CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 397 /TTr-CP	*Hà Nội, ngày 26 tháng 9 năm 2017*

TỜ TRÌNH
Dự án Luật An ninh mạng[1]

Kính gửi: Quốc hội

Thực hiện Nghị quyết số 22/2016/QH14 ngày 29 tháng 7 năm 2016 của Quốc hội khóa XIV về Chương trình xây dựng Luật, Pháp lệnh năm 2016 và năm 2017, Chính phủ xin trình Quốc hội dự án Luật An ninh mạng như sau:

I. SỰ CẦN THIẾT BAN HÀNH LUẬT

1. Đáp ứng yêu cầu của công tác an ninh mạng trong bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội

Cùng với quá trình hội nhập quốc tế, phát triển công nghệ thông tin, đặc biệt là cuộc cách mạng công nghệ 4.0, thực trạng, tình hình diễn ra trên không gian mạng đã đặt ra yêu cầu cấp thiết đối với công tác an ninh mạng trong bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội, cụ thể:

Thứ nhất, phòng ngừa, đấu tranh, làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, phá hoại khối đại đoàn kết toàn dân tộc, kích động biểu tình, phá rối an ninh trên không gian mạng của các thế lực thù địch, phản động.

Thứ hai, phòng ngừa, ngăn chặn, ứng phó, khắc phục hậu quả của các hoạt động tấn công mạng, khủng bố mạng, phòng, chống chiến tranh mạng khi hoạt động tấn công mạng nhằm vào hệ thống thông tin nước ta gia tăng về số lượng và mức độ nguy hiểm, ảnh hưởng nghiêm trọng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội. Trong khi đó, khủng bố mạng nổi lên như một thách thức toàn cầu, chiến tranh mạng là một trong những nguy cơ đe dọa an ninh quốc gia. Những vấn đề trên đòi hỏi phải chủ động phòng ngừa, ngăn chặn, ứng phó, có phương án và sự chuẩn bị sẵn sàng để kịp thời xử lý các tình huống xấu có thể xảy ra.

Thứ ba, phòng ngừa, ngăn chặn, loại bỏ tác nhân tiến hành hoạt động gián điệp mạng, sử dụng không gian mạng để chiếm đoạt thông tin, tài liệu bí

---

[1] Thay thế Tờ trình số 366/TTr-CP ngày 31/8/2017

mật nhà nước, đặc biệt là hoạt động xâm nhập, tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia; đồng thời, hạn chế và tiến tới chấm dứt tình trạng đăng tải bí mật nhà nước trên mạng internet do chủ quan hoặc thiếu kiến thức an ninh mạng.

Thứ tư, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia và áp dụng các biện pháp cần thiết, tương xứng. Đây là hệ thống thông tin của các mục tiêu quan trọng quốc gia, cơ sở hạ tầng quan trọng quốc gia, cơ quan chứa đựng bí mật nhà nước, nếu bị tấn công, xâm nhập, phá hoại, chiếm đoạt thông tin có thể gây hậu quả nghiêm trọng, ảnh hưởng chủ quyền, lợi ích, an ninh quốc gia, gây rối loạn trật tự an toàn xã hội nên cần có biện pháp bảo vệ chặt chẽ, tương xứng và ở mức độ cao hơn so với những mục tiêu cần bảo vệ ít quan trọng hơn. Việc bảo vệ những hệ thống thông tin này không chỉ bao gồm hoạt động kiểm tra, đánh giá quá trình vận hành, áp dụng các tiêu chuẩn an ninh mạng phù hợp, riêng biệt mà phải tiến hành hoạt động thẩm định ngay từ khi xây dựng hồ sơ thiết kế, vận hành hệ thống thông tin để sớm phát hiện, loại bỏ các nguy cơ đe dọa an ninh mạng.

Để góp phần cải cách thủ tục hành chính, tránh trùng lặp về thẩm quyền quản lý nhà nước, hướng tới mục tiêu chỉ một cơ quan quản lý nhà nước đối với một hệ thống thông tin, dự thảo Luật An ninh mạng đã quy định Chính phủ quy định chi tiết Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trường hợp hệ thống thông tin được phân loại theo quy định của luật khác mà trùng với hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo quy định của Luật An ninh mạng thì áp dụng quy định của Luật An ninh mạng; Bộ Công an thẩm định về năng lực, điều kiện đối với doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Thứ năm, quy định và thống nhất thực hiện phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Hoạt động ứng cứu sự cố an toàn thông tin mạng theo quy định của Luật An toàn thông tin mạng hiện nay chỉ phát huy được vai trò bảo đảm 03 thuộc tính của thông tin là tính nguyên vẹn, tính bảo mật và tính khả dụng, chưa đáp ứng được yêu cầu bảo vệ quốc phòng, an ninh, trật tự an toàn xã hội, xử lý sự cố, huy động lực lượng ứng phó, cũng như loại bỏ các tác nhân gây hại tồn tại sẵn bên trong hệ thống thông tin hoặc hành vi vi phạm pháp luật trên không gian mạng ảnh hưởng tới hệ thống thông tin quan trọng về an ninh quốc gia. Phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là một quy trình thống nhất. Việc phân tích các

sự cố an ninh mạng liên quan trực tiếp tới dấu vết hiện trường và các dấu hiệu phạm tội, góp phần vào công tác điều tra, xử lý hành vi vi phạm của cơ quan chức năng Bộ Công an, Bộ Quốc phòng. Do đó, thống nhất đầu mối trong giám sát, dự báo, ứng phó và diễn tập ứng phó khẩn cấp sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là cấp bách, cần thiết, không trùng dẫm với ứng cứu sự cố an toàn thông tin mạng.

Thứ sáu, quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Tham khảo kinh nghiệm nước ngoài cho thấy, một số quốc gia trên thế giới đã xây dựng các bộ tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng để áp dụng cho các mục tiêu, đối tượng và yêu cầu bảo vệ an ninh mạng cụ thể. Ở nước ta, tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng được ban hành rộng rãi, được áp dụng chung cho toàn xã hội, mang tính phổ thông, đại chúng. Tuy nhiên, đối với hệ thống thông tin quan trọng về an ninh quốc gia, ngoài những tiêu chuẩn an toàn thông tin mạng, cần có những quy định về tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng ở mức độ cao hơn để đáp ứng yêu cầu đặt ra.

Thứ bảy, triển khai công tác bảo vệ an ninh mạng trong hệ thống cơ quan nhà nước từ Trung ương đến địa phương. Hiện nay, hệ thống thông tin của cơ quan nhà nước tồn tại nhiều lỗ hổng bảo mật không được khắc phục, nhận thức của cán bộ, nhân viên còn nhiều hạn chế, chưa nhận thức được mức độ cần thiết của công tác an ninh mạng. Trong khi đó, công nghệ thông tin đã được ứng dụng rộng rãi từ Trung ương đến địa phương, chính phủ điện tử và các hệ thống điều khiển, xử lý tự động đã xuất hiện ở mọi ngành, cấp, lĩnh vực. Hệ thống thông tin của cơ quan nhà nước đang là đối tượng của hoạt động tấn công mạng, xâm nhập mạng, gián điệp mạng; tình trạng đăng tải thông tin, tài liệu bí mật nhà nước trên mạng internet vẫn còn tồn tại. Do đó, tình hình thực tiễn đã đặt ra yêu cầu triển khai công tác bảo vệ an ninh mạng và lực lượng an ninh mạng từ Trung ương đến địa phương.

Thứ tám, đặt nền móng và triển khai công tác nghiên cứu, dự báo, phát triển các giải pháp bảo đảm an ninh mạng. Hiện nay, công tác này chưa được chú trọng, nhà nước cũng chưa có định hướng quản lý, bảo đảm an ninh mạng đối với các xu hướng công nghệ có khả năng thay đổi tương lai như cuộc cách mạng công nghiệp lần thứ 4, điện toán đám mây, dữ liệu lớn, dữ liệu nhanh. Tham khảo kinh nghiệm nước ngoài cho thấy, một số quốc gia đã xây dựng nhiều đạo luật chuyên ngành của an ninh mạng, tập trung nâng cao năng lực dự báo, chia sẻ thông tin và tăng cường năng lực an ninh mạng.

Thứ chín, thường xuyên kiểm tra, đánh giá thực trạng an ninh mạng đối với hệ thống thông tin của các bộ, ngành, địa phương. Mặc dù Chính phủ đã giao Bộ Công an đã chủ trì, phối hợp với các bộ, ngành liên quan triển khai nhiều kế hoạch kiểm tra, đánh giá thực trạng an ninh mạng tại hàng chục bộ, ngành, địa phương nhưng đây là hoạt động đột xuất, chưa được triển khai hằng năm, không tạo thành được trách nhiệm và ý thức kiểm tra, đánh giá an ninh mạng định kỳ. Trong khi đó, cơ quan chủ quản hệ thống thông tin chưa nhận thức rõ trách nhiệm của mình, chưa chủ động hoặc triển khai các hoạt động bảo vệ an ninh mạng một cách chiếu lệ, hình thức. Để phòng ngừa, hạn chế nguy cơ an ninh mạng, cần xây dựng quy trình, cơ chế kiểm tra, đánh giá thực trạng an ninh mạng phù hợp, thống nhất trên phạm vi cả nước.

Thứ mười, xây dựng cơ chế chia sẻ thông tin, thông báo tình hình an ninh mạng để nâng cao nhận thức về an ninh mạng, chủ động phòng ngừa các nguy cơ an ninh mạng có thể xảy ra. Việc chia sẻ thông tin, thông báo tình hình an ninh mạng có thể được thực hiện bởi cơ quan chức năng để tổ chức, cá nhân nâng cao nhận thức, áp dụng biện pháp phòng tránh hoặc nghiên cứu, tham khảo.

2. Phòng ngừa, ứng phó với các nguy cơ đe dọa an ninh mạng

Các nguy cơ đe dọa an ninh mạng hiện đang tồn tại là:

- Thông qua không gian mạng thực hiện âm mưu "diễn biến hòa bình", phá hoại tư tưởng, chuyển hóa chế độ chính trị nước ta. Trong bối cảnh toàn cầu hóa, hội nhập quốc tế và đặc biệt là sự phát triển mạnh mẽ của khoa học công nghệ, âm mưu này được triển khai dưới nhiều phương thức thức khác nhau. Không gian mạng trở thành môi trường lý tưởng cho âm mưu "diễn biến hòa bình", phá hoại tư tưởng, chuyển hóa chế độ chính trị nước ta, thông qua các hoạt động thúc đẩy "tự diễn biến", "tự chuyển hóa"; liên lạc, móc nối, chỉ đạo và thành lập tổ chức hoạt động chống phá; sử dụng không gian mạng để kích động biểu tình, gây rối an ninh, chuyển hóa chế độ chính trị ở nước ta.

- Đối mặt với các cuộc tấn công mạng trên quy mô lớn, cường độ cao. Mục tiêu tấn công mạng là hạ tầng truyền dẫn vật lý (cáp truyền dẫn quốc tế, trục truyền dẫn nội bộ quốc gia...), hạ tầng dịch vụ lõi (router, thiết bị mạng...), hệ thống điều khiển tự động hóa (SCADA) của các cơ sở quan trọng về kinh tế, quốc phòng, an ninh... Tấn công mạng có thể diễn ra theo kiểu ra tự phát, đơn lẻ, theo các chiến dịch với mục đích khống chế và thu thập thông tin, khủng bố, đe dọa và tán phát các thông điệp xấu, phá hủy cơ sở hạ tầng trọng yếu quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia, thậm chí là phục vụ chiến tranh.

- Mất kiểm soát về an ninh, an toàn thông tin mạng. Nguy cơ này chịu tác động trực tiếp từ bốn yếu tố: Sự phụ thuộc vào hạ tầng và dịch vụ công nghệ, thiếu hụt nguồn nhân lực công nghệ thông tin chất lượng cao, ý thức người dùng hạn chế và bất cập, hạn chế, yếu kém trong quản lý nhà nước về an ninh, an toàn thông tin mạng.

3. Khắc phục tồn tại, hạn chế liên quan bảo vệ an ninh mạng

Một là, chồng chéo, trùng dẫm trong thực hiện chức năng, nhiệm vụ bảo vệ an ninh mạng giữa các bộ, ngành chức năng; tồn tại cách hiểu chưa rõ ràng giữa an ninh mạng và an toàn thông tin mạng. Cần thống nhất nhận thức rằng, an ninh mạng bao gồm hoạt động bảo vệ an ninh quốc gia, trật tự an toàn xã hội theo chức năng, nhiệm vụ của Bộ Công an; hoạt động tác chiến trên không gian mạng theo chức năng, nhiệm vụ của Bộ Quốc phòng và bảo đảm an toàn thông tin mạng theo chức năng, nhiệm vụ của Bộ Thông tin và Truyền thông. An toàn thông tin mạng là điều kiện cho bảo đảm an ninh mạng được thực thi có hiệu quả, bền vững.

Có nhiều nguyên nhân dẫn đến tồn tại, vướng mắc nêu trên, trong đó nguyên nhân chủ yếu là từ sự vướng mắc, bất cập được biểu hiện thông qua hai vấn đề. **Thứ nhất**, do chưa có sự nhận thức thống nhất về an ninh mạng nên hiện nay, Bộ Công an thực hiện nhiệm vụ bảo vệ an ninh mạng đều dựa trên cơ sở quy định của Luật An ninh quốc gia, Luật Công an nhân dân và các văn bản dưới luật về bảo vệ an ninh quốc gia nói chung và nguyên tắc tổ chức, hoạt động, chức năng, nhiệm vụ, quyền hạn và chế độ, chính sách đối với lực lượng Công an nhân dân nói riêng; chưa có quy định cụ thể về an ninh mạng và chức năng, nhiệm vụ, quyền hạn của lực lượng an ninh mạng trong Công an nhân dân. **Thứ hai**, qua rà soát hệ thống pháp luật của một số quốc gia trên thế giới (Anh, Mỹ, Nhật, Úc...) cho thấy, các quốc gia này không phân tách "cyber security" thành "an ninh mạng" và "an toàn thông tin mạng" như ở nước ta, mà thống nhất giao một đầu mối thực hiện chức năng quản lý nhà nước, căn cứ vào chức năng, nhiệm vụ của các bộ, ngành để có sự phân công phù hợp. Hai vấn đề trên đã dẫn tới công tác bảo vệ an ninh mạng chưa được triển khai trên tất cả các lĩnh vực, đối tượng mà không gian mạng bao phủ và hiện đang có ảnh hưởng sâu sắc.

Hai là, chưa có văn bản luật quy định về công tác an ninh mạng. Trong những năm qua, nước ta đã ban hành nhiều văn bản quy phạm pháp luật liên quan đến lĩnh vực công nghệ thông tin, viễn thông, internet nhưng chưa có văn bản quy phạm pháp luật quy định cụ thể về an ninh mạng nên chưa có đầy đủ căn cứ pháp lý để triển khai các biện pháp phòng ngừa, phát hiện, xử lý, đấu

tranh với các nguy cơ đe dọa an ninh mạng, hành vi vi phạm pháp luật trên không gian mạng. Các quy định hiện nay về an toàn thông tin mạng chưa đủ sức răn đe, ngăn chặn các hành vi vi phạm trên không gian mạng; chưa đáp ứng được yêu cầu thực tiễn của công tác an ninh mạng đặt ra trong tình hình mới. Thực trạng này đã gây khó khăn, vướng mắc trong tổ chức, triển khai các phương án bảo đảm an ninh thông tin, an ninh mạng cũng như trong công tác phòng ngừa, đấu tranh ngăn chặn các hoạt động sử dụng internet để xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

4. Thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối của Đảng về an ninh mạng

Quan điểm, tư tưởng chỉ đạo của Đảng, Nhà nước về an ninh mạng đã thể hiện rõ, nhất quán, có hệ thống và phù hợp với từng thời kỳ, kịp thời điều chỉnh, đưa ra các quan điểm, tư tưởng chỉ đạo về vấn đề an ninh mạng trong tình hình mới. Việc ban hành Luật an ninh mạng là nhằm thể chế hóa đầy đủ, kịp thời chủ trương, đường lối của Đảng về an ninh mạng được nêu tại một số văn bản như:

Nghị quyết số 13-NQ/TW ngày 16/01/2012 của Hội nghị TW4 khóa XI về xây dựng hệ thống kết cấu hạ tầng đồng bộ nhằm đưa nước ta cơ bản trở thành nước công nghiệp theo hướng hiện đại vào năm 2020. Nghị quyết số 28-NQ/TW của Hội nghị TW VIII khóa XI về chiến lược bảo vệ Tổ quốc trong tình hình mới. Chỉ thị số 46-CT/TW của Bộ Chính trị về tăng cường sự lãnh đạo của Đảng đối với công tác bảo đảm an ninh trật tự trong tình hình mới, trong đó khẳng định vấn đề an ninh mạng đang là vấn đề rất phức tạp, cần được chú trọng giải quyết đồng bộ, hiệu quả. Chỉ thị số 28-CT/TW của Ban Bí thư Trung ương Đảng, Chỉ thị số 15-CT/TTg của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng; Chỉ thị số 30-CT/TW của Bộ Chính trị ban hành về phát triển và tăng cường quản lý báo chí điện tử, mạng xã hội và các loại hình truyền thông khác trên Internet. Nghị định 101/2016/NĐ-CP của Chính phủ quy định chi tiết trách nhiệm thực hiện và các biện pháp ngăn chặn hoạt động sử dụng không gian mạng để khủng bố.

5. Bảo đảm sự phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và bảo vệ Tổ quốc

Theo quy định tại khoản 2 Điều 14 của Hiến pháp năm 2013 thì Quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng. Dự kiến Luật An ninh mạng sẽ quy định các biện pháp nghiệp vụ an ninh mạng, trong đó có một số biện pháp có khả năng

ảnh hưởng tới quyền con người, quyền và nghĩa vụ cơ bản của công dân như giám sát an ninh mạng, hạn chế thông tin mạng... Do vậy, việc ban hành Luật An ninh mạng để bảo đảm quyền con người, quyền công dân theo quy định của Hiến pháp là cần thiết. Bên cạnh đó, việc ban hành Luật này cũng góp phần cụ thể hóa tinh thần và nội dung mới của Hiến pháp về bảo vệ Tổ quốc, đặc biệt là quy định "Tổ quốc Việt Nam là thiêng liêng, bất khả xâm phạm" và "mọi hành vi chống lại độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ, chống lại sự nghiệp xây dựng và bảo vệ Tổ quốc đều bị nghiêm trị".

6. Bảo đảm sự phù hợp với thông lệ quốc tế

Qua nghiên cứu cho thấy, hiện đã có nhiều quốc gia trên thế giới ban hành các văn bản luật về an ninh mạng, điển hình như: Mỹ, Nhật, Trung Quốc, Anh, Úc, Cộng hòa Séc, Hàn Quốc... Riêng Mỹ đã ban hành tới 06 đạo luật chuyên ngành về các vấn đề về an ninh mạng là: Đạo luật Đánh giá Lực lượng An ninh mạng, Đạo luật Tăng cường An ninh mạng năm 2014, Đạo luật Bảo vệ An ninh mạng Quốc gia 2014, Đạo luật hiện đại hóa An ninh thông tin Liên bang năm 2014, Dự luật Chia sẻ thông tin An ninh mạng năm 2015, Dự luật Tăng cường Bảo vệ An ninh mạng Quốc gia năm 2015. Ngày 7/12/2015, Hội đồng và Nghị viện Châu Âu đạt được sự thống nhất về các biện pháp thúc đẩy an ninh mạng tổng thể trong Liên minh Châu Âu tại Chỉ thị An ninh thông tin và mạng (Network and Information Security) nhằm tăng cường các khả năng an ninh mạng của các quốc gia thành viên, tăng cường sự hợp tác của các quốc gia thành viên trong lĩnh vực an ninh mạng. Việc xây dựng, ban hành Luật An ninh mạng sẽ bảo đảm công tác an ninh mạng của nước ta có sự phù hợp nhất định với thông lệ quốc tế và bảo đảm các điều kiện hội nhập quốc tế về an ninh mạng.

II. QUAN ĐIỂM CHỈ ĐẠO VÀ MỤC ĐÍCH XÂY DỰNG LUẬT

1. Quan điểm chỉ đạo

- Thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối, chính sách của Đảng, Nhà nước về an ninh mạng. Xác định bảo đảm an ninh mạng là một bộ phận cấu thành đặc biệt quan trọng của sự nghiệp bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa; là nhiệm vụ vừa cấp bách vừa lâu dài của cả hệ thống chính trị, giao Bộ Công an chủ trì, đặt dưới sự lãnh đạo xuyên suốt của Đảng và sự quản lý thống nhất của Nhà nước.

- Bảo đảm phù hợp với quy định của Hiến pháp mới; cụ thể hóa đầy đủ các quy định có tính đổi mới của Hiến pháp, nhất là quy định về bảo vệ Tổ quốc và quy định về quyền con người, quyền và nghĩa vụ cơ bản của công dân.

- Bảo đảm tính đồng bộ, thống nhất của hệ thống pháp luật, xác định hợp lý mối quan hệ giữa Luật này và các luật liên quan.

- Kế thừa các quy định hiện hành còn phù hợp, sửa đổi, bổ sung các quy định đã bộc lộ những hạn chế.

- Tham khảo có chọn lọc kinh nghiệm của các nước trong khu vực và trên thế giới để vận dụng linh hoạt vào điều kiện thực tiễn của Việt Nam; bảo đảm sự phù hợp với các quy định, cam kết quốc tế mà Việt Nam tham gia ký kết hoặc là thành viên.

2. Mục đích xây dựng Luật

- Hoàn thiện cơ sở pháp lý ổn định về an ninh mạng theo hướng áp dụng các quy định pháp luật một cách đồng bộ, khả thi trong thực tiễn thi hành.

- Phát huy các nguồn lực của đất nước để bảo đảm an ninh mạng, phát triển lĩnh vực an ninh mạng đáp ứng yêu cầu phát triển kinh tế - xã hội, quốc phòng, an ninh, góp phần nâng cao chất lượng cuộc sống của nhân dân và bảo đảm quốc phòng, an ninh.

- Bảo vệ chủ quyền, lợi ích, an ninh quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động trên không gian mạng, xây dựng môi trường không gian mạng lành mạnh.

- Triển khai công tác an ninh mạng trên phạm vi toàn quốc, đẩy mạnh công tác giám sát, dự báo, ứng phó và diễn tập ứng phó sự cố an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; đảm bảo hiệu quả công tác quản lý nhà nước trong lĩnh vực này.

- Nâng cao năng lực tự chủ về an ninh mạng, hoàn thiện chính sách nghiên cứu, phát triển chiến lược, chia sẻ thông tin về an ninh mạng.

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

III. QUÁ TRÌNH SOẠN THẢO

Thực hiện Nghị quyết số 22/2016/QH14 ngày 29 tháng 7 năm 2016 của Quốc hội khóa XIV về Chương trình xây dựng Luật, Pháp lệnh năm 2016 và năm 2017, Chính phủ đã ban hành Quyết định số 1840/2016/QĐ-TTg ngày 23 tháng 9 năm 2016 phân công cơ quan chủ trì soạn thảo và thời hạn trình các dự án luật, pháp lệnh, nghị quyết được bổ sung vào Chương trình xây dựng luật, pháp lệnh năm 2016 và Chương trình xây dựng luật, pháp lệnh năm 2017.

Căn cứ Nghị quyết của Quốc hội và Quyết định của Thủ tướng Chính phủ, Bộ Công an đã ban hành Quyết định số 951/QĐ-BCA ngày 27/3/2017 thành lập Ban Soạn thảo dự án Luật An ninh mạng, Quyết định số 954/QĐ-BST ngày 28/3/2017 thành lập Tổ Biên tập dự án Luật An ninh mạng.

Thời gian qua, Chính phủ đã giao Bộ Công an đã chủ trì, phối hợp với các bộ, ngành liên quan thực hiện các hoạt động sau đây:

1. Rà soát, tổng kết, đánh giá thực hiện các văn bản quy phạm pháp luật về an ninh mạng và các quy định khác liên quan đến an ninh mạng.

2. Tổ chức nghiên cứu khoa học, nghiên cứu chuyên đề về an ninh mạng; thành lập các nhóm nghiên cứu và hoàn thành các báo cáo chuyên đề phục vụ việc xây dựng dự thảo Luật An ninh mạng, bao gồm: Báo cáo đánh giá tác động của dự thảo Luật An ninh mạng; Báo cáo nghiên cứu chuyên đề về tên Luật và phạm vi điều chỉnh của Luật An ninh mạng; Báo cáo nghiên cứu chuyên đề rà soát, đánh giá hệ thống văn bản quy phạm pháp luật hiện hành của Việt Nam về an ninh mạng; Báo cáo nghiên cứu chuyên đề nghiên cứu, khảo sát kinh nghiệm nước ngoài về an ninh mạng; Báo cáo nghiên cứu về đào tạo, phát triển nguồn nhân lực về an ninh mạng; Báo cáo nghiên cứu chuyên đề về tiêu chuẩn, quy chuẩn kỹ thuật, kiểm định, đánh giá an ninh mạng.

3. Tham khảo kinh nghiệm của một số quốc gia trong khu vực và trên thế giới về an ninh mạng, đặc biệt là Nhật Bản, Trung Quốc, Mỹ, Đức, Anh, Úc...

4. Xây dựng dự án Luật An ninh mạng đúng quy trình theo pháp luật về thẩm quyền ban hành văn bản quy phạm pháp luật. Ban Soạn thảo xây dựng Luật An ninh mạng bao gồm thành viên của nhiều bộ, ngành liên quan đã họp nhiều lần để thảo luận và quyết định những nội dung quan trọng của Luật. Bộ Công an đã tổ chức lấy ý kiến đóng góp trực tiếp thông qua các tọa đàm, hội thảo[2] và bằng văn bản của các bộ, ngành, Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương, các doanh nghiệp cung cấp dịch vụ viễn thông, internet[3] và lấy ý kiến đóng góp của toàn xã hội trên Cổng thông tin điện tử Chính phủ,

---

[2] Hội thảo "bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia" được tổ chức vào ngày 25/8/2017 tại Hạ Long, Quảng Ninh, với sự tham gia của hơn 300 đại biểu đến từ các cơ quan quản lý nhà nước, cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, các doanh nghiệp cung cấp dịch vụ viễn thông, internet trong và ngoài nước, các chuyên gia pháp luật, công nghệ thông tin, an toàn thông tin, an ninh mạng, các cơ quan thông tấn, báo chí.

[3] Bộ Công an đã tổ chức lấy ý kiến dự thảo Luật An ninh mạng của hơn 30 doanh nghiệp cung cấp dịch vụ viễn thông, internet, kinh doanh thiết bị số, cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia.

Trang thông tin điện tử của Bộ Công an, Bộ Tư pháp. Đồng thời, tổ chức làm việc với Bộ Tư pháp, Văn phòng Chính phủ, Bộ Thông tin và Truyền thông về nội dung chi tiết của dự án Luật An ninh mạng. Bộ Tư Pháp đã thẩm định theo đúng quy trình ban hành văn bản quy phạm pháp luật hiện hành. Chính phủ đã xem xét tại Phiên họp thường kỳ tháng 7/2017, Ủy ban Quốc phòng An ninh đã thẩm tra sơ bộ (ngày 01/9/2017), Ủy ban thường vụ Quốc hội đã cho ý kiến đồng ý trình Quốc hội dự án Luật An ninh mạng (ngày 14/9/2017).

IV. BỐ CỤC VÀ NỘI DUNG CƠ BẢN CỦA DỰ THẢO LUẬT

Dự thảo Luật an ninh mạng gồm 8 chương, 55 điều với nội dung cơ bản như sau:

1. Chương I: Những quy định chung, bao gồm 08 điều (từ Điều 1 đến Điều 8) quy định về phạm vi điều chỉnh, đối tượng áp dụng, giải thích từ ngữ, chính sách an ninh mạng, nguyên tắc, biện pháp bảo vệ an ninh mạng, hợp tác quốc tế về an ninh mạng, các hành vi bị nghiêm cấm.

Về phạm vi điều chỉnh: Luật này quy định về nguyên tắc, biện pháp, nội dung, hoạt động, điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng; trách nhiệm của cơ quan, tổ chức, cá nhân tham gia không gian mạng và có liên quan tới hoạt động bảo vệ an ninh mạng của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

Về đối tượng áp dụng: Luật này áp dụng đối với cơ quan, tổ chức, công dân Việt Nam, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan tới hoạt động trên không gian mạng và bảo vệ an ninh mạng của nước Cộng hòa xã hội chủ nghĩa Việt Nam.

2. Chương II: Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, gồm 03 mục, 13 điều (Điều 09 đến Điều 21) quy định về các hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, với các nội dung chính sau:

Mục 1: Bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm: hệ thống thông tin quan trọng về an ninh quốc gia; Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; Thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; Kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; Giám sát, cảnh báo, ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Mục 2: Tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm: xây dựng tiêu chuẩn, quy chuẩn kỹ thuật an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; chứng nhận, công bố hợp chuẩn, hợp quy về an ninh mạng đối với đối với hệ thống thông tin quan trọng về an ninh quốc gia; đánh giá hợp chuẩn, hợp quy về an ninh mạng đối với đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Mục 3: Phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, bao gồm: Phòng ngừa, ứng phó nguy cơ, sự cố an ninh mạng; Dự báo an ninh mạng; Diễn tập phòng, chống tấn công mạng và ứng cứu, khắc phục sự cố an ninh mạng; Ứng cứu, khắc phục sự cố an ninh mạng; Ngừng cung cấp thông tin mạng.

3. Chương III. Xử lý hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự an toàn xã hội, gồm 07 Điều (từ Điều 22 đến Điều 28), cụ thể: Xử lý thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; Phòng, chống gián điệp mạng, bảo vệ thông tin, tài liệu có nội dung thuộc danh mục bí mật nhà nước, thông tin cá nhân trên không gian mạng; Phòng, chống tấn công mạng; Phòng, chống khủng bố mạng; Phòng, chống chiến tranh mạng; Tình huống nguy hiểm về an ninh mạng; Các biện pháp áp dụng khi gia tăng nguy cơ xảy ra tình huống nguy hiểm về an ninh mạng.

4. Chương IV: Triển khai hoạt động bảo đảm an ninh mạng, gồm 03 mục, 09 điều (từ Điều 29 đến Điều 37), quy định về các hoạt động nhằm triển khai công tác an ninh mạng trên phạm vi cả nước, bao gồm:

Mục 1: Triển khai hoạt động bảo đảm an ninh mạng trong hệ thống cơ quan nhà nước: Nguyên tắc, điều kiện, nội dung triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước; Kiểm tra, đánh giá an ninh mạng đối với hệ thống thông tin thuộc cơ quan, tổ chức, doanh nghiệp nhà nước.

Mục 2: Triển khai hoạt động bảo đảm an ninh mạng trong một số lĩnh vực: Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế; Nghiên cứu, ứng dụng và phát triển quản lý định danh; Bảo đảm an ninh thông tin mạng.

Mục 3: Nghiên cứu, phát triển an ninh mạng: Nghiên cứu chiến lược phát triển và bảo vệ an ninh mạng; Nghiên cứu, 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.

5. Chương V: Phát triển nguồn nhân lực an ninh mạng, gồm 04 Điều (từ Điều 38 đến Điều 41) quy định: chính sách đào tạo, phát triển nguồn nhân lực an ninh mạng; đào tạo, phát triển nguồn nhân lực an ninh mạng; văn bằng, chứng chỉ về an ninh mạng; phổ biến kiến thức và nâng cao nhận thức về an ninh mạng.

6. Chương VI: Bảo đảm điều kiện triển khai công tác an ninh mạng, gồm 03 điều, từ Điều 42 đến Điều 44: Bảo đảm trang thiết bị, cơ sở vật chất phục vụ triển khai hoạt động bảo vệ an ninh mạng; kinh phí bảo đảm công tác an ninh mạng; bảo đảm nguồn nhân lực bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng.

7. Chương VII: Trách nhiệm của cơ quan, tổ chức, cá nhân, gồm 09 Điều (từ Điều 45 đến Điều 53) quy định: Trách nhiệm của tổ chức, cá nhân tham gia sử dụng không gian mạng; Trách nhiệm của chủ thể sản xuất, kinh doanh thiết bị số và cung cấp dịch vụ mạng, ứng dụng mạng; Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, internet; Trách nhiệm của cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia; Trách nhiệm của Bộ Công an; Trách nhiệm của Bộ Quốc phòng; Trách nhiệm của Bộ Thông tin và Truyền thông; Trách nhiệm của các bộ, ngành liên quan (*Bộ Khoa học và Công nghệ, Bộ Nội vụ, Bộ Giáo dục và Đào tạo, Bộ Lao động, Thương binh và Xã hội, Bộ Tài chính, Bộ Kế hoạch và Đầu tư, Bộ Ngoại giao, Bộ Công thương, Ban Cơ yếu Chính phủ*); trách nhiệm của ủy ban nhân dân cấp tỉnh.

8. Chương VII: Điều khoản thi hành gồm 02 điều (Điều 54, Điều 55), gồm: hiệu lực thi hành và quy định chi tiết.

Trên đây là những nội dung chính về dự án Luật An ninh mạng, Chính phủ xin trình Quốc hội xem xét, cho ý kiến./.

Nơi nhận:
- Như trên;
- Thủ tướng, các Phó Thủ tướng;
- Các Ủy ban của QH: QP-AN, PL, KH CN&MT;
- Các Bộ: Công an, Tư pháp;
- VPCP: BTCN, các PCN, các Vụ: NC, KGVX;
- Lưu: VT, PL (3) 105b

TM. CHÍNH PHỦ
TUQ. THỦ TƯỚNG
BỘ TRƯỞNG BỘ CÔNG AN

Thượng tướng Tô Lâm