ĐỀ XUẤT XÂY DỰNG CHIẾN LƯỢC QUỐC GIA VỀ AN TOÀN KHÔNG GIAN MẠNG

TS. Nguyễn Kim Quang

Email: quangnk@ptit.edu.vn

Tóm tắt: *Bài báo tóm tắt kết quả nghiên cứu kinh nghiệm xây dựng chiến lược quốc gia về an toàn không gian mạng của các nước trên thế giới và đề xuất cho Việt Nam trong bối cảnh hiện nay.*

1. KHÔNG GIAN MẠNG VÀ TẦM QUAN TRỌNG CỦA MỘT CHIẾN LƯỢC AN TOÀN KHÔNG GIAN MẠNG

Mặc dù có nhiều định nghĩa khác nhau về Không gian mạng (theo F. D. Kramer, hiện có khoảng 28 định nghĩa khác nhau của các tổ chức thế giới cho cụm từ "không gian mạng") nhưng chưa có định nghĩa nào được thừa nhận rộng rãi. Bài báo sử dụng định nghĩa về không gian mạng theo Nghị định quy định về bảo đảm an ninh không gian mạng quốc gia, do Thủ tướng Nguyễn Xuân Phúc ký ban hành ngày 05/04/2017 như sau: *"Không gian mạng quốc gia là mạng lưới kết nối toàn cầu của các cơ sở hạ tầng công nghệ thông tin, bao gồm: mạng Internet, mạng viễn thông, hệ thống máy tính, hệ thống xử lý và điều khiển thông tin được Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam xác lập phạm vi quản lý, kiểm soát trực tiếp hoặc gián tiếp bằng chính sách, pháp luật và năng lực công nghệ".*

Trong không gian mạng này, các hành vi độc hại ngày càng phổ biến. Hoạt động đánh cắp thông tin cá nhân, doanh nghiệp và tổ chức cũng như tài sản gia tăng liên tục. Các mối đe dọa đối với an toàn và an ninh quốc gia (QG) ngày một ra tăng. Trong những năm qua, thế giới đã từng đối mặt với các cuộc tấn công không gian mạng có quy mô lớn, gây nguy hiểm cho hoạt động kinh doanh, cho xã hội ở tầm QG. Các cuộc chạy đua trên không gian mạng giữa các nước bắt đầu diễn ra công khai với tốc độ chưa từng có. Năm 2010, Mỹ chính thức công nhận "không gian mạng là một lãnh thổ mới, có tầm quan trọng ngang hàng như các lãnh thổ khác trong chiến tranh như trên bộ, trên biển, trên không và vũ trụ". Trung Quốc cũng từng tuyên bố: "Không gian mạng là chiến trường thứ năm và là mặt trận tình báo mới". Các nhà lãnh đạo Trung Quốc thừa nhận: "Việc sớm kiểm soát thông tin và các hệ thống thông tin của đối phương sẽ là chìa khoá của thành công trong mọi cuộc chiến", và khẳng định: "Không có an toàn không gian mạng đồng nghĩa không có an toàn quốc gia".

Trong bối cảnh đó các QG cần đưa ra tầm nhìn và nêu rõ các ưu tiên, các nguyên nguyên tắc và cách tiếp cận để hiểu và quản lý rủi ro trong không gian mạng ở cấp QG; cần xác định các mục tiêu chiến lược; xây dựng các chính sách chặt chẽ và khả thi; xác định các nguồn lực cho các mục tiêu đó và làm thế nào để sử dụng các nguồn

lực này một cách hiệu quả. Đó chính là những nội dung cơ bản của một chiến lược an toàn không gian mạng QG.

2. TÌNH HÌNH NGHIÊN CỨU VỀ CHIẾN LƯỢC AN TOÀN KHÔNG GIAN MẠNG CỦA CÁC QUỐC GIA TRÊN THẾ GIỚI

2.1. Các vấn đề cần nghiên cứu và phương pháp nghiên cứu

Mặc dù đã có rất nhiều nghiên cứu về An toàn thông tin nhưng các công trình nghiên cứu đi sâu vào việc xây dựng, phát triển Chiến lược An toàn không gian mạng QG trên thế giới nói chung và ở Việt Nam nói riêng vẫn chưa được công bố. Do đó, việc nghiên cứu cách các nước giải quyết những thách thức, khó khăn trong xây dựng Chiến lược này sẽ mang lại những kinh nghiệm quý báu, góp phần xây dựng Chiến lược An toàn không gian mạng cho Việt Nam.

Để rút ra được kinh nghiệm của các nước trong việc xây dựng Chiến lược An toàn không gian mạng và đề xuất cho Việt Nam, cần giải quyết các vấn đề sau: Thứ nhất, cần hiểu được nguyên nhân tại sao các nước lại xây dựng Chiến lược An toàn không gian mạng của mình như vậy, họ xây dựng Chiến lược trong bối cảnh đất nước như thế nào, cần phải tìm hiểu về hiện trạng An toàn không gian mạng mà các nước đang phải đối mặt. Thứ hai, họ đã xây dựng nó như thế nào, tức là tìm hiểu các quan điểm xây dựng của mỗi nước, xác định các khía cạnh trong việc xây dựng Chiến lược An toàn không gian mạng, xác định mục tiêu, tầm nhìn, nguyên tắc hoạt động và kế hoạch hành động trong Chiến lược của các nước, tìm hiểu các khung hướng dẫn xây dựng mà các nước đã áp dụng. *Cuối cùng* là làm thế nào để áp dụng các kinh nghiệm đó vào Việt Nam, tình hình an toàn không gian mạng ở Việt Nam so với các quốc gia khác có điểm gì giống và khác nhau, chủ trương, quan điểm của Việt Nam có gì khác, từ đó xác định tầm nhìn, mục tiêu, nguyên tắc hoạt động, kế hoạch hành động trong Chiến lược An toàn không gian mạng cho Việt Nam và xác định được khung hướng dẫn nào có thể áp dụng cho Việt Nam.

Đối với bài toán đặt ra, cách tiếp cận của chúng tôi là **tiếp cận định tính** (*Qualitative Approach*). Đây là cách tiếp cận trong đó tìm hiểu hành vi, động cơ và ý đồ đối tượng nghiên cứu và những lý do điều khiển những hành vi đó. Theo cách tiếp cận này, chúng tôi sử dụng hai phương pháp là : phương pháp nghiên cứu định tính và phương pháp phân tích so sánh định tính. Đối tượng nghiên cứu là các bộ tài liệu về Chiến lược an toàn không gian mạng đã ban hành chính thức của 54 QG và vùng lãnh thổ mà chúng tôi tổng hợp được. Công cụ sử dụng trong nghiên cứu là phần mềm Nvivo, một bộ công cụ hỗ trợ các nghiên cứu định tính và hỗn hợp. Nó được thiết kế nhằm giúp tổ chức, phân tích và tìm kiếm thông tin chi tiết về dữ liệu định dạng phi cấu trúc hoặc dữ liệu định tính như: cuộc phỏng vấn, câu trả lời khảo sát mở, bài viết, phương tiện truyền thông xã hội.

Hai câu hỏi định tính mà chúng tôi đặt ra trong quá trình nghiên cứu là:

1) ***Động cơ đằng sau Chiến lược An toàn không gian mạng của các nước là gì?***

2) Các nước đã xây dựng Chiến lược An toàn không gian mạng của họ như thế nào?

2.2. Kết quả nghiên cứu

Các kết quả nghiên cứu nhằm trả lời hai câu hỏi định tính như đã trình bày ở trên được thể hiện như sau:

Câu hỏi 1: Động cơ đằng sau Chiến lược An toàn không gian mạng của các nước là gì?

Chiến lược An toàn không gian mạng QG của các nước nhìn chung đều mô tả về tầm nhìn an toàn không gian mạng QG, các điều kiện tiền đề, các giả định, và nền tảng cho các thuộc tính khác trong Chiến lược của mỗi nước. Kết quả tổng hợp cho thấy có 09 động cơ chính trong Chiến lược An toàn không gian mạng là:

(1) Giảm mối đe dọa trên không gian mạng
(2) Đảm bảo an toàn kinh tế
(3) Yêu cầu bởi các chính sách quốc gia khác
(4) Tăng cường khả năng phục hồi quốc gia
(5) Nhu cầu chính trị
(6) Ủy thác hợp pháp
(7) Bảo vệ bí mật quốc gia
(8) Tăng cường ngoại giao
(9) Tăng cường hình ảnh quốc gia

Bảng 1. Thống kê định nghĩa các động cơ trong Chiến lược An toàn không gian mạng của mỗi QG

Động cơ	Mục tiêu/Quốc gia
Giảm mối đe dọa trên không gian mạng	Giảm thiểu các hoạt động độc hại trên không gian mạng có khả năng gây ra các cuộc tấn công mạng.
	Quốc gia: AFG, AUS, BGD, BEL, CAN, CZE, COL, CYP, EGY, EST, FIN, FRA, GEO, DEU, GHA, ISL, IND, IRL, ISR, ITA, JPN, JOR, KEN, LVA, LTU, MUS, MNE, NLD, NZL, NGA, NOR, PAK, POL, QAT, RUS, RWA, SAU, SRB, ZAF, PRK, CHE, TTO, TUR, UGA, GBR, USA
Đảm bảo an toàn kinh tế	Đảm bảo sự tự chủ, tin tưởng vào giao dịch trên không gian mạng, và bảo vệ cấu trúc nền kinh tế quốc gia trong lĩnh vực kỹ thuật số.
	Quốc gia: AFG, AUS, AUT, BGD, CAN, CZE, COL, HRV, CYP, FIN, FRA, DEU, GHA, ISL, IND, IRL, ITA, JPN, JOR, KEN, LVA, MNE, MAR, NLD, NZL, NGA, NOR, POL, QAT, RUS, ZAF, ESP, TUR, GBR, USA
Yêu cầu bởi các chính sách quốc gia khác	Được yêu cầu dựa trên các chương trình quốc gia trước đó như Chiến lược An ninh Quốc gia, Lộ trình Quốc gia, yêu cầu chính thức hoặc đánh giá từ chính phủ.
	Quốc gia: AUT, COL, CYP, FIN, ISR, ITA, JPN, KEN, NLD, NGA, POL, QAT, RUS, SAU, SVK, ZAF, PRK, ESP, CHE, TTO, TUR, UGA, USA
Tăng cường	Duy trì tính toàn vẹn của hoạt động liên tục và khả năng phục hồi của các

khả năng phục hồi quốc gia	dịch vụ ICT có tầm quan trọng lớn và tác động tàn phá đến công chúng ở cấp quốc gia
	Quốc gia: AUS, CZE, COL, HRV, FRA, GHA, JPN, NLD, NZL, RUS, RWA, SAU, SVK, ZAF, PRK, SGP, CHE, USA
Nhu cầu chính trị	Yêu cầu chính trị có thể được xem như một lý do nhằm kết hợp lợi ích QG (tức là thúc đẩy các giá trị QG, giữ thịnh vượng ĐN) hoặc tình hình chính trị (khẳng định các giá trị dân chủ, đảm bảo quyền con người, hoặc đảm bảo luồng thông tin tự do).
	Quốc gia: AUS, AUT, BGD, CAN, CZE, COL, EST, FRA, ITA, JPN, KEN, LTU, NLD, NZL, QAT, RUS, RWA, TUR, GBR, USA
Ủy thác hợp pháp	Một điều kiện để có thẩm quyền pháp lý để thi hành luật trong không gian mạng.
	Quốc gia: COL, GHA, IND, MUS, NZL, NGA, PAK, RUS, TTO, TUR
Bảo vệ bí mật quốc gia	Bảo vệ thông tin QG mà việc tiết lộ trái phép có thể gây nguy hiểm cho an ninh QG
	Quốc gia: CZE, COL, JPN, NLD, NZL, RWA, ESP
Tăng cường ngoại giao	Phục vụ cho đàm phán ngoại giao
	Quốc gia: BEL, GEO, NLD, RUS, USA
Tăng cường hình ảnh QG	Tăng cường hình ảnh một đất nước an toàn trước thế giới.
	Quốc gia: GHA, JPN, TTO

Các động cơ này vừa đại diện cho việc bảo vệ an toàn không gian mạng quốc gia, vừa thể hiện ý muốn về mặt chính trị cũng như pháp luật. Đầu tiên, các động cơ về bảo vệ bí mật quốc gia, giảm các mối đe dọa, tăng cường khả năng phục hồi và bảo đảm an toàn kinh tế là hoàn toàn hợp lý và xuất hiện trong hầu hết Chiến lược An toàn không gian mạng của các quốc gia, bởi internet không chỉ mang lại lợi ích to lớn mà còn đem đến những nguy hiểm tiềm tàng. Bên cạnh đó, tăng cường an toàn không gian mạng quốc gia cũng yêu cầu chính phủ phải đối mặt với các kỹ thuật công nghệ mới trên internet. Việc này không chỉ là đối phó với các mối đe dọa đã biết, mà còn cần tầm nhìn đối với các đe dọa trong tương lai.

Vấn đề về pháp luật cũng chỉ ra vai trò quan trọng của chính phủ trên không gian mạng. Không gian mạng cũng được xem như một không gian pháp lý, cùng với đất liền, trời và biển, và cũng cần bảo vệ chủ quyền quốc gia.

Từ đây cũng dẫn tới dạng động cơ thứ ba là động cơ về chính trị. Động cơ chính trị có xu hướng phát triển từ nhận thức của người ra quyết định và các nhà hoạch định chính sách có thể thay đổi để đáp ứng với tình hình hiện tại. Do đó, chính trị được xem như một động lực bao trùm ảnh hưởng đến các khu vực khác của Chiến lược An toàn không gian mạng quốc gia.

Câu hỏi 2: Các nước đã xây dựng Chiến lược An toàn không gian mạng của họ như thế nào?

Để trả lời câu hỏi này, chúng tôi sử dụng phương pháp so phân tích so sánh định tính. Các kết quả phân tích được trình bày tại bảng sau:

Bảng 2. Tổng quan về chiến lược an toàn không gian mạng các nước

	AUS	CAN	CZE	DEU	FRA	GBR
Phiên bản ngôn ngữ gốc	(AG, 2009)	(PSC, 2010a)	(MoI, 2011a)	(BMI, 2011a)	(SGDN, 2011a)	(CO, 2011)
Ngôn ngữ khác	n/a	Pháp: (PSC, 2010b)	Anh: (MoI, 2011b)	Anh: (BMI, 2011b)	Anh: (SGDN, 2011b)	n/a
Ban hành	11/2009	10/2010	07/2011	02/2011	02/2011	11/2011
Số trang	38	14	10	10	22	44
Có bao gồm tất cả các dạng ICT?	Chỉ các hệ thống kết nối internet	Chỉ các hệ thống kết nối internet	Có	Chỉ các hệ thống kết nối internet	Có	Không rõ ràng
Liên quan với: - Chiến lược an ninh quốc gia - Chiến lược bảo vệ cơ sở hạ tầng quan trọng - Chương trình nghị sự số quốc gia - Chương trình nghị sự số Châu Âu - Chiến lược quốc phòng	■ ■ n/a	■ ■ n/a	■ Không	■ ■ ■ □	■ □ Không ■ (1)	■ (2) □ Không □
Mối đe dọa trên không gian mạng đối với: - Cơ sở hạ tầng quan trọng - Khả năng phòng thủ - Tài sản kinh tế - Toàn cầu hóa - An ninh quốc gia - Sự tin cậy trong ICT - Đời sống xã hội của người dân	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■ □	■ ■ ■ □	■ □ □ ■	■ ■ ■ ■ ■
Mối đe dọa đến từ: - Chủ nghĩa hoạt động/cực đoan - Tội phạm/các tổ chức tội phạm - Gián điệp - Nước ngoài/chiến tranh mạng - Khủng bố - Các cuộc tấn công diện rộng - Sự không phù hợp về phát triển công nghệ và bảo mật	 ■ ■ ■ 	 ■ ■ ■ ■ □	 ■ ■ ■ 	 ■ ■ ■ ■ ■ ■	 ■ ■ ■ ■ 	■ ■ ■ ■ ■ ■

Chú thích: ■ - được mô tả rõ ràng; □ - hàm ý ngầm

(1) Xem SGDN (2008).
(2) Xem HMG (2009, 2010).
(3) Bản chiến lược dài 5 trang. Phần phụ lục dài 11 trang.
(4) Tham khảo EC (2009).
(5) Kế hoạch phòng thủ mạng quốc gia dự kiến hoàn thành năm 2015, xem LRV (2011b, Phụ lục p.7).
(6) Bản dự thảo chiến lược an toàn không gian mạng được thông qua năm 2012, xem DSS (2012).

Bảng 2. Tổng quan về chiến lược an toàn không gian mạng các nước (tiếp)

	IND	ISR	JPN	LTU	LUX	NLD	NZL
Ngôn ngữ gốc	(DIT, 2011)	(NCB, 2015)	Japanese	(LRV, 2011a)	(GGDL, 2011)	(MinV&J, 2011a)	(MoED, 2011)
Ngôn ngữ khác	n/a	n/a	Anh: (ISPC, 2009)	Anh: (LRV, 2011b)	Không	Anh: (MinV&J, 2011b)	n/a
Ban hành	04/2011	11/2015	02/2009	06/2011	11/2011	02/2011	06/2011
Số trang	20	15	20	5+11 (3)	11	9	52
Có bao gồm tất cả các dạng ICT?	Không rõ ràng	Không rõ ràng	Không rõ ràng	Không rõ ràng	Không rõ ràng	Có	Chỉ các hệ thống mạng
Liên quan với: - Chiến lược an ninh quốc gia - Chiến lược bảo vệ cơ sở hạ tầng quan trọng - Chương trình nghị sự số quốc gia - Chương trình nghị sự số Châu Âu - Chiến lược quốc phòng	 □ ■ 	 □ ■ n/a	 ■ n/a	 ■ (4) ■ Không □ (5)	 □ Không	 □ □ ■ ■ □	 n/a
Mối đe dọa trên không gian mạng đối với: - Cơ sở hạ tầng quan trọng - Khả năng phòng thủ - Tài sản kinh tế - Toàn cầu hóa - An ninh quốc gia - Sự tin cậy trong ICT - Đời sống xã hội của người dân	 ■ ■ □ 	 ■ ■ ■ ■	 □ ■ ■ ■ ■	 ■ □ □ ■ 	 ■ ■ □ 	 ■ □ ■ □ ■ ■	 ■ ■ ■ □

Mối đe dọa đến từ: - Chủ nghĩa hoạt động/cực đoan - Tội phạm/các tổ chức tội phạm - Gián điệp - Nước ngoài/chiến tranh mạng - Khủng bố - Các cuộc tấn công diện rộng - Sự không phù hợp về phát triển công nghệ và bảo mật	■ ■ □	□ ■ ■	□ □ ■ ■ ■	■ ■	■	■ ■ ■ ■ ■	■ ■ ■ ■

Chú thích: ■ - được mô tả rõ ràng; □ - hàm ý ngầm

(1) Xem SGDN (2008).
(2) Xem HMG (2009, 2010).
(3) Bản chiến lược dài 5 trang. Phần phụ lục dài 11 trang.
(4) Tham khảo EC (2009).
(5) Kế hoạch phòng thủ mạng quốc gia dự kiến hoàn thành năm 2015, xem LRV (2011b, Phụ lục p.7).
(6) Bản dự thảo chiến lược an toàn không gian mạng được thông qua năm 2012, xem DSS (2012).

Bảng 2. Tổng quan về chiến lược an toàn không gian mạng các nước (tiếp)

	ROU	RUS	SIN	UGA	USA	ZAF
Ngôn ngữ gốc	(MSCI, 2011)	(RFPE, 2015)	(CSAS, 2016)	(MoICT, 2011)	(TWH, 2003)	(DSS, 2010)
Ngôn ngữ khác	Không	n/a	Không	n/a	n/a	n/a
Ban hành	05/2011	12/2015	2016	11/2011	02/2003	02/2010 (6)
Số trang	10	29	47	54	25	15
Có bao gồm tất cả các dạng ICT?	Không rõ ràng	Có	Có	Không rõ ràng	Không rõ ràng	Có
Liên quan với: - Chiến lược an ninh quốc gia - Chiến lược bảo vệ cơ sở hạ tầng quan trọng - Chương trình nghị sự số quốc gia - Chương trình nghị sự số Châu Âu - Chiến lược quốc phòng	Không	■ ■	■ ■ n/a	□ n/a	■ n/a	n/a
Mối đe dọa trên không gian mạng đối với: - Cơ sở hạ tầng quan trọng	■	■	■	■	□	■

- Khả năng phòng thủ - Tài sản kinh tế - Toàn cầu hóa - An ninh quốc gia - Sự tin cậy trong ICT - Đời sống xã hội của người dân	■ □ ■	■ ■ □ ■ ■	■ ■ ■	■ ■	■ ■ ■	■ □ ■
Mối đe dọa đến từ: - Chủ nghĩa hoạt động/cực đoan - Tội phạm/các tổ chức tội phạm - Gián điệp - Nước ngoài/chiến tranh mạng - Khủng bố - Các cuộc tấn công diện rộng - Sự không phù hợp về phát triển công nghệ và bảo mật	■ ■ ■ ■ ■	■ ■ ■ ■ ■	■ ■ ■	■ ■ ■ □	□ ■ ■ ■ □	■

Chú thích: ■ - được mô tả rõ ràng; □ - hàm ý ngầm

(1) Xem SGDN (2008).
(2) Xem HMG (2009, 2010).
(3) Bản chiến lược dài 5 trang. Phần phụ lục dài 11 trang.
(4) Tham khảo EC (2009).
(5) Kế hoạch phòng thủ mạng quốc gia dự kiến hoàn thành năm 2015, xem LRV (2011b, Phụ lục p.7).
(6) Bản dự thảo chiến lược an toàn không gian mạng được thông qua năm 2012, xem DSS (2012).

3. ĐỀ XUẤT XÂY DỰNG CHIẾN LƯỢC AN TOÀN KHÔNG GIAN MẠNG CHO VIỆT NAM

3.1 Các thành phần cần có trong chiến lược an toàn không gian mạng quốc gia

Từ kết quả nghiên cứu, phân tích kinh nghiệm quốc tế kết hợp với điều kiện của Việt Nam, chúng tôi đề xuất cấu trúc của Chiến lược quốc gia về an toàn không gian mạng cho Việt Nam gồm các mục nội dung sau:

1. Tóm tắt bố cục chiến lược: trình bày các mục thông tin cơ bản, khối lượng nội dung chiến lược quốc gia về an toàn không gian mạng cho Việt Nam

2. Giới thiệu: tổng quan về chiến lược, các thông tin như ngày ban hành, ngôn ngữ, số trang, cơ quan ban hành, phạm vi tác động…

3. Tầm nhìn chiến lược quốc gia về an ninh mạng: nêu các mục tiêu, số liệu cụ thể cần đạt được trong ngắn hạn và trung hạn

4. Quan hệ của chiến lược quốc gia về an toàn không gian mạng với các chiến lược khác, cả trong và ngoài nước, và các khung pháp lý hiện hành của Việt Nam và các Nghị quyết, Chỉ thị định hướng của Đảng và Nhà nước

5. Nguyên tắc hướng dẫn: đưa ra các nội dung hướng dẫn các Bộ, ngành, địa phương thực hiện chiến lược quốc gia về an toàn không gian mạng của Việt Nam. Nguyên tắc thực hiện các nội dung chiến lược phù hợp với các khung pháp lý hiện có.

6. Các mục tiêu an ninh mạng: theo kinh nghiệm quốc tế, tốt nhất là có từ một đến bốn mục tiêu; trong đó đưa ra mục tiêu cụ thể để đảm bảo an toàn không gian mạng quốc gia, có số liệu định lượng và lộ trình để xác định đạt mục tiêu.

7. Đề cương các kế hoạch hành động: quy định ai làm, nguồn lực (ngân sách, tiền, kinh phí và con người) bố trí ở đâu, và làm như thế nào để đạt các mục tiêu nêu ra.

8. Kế hoạch tham gia các điều ước quốc tế: quy định và đưa ra một tập hợp các điều ước, thỏa thuận quốc tế song phương, đa phương quốc tế cần tham gia theo lộ trình và các thỏa thuận đã ký cần được điều chỉnh; Phân tích rõ sự phù hợp và lý do lựa chọn.

9. Phụ lục. Dự kiến các hoạt động được xác định theo nội dung, nêu tên các Bộ ngành chủ trì, nguồn lực huy động từ xã hội và ngân sách nhà nước, được sắp xếp thứ tự ưu tiên một cách hợp lý.

Các thành phần nêu trên cần có cho chiến lược QG về an toàn không gian mạng cho Việt Nam. Các mục nội dung trong chiến lược có thể được liên kết với các mô tả, thống kê và hỗ trợ bởi các tổ chức chính trị, tổ chức chính trị xã hội, các tổ chức nghiên cứu và giới công nghiệp, tập trung vào doanh nghiệp nhà nước. Điều này góp phần nâng cao nhận thức, quy định rõ trách nhiệm và nhấn mạnh tầm quan trọng và sự

liên quan, vị trí, vai trò của các Bộ, ngành, địa phương đối với chiến lược quốc gia về an toàn không gian mạng Việt Nam.

3.2 Mục tiêu, nguyên tắc và các kế hoạch hành động trong chiến lược an toàn không gian mạng của Việt Nam

a) Nội dung tầm nhìn và mục tiêu

Tầm nhìn và mục tiêu áp dụng trong chiến lược an toàn không gian mạng QG cho Việt Nam cũng phải phù hợp với các chiến lược, mục tiêu và tầm nhìn phát triển kinh tế-xã hội của đất nước. Khi nghiên cứu, phân tích và xây dựng chiến lược an toàn không gian mạng, cần phải rà soát, tham khảo các văn bản có tính "kim chỉ nam" của QG để hiểu rõ các chiến lược, mục tiêu và tầm nhìn kinh tế-xã hội của đất nước, qua đó hình dung được viễn cảnh mà QG đang hướng tới. Đồng thời tham khảo các văn bản thể hiện chủ trương của Đảng và Chính phủ đối với phát triển ngành ICT và vấn đề bảo đảm an toàn thông tin mạng, an toàn không gian mạng.

Tầm nhìn và mục tiêu cho chiến lược an toàn không gian mạng Việt Nam nên thực hiện theo tiêu chuẩn Châu Âu. Theo đó, ENISA (2012) đã xác định mục đích của chiến lược an ninh trên mạng là tăng khả năng phục hồi toàn cầu và an ninh của các tài sản ICT quốc gia, hỗ trợ các chức năng quan trọng của nhà nước hoặc của toàn xã hội. Đồng thời cần đặt ra các mục tiêu và ưu tiên rõ ràng là điều tối quan trọng để đạt được mục tiêu này.

b) Nguyên tắc và kế hoạch hành động

Trên cơ sở tham khảo ENISA (2012), nhóm đề tài đề xuất một số yêu cầu nhiệm vụ cần cân nhắc để đạt được mục tiêu được liệt kê dưới đây:

- Xác định tầm nhìn và phạm vi đặt ra các mục tiêu cao cấp sẽ được thực hiện trong một khung thời gian cụ thể (thường là 5-10 năm).
- Xác định các lĩnh vực kinh doanh và dịch vụ trong phạm vi cho chiến lược này.
- Thực hiện đánh giá rủi ro quốc gia toàn diện để xác định mục tiêu và phạm vi chiến lược.
- Ưu tiên các mục tiêu về tác động đến xã hội, nền kinh tế và công dân.
- Theo dõi tình hình hiện tại (ví dụ như chính sách, quy định, hoạt động, v.v ...).
- Tham gia vào các bên liên quan ngay từ khi bắt đầu quá trình để đạt được mục tiêu.
- Xác định lộ trình thực hiện chiến lược, có thể bao gồm nhiều bước.
- Xác định các hoạt động cụ thể có thể đáp ứng các mục tiêu của chiến lược.
- Xây dựng một khuôn khổ quản trị để thực hiện, đánh giá và duy trì chiến lược.
- Xây dựng một kế hoạch tổng thể để thực hiện chiến lược.
- Xây dựng kế hoạch hành động cụ thể cho từng hoạt động.

Trong chiến lược, cần xác định rõ ràng tiêu chí đánh giá kết quả thực hiện chiến lược và các hành động chính của nó trong từng giai đoạn. Sử dụng chỉ số hiệu suất (KPIs) để đánh giá các nội dung sẽ được thực hiện như thế nào và bởi Bộ, ngành, địa phương nào thực hiện.

Trong trường hợp xác định một kế hoạch hành động hoặc một nhiệm vụ cụ thể, chiến lược nên quyết định bao gồm xác định các mối đe dọa và đánh giá rủi ro bằng một phân tích SWOT, nó có thể được đưa vào giữa phần nội dung chiến lược QG về an ninh mạng hoặc như một nghiên cứu phân tích sâu riêng.

Chúng tôi cũng đề xuất Việt Nam nên xây dựng các nhiệm vụ và kế hoạch hành động theo kinh nghiệm của Israel. Theo đó, chiến lược an ninh mạng không gian QG cần có ba lớp chính: sức mạnh hệ thống bảo vệ, khả năng phục hồi hệ thống và bảo đảm an ninh quốc phòng. Chính phủ đóng một vai trò khác nhau trong mỗi lớp. Chính phủ có thể điều chỉnh sức mạnh hệ thống bảo vệ và hỗ trợ khả năng phục hồi của mọi cơ quan, tổ chức. Hầu hết các cuộc tấn công trên không gian mạng có thể được xử lý, giải quyết ở cả hai cấp đầu tiên. Nhưng có những trường hợp chính phủ phải chuyển sang tầng thứ ba - an ninh quốc phòng - là điều cần thiết để giảm thiểu, ngăn chặn và trả đũa. Trong trường hợp Israel, khi bộ máy dân sự không thể đối phó, kể cả các cơ quan dân sự trung ương xử lý không ổn thì bộ máy an ninh, quốc phòng, quân đội có thể bị kêu gọi để phản ứng, và các cơ quan thi hành luật pháp để điều tra hình sự và chống khủng bố. Israel cũng đã ban hành khung hướng dẫn xây dựng chiến lược an toàn không gian mạng quốc gia phù hợp với các cuộc tấn công không gian mạng có quy mô nhỏ và vừa.

Từ các kết quả nghiên cứu,chúng tôi đề xuất một số nguyên tắc và nội dung cơ bản khi xây dựng chiến lược an toàn không gian mạng của Việt Nam, đây cũng là những điểm chung, quan trọng thường có trong chiến lược QG về an toàn không gian mạng của các nước. Các nội dung cụ thể như sau:

- *Quan điểm khi xây dựng chiến lược an toàn không gian mạng:* giữ gìn hòa bình, bảo vệ không gian mạng quốc gia, không chủ động tấn công, không làm phương hại đến an toàn không gian mạng quốc gia khác; sử dụng mọi nguồn lực tăng cường và giữ vững chủ quyền số quốc gia trên không gian mạng.

- *Học thuyết chiến tranh nhân dân làm cơ sở nền tảng tư tưởng cho chiến trang mạng:* Tất cả người dân đều tham gia bảo vệ không gian mạng, mọi người dân được biết về những rủi ro không gian mạng, tham gia và có trách nhiệm bảo mật máy tính của mình. Với bản chất của việc đảm bảo an toàn, an ninh mạng là việc của toàn xã hội, từng cá nhân, từng tổ chức phải có trách nhiệm tốt trong ứng cứu sự cố an toàn không gian mạng quốc gia, tạo ra thế trận nhân dân trong việc phòng thủ đối với chiến tranh mạng, chiến tranh thông tin.

- *Chuẩn bị các công cụ, sẵn sàng mọi phương tiện để bảo vệ chủ quyền số quốc gia trên không gian mạng:* phát triển KHCN, nghiên cứu chuyên sâu, làm chủ công nghệ và sản xuất các sản phẩm nội địa chủ lực để bảo vệ không gian mạng quốc gia.

- *Phát triển nhân sự trong mọi cấp chính quyền từ trung ương đến các địa phương:* phát triển các cơ sở đào tạo, nâng cao năng lực phát triển nguồn nhân lực an toàn, an ninh không gian mạng đạt trình độ tiên tiến của quốc tế;

- *Đảm bảo sự phối hợp liên ngành, giữa các Bộ, ngành, địa phương:* Trong chiến lược an toàn không gian mạng của Việt Nam, một trong những nội dung quan trọng là cần đề xuất được nhiệm vụ cụ thể, phân công trách nhiệm rõ ràng và đảm bảo sự phối hợp liên ngành, thông suốt giữa các Bộ, ngành, địa phương để đối phó với một cuộc tấn công mạng quy mô quốc gia tấn công vào Việt Nam.

4. KẾT LUẬN

Có thể thấy rằng an toàn không gian mạng ở Việt Nam đã được sự quan tâm của chính phủ và việc ban hành chiến lược an toàn không gian mạng Việt Nam đã trở nên cấp bách. Để phục vụ cho việc xây dựng chiến lược an toàn không gian mạng của Việt Nam, chúng tôi đã áp dụng phương pháp nghiên cứu định tính để tiến hành phân tích tầm nhìn, mục tiêu, nguyên tắc và kế hoạch hành động của chiến lược an toàn không gian mạng của các quốc gia. Sử dụng các công cụ phân tích định tính và định tính so sánh để tìm ra đặc điểm chung và khám phá động cơ đằng sau các chiến lược đó. Bên cạnh phương pháp nghiên cứu định tính và định tính so sánh truyền thống, sử dụng các bảng biểu trực tiếp, nhóm đề tài sử dụng phần mềm Nvivo chuyên phân tích dữ liệu định tính để xác định các thành phần chung trong chiến lược an toàn không gian mạng các quốc gia trên thế giới.

Từ các kinh nghiệm thu được ở các nghiên cứu, đề tài đã phân tích các yếu tố ảnh hưởng tới việc xây dựng chiến lược an toàn không gian mạng ở Việt Nam, từ đó đề xuất phương pháp xây dựng chiến lược an toàn không gian mạng và đề xuất một số nét chính về tầm nhìn, mục tiêu, nguyên tắc và các kế hoạch hành động trong chiến lược an toàn không gian mạng của Việt Nam.

TÀI LIỆU THAM KHẢO

1. *FD Kramer, S. Starr, L.K. Wentz, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," National Defense University Press, Washington (DC) 2009.*
2. *Azmi, Tibben, Win, "Motives behind Cyber Security Strategy Development" , Australasian Conference on Information Systems. 2016*
3. *Anna-Maria Osula, Kadri Kaska, "National Cyber Security Strategy Guidelines," NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2013*
4. *Punch, Keith, "Introduction to Social Research: Quantitative and Qualitative Approaches (2nd Ed)", London, Sage Publications*
5. *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation – Microsoft*