20/9/2018, Xingapo đã chủ trì cuộc họp cấp bộ trưởng ASEAN về an ninh mạng. Các bộ trưởng đã nhất trí thông qua việc thiết lập một cơ chế chính thức nhằm thảo luận vấn đề ngoại giao không gian mạng, các vấn đề về chính sách và phối hợp hoạt động để bảo vệ khối trước các cuộc tấn công mạng ngày càng gia tăng[1]. Cũng trong năm đó, một trung tâm đào tạo năng lực an ninh ASEAN - Nhật Bản đã được thành lập tại Băng Cốc, Thái Lan.

Dưới góc độ hợp tác quốc tế, Diễn đàn Khu vực ASEAN (gồm 27 nước thành viên) đã cùng với Liên minh châu Âu (EU) thành lập Nhóm làm việc giữa kỳ ARF (do Xingapo,

---

1. Hariz Baharudin, Singapore to draw up formal Asean mechanism for cyber security, Straitstimes, truy cập ngày 10/10/2018, https://www.straitstimes.com/singapore/singapore-to-draw-up-formal-asean-mechanism-for-cyber-security.

Malaixia và Nhật Bản đồng chủ trì) nhằm thảo luận về các vấn đề không gian mạng. Nhóm làm việc này có chức năng, nhiệm vụ tương tự UN GGE. Nhóm làm việc của Liên hợp quốc hằng năm đều ra các báo cáo về việc duy trì hòa bình và an ninh trên không gian mạng. Năm 2015, ASEAN cũng đã thông qua kế hoạch hành động với Ôxtrâylia, Malaixia và Nga nhằm ngăn ngừa xung đột và khủng hoảng thông qua việc tăng cường lòng tin.

Trên cơ sở phân tích chính sách an ninh mạng của các quốc gia Đông Nam Á, có thể thấy, các quốc gia này đã chưa chuẩn bị một cách kỹ càng để hợp tác về an ninh mạng do sự khác biệt về trình độ công nghệ thông tin và truyền thông. Do đó, ASEAN cần cân nhắc các biện pháp nhằm thống nhất quan điểm giữa các thành viên về tầm quan trọng của hợp tác trong lĩnh vực này. Tuy nhiên, một điểm đồng thuận trong ASEAN là việc khối đã đặt sự phát triển của công nghệ thông tin và truyền thông là một phần chính yếu của kế hoạch kết nối ASEAN.

Sự phát triển của công nghệ thông tin không nên chỉ tập trung vào việc tăng cường hệ thống mạng mà còn phải tập trung vào việc việc ngăn chặn các nguy cơ đối với hệ thống. Kế hoạch tổng thể kết nối ASEAN bao gồm kết nối hạ tầng, thể chế và con người với việc coi công nghệ thông tin và truyền thông là một phần của kết nối hạ tầng. Mục tiêu của ASEAN trong lĩnh vực thông tin và truyền thông là xây

dựng một khu vực tiên tiến và được kết nối, tuy nhiên kế hoạch này chưa xem xét đến khía cạnh an ninh trong lĩnh vực này.

Tuy nhiên, các nỗ lực về an ninh mạng của khu vực hiện nay mới chủ yếu tập trung vào chống lại các loại tội phạm xuyên quốc gia nhằm bảo đảm cho sự thúc đẩy hội nhập kinh tế khu vực. Tội phạm không gian mạng và khủng bố mạng được đưa vào nhiều văn kiện và tuyên bố của ASEAN kể từ sau cuộc tấn công khủng bố năm 2001 tại Mỹ (ASEAN đã thông qua các tuyên bố chung về vấn đề khủng bố và tội phạm trên không gian mạng).

Thực tế, ASEAN là hiệp hội có nhóm các quốc gia đang phát triển đầu tiên trên thế giới thực hiện việc đồng bộ hóa khung pháp lý về thương mại điện tử. ASEAN đặt mục tiêu trở thành nền kinh tế số hóa vào năm 2020. Mục tiêu này có thể được hiện thực hóa khi các nước trong khu vực xây dựng được một cơ chế hợp tác, giải quyết kịp thời các sự cố và giảm thiểu tối đa nguy cơ an ninh mạng. Đến nay, đa số các nước Đông Nam Á đều đã thông qua luật về giao dịch điện tử, trong đó 8 nước có luật liên quan đến tội phạm trên không gian mạng và tương đối sát với các tiêu chuẩn quốc tế hiện nay[1]. Tại khu vực, 9/10 nước ASEAN, ngoại trừ Lào, cũng đang

1. Http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=613.

triển khai các chương trình an ninh mạng. Trong đó, Malaixia đã thành lập một trung tâm điều phối và chỉ huy quốc gia về an ninh mạng. Thái Lan tăng cường theo dõi và giám sát hoạt động trực tuyến, đồng thời xây dựng một bộ luật về an ninh mạng, mở rộng quyền hạn tiếp cận thông tin cá nhân. Trong khi đó, Xingapo đã công bố một Chiến lược quốc gia về an ninh mạng[1].

Tuy nhiên với đặc thù của các cuộc tấn công mạng là không phân biệt lãnh thổ hay quốc gia nên không một tổ chức, một quốc gia nào có thể đơn độc bảo vệ mình an toàn trước các tấn công. Với cách tiếp cận này, Xingapo đã thành lập Quỹ xây dựng năng lực an ninh mạng ASEAN (ACCP) để giúp các thành viên trong khối mua sắm trang thiết bị, thuê chuyên gia, huấn luyện nhân sự, xây dựng hành lang pháp lý.

*

* *

Có thể thấy, hợp tác song phương giữa các quốc gia trong lĩnh vực an ninh mạng và không gian mạng bị chi phối bởi tổng thể quan hệ song phương của từng cặp quốc gia. Trong các cặp quan hệ nói trên, hợp tác đều diễn ra trong khuôn khổ các hiệp định được ký kết. Nội

1. Http://vtv.vn/cong-nghe/asean-doi-pho-thach-thuc-an-ninh-mang-20170919202247214.htm.

dung hợp tác trong từng hiệp định phụ thuộc tình hình quan hệ mỗi nước. Cụ thể, trường hợp Mỹ - Trung Quốc, hai nước còn nhiều nghị kỵ và cách tiếp cận khác nhau trong vấn đề an ninh mạng và không gian mạng, do đó nội dung hợp tác mới chỉ dừng lại ở vấn đề hạn chế hoạt động gián điệp kinh tế. Trường hợp Mỹ - Nga, hai nước đồng ý thiết lập nhóm làm việc về các mối đe dọa đối với việc sử dụng thông tin - truyền thông, tuy nhiên nội dung hợp tác mới chủ yếu dừng lại ở xây dựng lòng tin, khi hai quan hệ hai nước xấu đi thì cơ chế hợp tác này cũng bị tạm dừng. Ngược lại, hợp tác Nga - Trung Quốc diễn ra trên cơ sở hai nước có nhiều điểm tương đồng trong cách tiếp cận an ninh mạng.

Tuy các nước đều nhận thấy tầm quan trọng của hợp tác trong lĩnh vực an ninh mạng nhưng sự thay đổi của quan hệ song phương là nhân tố quyết định đến mức độ và tốc độ hợp tác giữa các nước. Thực tế cho thấy, hợp tác Mỹ - Trung Quốc còn hạn chế và chưa đi vào các vấn đề cốt lõi của an ninh mạng. Hợp tác Mỹ - Nga bị tác động mạnh bởi tình hình thực tế trong quan hệ song phương do các sự căng thẳng giữa Mỹ và Nga trong vấn đề Crưm. Tuy nhiên, do đặc thù của khía cạnh kỹ thuật, hai nước vẫn duy trì đường dây nóng để phản ứng nhanh trong trường hợp khủng khoảng, tránh xảy ra hiểu lầm chiến lược trong vấn đề an ninh mạng. Trong khi đó, tuy có sự tương đồng,

hợp tác Nga - Trung Quốc chưa đi vào thực chất và chưa hiệu quả. Các cuộc tấn công mạng vẫn tiếp tục diễn ra và Nga không hoàn toàn theo mô hình của Trung Quốc trong việc quản lý không gian mạng.

Trong hợp tác đa phương, để nhằm khắc phục những khó khăn trong việc bảo đảm an ninh mạng và dần đi đến việc thống nhất các biện pháp của các quốc gia trong bảo đảm an ninh mạng, từ đó hình thành nên các quy phạm bảo đảm an ninh mạng, nhiều tổ chức khu vực và quốc tế như OSCE, ASEAN, ARF,... đã có nhiều chương trình hội thảo nhằm trao đổi, kiến nghị các giải pháp, trong đó đáng chú ý có:

- Quy phạm và các biện pháp xây dựng lòng tin: Hiện nay, UN GGE đã khẳng định, luật pháp quốc tế có thể được áp dụng trên không gian mạng, nhưng vẫn còn nhiều hoài nghi về cách thức áp dụng các quy phạm pháp luật quốc tế và các quốc gia cũng tỏ ra dè dặt do thiếu tin tưởng rằng các nước khác cũng sẽ tuân thủ các quy phạm pháp luật đó cũng như quan ngại về những hạn chế có thể đặt ra đối với chính quốc gia mình. Do đó, việc xây dựng và áp dụng các biện pháp xây dựng lòng tin được cho là sẽ giải quyết được bất cập này. Năm 2013, OSCE đã thông qua Quyết định số 1106, trong đó đưa ra 11 biện pháp xây dựng lòng tin nhằm giảm thiểu nguy cơ xung đột phát sinh từ việc sử dụng công nghệ thông tin

và truyền thông. Những biện pháp này khuyến khích các nước tự nguyện chia sẻ thông tin, quan điểm, chính sách, chiến lược, biện pháp cũng như hợp tác nhằm tăng cường an ninh trên không gian mạng và qua đó giảm thiểu nguy cơ xung đột. Mục đích của những biện pháp xây dựng lòng tin này là tạo cơ hội cho các nước có lợi ích và quan điểm khác nhau có thể trao đổi và giải quyết những bất đồng liên quan đến chính sách an ninh mạng, qua đó củng cố niềm tin về việc tuân thủ các quy tắc trên môi trường mạng giữa các quốc gia với nhau và dần dần tạo thành các thực tiễn cấu thành luật tập quán quốc tế.

- Nâng cao năng lực nhằm tăng cường an ninh mạng: không thể phủ nhận một trong những thách thức đối với việc bảo đảm an ninh mạng trên toàn thế giới là sự không đồng đều về năng lực giữa các quốc gia phát triển và các quốc gia đang phát triển, thậm chí là giữa các khu vực khác nhau trong cùng một quốc gia (như ở Trung Quốc hay Ấn Độ). Do đó, việc nâng cao năng lực bảo đảm an ninh mạng là hết sức cần thiết. Để thực hiện mục tiêu này, trong những năm gần đây, các nước trong và ngoài khu vực đã tổ chức nhiều hội thảo nhằm chia sẻ kinh nghiệm, xác định phương hướng phát triển năng lực an ninh mạng. Bên cạnh đó, Bộ Ngoại giao của một số nước cũng đã thành lập bộ phận chuyên trách về an ninh mạng nhằm điều phối nỗ lực quốc tế, khu vực trong việc nâng

cao năng lực an ninh mạng, xây dựng chính sách đối ngoại liên quan đến an ninh mạng và ứng phó với những sự cố lớn về an ninh mạng liên quan đến nhiều quốc gia, đối tượng phức tạp.

- Hướng tới an ninh mạng toàn cầu: thế giới đang ngày càng lệ thuộc vào công nghệ - thông tin và truyền thông, từ những tiện ích giao dịch cho đến sự vận hành chính phủ. Do đó, việc bảo đảm an ninh trên không gian mạng trở nên vô cùng thiết yếu. Nhiều ý kiến cho rằng, những nỗ lực hiện tại của các nước và các khu vực còn chưa đồng đều, có nhiều sự khác biệt về cách tiếp cận đối với vấn đề an ninh mạng cũng như năng lực thực hiện bảo đảm an ninh mạng. Do đó, cần phải xây dựng cơ chế để các nước trên thế giới có thể đồng bộ hóa các tiêu chuẩn, chính sách, chiến lược cũng như hợp tác trong các nỗ lực phòng, chống tội phạm mạng và bảo đảm an ninh trên không gian mạng. Những biện pháp được đề xuất gồm có xây dựng quy phạm pháp luật quốc tế trên không gian mạng, tăng cường lòng tin ở tầm quốc tế, hợp tác giữa các cơ quan bảo đảm an ninh mạng của các nước, xây dựng cơ chế đào tạo nguồn lực bảo đảm an ninh mạng,... Tuy nhiên, cũng có ý kiến cho rằng, vấn đề an ninh mạng vốn mang tính khu vực, do đó những nỗ lực nhằm tăng cường an ninh trên không gian mạng cần phải được định hướng ở tầm khu vực, trên cơ sở xem xét đến

điều kiện kinh tế - chính trị và năng lực kỹ thuật của các nước trong khu vực đó.

- Vấn đề trách nhiệm bảo đảm an ninh mạng: một trong những giải pháp được kiến nghị nhằm khắc phục những hạn chế về lòng tin và năng lực của các quốc gia là chỉ định ra một cơ quan trung lập có trách nhiệm bảo đảm an ninh mạng. Cơ quan này có tính chất trung lập về mặt chính trị, hoạt động trên cơ sở phân tích các dữ liệu thực tế (fact-based) và là một nguồn đáng tin cậy để kiến nghị những hoạt động thiết thực cho các quốc gia trong bảo đảm an ninh mạng. Một cơ chế như vậy có thể được coi như một "Công ước Geneva cho công nghệ số" (Digital Geneva Convention).

- Tăng cường hợp tác giữa nhóm hoạch định chính sách và nhóm kỹ thuật: các cơ quan hoạch định chính sách của quốc gia có năng lực ban hành chính sách, luật pháp để tăng cường bảo đảm an ninh mạng; phòng, chống tội phạm mạng,... Tuy nhiên, những chính sách, luật pháp thường bị lạc hậu so với những thủ đoạn ngày càng tinh vi của tội phạm mạng. Trong khi đó, nhóm kỹ thuật (chủ yếu là khối tư nhân) là tác giả của những công nghệ phần mềm, máy tính với nhiều phát minh mới (như thuật toán đám mây, IoT,...), có năng lực xây dựng các cơ chế bảo mật, an ninh cho môi trường mạng và sự linh hoạt trong các biện pháp, chính sách ứng phó với những sự cố, rủi ro trên môi trường mạng. Do đó, cần phải tăng cường hơn nữa sự hợp tác giữa

hai nhóm này để bảo đảm được cả về mặt năng lực và biện pháp bảo đảm an ninh mạng.

Các quốc gia có cách tiếp cận và cách thức thực hiện chính sách khác nhau trong lĩnh vực an ninh mạng. Một điểm chung trong chính sách của các nước là bảo đảm khả năng độc lập, tự chủ về mặt công nghệ và một môi trường Internet an toàn, lành mạnh; thúc đẩy sáng tạo, phát triển đồng thời giành ưu thế trong không gian mạng. Ngoài ra, các nước đều nhấn mạnh đến yếu tố hợp tác quốc tế nhằm ứng phó với các thách thức an ninh mạng do đây là vấn đề xuyên quốc gia, đòi hỏi sự phối hợp, hợp tác quốc tế.

Chính sách và việc thực thi chính sách an ninh mạng giữa các quốc gia, khu vực trên thế giới còn nhiều điểm khác nhau do sự khác biệt về quan điểm, cách tiếp cận. Một số khác biệt chính hiện nay là vấn đề luật pháp và áp dụng luật pháp quốc tế, vấn đề quyền tự do cá nhân và lợi ích quốc gia, vấn đề chủ quyền không gian mạng, vấn đề dữ liệu cá nhân,... Đặc biệt, giữa các nước còn có sự khác nhau về trình độ và năng lực khoa học - kỹ thuật trong lĩnh vực không gian mạng và bảo đảm an ninh mạng.

Sự khác biệt về cách tiếp cận, quan điểm trong việc quản lý không gian mạng cũng là lĩnh vực hợp tác và cạnh tranh giữa các nước, đặc biệt là các nước lớn. Các chủ thể chính hiện nay cũng là ba nước lớn Mỹ, Nga, Trung Quốc. Đặc điểm trong hợp tác và cạnh tranh giữa các chủ thế là hai mặt hợp tác, cạnh tranh diễn ra song song. Giữa các nước không

hoàn toàn là hợp tác cũng không hoàn toàn là cạnh tranh trong lĩnh vực an ninh mạng. Việc mặt hợp tác hay cạnh tranh nổi hơn bị chi phối bởi tổng thể quan hệ song phương của từng cặp quốc gia. Trong ba cặp quan hệ nói trên, hợp tác đều diễn ra trong khuôn khổ các hiệp định được ký kết. Nội dung hợp tác trong từng hiệp định phụ thuộc thực trạng quan hệ mỗi nước và chưa đi vào thực chất.

Chương 3

KIẾN NGHỊ, ĐỀ XUẤT CHÍNH SÁCH VỀ AN NINH MẠNG CHO VIỆT NAM

1. Cơ sở lý luận và thực tiễn

1.1. Cơ sở lý luận

(i) Vấn đề an ninh mạng trong một số lý thuyết quan hệ quốc tế

Cùng với sự phát triển của công nghệ thông tin, vấn đề an ninh mạng hiện không chỉ dừng lại ở khía cạnh bảo mật, bảo đảm an ninh, an toàn thông tin, mà đã trở thành vấn đề an ninh quốc gia, và do đó trở thành vấn đề trong quan hệ giữa các nước, là lĩnh vực vừa hợp tác vừa cạnh tranh giữa các chủ thể trong quan hệ quốc tế.

Theo Thuyết hiện thực, mục tiêu của các quốc gia là tìm cách nâng cao quyền lực nhằm tự bảo đảm an ninh và sự tồn tại của mình trong hệ thống thông qua việc cố gắng giành được càng nhiều nguồn lực càng tốt. Điều này dẫn tới việc các quốc gia luôn ở trong thế cạnh tranh và đối đầu lẫn nhau (trong nhiều trường hợp còn xảy chiến tranh, xung đột vũ trang) nhằm theo đuổi lợi ích quốc gia dưới dạng

quyền lực, khiến các quốc gia không thể duy trì việc hợp tác một cách lâu dài. Theo cách hiểu này, trong quan hệ quốc tế, đặc biệt là giữa các nước lớn, mặt cạnh tranh trong lĩnh vực an ninh mạng sẽ mang tính bản chất và nổi trội. Việc hợp tác sẽ chủ yếu mang tính tạm thời và chiến thuật như trong trường hợp quan hệ Mỹ - Trung Quốc, với việc hai nước tuy đã thiết lập cơ chế hợp tác nhằm kiểm soát bất đồng nhưng các kết quả đạt được mới chủ yếu dừng lại ở việc giảm số vụ gián điệp kinh tế, ăn cắp quyền sở hữu trí tuệ trong khi hoạt động gián điệp nhằm vào các mục tiêu của chính phủ Mỹ vẫn tiếp tục. Cùng với đó, các nước sẽ tiếp tục thúc đẩy phát triển, nâng cao năng lực công nghệ thông tin nhằm giành ưu thế hơn về công nghệ trong việc vừa bảo đảm an ninh mạng quốc gia, vừa có khả năng tấn công đối phương trên không gian mạng. Chủ nghĩa hiện thực cũng góp phần giải thích nguyên nhân khiến việc hợp tác đa phương đến nay, đặc biệt là trong việc xây dựng khung pháp lý, tập quán, diễn ra chậm và không mấy tiến triển.

Trong khi đó, chủ nghĩa tự do cho rằng, các quốc gia thay vì cạnh tranh có thể hợp tác với nhau để cùng đạt được lợi ích chung, đặc biệt là thông qua các thể chế quốc tế. Dưới góc nhìn này, các quốc gia, trong đó có các nước lớn hoàn toàn có thể tiến hành hợp tác trong lĩnh vực an ninh mạng vì lợi ích chung; các thể chế quốc tế và khu vực sẽ đóng vai trò quan trọng trong việc thúc đẩy hợp tác, đặc biệt trong việc xây dựng hệ thống pháp luật và quy chuẩn

quốc tế. Trên thực tế, các nước đều nhận thấy nhu cầu hợp tác và đã triển khai hợp tác với các quốc gia, đối tác bên ngoài, tuy nhiên mức độ và kết quả hợp tác còn khác nhau. Đáng chú ý là việc hợp tác trong lĩnh vực an ninh mạng bị tác động bởi nhiều yếu tố bên ngoài như cạnh tranh địa - chính trị, sự nghi kỵ, sự khác biệt về trình độ khoa học - công nghệ.

Thuyết kiến tạo cho rằng, mỗi quốc gia có một bản sắc quốc gia, hay cách quốc gia đó nhận thức về bản thân mình, và bản sắc quốc gia này giúp định hình các mục tiêu mà quốc gia đó theo đuổi, như an ninh, chính sách đối ngoại hay phát triển triển kinh tế. Tuy nhiên cách thức mà các quốc gia hiện thực hóa các mục tiêu này như thế nào lại phụ thuộc vào bản sắc xã hội, hay là cách các quốc gia nhận thức về bản thân mình trong mối quan hệ với các quốc gia khác. Các quốc gia sẽ xác định lợi ích quốc gia mình dựa trên cơ sở những bản sắc này. Do vậy, trong lĩnh vực an ninh mạng, việc các quốc gia cạnh tranh và hợp tác với nhau như thế nào phụ thuộc rất lớn vào việc từng quốc gia nhận thức như thế nào về vấn đề an ninh mạng, các mối đe dọa an ninh mạng cũng như môi trường, đối tác quốc tế bên ngoài. Cách tiếp cận này có thể góp phần lý giải việc các quốc gia đều có nhu cầu hợp tác trong lĩnh vực bảo đảm an ninh mạng, tuy nhiên mức độ hợp tác lại tùy thuộc vào việc các quốc gia đó nhận thức về mức độ nguy hại của các nguy cơ không gian mạng đối với an ninh quốc gia đến đâu, cũng như đối tác

hợp tác hay đối tượng cạnh tranh là ai. Theo đó, các nước nhỏ, có trình độ công nghệ thấp, không có quan hệ thù địch sẽ có xu hướng dễ hợp tác với nhau.

(ii) Quan điểm của Việt Nam về vấn đề an ninh mạng

Công nghệ thông tin xuất hiện ở Việt Nam từ khá sớm, là một ngành tổng thể bao gồm nhiều nhánh nhỏ như mạng lưới bưu chính viễn thông, truyền thông đa phương tiện, Internet,... Cho đến nay, có thể khẳng định rằng ở Việt Nam đã xây dựng được một cơ cấu hạ tầng công nghệ thông tin đồng bộ, đầy đủ. Dấu mốc đáng nhớ trong sự phát triển ngành công nghệ thông tin là năm 1997 với việc tham gia kết nối vào mạng toàn cầu và tính cho tới thời điểm này, Việt Nam đã trở thành quốc gia có tỷ lệ tăng trưởng Internet nhanh nhất trong khu vực và nằm trong số những quốc gia có tỷ lệ tăng trưởng cao nhất thế giới.

Vấn đề an ninh mạng trong các văn bản chính thức, như các nghị quyết của Đảng, chiến lược phát triển kinh tế - xã hội,... thường được gắn liền với khái niệm công nghệ thông tin. Khái niệm này được hiểu và định nghĩa trong Nghị quyết số 49/NQ-CP ngày 04/8/1993 về phát triển công nghệ thông tin ở nước ta trong những năm 90 của Chính phủ, theo đó công nghệ thông tin là tập hợp các phương pháp khoa học, các phương tiện và công cụ kỹ thuật hiện đại - chủ yếu là kỹ thuật máy tính và viễn thông - nhằm tổ chức khai thác và sử dụng có hiệu quả các nguồn tài nguyên thông tin rất phong phú và tiềm tàng trong mọi lĩnh vực hoạt động của con người và xã hội.

Ngày 17/10/2000, Bộ Chính trị Ban Chấp hành Trung ương Đảng Cộng sản Việt Nam (khóa VIII) đã ban hành Chỉ thị số 58-CT/TW về đẩy mạnh ứng dụng và phát triển công nghệ thông tin phục vụ sự nghiệp công nghiệp hóa, hiện đại hóa. Dưới sự chỉ đạo của Đảng và sự điều hành của Chính phủ, trong những năm qua công nghệ thông tin và truyền thông ở Việt Nam đã đạt được nhiều thành tựu quan trọng và đáp ứng được những mục tiêu đề ra.

Dưới góc độ an ninh, Đảng, Nhà nước luôn quan tâm lãnh đạo, chỉ đạo công tác bảo đảm an toàn, an ninh mạng, ban hành nhiều chủ trương, chính sách, pháp luật và giải pháp thúc đẩy ứng dụng, phát triển công nghệ thông tin trong các lĩnh vực gắn với bảo vệ vững chắc chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng; xây dựng không gian mạng an toàn, trở thành nguồn lực mạnh mẽ để xây dựng, bảo vệ và phát triển đất nước. Đặc biệt, Ban Bí thư Trung ương Đảng đã ban hành Chỉ thị số 28-CT/TW, ngày 16/9/2013 về tăng cường công tác bảo đảm an toàn thông tin mạng; Thủ tướng Chính phủ đã ban hành Chỉ thị số 15/CT-TTg, ngày 17/6/2014 về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới.

Nghị quyết số 28-NQ/TW ngày 25/10/2013 của Ban Chấp hành Trung ương Đảng (khóa XI) về Chiến lược bảo vệ Tổ quốc trong tình hình mới cũng xác định việc bảo đảm an ninh, an toàn thông tin, an ninh mạng là một nhiệm vụ trong kế sách phòng, chống các nguy cơ chiến tranh, xung

đột từ sớm, từ xa; chủ động phòng ngừa, khắc phục các yếu tố tác động tiêu cực đến sự nghiệp củng cố quốc phòng, giữ vững an ninh, bảo vệ vững chắc Tổ quốc trong tình hình mới. Theo đó, quốc phòng và an ninh phải có đủ sức mạnh để "ngăn ngừa các nguy cơ chiến tranh, xung đột từ sớm, từ xa; chủ động phòng ngừa, phát hiện sớm và triệt tiêu các nhân tố bất lợi, nhất là các nhân tố bên trong có thể gây ra đột biến"[1], để đất nước "không bị động, bất ngờ"; giữ vững môi trường hòa bình, ổn định và tạo điều kiện thuận lợi cho bạn bè quốc tế trong hợp tác với Việt Nam. Đại hội XII chỉ rõ: phải "Chủ động đấu tranh làm thất bại mọi âm mưu, hoạt động chống phá của các thế lực thù địch; ngăn chặn, phản bác những thông tin và luận điệu sai trái, đẩy lùi các loại tội phạm và tệ nạn xã hội; sẵn sàng ứng phó với các mối đe dọa an ninh truyền thống và phi truyền thống; bảo đảm an ninh, an toàn thông tin, an ninh mạng. Kiên quyết, kiên trì đấu tranh bảo vệ độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ, bảo vệ vững chắc biên giới và chủ quyền biển, đảo, vùng trời của Tổ quốc; đồng thời giữ vững môi trường hòa bình, ổn định để phát triển bền vững đất nước"[2].

Có thể nói, vấn đề an ninh mạng đã được Đảng, Nhà nước quan tâm, chú ý từ sớm và coi đây là một thành tố của

---

1, 2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XII,* Nxb. Chính trị quốc gia Sự thật, Hà Nội, 2016, tr.149, 148.

an ninh quốc gia, gắn vấn đề bảo đảm an ninh mạng với vấn đề bảo đảm an ninh, an toàn thông tin và đi liền với việc ứng dụng và phát triển công nghệ thông tin. Đảng đã có quan điểm nhất quán và thể hiện qua nhiều văn bản về vai trò, tầm quan trọng của việc ứng dụng và phát triển công nghệ thông tin trong sự nghiệp xây dựng và bảo vệ Tổ quốc. Trên thực tế, việc ứng dụng và phát triển công nghệ thông tin đã đạt được nhiều thành tựu to lớn, đóng góp quan trọng vào sự phát triển kinh tế - xã hội. Cuối năm 2018, Luật an ninh mạng đã được thông qua với 7 chương, 43 điều, trong đó nêu rõ những quy định cơ bản về an ninh mạng đối với hệ thống thông tin 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 giao trách nhiệm cho cơ quan, tổ chức, cá nhân. Luật có hiệu lực kể từ ngày 01/01/2019 nhằm bảo vệ tối đa quyền và lợi ích hợp pháp của các tổ chức, cá nhân khi gặp phải những nguy cơ bị đe dọa về an ninh mạng, tạo khung pháp lý để xử lý các hành vi vi phạm trên không gian mạng.

Hơn nữa, tình hình mất an toàn thông tin mạng đang diễn biến ngày càng phức tạp. Trong khi đó hệ thống văn bản quy phạm pháp luật về bảo đảm an toàn, an ninh mạng thông tin quốc gia chưa đồng bộ, hiệu lực thi hành chưa cao. Công tác quản lý nhà nước về an toàn, an ninh mạng còn nhiều kẽ hở, chưa theo kịp tốc độ phát triển và ứng dụng công nghệ thông tin, nhất là đối với báo điện tử,

mạng xã hội, trò chơi trực tuyến, thuê bao di động trả trước, hoạt động cung cấp dịch vụ viễn thông, Internet. Một số cơ quan, tổ chức, cá nhân còn chủ quan, sơ hở trong quản lý thông tin nội bộ, bí mật nhà nước; chưa nhận thức đầy đủ vị trí, tầm quan trọng của công tác bảo đảm an toàn, an ninh mạng cũng như tính chất nguy hiểm trong âm mưu, hoạt động của các thế lực thù địch, tội phạm mạng chống phá ta trên không gian mạng; công tác phòng ngừa còn để lộ, lọt bí mật nhà nước, bí mật nội bộ trên mạng,... Cùng với đó, Internet kết nối vạn vật và các hệ thống, hoạt động tấn công mạng của các thế lực thù địch, tội phạm mạng sẽ ngày càng gia tăng, không chỉ dừng lại ở mục đích thu thập thông tin bí mật, mà còn phá hoại cơ sở dữ liệu, hạ tầng công nghệ thông tin, thậm chí trở thành những loại vũ khí nguy hiểm, có sức tàn phá nặng nề, được sử dụng song hành cùng các loại vũ khí truyền thống một khi xung đột vũ trang xảy ra.

Bối cảnh trên đặt ra yêu cầu cấp bách phải tạo được sự chuyển biến sâu sắc trong nhận thức của các cấp ủy đảng, chính quyền, các đoàn thể từ Trung ương đến địa phương về tầm quan trọng của công tác bảo đảm an toàn, an ninh mạng, coi đây là nhiệm vụ quan trọng, cấp bách, thường xuyên, lâu dài của cả hệ thống chính trị và toàn dân dưới sự lãnh đạo của Đảng, sự quản lý của Nhà nước. Công tác bảo đảm an toàn, an ninh mạng, tạo sức đề kháng trước những luận điệu tuyên truyền xuyên tạc, kích động, phá hoại của

các thế lực thù địch và phần tử xấu cần được gắn kết chặt chẽ giữa "xây" và "chống"[1].

Việc thực hiện các yêu cầu nói trên đòi hỏi việc hoàn thiện việc nhận thức của Đảng về vấn đề an ninh mạng, để từ đó đưa ra các chủ trương, chính sách, chiến lược kịp thời, chính xác nhằm ứng phó với các thách thức an ninh mạng cũng như bảo đảm môi trường không gian mạng an toàn, ổn định nhằm phục vụ phát triển kinh tế, xã hội.

1.2. Cơ sở thực tiễn

Thực tế vấn đề an ninh mạng tại Việt Nam luôn đi liền với sự phát triển của công nghệ - thông tin. Trong nhiều năm qua, việc áp dụng và ứng dụng công nghệ - thông tin góp phần bảo đảm an ninh - quốc phòng, chính trị - ngoại giao, phát triển kinh tế - xã hội đã đạt được nhiều kết quả, đóng góp thiết thực vào sự nghiệp xây dựng và bảo vệ Tổ quốc.

Chỉ thị số 58-CT/TW ngày 17/10/2000 của Bộ Chính trị về đẩy mạnh ứng dụng và phát triển công nghệ thông tin phục vụ sự nghiệp công nghiệp hóa, hiện đại hóa nhận định công nghệ thông tin đã ở một bước phát triển cao, đó là số hóa tất cả các dữ liệu thông tin, luân chuyển mạnh mẽ và kết nối tất cả chúng ta lại với nhau. Mọi loại thông tin, số

---

1. Xem "Chủ tịch nước Trần Đại Quang yêu cầu tăng cường an ninh mạng", https://tuoitre.vn/chu-tich-nuoc-tran-dai-quang-yeu-cau-tang-cuong-an-ninh-mang-1372237.htm.

liệu âm thanh, hình ảnh có thể được đưa về dạng kỹ thuật số để bất kỳ máy tính nào cũng có thể lưu trữ, xử lý và chuyển tiếp cho nhiều người. Những công cụ và sự kết nối trong thời đại kỹ thuật số cho phép chúng ta dễ dàng thu thập, chia sẻ thông tin và hành động trên cơ sở những thông tin này theo phương thức hoàn toàn mới, kéo theo hàng loạt sự thay đổi về các quan niệm, tập tục, thói quen truyền thống, và thậm chí cả cách nhìn các giá trị trong cuộc sống. Công nghệ thông tin đến với từng người dân, từng nhà quản lý, nhà khoa học, người nông dân, bà nội trợ, học sinh,... Không có lĩnh vực nào, không có nơi nào không có sự hiện hữu của công nghệ thông tin. Công nghệ thông tin là một trong những động lực quan trọng nhất của sự phát triển. Việc ứng dụng và phát triển công nghệ thông tin ở nước ta góp phần giải phóng sức mạnh vật chất, trí tuệ và tinh thần của toàn dân tộc, thúc đẩy công cuộc đổi mới, phát triển nhanh và hiện đại hóa các ngành kinh tế, tăng cường năng lực cạnh tranh của các doanh nghiệp, hỗ trợ có hiệu quả cho quá trình hội nhập kinh tế quốc tế, nâng cao chất lượng cuộc sống của nhân dân, bảo đảm an ninh quốc phòng và tạo ra khả năng "đi tắt đón đầu" để thực hiện thắng lợi sự nghiệp công nghiệp hóa, hiện đại hóa đất nước.

Hiện nay, không chỉ các doanh nghiệp, tổ chức, cá nhân quan tâm đến việc ứng dụng công nghệ thông tin phục vụ cho công việc mà còn là một kênh hỗ trợ đắc lực cho sự phát triển của đơn vị mình. Chính phủ cũng xem việc ứng

dụng công nghệ thông tin và truyền thông là yếu tố cốt lõi để thúc đẩy cải cách hành chính từ Trung ương đến các địa phương, vào từng công đoạn trong công việc hành chính hằng ngày của mỗi một cán bộ, công chức tại cơ quan hành chính, góp phần nâng cao hiệu quả quản lý, điều hành và tác nghiệp của cơ quan, đáp ứng tốt hơn nhu cầu của công dân, tổ chức và là tiền đề quan trọng để tiến đến chính quyền điện tử.

Các trang tin, cổng thông tin điện tử của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương hoàn thành việc kết nối với Cổng Thông tin điện tử Chính phủ, hình thành đầy đủ Mạng thông tin điện tử hành chính của Chính phủ. Các chỉ tiêu đưa ra phải đạt được đến năm 2020 còn cao hơn rất nhiều. Ứng dụng công nghệ thông tin và truyền thông nhằm cải thiện chất lượng dịch vụ công đã và đang trở thành mối quan tâm hàng đầu của Chính phủ trong những năm gần đây. Với sự quyết tâm phát triển Chính phủ điện tử hơn 10 năm qua, Chính phủ đã ưu tiên, chủ động đẩy mạnh sự phát triển của ngành công nghệ thông tin và truyền thông của nước ta.

Có thể nói công nghệ thông tin và truyền thông trong thời đại ngày nay có tầm ảnh hưởng, tác động rất lớn đến sự phát triển, ổn định của các doanh nghiệp và chính phủ của mỗi quốc gia nói chung và Việt Nam nói riêng. Tuy nhiên, điều này cũng đặt ra yêu cầu phải thực hiện tốt việc

bảo đảm an ninh mạng nhằm tạo nền tảng cho việc phát triển kinh tế - xã hội trong bối cảnh công nghệ thông tin đã len lỏi vào mọi mặt của đời sống chính trị - xã hội, quốc phòng - an ninh không chỉ của nước ta mà còn các nước trên thế giới.

Thực tế cho thấy, các vụ việc liên quan đến vấn đề an ninh mạng, an toàn, an ninh thông tin, công nghệ thông tin tại nước ta đã và đang diễn ra với tần suất ngày càng tăng và mức độ ảnh hưởng có chiều hướng mở rộng. Theo thống kê của Bộ Thông tin và Truyền thông, đến năm 2017, tỷ lệ người dùng Internet tại Việt Nam đạt 53% trên tổng số dân. Việt Nam đứng vị trí 16 trong top 20 quốc gia có số người sử dụng Internet nhiều nhất châu Á và độ tuổi người sử dụng đa phần là người trẻ. Trong bảng xếp hạng quốc gia sử dụng Facebook nhiều nhất thế giới, Việt Nam đứng ở vị trí thứ 7 với khoảng 64 triệu người dùng mỗi tháng trong khi chỉ số về tình hình an ninh mạng của Việt Nam ở mức khá thấp. Theo báo cáo của Liên minh Viễn thông quốc tế (ITU) về bảng xếp hạng Chỉ số An ninh mạng toàn cầu (GCI), Việt Nam xếp thứ 101 trên tổng số 193 nước thành viên về khả năng bảo đảm an ninh mạng[1]. Ông Nguyễn Viết Thế - Đại diện Hiệp hội Internet Việt Nam cho biết trong một nghiên cứu mới đây, hãng bảo mật Kaspersky kết luận

1. "53% dân số Việt Nam dùng Internet và vấn đề rủi ro an ninh mạng", website của Bộ Giao thông vận tải, xem tại: mt.gov.vn/tin-tuc/51864/53--dan-so-viet-nam-dung-internet-va-van-de-rui-ro-an-ninh-mang-.aspx.

rằng 3/4 người dùng Internet ở Việt Nam không biết tự bảo vệ mình trên mạng, 45% người sử dụng Internet gặp sự cố phần mềm độc hại, nhưng 13% người dùng bình thường không biết mình gặp phải vấn đề này[1].

Dưới góc độ an ninh mạng, thống kê một cách đầy đủ hơn cho thấy: Năm 2016, có tới gần 7.000 trang/cổng thông tin điện tử của nước ta bị tấn công. Nhiều thiết bị IoT chứa lỗ hổng bảo mật tạo điều kiện cho tin tặc khai thác đe dọa tống tiền hoặc ăn cắp dữ liệu. Đáng lưu ý, vụ tấn công mạng WannaCry đã làm hàng loạt các doanh nghiệp tại Việt Nam phải điêu đứng. Một số nạn nhân thì mất tiền chuộc, số khác bị mất dữ liệu và thông tin. Trong 9 tháng đầu năm 2017, có 9.964 sự cố tấn công mạng vào cá nhân, tổ chức tại Việt Nam[2]. Các cuộc tấn công bao gồm cả ba loại hình chính: Malware, Phishing và Deface. Trong đó, tấn công bằng mã độc (Malware) phát tán chiếm nhiều nhất với 4.595 lần, chiếm hơn 46% tổng số các cuộc tấn công. Trong số các nạn nhân bị tấn công bởi Malware có tới hơn 20 website có tên miền đuôi gov.vn. Loại hình tấn công thay đổi giao diện (Deface) được đánh giá là loại hình tấn công quy mô lớn với 3.607 trường hợp đã được ghi nhận. Trong đó, 21 trường hợp nhắm vào các website chính

---

1. Xem thêm http://mt.gov.vn/vn/tin-tuc/51765/van-de-dam-bao-an-toan-an-ninh-mang-o-viet-nam-dang-o-muc-thap-.aspx.

2. Xem thêm tại https://tinhte.vn/threads/nhung-van-de-an-ninh-mang-noi-bat-tai-viet-nam-nam-2017.2750668/.

phủ có tên miền là "gov.vn" nhưng đến nay đã khắc phục được gần hết. Loại hình website lừa đảo (Phishing) chiếm số lượng ít hơn với 1.762 sự cố. Báo cáo cũng ghi nhận 987 sự cố đã được khắc phục, trong đó có ba website tên miền gov.vn[1].

Dưới góc độ an ninh quốc gia, vấn đề an ninh mạng bị đe dọa thông qua việc các thế lực thù địch, tội phạm mạng gia tăng hoạt động tấn công mạng nhằm thu thập thông tin, bí mật nhà nước, bí mật nội bộ, chiếm quyền điều khiển, phá hoại hệ thống mạng thông tin; sử dụng Internet, nhất là các trang mạng xã hội với nhiều phương thức, thủ đoạn tinh vi, xảo quyệt nhằm gây chia rẽ nội bộ, xâm phạm lợi ích, an ninh quốc gia,... Những hoạt động đó đã tác động tiêu cực tới tư tưởng, nhận thức của một bộ phận cán bộ, đảng viên và nhân dân; gây tâm lý hoang mang, nghi ngờ, làm suy giảm lòng tin vào chế độ xã hội chủ nghĩa và vai trò lãnh đạo của Đảng, Nhà nước[2].

2. Thực trạng an ninh mạng tại Việt Nam

Trong những năm gần đây, Việt Nam trở thành một trong những quốc gia có tốc độ phát triển và ứng dụng

---

1. Xem thêm tại http://securitybox.vn/2540/an-toan-thong-tin-tai-viet-nam-2017/.

2. Xem thêm tại http://baodaknong.org.vn/an-ninh-trat-tu/bao-dam-an-ninh-mang-la-nhiem-vu-quan-trong-cap-bach-56939.html.

Internet nhanh nhất trên thế giới; đứng đầu Đông Nam Á về số lượng tên miền quốc gia; xếp thứ 2 khu vực Đông Nam Á, thứ 8 khu vực châu Á, thứ 30 thế giới về địa chỉ Ipv4 (tính đến tháng 12/2016). Việt Nam cũng đang nỗ lực trở thành quốc gia thứ 2 trong khu vực Đông Nam Á triển khai xây dựng thành phố thông minh để tạo môi trường sống cho người dân được tốt hơn, nâng cao hiệu quả phát triển kinh tế - xã hội bền vững.

Ở Việt Nam, ứng dụng công nghệ thông tin và các dịch vụ trên không gian mạng đã trở thành động lực quan trọng để phát triển kinh tế - xã hội, tạo thời cơ mới cho Việt Nam sử dụng thành tựu khoa học - công nghệ tiên tiến nhằm đẩy nhanh hơn tiến trình công nghiệp hóa, hiện đại hóa đất nước và thu hẹp khoảng cách phát triển, hội nhập sâu rộng hơn, hiệu quả hơn vào nền kinh tế thế giới, phát triển văn hóa - xã hội, củng cố quốc phòng, an ninh.

Hiện nay, Chính phủ điện tử đã được triển khai rộng khắp các địa phương, giúp giảm thiểu các thủ tục hành chính, nâng cao hiệu quả công tác quản lý nhà nước, tạo thuận lợi cho người dân và doanh nghiệp. Tại Bộ Ngoại giao, dưới sự chỉ đạo trực tiếp của Phó Thủ tướng, Bộ trưởng Ngoại giao Phạm Bình Minh, trong năm 2017, Bộ Ngoại giao đã hoàn thành nhiều nhiệm vụ quan trọng nhằm thực hiện Nghị quyết 36a/NQ-CP ngày 14/10/2015 của Chính phủ về Chính phủ điện tử như hoàn thành xây dựng hệ thống và hướng dẫn thực hiện qua mạng điện tử

đối với các dịch vụ công tại các Cơ quan đại diện của Việt Nam ở nước ngoài; tích hợp thông tin về các dịch vụ công trên Cổng dịch vụ công quốc gia; công khai tiến độ giải quyết hồ sơ trên Cổng thông tin điện tử chính phủ,... Đây là những kết quả cụ thể trong công tác chỉ đạo, điều hành thực hiện Nghị quyết 36a/NQ-CP đã được Văn phòng Chính phủ ghi nhận và đánh giá Bộ Ngoại giao là một trong 7/23 bộ, cơ quan đã hoàn thành toàn bộ các nhiệm vụ được giao.

Bên cạnh những lợi ích to lớn không thể phủ nhận mà không gian mạng đem lại, những thành tựu công nghệ thông tin mới cũng như những dịch vụ, ứng dụng thông minh trên không gian mạng cũng đã làm xuất hiện nhiều nguy cơ tiềm ẩn vô cùng lớn. Ở cấp độ quốc gia, khu vực và toàn cầu, những năm vừa qua, thông qua các cuộc tấn công mạng, hàng loạt thông tin, tài liệu mật, tài liệu nhạy cảm liên tục được công bố, ảnh hưởng nghiêm trọng đến đời sống chính trị trên thế giới, điển hình như vụ Wikileaks, "hồ sơ Panama" (năm 2016),... Nhiều quốc gia liên tục bị cáo buộc hoặc đổ lỗi cho nhau về hoạt động tiến công, thu thập thông tin tình báo qua mạng, tác động tâm lý, định hướng ý thức qua mạng; thậm chí, nhiều chuyên gia đã cảnh báo về nguy cơ các cuộc "chiến tranh mạng" giữa các quốc gia, các "chiến dịch xâm lược bằng công nghệ", nhất là từ các quốc gia đi trước hoặc đang có lợi thế hơn về trình độ công nghệ.

Sự phát triển của không gian mạng làm nảy sinh nhiều nguy cơ, thách thức mới đối với an ninh quốc gia cũng như an toàn, bảo mật thông tin của các cơ quan, doanh nghiệp và cá nhân. Vì thế, các chính sách, quy định về an ninh mạng phải được cập nhật thường xuyên và phù hợp với môi trường thực tế hiện nay.

2.1. Thực trạng

Thực trạng an ninh mạng và an toàn, an ninh thông tin mạng tại Việt Nam đang diễn biến phức tạp và nguy hiểm. Các cuộc tấn công mạng có quy mô, mức độ ngày càng lớn, tinh vi hơn và được chuẩn bị một cách kỹ lưỡng. Trong đó, các mục tiêu tấn công đang dần chuyển từ các mục tiêu cá nhân sang các mục tiêu là các tập đoàn kinh tế lớn hay nghiêm trọng hơn là các hệ thống thông tin quan trọng và hạ tầng mạng quốc gia.

Nửa đầu năm 2017, các cuộc tấn công của hai loại mã độc mã hóa dữ liệu, tống tiền WannaCry và Petya đã khai thác một lỗ hổng bảo mật của hệ điều hành Windows khiến cho hệ thống của nhiều cá nhân, doanh nghiệp cũng như cơ quan nhà nước tê liệt. Mặc dù ngay sau đó các hãng bảo mật trong và ngoài nước và chính Công ty Microsoft đã cập nhật ngay các bản vá lỗ hổng cho hệ điều hành, các công cụ xử lý nhưng nhiều đơn vị vẫn thờ ơ với vấn đề này và cho đến nay hệ thống giám sát an toàn mạng quốc gia của Bộ Thông tin và Truyền thông vẫn ghi nhận nhiều địa chỉ IP trong nước đang kết nối đến các máy chủ điều khiển mã độc này.

Hội thảo quốc tế Ngày An toàn thông tin Việt Nam năm 2017 với chủ đề "An toàn thông minh trong thế giới kết nối mới" đã công bố nhiều báo cáo quan trọng liên quan đến thực trạng an toàn thông tin hiện nay[1]. Tại hội thảo này, Hiệp hội An toàn thông tin Việt Nam (VNISA) đã trình bày báo cáo tổng hợp kết quả điều tra, đánh giá thực trạng an toàn thông tin tại Việt Nam năm 2017 và công bố Chỉ số an toàn thông tin của Việt Nam (Vietnam Information Security Index) năm 2017 và được đông đảo cộng đồng quan tâm. Phát biểu tại sự kiện khai mạc, Thứ trưởng Bộ Thông tin và Truyền thông Phạm Hồng Hải cho biết: Thời gian gần đây, các cuộc tấn công mạng đang gia tăng cả về số lượng và quy mô, diễn ra ngày càng tinh vi và phức tạp. Nhiều cuộc tấn công có chủ đích nhằm vào các cơ quan chính phủ, các hệ thống thông tin quan trọng trong nhiều lĩnh vực.

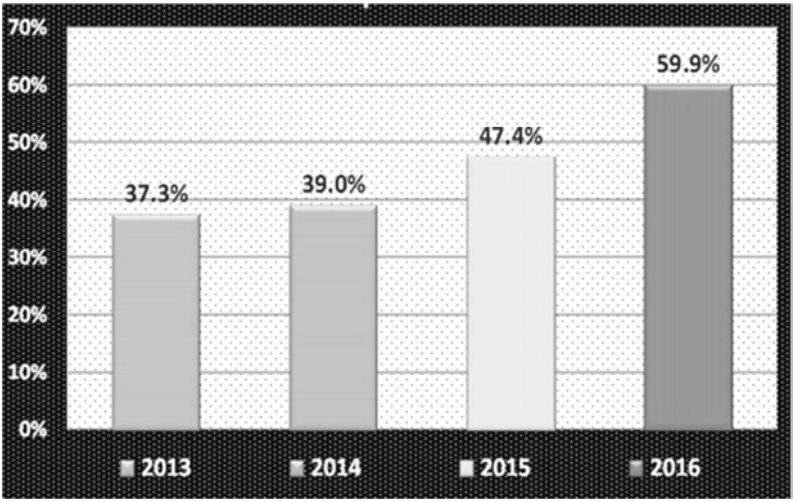
Năm 2017, chỉ số an toàn thông tin của Việt Nam là 54,2%, thấp hơn so với năm 2016 (59,9%) nhưng vẫn cao hơn so với năm 2015. Đại diện VNISA cho rằng, xu hướng phát triển an toàn thông tin năm 2017 là tích cực, do tác động của Luật An toàn thông tin mạng năm 2015, cùng các

---

1. Hội thảo này là sự kiện thường niên lần thứ 10, do Hiệp hội An toàn thông tin Việt Nam (VNISA) chủ trì, phối hợp với Cục An toàn thông tin, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (Bộ Thông tin và Truyền thông) và Cục Công nghệ thông tin (Bộ Quốc phòng) tổ chức, dưới sự bảo trợ của Bộ Thông tin và Truyền thông, Bộ Giáo dục và Đào tạo.

quy định pháp lý mới. Tuy nhiên, chỉ số an toàn thông tin của các doanh nghiệp vẫn còn thấp, đặc biệt là các doanh nghiệp vừa và nhỏ với nguy cơ mất an toàn thông tin rất cao. Các khâu thiết lập và thực thi chính sách an toàn thông tin vẫn còn hạn chế. Tốc độ phát triển an toàn thông tin tại Việt Nam còn chậm.

Chỉ số an toàn thông tin của Việt Nam giai đoạn 2013-2016



Nguồn: VNCERT.

Thay mặt VNISA, ông Vũ Quốc Khánh cũng đưa ra một số kiến nghị về tan toàn thông tin trong thời gian tới. Đó là Việt Nam cần có một cơ quan điều phối chiến lược toàn bộ hoạt động bảo đảm an ninh, an toàn thông tin mạng; tiếp

tục đẩy mạnh các hoạt động đào tạo nâng cao nhận thức và chuyên sâu; xây dựng cơ chế phối hợp và chia sẻ thông tin trong cộng đồng; đẩy mạnh các hoạt động khuyến khích phát triển an toàn thông tin, đặc biệt cần tiếp thu và phát triển công nghệ mới thông minh; mở rộng hợp tác quốc tế; tham gia tích cực vào công tác xây dựng môi trường pháp lý về an toàn thông tin và phát triển ứng dụng công nghệ thông tin thông minh trong bối cảnh Cuộc cách mạng công nghiệp 4.0. Bên cạnh đó, việc bảo đảm an toàn, an ninh thông tin quốc gia đòi hỏi sự phối hợp thống nhất của nhiều bộ, ngành, địa phương và toàn xã hội.

Tại Hội thảo - Triển lãm quốc gia về an ninh bảo mật năm 2017 (Security World 2017) với chủ đề chính "Chiến lược bảo đảm an ninh, an toàn thông tin trong thời kỳ Cách mạng công nghiệp lần thứ tư", Trung tướng Hoàng Phước Thuận, Cục trưởng Cục An ninh mạng - Bộ Công an đã có bài viết về tình hình an ninh mạng tại Việt Nam năm 2017 với năm nguy cơ chính, đó là: (i) Sự nhiễu loạn thông tin trên không gian mạng đe dọa đến cuộc sống an toàn của mỗi người dân, làm mất an ninh, trật tự xã hội; (ii) Hoạt động tấn công mạng nhằm vào các cơ sở hạ tầng thông tin trọng yếu ngày càng gia tăng về quy mô và tính chất nguy hiểm; (iii) Tội phạm sử dụng mạng máy tính xảy ra trên tất cả các lĩnh vực của đời sống xã hội, gia tăng cả về số vụ, tính chất, mức độ nghiêm trọng; (iv) Cơ sở hạ tầng viễn thông và công nghệ thông tin của Việt Nam chưa đáp ứng

yêu cầu bảo mật thiết yếu dẫn đến gia tăng nguy cơ bị tấn công mạng; (v) Công tác quản lý nhà nước về an ninh, an toàn thông tin còn nhiều hạn chế, bất cập, chưa đáp ứng được yêu cầu bảo đảm an ninh, an toàn thông tin trong tình hình hiện nay. Qua đó cho thấy cần thiết phải có giải pháp tổng thể từ việc ban hành và thực thi chính sách, pháp luật của cơ quan quản lý nhà nước về an ninh mạng.

Tại Bộ Ngoại giao, trong năm 2017, theo ghi nhận từ Hệ thống giám sát an ninh mạng do Ban Cơ yếu chính phủ triển khai tại Bộ Ngoại giao đã phát hiện hơn 100.000 cảnh báo tấn công vào hệ thống mạng công nghệ thông tin của Bộ Ngoại giao với nhiều thủ đoạn tinh vi, phức tạp như trinh sát hệ thống, do thám mật khẩu, khai thác lỗ hổng nhằm chiếm quyền điều khiển của các máy chủ trong hệ thống, bí mật mở kết nối tới máy chủ điều khiển ở nước ngoài để chuyển dữ liệu đã đánh cắp. Thủ đoạn nhúng mã độc vào các liên kết web nhằm đánh cắp thông tin xác thực người dùng, tấn công từ chối dịch vụ làm tê liệt hệ thống và tấn công gây lỗi tràn bộ đệm hệ thống để xâm nhập và leo thang đặc quyền cũng thường xuyên được tin tặc sử dụng nhưng sớm bị phát hiện. Đặc biệt trong giai đoạn bùng nổ mã độc tống tiền WannaCry, nhờ nâng cao cảnh giác và chủ động trong công tác bảo đảm an toàn thông tin nên hệ thống công nghệ thông tin của Bộ Ngoại giao không để xảy ra sự cố đáng tiếc, góp phần quan trọng bảo đảm thông tin liên lạc được an toàn, thông suốt, phục vụ công tác chỉ đạo, điều hành của Bộ.

Bộ Ngoại giao luôn coi công tác bảo vệ bí mật nhà nước, bảo đảm an ninh, an toàn mạng thông tin là công tác quan trọng hàng đầu, "có tính sống còn đối với hoạt động của Bộ". Bộ Ngoại giao luôn quan tâm, chỉ đạo sát sao với mục tiêu vừa thiết lập được một không gian mạng thông tin kỹ thuật số nhằm phục vụ hiệu quả cho công tác đối ngoại trong tình hình mới, vừa bảo đảm vững chắc an toàn, an ninh thông tin cho các hệ thống và ứng dụng công nghệ thông tin này. Để hoàn thành tốt các nhiệm vụ chính trị được giao theo Nghị định số 58/2013/NĐ-CP của Chính phủ ban hành ngày 11/6/2013 về quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Ngoại giao, Bộ Ngoại giao coi trọng công tác bảo đảm an toàn thông tin và an ninh mạng, đồng thời chủ động đề xuất các cơ chế, chính sách về hợp tác quốc tế trong lĩnh vực này nhằm cập nhật, khai thác thông tin từ các tổ chức an ninh mạng theo hướng đa chiều, đa quốc gia về các nguy cơ tấn công mạng nhằm phối hợp hiệu quả với các cơ quan chức năng trong nước như Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông sớm phát hiện các nguy cơ mất an toàn, an ninh thông tin, kịp thời xử lý các vấn đề phát sinh đối với hệ thống mạng, máy tính của Bộ Ngoại giao cũng như việc bảo đảm an ninh mạng và an toàn thông tin trong các hoạt động đối ngoại, quốc phòng, an ninh của Việt Nam.

2.2. Chính sách, hệ thống pháp lý về an ninh mạng

Sự kết nối và tương tác thông qua Internet đã mở ra một kỷ nguyên mới thúc đẩy tiến trình phát triển xã hội của nhân loại. Không gian mạng đã trở thành một bộ phận cấu thành và đóng vai trò rất quan trọng trong việc xây dựng xã hội thông tin và kinh tế tri thức. Do vậy, phát triển và làm chủ không gian mạng là một trong những nhiệm vụ quan trọng, cấp bách của các nước trên thế giới. Tuy nhiên, bên cạnh những lợi ích to lớn mà không gian mạng đem lại, các nước cũng phải đối mặt với các nguy cơ như chiến tranh mạng, gián điệp mạng, tấn công mạng, tội phạm mạng và nhiều vấn đề phức tạp mới.

Quan điểm xuyên suốt của Việt Nam là thúc đẩy sự phát triển thông qua việc ứng dụng các thành tựu mới nhất của khoa học - công nghệ, trong đó có công nghệ thông tin và dịch vụ không gian mạng. Tuy nhiên, việc áp dụng tiến bộ khoa học - kỹ thuật trong lĩnh vực này cũng tiềm ẩn những mối đe dọa, ví dụ như việc lợi dụng các dịch vụ mạng, không gian mạng để xâm phạm an ninh quốc gia, gây rối, mất trật tự an toàn, an ninh xã hội, xâm phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân. Một số hoạt động cụ thể như thiết lập hệ thống thông tin giả mạo nhằm lừa đảo trực tuyến, thu thập và khai thác thông tin cá nhân người sử dụng, phát tán mã độc trên diện rộng. Điều này đòi hỏi các tập đoàn, công ty khi cung cấp dịch vụ mạng phải bảo đảm việc an toàn thông tin cho người sử dụng.

Tuy nhiên, ngay cả các tập đoàn hàng đầu tư Google hay Facebook cũng chưa quan tâm đúng mức và có các giải pháp hiệu quả cho các vấn đề này. Việc các doanh nghiệp chưa quan tâm đúng mức đến vấn đề này đòi hỏi phải thiết lập một hành lang pháp lý quy định cho việc bảo đảm an ninh, an toàn trên không gian mạng. Đến nay, nhiều quốc gia trong đó có Mỹ, Đức, Anh, Nga, Trung Quốc,... đều đã ban hành các Luật về an ninh mạng, không gian mạng và đang tiếp tục hoàn thiện hành lang pháp lý cho vấn đề an ninh mạng[1]. Việt Nam cũng đang tìm hiểu và hoàn thiện các quy định pháp luật của riêng mình.

Để ứng phó với các thách thức kể trên, Đảng, Nhà nước Việt Nam luôn lãnh đạo, chỉ đạo công tác bảo đảm an toàn, an ninh mạng thông qua việc ban hành nhiều chủ trương, chính sách, pháp luật và giải pháp thúc đẩy ứng dụng, phát triển công nghệ thông tin trong các lĩnh vực gắn với bảo vệ vững chắc chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng; xây dựng không gian mạng an toàn, trở thành nguồn lực mạnh mẽ để xây dựng, bảo vệ và phát triển đất nước.

Đặc biệt, Nghị quyết số 28-NQ/TW ngày 25/10/2013 của Ban Chấp hành Trung ương Đảng (khóa XI) về Chiến lược bảo vệ Tổ quốc trong tình hình mới đã xác định nhiệm vụ phòng ngừa, ngăn chặn hiệu quả những nguy cơ xung

---

1. Xem thêm tại http://quochoi.org/khong-vi-pham-dieu-uoc-quoc-te-khi-yeu-cau-facebook-google-dat-may-chu-tai-viet-nam.html.

đột, chiến tranh biên giới, chiến tranh mạng. Bộ Chính trị ban hành Chỉ thị số 30-CT/TW ngày 25/12/2013 về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên Internet. Ban Bí thư ban hành Chỉ thị số 28-CT/TW ngày 16/9/2013 về tăng cường công tác bảo đảm an toàn thông tin mạng. Chỉ thị xác định công tác bảo đảm an toàn thông tin mạng là nhiệm vụ cấp bách, thường xuyên, lâu dài của cả hệ thống chính trị, là một bộ phận trọng yếu của cuộc đấu tranh bảo vệ an ninh quốc gia và giữ gìn trật tự an toàn xã hội[1]. Thủ tướng Chính phủ đã ban hành Chỉ thị số 15/CT-TTg ngày 17/6/2014 về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới.

Hành lang pháp lý trong lĩnh vực an toàn thông tin về cơ bản đã được xây dựng và đang dần hoàn thiện với việc Quốc hội thông qua Luật an toàn thông tin mạng năm 2015 (hiện đã có Luật an toàn thông tin mạng (sửa đổi, bổ sung năm 2018)) và các Nghị định hướng dẫn luật đã được ban hành. Ngày 27/5/2016, Thủ tướng Chính phủ cũng đã ban hành Quyết định số 898/QĐ-TTg phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016-2020. Điều này thể hiện sự quan tâm

---

1. Xem thêm tại http://netnam.vn/index.php/vi/tin-tuc/diem-bao/52-bao-chi-noi-v-netnam/621-giai-phap-bao-dam-an-toan-thong-tin-trong-tinh-hinh-hien-nay.html.

sâu sắc của lãnh đạo Đảng, Nhà nước đối với công tác bảo đảm an ninh mạng trong tình hình hiện nay.

Cũng trong lĩnh vực bảo đảm an toàn thông tin mạng, Bộ Thông tin - Truyền thông đã thành lập Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT). VNCERT được thành lập ngày 20/12/2005, theo Quyết định số 339/QĐ-TTg của Thủ tướng Chính phủ với nhiệm vụ điều phối các hoạt động ứng cứu sự cố máy tính toàn quốc, cảnh báo kịp thời các vấn đề về an toàn mạng máy tính, thúc đẩy hình thành hệ thống các đơn vị ứng cứu (CERT) trong các cơ quan, tổ chức, doanh nghiệp và là đầu mối thực hiện hợp tác với các tổ chức ứng cứu nước ngoài. Việc thành lập trung tâm ứng cứu khẩn cấp máy tính là mô hình khá phổ biến đã được nhiều nước trên thế giới áp dụng.

Các cơ quan, bộ, ngành được giao nhiệm vụ liên quan đến lĩnh vực an toàn thông tin bao gồm Bộ Quốc phòng, Bộ Công an, Bộ Thông tin và Truyền thông, Văn phòng Chính phủ, Bộ Khoa học và Công nghệ,... Trong đó, Bộ Thông tin và Truyền thông được giao nhiệm vụ bảo vệ, cảnh báo, điều phối, ứng cứu sự cố liên quan đến an toàn, an ninh mạng.

Về vấn đề thông tin cá nhân của người sử dụng dịch vụ mạng, Hiến pháp, Bộ luật dân sự, Luật bảo vệ người tiêu dùng và nhiều văn bản pháp luật chuyên ngành như các luật về viễn thông, công nghệ thông tin, giao dịch điện tử đều đã có quy định về quyền cơ bản của công dân và bảo vệ thông

tin cá nhân[1]. Phạm vi điều chỉnh của Luật an toàn thông tin mạng hiện chỉ quy định các vấn đề liên quan đến kỹ thuật nhằm bảo đảm thông tin truyền đi trên mạng được nguyên vẹn, không bị gián đoạn, sửa đổi hoặc phá hoại, được bảo đảm bí mật, nhưng không điều chỉnh vấn đề liên quan đến nội dung thông tin và thông tin riêng.

Luật an toàn thông tin mạng cùng với Bộ luật Dân sự, Luật bảo vệ người tiêu dùng và các văn bản pháp luật chuyên ngành khác như Luật viễn thông, Luật giao dịch điện tử,... tạo thành hệ thống pháp luật đồng bộ, đầy đủ cho công tác bảo vệ thông tin cá nhân của người sử dụng trong kỷ nguyên Internet hiện nay, góp phần thúc đẩy hơn nữa hoạt động giao dịch điện tử phục vụ phát triển kinh tế - xã hội của đất nước.

Trong vấn đề chiến tranh mạng, ngày 8/01/2018, Bộ Quốc phòng đã thành lập Bộ Tư lệnh Tác chiến không gian mạng theo Quyết định số 1198/QĐ-TTG ngày 15/8/2017 của Thủ tướng Chính phủ[2]. Điều này thể hiện sự tin tưởng của Đảng, Nhà nước đối với quân đội ta trong việc giao nhiệm vụ chiến đấu trên mặt trận mới. Trong "Chiến lược bảo vệ Tổ quốc trong tình hình mới", Đảng ta đã đề cao

---

1. Xem thêm tại http://antoanthongtin.vn/Detail.aspx?NewsID=3c5779c7-7f1e-4875-944a-d413317c6809&CatID=d9e1b0f7-8656-49ef-93de-c90c7d90d4e1.

2. Xem thêm tại http://vietnamnet.vn/vn/thoi-su/chinh-tri/thu-tuong-giao-nhiem-vu-cho-luc-luong-tac-chien-khong-gian-mang-422463.html.

trách nhiệm bảo vệ Tổ quốc trên không gian mạng, nhận định nguy cơ xảy ra chiến tranh mạng, mất an ninh thông tin ngày càng tăng và đặt ra mục tiêu phải chủ động phòng ngừa, ngăn chặn có hiệu quả chiến tranh mạng. Quán triệt chủ trương, quan điểm mới của Đảng trong việc thực hiện nhiệm vụ tăng cường quốc phòng, an ninh, đáp ứng yêu cầu nhiệm vụ bảo vệ vững chắc Tổ quốc, Quân ủy Trung ương, Bộ Quốc phòng đã tập trung chỉ đạo xây dựng chiến lược bảo vệ Tổ quốc trên không gian mạng để trình Bộ Chính trị, đồng thời chuẩn bị nguồn lực sẵn sàng để thực hiện nhiệm vụ tác chiến trên không gian mạng, góp phần bảo vệ Tổ quốc từ sớm, từ xa.

Luật an ninh mạng

Luật an ninh mạng năm 2018 được thông qua vào kỳ họp thứ 5 Quốc hội khóa XIV ngày 25/6/2018 gồm 07 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, quy định trách nhiệm của cơ quan, tổ chức, cá nhân[1]. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an

---

1. Lam Viet Nguyen: "Government - Private Cyber Security Cooperation: Lesson Learned from Viet Nam", in Centre for strategic and International Studies: *Towards a Resilient Regional Cyber Security: Prerspectives and challenges in Southeast Asia,* Kanisius Printing House Yoyarkata, 2019, pp.156-160.

ninh quốc gia là một trong những nội dung đặc biệt quan trọng của Luật an ninh mạng năm 2018 trong đó quy định đầy đủ các biện pháp, hoạt động bảo vệ tương xứng với mức độ quan trọng của hệ thống thông tin này, 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 và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia,...[1].

Để bảo vệ tối đa quyền và lợi ích hợp pháp của tổ chức, cá nhân, Luật an ninh mạng đã dành một chương (Chương III) quy định đầy đủ các biện pháp phòng ngừa, xử lý nhằm loại bỏ các nguy cơ đe dọa, các hành vi xâm phạm an ninh mạng, bao gồm: 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; phòng, chống gián điệp mạng, bảo vệ thông tin bí mật nhà nước, bí mật công tác, thông tin cá nhân trên không gian mạng; phòng ngừa, xử lý hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh, trật tự; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng, chống chiến tranh mạng;

---

1. "Hiểu về Luật an ninh mạng", http://tuyengiao.vn/ban-can-biet/hieu-ve-luat-an-ninh-mang-113375.

phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; 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 của Luật an ninh mạng 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 Việt Nam trên không gian mạng đã và đang bị sử dụng tràn lan với nhiều mục đích 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 nguồn dữ liệu này, 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 giá trị 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 Luật an ninh mạng, 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, ủy ban nhân dân cấp tỉnh 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.

Trên thực tế, Bộ Công an là đơn vị được giao chủ trì soạn thảo dự luật. Theo quan điểm của Bộ Công an, an ninh mạng trước hết cần nhìn nhận là vấn đề an ninh phi

truyền thống, có tác động qua lại với các vấn đề an ninh truyền thống là an ninh chính trị và an ninh quân sự. An ninh mạng là đảm bảo sự bất khả xâm phạm về chủ quyền quốc gia trên không gian mạng, đảm bảo thông tin trên mạng không gây hại đến chế độ chính trị, kinh tế, nền văn hóa, an ninh, quốc phòng, đối ngoại, độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ quốc gia, cũng như sự vận hành ổn định, đảm bảo an ninh của hệ thống mạng thông tin quốc gia. Bên cạnh đó, an ninh mạng còn gắn kết chặt chẽ với an ninh tài chính, tiền tệ, hoạt động ổn định của hệ thống ngân hàng, thị trường chứng khoán và sở hữu trí tuệ[1].

Trong quá trình xây dựng và ban hành Luật, an ninh mạng nội dung gây tranh cãi là việc quy định các hãng công nghệ nước ngoài phải đặt máy chủ và có văn phòng đại diện tại Việt Nam thì mới được cấp phép cung cấp các dịch vụ mạng trong nước. Tuy nhiên, thực tế cho thấy, việc có văn phòng đại diện tại thị trường cung cấp dịch vụ là cần thiết để bảo vệ lợi ích của nhà cung cấp cũng như người sử dụng. Về vấn đề máy chủ, hiện nay, một số công ty dịch vụ xuyên biên giới như Google, Facebook đã đặt một phần hoặc một số loại hình máy chủ dữ liệu tại nước ta. Việc đặt máy chủ như vậy đem lại lợi ích cho cả nhà cung cấp dịch vụ và người sử dụng. Bộ Công an cho rằng, khi đặt văn phòng,

---

1. Xem thêm tại http://jetking.fpt.edu.vn/du-thao-luat-anm-va-su-chuyen-bien-trong-nhan-thuc-cua-viet-nam/.

máy chủ ở Việt Nam, các nhà cung cấp dịch vụ viễn thông sẽ phối hợp nhanh trong việc phòng, chống tội phạm, chống mã độc với các cơ quan chức năng. Ngoài ra, các cơ quan còn phối hợp tốt trong các hoạt động khác như kinh doanh, chống thất thu tiền thuế. Đặc biệt, việc đặt máy chủ ở Việt Nam sẽ giúp tốc độ truy cập nhanh, truy thu hàng tỷ đôla mỗi năm về băng thông khi đi thuê ở nước ngoài, tăng cường công tác bảo vệ an ninh quốc gia[1].

Hiện nay, nhiều quốc gia trên thế giới cũng đã yêu cầu các nhà cung cấp dịch vụ mạng phải địa phương hóa dữ liệu để đảm bảo vấn đề an ninh thông tin. Ví dụ, Luật lưu trữ dữ liệu của Nga (2015) đã yêu cầu các hãng công nghệ như Facebook, Linked In, Google phải đặt máy chủ dữ liệu tại Nga. Linked In đã bị cấm hoạt động tại Nga kể từ 2016 do không đáp ứng yêu cầu về máy chủ. Liên minh châu Âu cũng có các quy định tương tự. Bốn trung tâm dữ liệu của Google đã được đặt tại Phần Lan, Bỉ, Hà Lan, Ailen. Tại Trung Quốc, hiện chỉ có icloud và Linked In là được phép hoạt động. Nhật Bản, Đài Loan và nhiều nước khác cũng đã ban hành chính sách quản lý địa phương hóa dữ liệu, tức là các doanh nghiệp nước ngoài muốn kinh doanh, khai thác phải đặt máy chủ ở nước sở tại[2].

---

1. Xem thêm tại https://vnexpress.net/tin-tuc/phap-luat/cuc-truong-an-ninh-mang-yeu-cau-facebook-dat-may-chu-o-viet-nam-3672035.html.

2. Xem thêm tại https://vnexpress.net/tin-tuc/phap-luat/cuc-truong-an-ninh-mang-yeu-cau-facebook-dat-may-chu-o-viet-nam-3672035.html.

Việt Nam tham gia hợp tác quốc tế trong lĩnh vực không gian mạng và an ninh mạng

Cùng với việc thiết lập Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), trung tâm này đã đại diện phía Việt Nam tham gia mạng lưới CERTs khu vực và thế giới, tham gia và chủ động tổ chức các hoạt động trong khuôn khổ mạng lưới CERTs.

- Trong khuôn khổ hợp tác giữa Campuchia, Lào, Mianma và Việt Nam (CLMV), Việt Nam đã chủ trì hội thảo về chính sách và hợp tác quốc tế trong lĩnh vực an toàn thông tin mạng lần thứ hai. Đây là sự kiện do CERTs phối hợp với ICT4Peace Foundation tổ chức tại Hà Nội trong hai ngày 12-13/10/2017. Hội thảo lần đầu tiên được tổ chức tại Lào năm 2016[1].

- Trong khuôn khổ ASEAN, một số cơ chế liên quan đến vấn đề an ninh mạng như trụ cột chính trị - an ninh, nhóm làm việc giữa kỳ về công nghệ thông tin và truyền thông,... Hiện nay, ASEAN đang thực hiện các bước đi nhằm tăng cường hợp tác quốc tế để xây dựng một chiến lược không gian mạng chung cho các nước trong cộng đồng ASEAN như: tổ chức hội thảo về các quy tắc, chuẩn mực trên mạng cho các nước ASEAN vào đầu năm nay và Hội nghị Bộ trưởng ASEAN về an ninh không gian mạng lần thứ hai vào tháng 9 năm 2017.

---

1. Xem thêm tại http://ictnews.vn/cntt/bao-mat/cac-nuoc-can-tang-cuong-hop-tac-de-giai-quyet-thach-thuc-ve-an-ninh-mang-159658.ict.

- Trong khuôn khổ Liên hợp quốc: Việt Nam trở thành thành viên của Liên minh Viễn thông quốc tế kể từ năm 1976. Đây là tổ chức chuyên môn của Liên hợp quốc, được thành lập ngày 15/7/1947. Việt Nam đã tham gia Hội đồng Điều hành ITU ba nhiệm kỳ liên tiếp 1994-1998, 1998-2002, 2002-2006 và hiện đang tiếp tục tham gia vào nhóm nghiên cứu số 3 trong lĩnh vực tiêu chuẩn hoá viễn thông về vấn đề tính cước và thanh toán nhằm bảo vệ quyền lợi cho các nước đang phát triển[1].

Một số kết quả đạt được trong việc hợp tác với các nhà cung cấp dịch mạng quốc tế nhằm bảo đảm vấn đề an ninh, an toàn mạng tại Việt Nam

Trong bối cảnh Việt Nam là thị trường tiềm năng về dịch vụ mạng, các cơ quan chức năng của Việt Nam và các nhà cung cấp dịch vụ mạng trong nước và quốc tế đã hợp tác cùng nhau để vừa đáp ứng yêu cầu của cơ quan quản lý và vừa bảo đảm sự phát triển của các dịch vụ mạng. Cụ thể, trong thời gian qua, Facebook đã hợp tác với Chính phủ Việt Nam và Bộ Thông tin và Truyền thông trong việc ngăn chặn, gỡ bỏ thông tin vi phạm pháp luật Việt Nam trên mạng xã hội Facebook, trong đó tập trung gỡ bỏ tài khoản giả mạo của các tổ chức, cá nhân và các nội dung rao bán, quảng cáo các sản phẩm, dịch vụ bất hợp pháp; cơ chế

---

1. Xem thêm tại http://www.mofahcm.gov.vn/en/mofa/ctc_quocte/un/nr040819155753/nr060928111253/ns060928104826.

thông tin liên lạc, phối hợp giữa đầu mối của Bộ với Facebook đã có nhiều tiến triển. Kết quả bước đầu của sự hợp tác này đã tạo được cơ chế liên lạc, trao đổi thông suốt, nhanh chóng, trực tiếp đến đại diện của Facebook tại Đông Nam Á. Trong thời gian qua, mạng xã hội Facebook đã gỡ bỏ hơn 670 tài khoản trong tổng số gần 5.000 tài khoản Facebook giả mạo, có hoạt động gây chia rẽ, xúc phạm danh dự cá nhân, tổ chức, quảng bá hình ảnh dâm ô, đồi trụy, kích động bạo lực. Tương tự, theo yêu cầu của Bộ Thông tin và Truyền thông, Google và Youtube đã chặn và hạ các video xấu, độc hại, vi phạm pháp luật Việt Nam. Tuy nhiên, con số 670 tài khoản bị gỡ bỏ vẫn còn nhỏ so với số lượng 5.000 tài khoản giả mạo, vi phạm pháp luật. Bên cạnh đó, cơ chế hợp tác giữa Facebook và Bộ Thông tin và Truyền thông thời gian qua được cho là chưa đạt được kết quả như mong muốn, do đó cần phải có cơ chế hợp tác tốt hơn để đưa Facebook phát triển lành mạnh hơn nữa trên lãnh thổ Việt Nam, tuân thủ pháp luật của Việt Nam, cùng chia sẻ, hợp tác với nhau trong việc xử lý các vấn đề mà Chính phủ Việt Nam quan ngại.

Hành lang pháp lý của Việt Nam trong lĩnh vực không gian và an ninh mạng

Tại Việt Nam trước khi Luật An toàn thông tin mạng có hiệu lực từ ngày 01/7/2016 thì hành lang pháp lý về an toàn

thông tin còn đơn giản và chưa hoàn chỉnh trong rất nhiều văn bản như:

- **Bảy bộ luật**: Luật giao dịch điện tử số 51/2005/QH11; Luật công nghệ thông tin số 67/2006/QH11; Luật quảng cáo số 16/2012/QH13; Luật cơ yếu số 05/2011/QH13; Luật sửa đổi, bổ sung một số điều của Bộ luật hình sự số 37/2009/QH12 (Điều 224-226b); Luật bảo vệ quyền lợi người tiêu dùng số 59/2010/QH12; Luật viễn thông số 41/2009/QH12.

- **Mười hai nghị định của Chính phủ**: Nghị định số 57/2006/NĐ-CP về thương mại điện tử; Nghị định số 72/2013/NĐ-CP về quản lý, cung cấp sử dụng dịch vụ Internet và thông tin trên mạng; Nghị định số 26/2007/NĐ-CP Quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số; Nghị định số 77/2012/NĐ-CP sửa đổi, bổ sung một số điều của Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 về chống thư rác; Nghị định số 63/2007/NĐ-CP Quy định xử phạt vi phạm hành chính trong lĩnh vực công nghệ thông tin; Nghị định số 83/2011/NĐ-CP Quy định xử phạt vi phạm hành chính trong lĩnh vực viễn thông; Nghị định số 64/2007/NĐ-CP Ứng dụng công nghệ thông tin trong cơ quan nhà nước; Nghị định số 43/2011/NĐ-CP Quy định về việc cung cấp thông tin và dịch vụ công trực tuyến trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ

quan nhà nước; Nghị định số 90/2008/NĐ-CP về chống thư rác; Nghị định số 25/2011/NĐ-CP Quy định chi tiết và hướng dẫn thi hành một số điều của Luật Viễn thông; Nghị định số 72/2013/NĐ-CP quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng; Nghị định số 28/2009/NĐ-CP Quy định xử phạt vi phạm hành chính trong quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử trên Internet.

- Mười thông tư: 8 Thông tư của Bộ Thông tin và Truyền thông gồm: Thông tư số 07/2008/TT-BTTTT hướng dẫn một số nội dung về hoạt động cung cấp thông tin trên trang thông tin điện tử cá nhân trong Nghị định số 97/2008/NĐ-CP ngày 28/8/2008 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử trên Internet; Thông tư số 27/2011/TT-BTTTT Quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam; Thông tư số 12/2008/TT-BTTTT hướng dẫn thực hiện một số nội dung của Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác; Thông tư số 37/2009/TT-BTTTT Quy định về hồ sơ và thủ tục liên quan đến cấp phép, đăng ký, công nhận các tổ chức cung cấp dịch vụ chứng thực chữ ký số; Thông tư số 23/2011/TT-BTTTT Quy định về việc quản lý, vận hành, sử dụng và bảo đảm an toàn thông tin mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; Thông tư số

14/2010/TT-BTTTT Quy định chi tiết một số điều của Nghị định số 97/2008/NĐ-CP ngày 28/8/2008 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử trên Internet đối với hoạt động quản lý trang thông tin điện tử và dịch vụ mạng xã hội trực tuyến; Thông tư số 09/2011/TT-BTTTT sửa đổi, bổ sung một số quy định của Thông tư số 09/2008/TT-BTTTT ngày 24/12/2008 (hướng dẫn về quản lý và sử dụng tài nguyên Internet) và Thông tư số 12/2008/TT-BTTTT ngày 30/12/2008 (hướng dẫn thực hiện một số nội dung của Nghị định số 90/2008/NĐ-CP ngày 13/8/2008 của Chính phủ về chống thư rác); Thông tư số 25/2010/TT-BTTTT quy định việc thu thập, sử dụng, chia sẻ, bảo đảm an toàn và bảo vệ thông tin cá nhân trên trang thông tin điện tử hoặc cổng thông tin điện tử của cơ quan nhà nước. Hai thông tư của Bộ Nội vụ và Ngân hàng Nhà nước gồm: Thông tư số 05/2010/TT-BNV của Bộ Nội vụ hướng dẫn về cung cấp, quản lý và sử dụng dịch vụ chứng thực chữ ký số chuyên dùng phục vụ các cơ quan thuộc hệ thống chính trị; Thông tư số 29/2011/TT-NHNN của Ngân hàng Nhà nước Quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet.

- **Một số Nghị quyết của Trung ương:** Nghị quyết số 28-NQ/TW ngày 25/10/2013 của Ban Chấp hành Trung ương Đảng (khóa XI) về Chiến lược bảo vệ Tổ quốc trong

tình hình mới đã xác định nhiệm vụ phòng ngừa, ngăn chặn hiệu quả các nguy cơ xung đột, chiến tranh biên giới, chiến tranh mạng,... Ngày 16/9/2013, Ban Bí thư Trung ương Đảng đã ban hành Chỉ thị số 28-CT/TW về tăng cường công tác bảo đảm an toàn thông tin mạng. Bộ Chính trị cũng đã ban hành Chỉ thị số 30-CT/TW ngày 25/12/2013 về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên Internet.

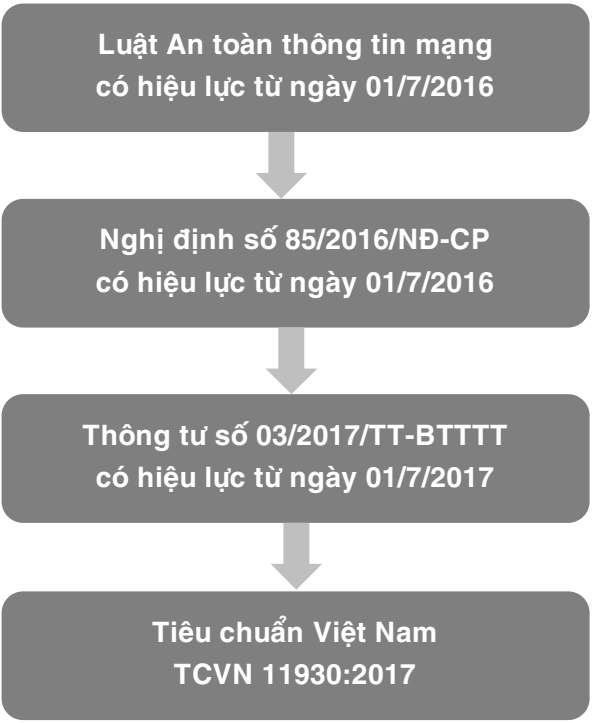
Một số văn bản điều hành của Chính phủ: Chỉ thị số 897/CT-TTg của Thủ tướng Chính phủ ngày 10/6/2011 về việc tăng cường triển khai các hoạt động bảo đảm an toàn thông tin số; Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an ninh và an toàn thông tin mạng trong tình hình mới; Quyết định số 63/QĐ-TTg của Thủ tướng Chính phủ ngày 13/01/2010 phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020; Quyết định số 1755/QĐ-TTg của Thủ tướng Chính phủ ngày 22/02/2010 phê duyệt Đề án "Đưa Việt Nam sớm trở thành nước mạnh về công nghệ thông tin và truyền thông"; Quyết định số 632/QĐ-TTg ngày 10/5/2017 của Thủ tướng Chính phủ về việc ban hành Danh mục lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin mạng và hệ thống thông tin quan trọng quốc gia.

- **Một số tiêu chuẩn kỹ thuật hướng dẫn việc thực hiện:**

Tiêu chuẩn TCVN	***9 dự thảo TCVN***
TCVN ISO/IEC 27001:2009	TCVN ~ SO/IEC 27000:2012
TCVN ISO/IEC 27002:2011	TCVN ~ SO/IEC 27003:2010
TCVN 8709-1:2011 (ISO/IEC 15408-1:2009)	TCVN ~ SO/IEC 27004:2009
TCVN 8709-2:2011 (ISO/IEC 15408-2:2008)	TCVN ~ ISO/IEC 27005:2011
TCVN 8709-3:2011 (ISO/IEC 15408-3:2008)	TCVN ~ ISO/IEC 27010:2012
	TCVN ~ ISO/IEC 27033-1:2009
	TCVN ~ ISO/IEC 27033-2:2012
	TCVN ~ ISO/IEC 27033-3:2010
	TCVN ~ ISO/IEC 27035:2011

Luật an toàn thông tin mạng có hiệu lực thi hành từ ngày 01/7/2016, trên cơ sở đó, môi trường pháp lý về an toàn thông tin đã phần nào được định hình, có trọng tâm, trọng điểm; thường xuyên, liên tục. Tiếp đến là Nghị định số 85/2016/NĐ-CP quy định chi tiết về tiêu chí, thẩm quyền, trình tự, thủ tục xác định cấp độ an toàn hệ thống thông tin và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ đối với cơ quan, tổ chức, cá nhân tham gia hoặc có liên quan đến hoạt động thông tin tại Việt Nam; Thông tư số 03/2017/TT-BTTTT của Bộ Thông tin và Truyền thông ngày 24/4/2017 quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP của Chính phủ ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ; Quyết định số 2582/QĐ-BKHCN của Bộ Khoa học và Công nghệ ngày 06/9/2018 về việc công bố Tiêu chuẩn quốc gia TCVN 11930:2017, tiêu

chuẩn về công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.



Đối với Luật an ninh mạng năm 2018, Bộ Công an đang là đơn vị chủ trì xây dựng Dự thảo Nghị định của Chính phủ quy định một số điều của Luật an ninh mạng và Dự thảo Quyết định của Thủ tướng Chính phủ ban hành Danh mục hệ thống thông tin quan trọng về an ninh quốc gia. Dự thảo Nghị định này gồm 06 chương, 30 điều, quy định các

nội dung cụ thể, trọng tâm của các vấn đề được giao xây dựng, trong đó tập trung chủ yếu vào xác định căn cứ xác lập, điều kiện và cơ chế phối hợp bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; vấn đề lưu trữ dữ liệu và đặt văn phòng đại diện tại Việt Nam[1]. Còn Dự thảo Quyết định nói trên của Thủ tướng Chính phủ gồm 03 điều, 01 Phụ lục Danh mục hệ thống, chỉ quy định việc ban hành Danh mục và trách nhiệm của các bộ, ngành liên quan tới Danh mục hệ thống thông tin quan trọng về an ninh quốc gia[2]. Việc sớm ban hành hai dự thảo nêu trên sẽ giúp việc triển khai áp dụng chính sách vào cuộc sống hiệu quả, thiết thực và minh bạch hơn; giải tỏa những suy nghĩ, tranh cãi về những nội dung như "vấn đề lưu trữ dữ liệu và đặt văn phòng đại diện tại Việt Nam",...

3. Kiến nghị chính sách đối ngoại của Việt Nam trong lĩnh vực an ninh mạng

Trên cơ sở phân tích tình hình an ninh mạng, hợp tác và đấu tranh giữa các quốc gia trong vấn đề không gian mạng

---

1. "Dự thảo Nghị định quy định chi tiết một số điều của Luật an ninh mạng", xem thêm tại http://bocongan.gov.vn/vanban/Pages/van-ban-moi.aspx?ItemID=314.

2. "Dự thảo Quyết định của Thủ tướng Chính phủ ban hành Danh mục hệ thống thông tin quan trọng về an ninh quốc gia", xem thêm tại http://bocongan.gov.vn/vanban/Pages/van-ban-moi. aspx?ItemID=314.

cũng như thực tiễn vấn đề an ninh mạng tại Việt Nam hiện nay, việc bảo đảm an ninh mạng của Việt Nam cần thực hiện theo các phương châm như sau:

-Thực thi việc bảo đảm an ninh mạng phù hợp với các công ước quốc tế.

- Bảo đảm không gian mạng được xây dựng, duy trì, phát triển theo các quy trình, tiêu chuẩn, quy chuẩn kỹ thuật.

- Bảo đảm sự phát triển bền vững của công nghệ thông tin và truyền thông, góp phần thúc đẩy sự phát triển kinh tế - xã hội.

- Động viên, khuyến khích toàn dân tham gia và có trách nhiệm trong công cuộc bảo vệ chủ quyền quốc gia trên không gian mạng.

Những phương châm này thể hiện cách tiếp cận toàn diện về việc bảo đảm an ninh mạng trong bối cảnh thực tiễn của Việt Nam hiện nay, đồng thời phù hợp với sự vận động của vấn đề an ninh mạng tại khu vực và trên thế giới.

Theo đó, từ khía cạnh đối ngoại, Việt Nam cần có cách tiếp cận và thực hiện theo một số giải pháp cụ thể như sau:

3.1. Bảo đảm an ninh mạng và bảo vệ chủ quyền, lợi ích quốc gia - dân tộc trên không gian mạng

Thực tế, văn kiện Đại hội lần thứ XII của Đảng đã chỉ rõ "... kiên quyết, kiên trì đấu tranh bảo vệ vững chắc độc lập, chủ quyền, thống nhất và toàn vẹn lãnh thổ của Tổ quốc, bảo vệ Đảng, Nhà nước, nhân dân và chế độ xã hội

chủ nghĩa"[1]. Hiện nay, chủ quyền lãnh thổ còn được hiểu là cả chủ quyền lãnh thổ trên không gian mạng (ngoài chủ quyền đất liền, biển, đảo, vùng trời). Do đó, đối với không gian mạng, Việt Nam cũng cần bảo đảm khả năng thực thi quyền và quản lý đối với không gian mạng. Cụ thể hơn, văn kiện khẳng định: "Tích cực, chủ động chuẩn bị lực lượng đủ mạnh và các kế hoạch, phương án tác chiến cụ thể, khoa học, sẵn sàng bảo vệ vững chắc độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ và an ninh của Tổ quốc trong mọi tình huống"[2].

Để thực hiện được các mục tiêu kể trên, Việt Nam cần chuẩn bị năng lực kỹ thuật, nhân lực để ứng phó hiệu quả với các cuộc tấn công mạng, tội phạm mạng và bảo đảm chủ quyền quốc gia trên không gian mạng.

Việc xây dựng chính sách của Việt Nam trong lĩnh vực an ninh mạng cần phải tính đến các yếu tố bảo đảm an ninh mạng, bảo đảm chủ quyền quốc gia trên không gian mạng, tham gia hợp tác quốc tế trong lĩnh vực không gian mạng nhưng tránh để không bị lôi kéo vào các cuộc cạnh tranh giữa các nước lớn trong lĩnh vực an ninh mạng. Các yếu tố này mang tính đen xen và bổ sung, hỗ trợ nhau. Do đó, khi triển khai thực hiện có hiệu quả chính sách an ninh mạng, Việt Nam nên:

1, 2. Đảng Cộng sản Việt Nam: *Văn kiện Đại hội đại biểu toàn quốc lần thứ XII, Sđd,* tr.153, 150.

Thứ nhất, thúc đẩy việc nâng cao năng lực về trình độ kỹ thuật, nguồn nhân lực có trình độ để nghiên cứu, sáng tạo và vận hành công nghệ thông tin và truyền thông để thực thi việc quản lý nhà nước trên không gian mạng.

Để nâng cao năng lực kỹ thuật và nguồn nhân lực, Việt Nam cần tính đến việc hợp tác công tư trong lĩnh vực không gian mạng. Đặc thù của lĩnh vực này là các cơ quan hoạch định chính sách quốc gia có năng lực ban hành chính sách, luật pháp để tăng cường bảo đảm an ninh mạng; phòng, chống tội phạm trên môi trường mạng, tuy nhiên, chính sách, luật pháp thường lạc hậu so với các biện pháp tấn công mạng ngày càng phức tạp và tinh vi của tội phạm mạng. Trong khi đó, nhóm kỹ thuật (chủ yếu là khối tư nhân) thường sáng tạo và phát triển ra các công nghệ mới, phần mềm mới,... nên có năng lực xây dựng các cơ chế bảo mật, an ninh cho môi trường mạng và sự linh hoạt trong các biện pháp, chính sách ứng phó với các sự cố, rủi ro trên không gian mạng. Do đó, khu vực công (chính phủ) và khu vực tư nhân cần tăng cường hợp tác để bảo đảm cả về mặt năng lực và biện pháp trong lĩnh vực an ninh mạng.

Thứ hai, trong bối cảnh năng lực công nghệ và nguồn nhân lực còn hạn chế, Việt Nam nên chủ động thúc đẩy hợp tác quốc tế trong lĩnh vực này, kể cả các cơ chế đa phương và song phương. Ở cấp độ song phương, ngoài hợp tác với các nước lớn, Việt Nam có thể tham khảo kinh

nghiệm của các nước vừa và nhỏ. Tuy các nước này có quy mô dân số, kinh tế, diện tích nhỏ nhưng có năng lực về công nghệ thì vẫn có khả năng bảo đảm an ninh mạng, thậm chí một số quốc gia nhỏ nhưng lại được coi là cường quốc trong lĩnh vực không gian mạng như Ixaren và Extônia. Tuy nhiên, trong hợp tác song phương, Việt Nam cần tránh không để bị lôi kéo, rơi vào vòng cạnh tranh giữa các nước lớn trong lĩnh vực không gian mạng. Việt Nam cần hết sức chú ý khi ký các hiệp định song phương trong lĩnh vực an ninh mạng để tránh rơi vào việc bị lôi vào các vụ việc cạnh tranh, xung đột về an ninh mạng (do tính khó định danh của tấn công mạng).

Ngoài hợp tác trong lĩnh vực kỹ thuật, công nghệ, đào tạo nguồn nhân lực, Việt Nam cũng cần chú trọng đến hợp tác xây dựng các quy chuẩn, tập quán và luật lệ trên không gian mạng theo hướng lồng ghép các ý tưởng, quan điểm có lợi cho nước ta vào các quá trình này. Đây vẫn là lĩnh vực còn nhiều tranh cãi do lợi ích, quan điểm của các quốc gia, đặc biệt là các nước lớn (Mỹ, Nga, Trung Quốc) còn khác nhau.

Thứ ba, để bảo đảm độc lập - tự chủ trong quản lý không gian mạng, Việt Nam cần nghiên cứu một cách kỹ lưỡng và tính toán việc hợp tác hiệu quả với các nhà cung cấp dịch vụ mạng, đặc biệt là các hãng nhà cung cấp dịch vụ nước ngoài trong việc quản lý các dịch vụ mạng, nội dung truyền tải trên không gian mạng.

3.2. Tăng cường hợp tác, theo dõi và thúc đẩy (theo khả năng) vấn đề an ninh mạng ở cấp độ khu vực

Như phân tích ở trên, để bảo đảm an ninh mạng, Việt Nam cần chú trọng đến hợp tác quốc tế ở cả cấp độ song phương và đa phương. Tuy nhiên, hợp tác đa phương trong lĩnh vực này đang gặp nhiều trở ngại.

Thực tiễn năng lực kỹ thuật cũng như quan điểm của các nước đối với vấn đề an ninh mạng còn nhiều khác biệt, việc thảo luận và xây dựng quy phạm pháp luật về an ninh mạng dự kiến còn nhiều khó khăn, bế tắc. Do đó, quá trình này cần sự tham gia rộng rãi của các bên liên quan (stakeholders). Để bảo đảm tính hiệu quả, thực chất, một số nước thậm chí đã đề xuất tạm dừng thảo luận các vấn đề an ninh mạng ở tầm quốc tế, thay vào đó, các quốc gia nên tập trung thảo luận ở các cơ chế khu vực. Trong khuôn khổ Liên hợp quốc, có thể tính đến một cuộc họp của UN GGE hoặc sử dụng các diễn đàn quốc tế khác như các ủy ban của Đại Hội đồng Liên hợp quốc hay Nhóm làm việc, trao đổi (Open ended working group - OEWG), Ủy ban Giải trừ quân bị của Liên hợp quốc (United Nations Disarmament Commission - UNDC),...

Do đó, dù tăng cường hợp tác quốc tế, cả đa phương và song phương, toàn cầu và khu vực, Việt Nam cần tính đến những khó khăn, hạn chế trong xây dựng luật, tập quán ở cấp độ toàn cầu. Từ đó, việc tham gia của Việt Nam trong khuôn khổ này nên ở mức vừa phải, đồng thời tập trung

nguồn lực và nỗ lực trong các khuôn khổ phù hợp, có lợi ích sát sườn với nước ta và có triển vọng đạt được tiến triển. Tại khu vực, hai cơ chế hợp tác an ninh chính hiện nay là Diễn đàn khu vực ASEAN (ARF) và ASEAN đang là hai cơ chế gồm nhiều đối tác chính của Việt Nam, bao gồm không chỉ các quốc gia láng giếng mà cả các nước lớn, có vai trò và ảnh hưởng đối với toàn cầu và khu vực (như Mỹ, Nga, Trung Quốc, Nhật Bản,...). Đây cũng là môi trường an ninh sát sườn, do đó cần tập trung nguồn lực vào hai cơ chế này.

ASEAN

ASEAN ngày càng đề cao sự cần thiết trong việc bảo đảm an ninh mạng. Do vấn đề an ninh mạng mang tính khu vực, chịu ảnh hưởng của tình hình địa - chính trị, kinh tế - xã hội của khu vực, nên các nỗ lực trong lĩnh vực an ninh mạng cần được tiến hành ở tầm khu vực dựa trên hoàn cảnh, điều kiện và năng lực kỹ thuật của từng nước. ASEAN hiện đã thông qua Bản ghi nhớ năm 2012 về việc hỗ trợ nâng cao năng lực và tăng cường hợp tác của nhóm kỹ thuật để đánh giá, nghiên cứu về vai trò của nhà nước, các quy phạm pháp luật và luật quốc tế đối với an ninh mạng, đồng thời nhấn mạnh sự cần thiết của việc đẩy mạng trao đổi, nghiên cứu về an ninh mạng trong kênh 2[1] của

1. Kênh 2 là Kênh đối thoại không chính thức về an ninh và chính trị của ASEAN (*BT*).

ASEAN với các quốc gia có liên quan. Do vậy, Việt Nam cần đẩy mạnh việc thực hiện các văn bản, thỏa thuận về vấn đề an ninh mạng trong ASEAN. Cụ thể, Việt Nam có thể thúc đẩy các biện pháp nhằm tăng cường khả năng của ASEAN trong bảo đảm an ninh mạng như sau:

(i) Thiết lập Nhóm hỗ trợ về an ninh mạng cho Ban Thư ký ASEAN với nhiệm vụ phục vụ, bảo đảm an ninh thông tin, đường truyền, trao đổi đối với các nước ASEAN, đặc biệt là các nước đảm nhiệm vai trò chủ tịch; đồng thời hiện thực hóa các nỗ lực xây dựng năng lực an ninh mạng như thành lập Tổ tư vấn quốc tế giúp tăng cường năng lực khu vực để hỗ trợ các quốc gia, tăng tính hiệu quả các chương trình nâng cao năng lực, thúc đẩy điều phối và hỗ trợ thực chất trong các chương trình này.

(ii) Thúc đẩy hợp tác, trao đổi về vấn đề an ninh mạng trong kênh lập pháp vì trong thời gian tới, nhu cầu về xây dựng pháp luật trong lĩnh vực không gian mạng ngày càng tăng lên.

(iii) Tiếp tục triển khai và mở rộng thành phần tham gia các cuộc diễn tập giữa các trung tâm CERTs ASEAN, xây dựng kế hoạch giám sát lẫn nhau tại các cuộc diễn tập an ninh mạng cấp quốc gia.

(iv) Đối với các đối tác có trụ sở tại Đông Nam Á: phát triển hướng dẫn báo cáo về an ninh mạng và đề xuất sáng kiến về thực hành các báo cáo an ninh mạng; triển khai các

điểm (hubs) đánh giá, chia sẻ thông tin cấp vùng và xây dựng quan hệ đối tác với các nhà quản lý nước sở tại.

(v) Đối với cộng đồng công nghệ ASEAN: hỗ trợ việc phát triển công khai các biện pháp và phương tiện nhằm tăng cường lòng tin trong môi trường Internet đối với người sử dụng.

Diễn đàn khu vực ASEAN - ARF

Diễn đàn khu vực ASEAN đã thông qua kế hoạch làm việc, trong đó tập trung xây dựng các biện pháp xây dựng lòng tin (CBMs) để gia tăng lòng tin giữa các nước trong khu vực. Hiện nay, các biện pháp xây dựng lòng tin là một phần quan trọng trong chiến lược an ninh mạng của các nước trong khu vực châu Á - Thái Bình Dương. CBMs được các nước sử dụng như một công cụ để tạo sự ổn định và gia tăng lòng tin bởi mục tiêu bao quát của CBMs là tăng cường tính minh bạch, trao đổi thông tin tốt hơn, nâng cao nhận thức và hiểu biết chung về an ninh mạng,... Trong những năm qua, các nhóm, tổ chức như Tổ chức an ninh và hợp tác châu Âu (OSCE), Nhóm chuyên gia chính phủ của Liên hợp quốc về an ninh mạng (UN GGE), Diễn đàn khu vực ASEAN (ARF) và Tổ chức các nước châu Mỹ (OAS) đã nỗ lực đưa ra các sáng kiến CBMs về an ninh mạng. Hiện nay, CBMs ở cấp độ song phương, khu vực và toàn cầu có thể cung cấp một khuôn khổ cho các tổ chức khu vực như ASEAN hoặc các nước Đông Nam Á sử dụng trong trường hợp cần thiết.

Các biện pháp nâng cao năng lực và xây dựng lòng tin có vai trò quan trọng trong giai đoạn hiện nay nhằm tăng tính minh bạch và sự tin tưởng giữa các quốc gia, từ đó giảm thiểu khả năng hiểu lầm lẫn nhau, qua đó giảm nguy cơ về xung đột từ việc sử dụng không gian mạng/công nghệ thông tin và truyền thông. Ví dụ điển hình là việc Mỹ - Trung Quốc ký thỏa thuận không tấn công mạng lẫn nhau. Một năm sau khi ký thỏa thuận đó, số lượng vụ tấn công vào hệ thống tài chính, ngân hàng của hai nước đã giảm đáng kể và tránh được các khoản thiệt hại hàng tỷ đôla.

Nếu không có sự tin tưởng thì khi xảy ra các cuộc tấn công mạng sẽ rất khó tìm kiếm các động cơ tấn công mạng. Do vậy, để có được các biện pháp ngăn chặn, phòng thủ và phản ứng có hiệu quả đòi hỏi mối quan hệ hợp tác giữa chính phủ và các bên có liên quan và cần có sự tin tưởng lẫn nhau. Một yếu tố quan trọng khi xây dựng CBMs là cần phải có các đầu mối liên lạc rõ ràng, bởi vì trong một số trường hợp khẩn cấp, các nước có thể dựa trên các đầu mối đó để nhanh chóng mở các cuộc đối thoại nhằm xử lý vấn đề.

Trong bối cảnh vấn đề an ninh mạng mới nổi và còn nhiều khác biệt về quan điểm, ARF cần khuyến khích: (i) tổ chức các hội thảo một cách thường xuyên nhằm tạo sự kết nối và chia sẻ thông tin, thúc đẩy đối thoại, hợp tác, phối hợp xử lý khi sự cố xảy ra. Chính phủ các nước là thành viên ARF cần phát triển và chia sẻ chiến lược quốc gia về

an ninh mạng và đánh giá, so sánh về các mối đe dọa an ninh cũng như hậu quả từ các mối đe dọa này; (ii) Chính phủ các quốc gia trong ARF cần nâng cao năng lực, cải thiện cơ sở vật chất, bảo đảm sự ổn định và xây dựng các tiêu chuẩn an ninh mạng, ưu tiên nâng cao nhận thức, đặc biệt đối với các công dân; (iii) Chính phủ các nước là thành viên ARF cần đưa ra các phương pháp thu hẹp khoảng cách giữa khu vực tư nhân và những người làm chính sách nhằm tạo điều kiện xây dựng những chính sách phù hợp; (iv) Chính phủ các nước cần hỗ trợ cho những sự hợp tác về an ninh mạng trong những ngành cụ thể, bao gồm hỗ trợ pháp lý, hợp tác Đội phản ứng nhanh sự cố máy tính (CERT); (v) ARF cần nghiên cứu các cam kết liên khu vực về vấn đề an ninh mạng, như hợp tác giữa OSCE và ARF.

Tháng 8/2017, Bộ trưởng Ngoại giao các nước thành viên ARF đã thông qua đề xuất thành lập Nhóm giữa kỳ ARF về an ninh công nghệ thông tin và truyền thông (ISM-ICTs). Việt Nam có thể tận dụng cơ chế này để nhấn mạnh tầm quan trọng của vấn đề an ninh mạng; tăng cường hiểu biết về các thách thức, nguy cơ an ninh mạng; thúc đẩy các sáng kiến liên quan đến không gian mạng và tăng cường hợp tác khu vực theo hướng tuân thủ Hiến chương Liên hợp quốc và các sáng kiến toàn cầu. Các mục tiêu này có thể được thực hiện thông qua các biện pháp cụ thể sau:

- Tăng cường trách nhiệm của các nước thành viên ARF.

(i) Phát triển và chia sẻ luật pháp/quy định, chiến lược quốc gia trong lĩnh vực an ninh mạng.

(ii) Thúc đẩy các chương trình quốc gia đánh giá các nguy cơ an ninh mạng, bao gồm đánh giá quan điểm quốc gia về an ninh mạng, năng lực quốc gia về kỹ thuật, khả năng điều phối, ứng phó với các vụ việc mạng và tội phạm mạng.

(iii) Thúc đẩy việc thành lập Danh bạ các đầu mối liên lạc quốc gia trong lĩnh vực không gian mạng để liên lạc, chia sẻ thông tin, đặc biệt trong trường hợp xảy ra các sự cố về an ninh mạng.

(iv) Thúc đẩy việc chia sẻ về chính sách an ninh mạng quốc gia, tăng cường tính minh bạch, hiểu biết về không gian mạng, từ đó giảm thiểu nguy cơ về hiểu nhầm và tính toán sai về nhau, góp phần giảm leo thang căng thẳng, xung đột trong lĩnh vực an ninh mạng.

(v) Thúc đẩy các chương trình, hoạt động trong khuôn khổ ARF liên quan đến việc xây dựng các quy định, tập quán, nguyên tắc về không gian mạng phù hợp với các chương trình, quy trình làm việc của Liên hợp quốc hiện nay.

- Thúc đẩy hợp tác giữa các chủ thể.

(i) Tận dụng các mô hình, kinh nghiệm tốt nhằm đánh giá tình hình và tiến triển trong quá trình thực hiện chính sách an ninh mạng quốc gia.

(ii) Thúc đẩy hợp tác công - tư trong lĩnh vực không gian mạng và sự tham gia của các chủ thể vào quá trình thảo luận và làm chính sách về an ninh mạng.

- Các biện pháp xây dựng lòng tin.

(i) Các quốc gia, chủ thể cần nhận thức được an ninh mạng là một vấn đề cần ưu tiên trong khuôn khổ ARF và việc bảo đảm an ninh mạng sẽ góp phần phát triển kinh tế - xã hội.

(ii) Tận dụng tối đa Nhóm giữa kỳ ARF về an ninh công nghệ thông tin và truyền thông (ISM-ICTs) nhằm thảo luận, giải quyết các vấn đề an ninh mạng đang nổi, phê duyệt các biện pháp xây dựng lòng tin.

(iii) Xem xét báo cáo UN GGE năm 2016 về "Phát triển trong lĩnh vực công nghệ thông tin và truyền thông trong bối cảnh an ninh quốc tế", trong đó có danh mục về các biện pháp xây dựng lòng tin có giá trị tham khảo.

- Thúc đẩy hợp tác kỹ thuật.

(i) Hỗ trợ và thúc đẩy các nỗ lực hợp tác trong các lĩnh vực cụ thể, bao gồm hỗ trợ kỹ thuật, hợp tác giữa các cơ quan ứng phó sự cố máy tính khẩn cấp (CERT/CSIRT).

(ii) Chia sẻ các thông tin về nguy cơ, rủi ro có thể xảy ra ảnh hưởng đến lĩnh vực công nghệ thông tin và truyền thông; chia sẻ thông tin về cách thức ứng phó với biện pháp phù hợp và bảo vệ các kênh liên lạc.

3.3. Tích cực hợp tác quốc tế về an ninh mạng

Đại hội lần thứ XII của Đảng đề ra đường lối đối ngoại độc lập, tự chủ và tích cực, chủ động hội nhập quốc tế. Theo đó, hội nhập quốc tế không chỉ dừng lại ở việc lựa chọn các luật lệ và chuẩn mực phù hợp với mục tiêu và khả

năng của mình trong từng giai đoạn phát triển để áp dụng. Chủ động, tích cực hội nhập quốc tế hiện nay còn thể hiện ở việc tham gia xây dựng chuẩn mực, luật chơi trong quan hệ quốc tế. Áp dụng vào lĩnh vực không gian mạng, Việt Nam cần tham gia vào quá trình thảo luận và xây dựng các quy định, tập quán và luật pháp về không gian mạng. Điều này đặc biệt có ý nghĩa trong bối cảnh các quá trình này mới ở giai đoạn khởi đầu, do đó Việt Nam có điều kiện và cơ hội để nêu quan điểm và lồng ghép các vấn đề vào các quá trình này theo hướng có lợi cho Việt Nam (hiện nay, các nước trong khu vực như Xingapo, Malaixia, Inđônêxia và Thái Lan cũng đang rất tích cực tham gia vào các quá trình này, vừa nhằm thúc đẩy việc xây dựng các quy định theo hướng có lợi cho họ vừa nhằm thể hiện vai trò tiên phong, dẫn dắt về ngoại giao trong lĩnh vực an ninh mạng). Trước đây, hội nhập quốc tế của Việt Nam trong các lĩnh vực chính trị, kinh tế, xã hội chủ yếu thể hiện ở việc nước ta tham gia và chấp nhận các luật chơi sẵn có do các luật chơi, thỏa thuận này đã hình thành trước khi ta tiến hành hội nhập quốc tế.

Chức năng thực hiện và điều phối hoạt động hội nhập quốc tế của nước ta hiện nay do Bộ Ngoại giao thực hiện, do đó Bộ Ngoại giao cần phối hợp chặt chẽ với các bộ chuyên ngành trong lĩnh vực không gian mạng (Bộ Quốc phòng, Bộ Công an và Bộ Thông tin và Truyền thông) nhằm phát huy vai trò đi đầu trong thúc đẩy quá trình hội nhập của Việt Nam trong lĩnh vực này.

Như đã phân tích, việc xây dựng các quy định, tập quán, luật pháp trong lĩnh vực không gian mạng còn nhiều tranh cãi, đặc biệt là ở cấp độ toàn cầu. Tuy nhiên, Việt Nam cần tăng cường hợp tác với các nước nhằm phục vụ lợi ích của mình trong việc bảo đảm an ninh mạng, hạn chế và ứng phó với các cuộc tấn công, sự cố mạng. Do đó, Bộ Ngoại giao có thể lồng ghép vấn đề an ninh mạng vào việc thúc đẩy hợp tác song phương, đa phương. Một số hướng hợp tác có thể được cụ thể hóa như sau:

(i) Xây dựng các quan hệ đối tác và tham gia vào các thể chế đa phương.

Xây dựng quan hệ đối tác với các quốc gia nhằm tăng cường các hành động và hợp tác tập thể trong việc ngăn ngừa và chống lại các nguy cơ chung. Quan hệ đối tác này được thể hiện qua việc tham vấn chính sách, chia sẻ thông tin, thực hành sáng kiến chung. Ở góc độ đa phương, nhiều tổ chức quốc tế (như Liên hợp quốc, G7, G20, ASEAN) đang quan tâm đến vấn đề an ninh mạng. Các cơ chế này tạo cơ hội để các nước cùng có các tầm nhìn chung trong lĩnh vực không gian mạng. Ngoài ra, ngoại giao an ninh mạng, thông qua thúc đẩy hành động và hợp tác, góp phần trực tiếp vào việc ứng phó với các mối đe dọa trong không gian mạng.

(ii) Thúc đẩy hợp tác, hành động và ứng phó tập thể đối với các sự cố mạng.

Theo đó, ngoại giao đóng vai trò quan trọng trong việc trực tiếp ứng phó với các thách thức cụ thể và tạo nền tảng cho sự hợp tác nhằm ứng phó với các vấn đề trong tương lai. Thực tế trong thời gian qua, các hành động tập thể được áp dụng bởi các quốc gia đã góp phần giải quyết các sự cố và ngăn chặn các hoạt động độc hại trên không gian mạng một cách hiệu quả. Ở một khía cạnh khác, các áp lực ngoại giao tập thể cũng đóng vai trò trong việc giải quyết vấn đề ăn cắp bí mật thương mại và quyền sở hữu trí tuệ.

Nâng cao năng lực cũng góp phần quan trọng trong việc thúc đẩy hợp tác và thuyết phục các nước cùng tiến tới các nhận thức chung về vấn đề an ninh mạng. Do đó, hợp tác và hành động chung còn cần thể hiện ở việc hỗ trợ nâng cao năng lực trong không gian mạng.

(iii) Thúc đẩy chia sẻ chính sách và xây dựng đồng thuận chung cho sự ổn định không gian mạng toàn cầu.

Các giá trị trong không gian mạng như tính mở, tự do Internet và cách tiếp cận quản trị nhiều thành phần đang gặp nhiều thách thức trong thời gian qua. Do đó, hợp tác quốc tế hiện nay còn nhằm thúc đẩy việc thiết lập các quy chuẩn, quy định quốc tế và cả các biện pháp trừng phạt đối với các hành vi đe dọa trên không gian mạng.

Các biện pháp ngoại giao cũng có thể được áp dụng để ngăn chặn các hành xử không phù hợp trên không gian mạng ví dụ như gián đoạn Internet, làm tổn hại đến các tiềm năng kinh tế, xã hội. Cùng với đó, ngoại giao trong

lĩnh vực an ninh mạng còn cần thúc đẩy: (a) hiểu biết chung ở cấp độ toàn cầu về việc sử dụng luật pháp quốc tế và các hoạt động phù hợp trên không gian mạng, (b) sự phát triển các tập quán tự nguyện và không mang tính ràng buộc về các hành động được phép của nhà nước trên không gian mạng, và (c) việc thành lập và áp dụng các biện pháp xây dựng lòng tin nhằm giảm thiểu nguy cơ hiểu lầm và leo thang căng thẳng trong không gian mạng.

Ngoài ra, điểm đáng chú ý là vấn đề an ninh mạng hiện đang là vấn đề mới, thu hút sự quan tâm của các nước nhưng chưa đạt được nhiều sự đồng thuận, đặc biệt là giữa các nước lớn. Do đó, ngoài các diễn đàn kênh 1 (kênh thực hiện ngoại giao chính thức của chính phủ), các hoạt động kênh 2 về vấn đề an ninh mạng đang đóng vai trò quan trọng trong việc thúc đẩy hiểu biết, chia sẻ thông tin, đặc biệt là tăng cường nhận thức, cách hiểu giữa các quốc gia đối với các khái niệm cơ bản cũng như các vấn đề còn tranh cãi liên quan đến không gian mạng. Do đó, Việt Nam cần tận dụng các cơ chế kênh 2 (CSCAP, ASEAN-ISIS,...) để tìm hiểu, nắm bắt tình hình an ninh mạng trên thế giới cũng như thúc đẩy xây dựng các tiêu chuẩn chung trong không gian mạng. Hiện nay, các hoạt động kênh 2 có thể hỗ trợ xây dựng CBMs thông qua: (i) cung cấp các nghiên cứu mang tính so sánh về nhận thức các mối đe dọa an ninh mạng của các nước, (ii) cung cấp tài liệu tiêu chuẩn về năng

lực quốc gia, và (iii) tiến hành nghiên cứu cách tiếp cận của khu vực đối với CBMs trong lĩnh vực không gian mạng.

*

* *

Cùng với quá trình đổi mới, mở cửa, tình hình kinh tế - xã hội của Việt Nam tiếp tục phát triển, trong đó có lĩnh vực công nghệ thông tin. Kinh tế số đóng vai trò ngày càng quan trọng vào sự đi lên chung của đất nước nhưng vấn đề an ninh mạng, không gian mạng cũng tiềm ẩn nhiều vấn đề phức tạp, khó lường không chỉ đối với phát triển kinh tế - xã hội mà còn đối với an ninh quốc gia, trật tự - an toàn xã hội, chủ quyền, an ninh chế độ,... Các thách thức này đòi hỏi Đảng và Nhà nước ta phải có chính sách phù hợp để bảo đảm an ninh mạng để vừa duy trì môi trường mạng cởi mở, an toàn, thúc đẩy sáng tạo và phát triển vừa bảo đảm và tăng cường an ninh quốc gia, an ninh chế độ, trật tự - an toàn xã hội, giữ gìn bản sắc văn hóa dân tộc. Thực tế, nhận thức và chính sách của Việt Nam trong lĩnh vực phát triển công nghệ thông tin, an ninh mạng cũng dần phát triển theo sự phát triển của lĩnh vực không gian mạng, ngày càng thực tế và toàn diện hơn khi bao gồm tất cả các khía cạnh của vấn đề an ninh mạng.

Vấn đề an ninh mạng tiếp tục là vấn đề gây tranh cãi. Các quốc gia, trung tâm lớn có quan điểm khác nhau vẫn đang vừa đấu tranh vừa hợp tác trên không gian mạng, coi đây là mặt trận mới và không ngừng đầu tư, gia tăng ảnh

hưởng trong lĩnh vực này. Thực tế đó khiến các cơ chế hợp tác quốc tế hiện nay gặp bế tắc, các quốc gia có xu hướng hợp tác quốc tế về an ninh mạng ở các cấp độ phù hợp hơn là khu vực và tiểu khu vực.

Trong bối cảnh đó, Việt Nam cần: (i) Thực thi việc bảo đảm an ninh mạng phù hợp với các công ước quốc tế; (ii) Bảo đảm không gian mạng được xây dựng, duy trì, phát triển theo các quy trình, tiêu chuẩn, quy chuẩn kỹ thuật; (iii) Bảo đảm sự phát triển bền vững của công nghệ thông tin và truyền thông, góp phần thúc đẩy phát triển kinh tế - xã hội; (iv) Động viên, khuyến khích toàn dân tham gia và có trách nhiệm trong công cuộc bảo vệ chủ quyền quốc gia trên không gian mạng.

Trong lĩnh vực đối ngoại, chính sách an ninh mạng cần coi trọng việc hợp tác quốc tế, đặc biệt là trong khuôn khổ ASEAN và các cơ chế do ASEAN chủ trì nhằm ứng phó với các thách thức chung, nâng cao năng lực của Việt Nam trong lĩnh vực không gian mạng. Việt Nam cũng cần chủ động tham gia vào các thể chế đa phương nhằm thúc đẩy việc xây dựng các quy chuẩn, tập quán chung về không gian mạng theo hướng tích cực, phù hợp với lợi ích của nước ta.

KẾT LUẬN

Vấn đề an ninh mạng đang trở thành mối quan tâm hàng đầu của nhiều quốc gia, tổ chức, doanh nghiệp và người dân trên thế giới. Sự phát triển trong không gian mạng đang được thúc đẩy mạnh mẽ bởi cuộc Cách mạng công nghiệp lần thứ tư với tác động nhiều chiều, ngày càng sâu rộng trên mọi mặt của đời sống kinh tế - xã hội. An ninh mạng đem lại các cơ hội thúc đẩy hợp tác giữa các chủ thể (bao gồm nhà nước, các tổ chức quốc tế và doanh nghiệp,...) trong quan hệ quốc tế cũng như cơ hội trong việc tiến tới xây dựng hệ thống pháp luật, quy định, tập quán quốc tế trong lĩnh vực an ninh mạng. Hiện nay, an ninh mạng đang là vấn đề nổi lên của an ninh phi truyền thống và các quốc gia đang tích cực đẩy mạnh hợp tác kết hợp đấu tranh về vấn đề này trong quan hệ quốc tế.

Về mặt hợp tác, các quốc gia có nhiều điểm chung trong chính sách là bảo đảm khả năng độc lập, tự chủ về mặt công nghệ và năng lực trong việc bảo đảm môi trường Internet an toàn, lành mạnh, thúc đẩy sáng tạo, phát triển đồng thời giành ưu thế trong không gian mạng. Thêm vào

đó, các quốc gia hiện nay đều nhấn mạnh đến việc đẩy mạnh hợp tác quốc tế nhằm ứng phó với các thách thức an ninh mạng vì đây là vấn đề xuyên quốc gia, đòi hỏi sự phối hợp, hợp tác quốc tế. Một số thách thức chủ yếu mà các quốc gia, chủ thể trong quan hệ quốc tế đang phải đối mặt gồm: (i) cơ sở pháp lý và cơ chế hợp tác còn manh mún; (ii) thiếu sự đồng thuận về diễn giải và áp dụng luật pháp quốc tế trong không gian mạng; (iii) chưa có sự thống nhất chung về cách tiếp cận và cách thức hợp tác trong không gian mạng; và (iv) sự chênh lệch về năng lực (bao gồm năng lực quốc phòng mạng), trình độ của các quốc gia trong việc bảo đảm an ninh mạng và không gian mạng.

Bên cạnh những điểm chung nêu trên, mặt đấu tranh giữa các nước về an ninh mạng, không gian mạng ngày càng tăng do các nước có nhiều khác biệt, chủ yếu là trong vấn đề luật pháp và áp dụng luật pháp quốc tế; vấn đề quyền tự do cá nhân và lợi ích quốc gia; vấn đề chủ quyền không gian mạng; vấn đề dữ liệu cá nhân;... Đặc biệt, giữa các nước còn có sự khác biệt về trình độ và năng lực khoa học - kỹ thuật trong lĩnh vực không gian mạng và bảo đảm an ninh mạng. Các chủ thể chính hiện nay là ba nước lớn Mỹ, Nga, Trung Quốc.

Đặc điểm trong hợp tác và đấu tranh giữa các chủ thể là hai mặt hợp tác, đấu tranh diễn ra song song. Nhìn chung, mặt hợp tác về an ninh mạng nổi trội hơn mặt đấu tranh

trong quan hệ quốc tế[1]. Thực tế, mặt hợp tác về an ninh mạng được thực hiện trong khuôn khổ các hiệp định, văn bản được ký kết giữa các bên, nhấn mạnh về việc hợp tác, chia sẻ thông tin, kinh nghiệm về an ninh mạng. Nội dung hợp tác trong từng hiệp định, văn bản ký kết phụ thuộc thực trạng quan hệ mỗi nước và chưa đi vào thực chất.

Đối với Việt Nam, từ sau đổi mới, mở cửa (năm 1986), tình hình kinh tế - xã hội liên tục phát triển trong nhiều năm qua, trong đó có lĩnh vực công nghệ thông tin. Kinh tế số đóng vai trò ngày càng quan trọng vào sự phát triển của đất nước nhưng an ninh mạng, không gian mạng cũng tiềm ẩn nhiều vấn đề phức tạp, khó lường không chỉ đối với sự phát triển kinh tế - xã hội mà còn đối với an ninh quốc gia, trật tự - an toàn xã hội, chủ quyền, an ninh chế độ,... Những thách thức này đòi hỏi việc phải có chính sách phù hợp nhằm duy trì môi trường mạng cởi mở, an toàn, thúc đẩy sáng tạo và phát triển; bảo đảm và tăng cường an ninh quốc gia, an ninh chế độ, trật tự - an toàn xã hội, giữ gìn bản sắc văn hóa dân tộc. Hiện nay, quan điểm và chính sách của Việt Nam trong lĩnh vực phát triển công nghệ thông tin, an ninh mạng cũng dần phát triển ngày càng thực tế và toàn diện hơn cùng với các diễn biến trong lĩnh vực không gian mạng, khi bao gồm tất cả các khía cạnh của vấn

---

1. Một số quan điểm cho rằng, việc mặt hợp tác hay đấu tranh nổi trội hơn là do tổng thể quan hệ song phương của từng cặp quốc gia.

đề an ninh mạng. Vấn đề an ninh mạng tiếp tục là vấn đề gây tranh cãi. Các nước lớn và các quốc gia trên thế giới coi là một mặt trận mới và không ngừng đầu tư, gia tăng ảnh hưởng trong lĩnh vực này. Do vậy, các quốc gia có xu hướng tập trung hợp tác quốc tế trong lĩnh vực an ninh mạng ở các cấp độ phù hợp hơn là khu vực và tiểu khu vực.

Trong bối cảnh đó, Việt Nam cần: (i) Độc lập, tự chủ, phát huy tối đa nội lực xây dựng năng lực quốc gia trong không gian mạng để bảo vệ Tổ quốc, đóng góp vào công cuộc xây dựng, phát triển đất nước theo hướng nhanh và bền vững; (ii) Kiên quyết, kiên trì bảo vệ chủ quyền, lợi ích quốc gia - dân tộc trong không gian mạng; (iii) Tham gia và thực thi việc bảo đảm an ninh mạng phù hợp với các công ước quốc tế; (iv) Bảo đảm không gian mạng được xây dựng, duy trì, phát triển theo các quy trình, tiêu chuẩn, quy chuẩn kỹ thuật theo tiêu chuẩn của Việt Nam và quốc tế; (v) Bảo đảm sự phát triển bền vững trong lĩnh vực công nghệ thông tin và truyền thông, góp phần thúc đẩy phát triển kinh tế - xã hội; (vi) Động viên, khuyến khích toàn dân tham gia và có trách nhiệm trong công cuộc bảo vệ chủ quyền quốc gia trên không gian mạng.

Trong lĩnh vực đối ngoại, (i) ở cấp độ quốc gia: Chính sách đối ngoại về an ninh mạng của Việt Nam phải góp phần giữ vững môi trường hoà bình, ổn định và đóng góp vào công cuộc xây dựng và nâng cao năng lực tự lực tự cường an ninh mạng về quốc phòng, an ninh, tài chính,... để bảo đảm

lợi ích - quốc gia dân tộc và thực hiện Chiến lược bảo vệ Tổ quốc trong tình hình mới trong Nghị quyết số 28-NQ/TW ngày 25/10/2013 của Ban Chấp hành Trung ương (khóa XI); (ii) ở cấp độ khu vực: Coi trọng việc hợp tác quốc tế, đặc biệt là trong khuôn khổ ASEAN và các cơ chế do ASEAN chủ trì nhằm ứng phó với các thách thức chung, nâng cao năng lực dân sự cũng như quốc phòng của Việt Nam trong lĩnh vực không gian mạng. Ngoài ra, trong bối cảnh vấn đề Biển Đông đang có những diễn biến phức tạp, việc tích cực, chủ động tham gia xây dựng các quy tắc chung về ứng xử, chuẩn mực của khu vực cũng như các biện pháp ngoại giao phòng ngừa về an ninh mạng sẽ giúp giảm thiểu nguy cơ xung đột/chiến tranh (có nguồn gốc từ an ninh mạng) có thể xảy ra trong khu vực; (iii) ở cấp độ toàn cầu: Tích cực, chủ động hội nhập quốc tế về an ninh mạng và không gian mạng, tranh thủ nguồn lực từ các cơ chế hợp tác quốc tế toàn cầu; chủ động tham gia các thể chế đa phương, cụ thể là các diễn đàn của Liên hợp quốc (nêu trong Văn kiện Đại hội Đảng toàn quốc lần thứ XII), nhằm thúc đẩy việc tham gia và xây dựng công ước, thỏa thuận quốc tế, các quy chuẩn, tập quán chung về bảo đảm an toàn thông tin, an ninh mạng và chủ quyền, lợi ích quốc gia - dân tộc theo hướng tích cực, an toàn và phù hợp với lợi ích của Việt Nam.

Việc thực hiện đồng bộ các kiến nghị, đề xuất nêu trên sẽ góp phần vào việc thực hiện đường lối đối ngoại độc lập, tự chủ của Đảng và Nhà nước Việt Nam, theo đó đối ngoại

tranh thủ điều kiện thuận lợi trong hợp tác quốc tế về an ninh mạng, đóng góp vào việc xây dựng tiềm lực và năng lực quốc gia về an ninh mạng của Việt Nam và xây dựng Chiến lược Quốc phòng - An ninh trong môi trường không gian mạng của Việt Nam trong tình hình mới, qua đó thực hiện chủ trương của Ban Bí thư về nâng tầm đối ngoại đa phương tại các diễn đàn quốc tế, đa phương, tiếp tục nâng cao thế và lực của Việt Nam.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. "An toàn thông tin ở Việt Nam 2017", http://securitybox.vn/2540/an-toan-thong-tin-tai-viet-nam-2017/, truy cập ngày 28/9/2018.
2. Anh Quân: "ASEAN đối phó thách thức an ninh mạng", http://vtv.vn/cong-nghe/asean-doi-pho-thach-thuc-an-ninh-mang-20170919202247214.htm, truy cập ngày 29/9/2018.
3. "Bộ trưởng Trương Minh Tuấn tiếp đại diện Facebook", http://vietnamnet.vn/vn/cong-nghe/tin-cong-nghe/bo-truong-truong-minh-tuan-tiep-dai-dien-facebook-423087.html, truy cập ngày 04/10/2018.
4. Thượng tướng, Thứ trưởng Công an Bùi Văn Nam: "Giải pháp bảo đảm an toàn thông tin trong tình hình hiện nay", http://netnam.vn/index.php/vi/tin-tuc/diem-bao/52-bao-chi-noi-v-netnam/621-giai-phap-bao-dam-an-toan-thong-tin-trong-tinh-hinh-hien-nay.html, truy cập ngày 20/9/2018.
5. "Các nước cần tăng cường hợp tác để giải quyết thách thức về an ninh mạng", http://ictnews.vn/cntt/bao-mat/cac-

nuoc-can-tang-cuong-hop-tac-de-giai-quyet-thach-thuc-ve-an-ninh-mang-159658.ict, truy cập ngày 01/10/2018.

6. Châu An: "Các vụ tấn công mạng bị nghi có nguồn gốc từ Triều Tiên", báo *Vnexpress*, http://sohoa.vnexpress.net/tin-tuc/doi-song-so/bao-mat/cac-vu-tan-cong-mang-bi-nghi-co-nguon-goc-tu-trieu-tien-3586309.html, truy cập ngày 15/9/2018.
7. "Cục trưởng An ninh mạng: Yêu cầu Facebook đặt máy chủ ở Việt Nam", https://vnexpress.net/tin-tuc/phap-luat/cuc-truong-an-ninh-mang-yeu-cau-facebook-dat-may-chu-o-viet-nam-3672035.html, truy cập ngày 30/9/2018.
8. Chính phủ Ixraen: *Quyết định về xây dựng các khả năng mạng ở Ixraen,* 2011.
9. Cục Thương mại điện tử và Công nghệ thông tin, Bộ Công thương: *Báo cáo Thương mại điện tử Việt Nam 2014.*
10. Cục Thương mại điện tử và Công nghệ thông tin, Bộ Công thương: *Báo cáo Thương mại điện tử Việt Nam 2015.*
11. "Dự thảo Luật An ninh mạng và sự chuyển biến trong nhận thức của Việt Nam", http://jetking.fpt.edu.vn/du-thao-luat-anm-va-su-chuyen-bien-trong-nhan-thuc-cua-viet-nam/, truy cập ngày 01/10/2018.
12. Đào Việt Hùng: *Nghiên cứu an ninh mạng sử dụng kỹ thuật điều khiển bằng phần mềm SDN*, Trường Đại học Bách khoa Hà Nội, 2015.
13. Hương Mai: "Nga - Trung hứa không hack lẫn nhau", http://vnreview.vn/ tin-tuc-an-ninh-mang/-/view_content/

content/1545180/nga-trung-hua-khong-hack-lan-nhau, truy cập ngày 03/10/2018.

14. "Không vi phạm điều ước quốc tế khi yêu cầu Facebook, Google đặt máy chủ tại Việt Nam", http://quochoi.org/khong-vi-pham-dieu-uoc-quoc-te-khi-yeu-cau-facebook-google-dat-may-chu-tai-viet-nam.html, truy cập ngày 28/9/2018.
15. "Liên minh Viễn thông quốc tế và quan hệ với Việt Nam", http://www. mofahcm.gov.vn/en/mofa/ctc_quocte/un/nr040819155753/nr060928111253/ns060928104826, truy cập ngày 29/9/2018.
16. Chỉ thị 54 về an ninh quốc gia và Chỉ thị số 23 về an ninh nội địa của Tổng thống Mỹ.
17. "Nga, Mỹ và cuộc chiến tranh lạnh trên không gian mạng", https://tuoitre.vn/nga-my-va-cuoc-chien-tranh-lanh-tren-khong-gian-mang-1216756.htm/, truy cập ngày 02/10/2018.
18. "Những vấn đề an ninh mạng nổi bật ở Việt Nam năm 2017", https://tinhte.vn/threads/nhung-van-de-an-ninh-mang-noi-bat-tai-viet-nam-nam-2017.2750668/, truy cập ngày 29/9/2018.
19. Thiên Minh: "Gián điệp mạng Trung Quốc tác động xấu đến lợi ích kinh tế Mỹ", báo *An ninh thế giới*, http://antg.cand.com.vn/Ho-so-mat/Gian-diep-mang-Trung-Quoc-tac-dong-xau-den-loi-ich-kinh-te-My-308673/, truy cập ngày 15/10/2018.
20. "Thủ tướng Chính phủ dự lễ công bố quyết định thành lập Bộ Tư lệnh Tác chiến không gian mạng", http://vpcp.chinhphu.vn/

Home/Thu-tuong-Chinh-phu-du-le-cong-bo-quyet-dinh-thanh-lap-Bo-Tu-lenh-Tac-chien-khong-gian-mang/20181/23127.vgp, truy cập ngày 03/10/2018.

21. "Thủ tướng giao nhiệm vụ cho lực lượng Tác chiến không gian mạng", http://vietnamnet.vn/vn/thoi-su/chinh-tri/thu-tuong-giao-nhiem-vu-cho-luc-luong-tac-chien-khong-gian-mang-422463.html, truy cập ngày 01/10/2018.
22. Thuận Phương: "Việt Nam và sự trỗi dậy của chiến tranh mạng", *Nghiên cứu quốc tế*, http://nghiencuuquocte.org/2016/08/02/viet-nam-va-su-troi-day-cua-chien-tranh-mang/.
23. Thùy Dương: "Bảo đảm an ninh mạng là nhiệm vụ quan trọng, cấp bách", http://baodaknong.org.vn/an-ninh-trat-tu/bao-dam-an-ninh-mang-la-nhiem-vu-quan-trong-cap-bach-56939.html, truy cập ngày 01/10/2018.
24. Trần Bình: "Diễn tập ứng cứu sự cố an ninh mạng khu vực ASEAN", http://www.sggp.org.vn/dien-tap-ung-cuu-su-co-an-ninh-mang-khu-vuc-asean-467220.html, truy cập ngày 04/10/2017.
25. Trần Đại Quang: *Không gian mạng - Tương lai và hành động*, Nxb. Công an Nhân dân, Hà Nội, 2015.
26. "Vấn đề bảo đảm an toàn an ninh mạng ở Việt Nam đang ở mức thấp", http://mt.gov.vn/vn/tin-tuc/51765/ van- de-dam-bao-an-toan-an-ninh-mang-o-viet-nam-dang-o-muc-thap-.aspx, truy cập ngày 30/9/2017.
27. Vũ Đình Cường: *Hack Internet OS và bảo mật - Từng bước khám phá an ninh mạng*, Nxb. Lao động - Xã hội, Hà Nội, 2008.

Tiếng Anh

1. Andreasson K.: *Cybersecurity: Public Sector Threats and Responses,* CRC Press, 2011.
2. "Southeast Asia Begins to Prepare for Cyber War; India Turns to AI", *AsiaToday*, https://www.huffingtonpost.com/asiatoday/southeast-asia-begins-to_b_14334812.html, truy cập ngày 03/10/2018.
3. Anna Ahronheim: "IDF decides not to have a cyber command department", *The Jerusalem Post*, truy cập ngày 01/01/2017.
4. Alan Charles Raul: "The Privacy, Data Protection and Cyber Security Law Review", *Law Business Research* (2nd ed.), 11/2015.
5. Buchanan B: *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations,* Oxford University Press, 2017.
6. Carr J.: *Inside Cyber Warfare*, O'Reilly Media, Inc. CA, US, 2011.
7. Clarke R. và Knake R.: *Cyberwar: The next threat to national security and what to do about it*, Harper Collins Publishers, UK, 2010.
8. Daniel Shkedi: *The Cybersecurity Sector in Ixraen*, Embassy of India in Ixraen, 2015.
9. Dave Chaffey: "Mobile Marketing Statistics compilation", https://www.smartinsights.com/mobile-marketing/mobile-

marketing-analytics/mobile-marketing-statistics/, truy cập ngày 02/10/2018, http://www.chinadaily.com.cn/business/tech/2015-12/21/content_22761073.htm>, truy cập ngày 01/10/2018.

10. Geers K.: *Strategic Cyber Security*, CCD COE Publication, 2011.
11. Green J. S.: *Cyber Security: An Introduction for Non-Technical Managers*, Gower, England, 2015.
12. Lucas E.: *The Snowden Operation: Inside the West's Greatest Intelligent Disaster*, Kindle Edition.
13. Emilio Iasiello: "The U.S. and Russia Re-engage in Cyber Cooperation", https://www.lookingglasscyber.com/blog/threat-intelligence-insights/the-u-s-and-russia-re-engage-in-cyber-cooperation/, truy cập ngày 02/10/2018.
14. Gori U.: *NATO Science for Peace and Security Series - E: Human and Societal Dynamics,* Volume 59, 2009.
15. Higgins M. và Regan M.: *Cybersecurity*, Abdo Publishing, 2016.
16. Hosmer C., Curtis G.: *Cyber Security: Protecting Businesses, Individuals, and the Government from the Next Cyber Attacks*, ABC-CLIO, 2016.
17. John Reed: "Unit 8200: Ixraen's cyber spy agency, Former insiders and whistle-blowers provide a view of the formidable military intelligence outfit", *Financial Times,* truy cập ngày 10/7/2015.

18. Karake Z.-Shalhoub và Lubna Al Qasimi: *Cyber Law and Cyber Security in Developing and Emerging Economies*, Edward Elgar Publishing Limited, 2010.
19. Knapp K. J.: *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*, IGI Global, 2009.
20. Kostopoulos G. K.: *Cyberspace and Cybersecurity*, CRC Press, 2012.
21. Kosseff J.: *Cybersecurity Law*, WILEY, USA, 2017.
22. LeClair J., Keeley G., và Ashcroft J.: *Cybersecurity in Our Digital Lives*, Hudson Whitman/Excelsior College Press, 2015.
23. Linsay J.R., Tai Ming Cheung, Reveron D. S.: *China and Cyber Security, Espinage, Strategy, and Politics in the Digital Domain*, Oxford University Press, UK, 2015.
24. Mitra A.: *Digital Security: Cyber Terror and Cyber Security (Digital World)*, Chelsea House Publications, 2010.
25. Nye, Joseph: "Làm thế nào để có thể hợp tác quốc tế về an ninh mạng?" (Nghiêm Hồng Sơn dịch), http://nghiencuuquocte.org/2015/5/22/lam-the-nao-de-co-the-hop-tac-quoc-te-ve-an-ninh-mang/, truy cập ngày 15/10/2018.
26. President's Information Technology Advisory Committee: "Cyber Security: A Crisis of Prioritization: Report to the President", Report to the president, 2005.
27. Rittinghouse J. W., Hancock W. M.: *Cybersecurity Operations Handbook*, Digital Press, 2003.

28. Russian Federation: "Doctrine of Information Security of the Russian Federation", http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, truy cập ngày 03/10/2018.
29. Russian Federation: *Federal Law No. 187-FZ of July 2, 2013, on Amendments to Certain Laws of the Russian Federation Concerning the Protection of Intellectual Rights in Information and Telecommunication Networks,* 2013, http://www.wipo.int/wipolex/en/text.jsp?file_id=334516, truy cập ngày 02/10/2018.
30. Russian Federation: "The Military Doctrine of the Russian Federation", http://carnegieendowment.org/files/2010russia_military_doctrine.pdf, truy cập ngày 02/10/2018.
31. Santanam R, Sethumadhavan M., Virendra M: "Cyber Security, Cyber Crime and Cyber Forensics: Applications and Pespectives", Information Science Reference, New York, 2010.
32. Segal A.: "The Development of Cyber Norms on the United Nations Ends in Deadlock. Now What?", https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what/, truy cập ngày 02/10/2018.
33. Singer, Friedman: *Cybersecurity and Cyber war: What everyone needs to know,* Oxford University Press, New York, 2014.

34. Westby J. R.: *International Guide to Cyber Security*, ABA Publishing, 2004.
35. The Digital and Cyberspace Policy program: "Promoting Norms for Cyberspace", https://www.cfr.org/report/promoting-norms-cyberspace/.
36. The Obama White House: "Presidential Policy directive United State cyber incident", https://obamawhitehouse.archives.gov/the-press-office/2016/7/26/presidential-policy-directive-united-states-cyber-incident, truy cập ngày 02/10/2018.
37. "UNCTAD review of ASEAN e-commerce laws", http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=613, truy cập ngày 30/9/2018.
38. US Department of Homeland Security: "Cybersecurity Overview", https://www.dhs.gov/cybersecurity-overview, truy cập ngày 05/10/2018.
39. Wilshusen: "Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information", United States Government Accountability Office, Washington D.C., 2009.
40. Zhu, Ningzhu: "Xi Jinping Leads Internet Security Group", http://www.chinadaily.com.cn/2014-02/27/content-17311358.htm, truy cập ngày 27/02/2014.

MỤC LỤC

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT
Số 6/86 Duy Tân, Cầu Giấy, Hà Nội
ĐT: 080.49221, Fax: 080.49222
Email: suthat@nxbctqg.vn, Website: www.nxbctqg.vn

TÌM ĐỌC SÁCH CỦA NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

Đại học Quốc gia Thành phố Hồ Chí Minh -
Trường Đại học Khoa học xã hội và Nhân văn
Đào Minh Hồng - Lê Hồng Hiệp (Đồng chủ biên)
*** THUẬT NGỮ QUAN HỆ QUỐC TẾ**

PGS.TS. Trần Thị Vân Hoa (Chủ biên)
*** CÁCH MẠNG CÔNG NGHIỆP 4.0 - VẤN ĐỀ ĐẶT RA CHO PHÁT TRIỂN KINH TẾ - XÃ HỘI VÀ HỘI NHẬP QUỐC TẾ CỦA VIỆT NAM**

Viện Đại học mở Hà Nội -
Khoa Kinh tế
*** THƯƠNG MẠI ĐIỆN TỬ TRONG CÁCH MẠNG CÔNG NGHIỆP 4.0**

ISBN 978-604-57-4616-5
9 786045 746165
8935279114870

Giá: 74.000đ