**KHÁI NIỆM "CHỦ QUYỀN QUỐC GIA TRÊN**

**KHÔNG GIAN MẠNG" VÀ Ý THỨC HỆ CỦA DÂN TỘC**

Từ bao đời nay, chúng ta chỉ bảo vệ chủ quyền quốc gia bằng việc chống giặc ngoại xâm, diệt nội xâm. Nếu chủ quyền quốc gia trên đất liền bằng lục quân, trên biển bằng hải quân và trên không bằng không quân… Còn khi cả thế giới đã xây dựng một lực lượng chủ quyền quốc gia trên không gian mạng, thì với Việt Nam vẫn là một khái niệm mới.

Quan niệm mới về chủ quyền – chủ quyền quốc gia trên không gian mạng.
Chủ quyền quốc gia là thuộc tính chính trị- pháp lý không thể tách rời của quốc gia. Bao gồm hai nội dung, đó là: quyền tối cao của quốc gia trong phạm vi lãnh thổ của mình và quyền độc lập của quốc gia trong quan hệ quốc tế.

Cách đây 4 thế kỷ, Francis Bacon – nhà triết học – chính trị gia người Anh đã dự báo tri thức sẽ là quyền lực trong một cuộc chiến mới. Và thực tế cho thấy, hiện nay dân số thế giới đều đã có thể tiếp cận được loại quyền lực này.

Nếu lĩnh vực chủ quyền Quốc gia trên thế giới hiện nay được khẳng định dựa trên 4 yếu tố cơ bản, đó là: Lãnh thổ – nền tảng; dân số; tài nguyên và chính quyền. Và 4 quyền lợi cơ bản, đó là: Bình đẳng, độc lập, tự vệ và quản trị.

Thì chủ quyền không gian mạng của mỗi quốc gia cũng bao hàm 4 yếu tố cơ bản tương ứng, đó là:

Thứ nhất, các hệ thống thông tin (lãnh thổ);

Thứ hai, chủ thể các hoạt động trên mạng – góc độ ảo (dân số);

Thư ba, số liệu – đối tượng thao tác trên mạng – biểu đạt trạng thái tín hiệu theo ý đồ mà con người có thể lý giải được (tài nguyên);

Thứ tư, quy tắc xử lý và truyền số liệu (chính quyền).

Và chủ quyền không gian mạng của mỗi quốc gia cũng phát triển dựa theo 4 quyền lợi cơ bản, bao gồm:

Các nước có quyền bình đẳng tham dự quản lý mạng Internet quốc tế (bình đẳng);

Nước khác không được can dự vào vận hành hạ tầng cơ sở thông tin thuộc lãnh thổ nước khác (độc lập);

Nhà nước dùng quyền lực và năng lực quân sự của mình để bảo vệ không gian mạng của quốc gia không bị xâm phạm (tự vệ);

Truyền tải số liệu cùng các hoạt động xử lý nó thuộc quyền tư pháp và quản lý hành chính của quốc gia (quản trị).

Các lĩnh vực chủ quyền cũ, mà các quốc gia (trong đó có Việt Nam) khẳng định bao gồm: đất liền, hải đảo, vùng biển và vùng trời. Mới chỉ là không gian vật lý và được gọi là không gian thứ nhất.

Còn khái niệm mới về không gian đang được bàn tới đây, đó là không gian thứ hai – không gian mạng do con người tạo ra (hay còn gọi là không gian ảo).

Thực tế ở lịch sử nhân loại cho thấy, quyền lực chính trị sẽ giúp cho một số quốc gia trở thành “bá chủ”, có thể thâu tóm được các nước “thấp cổ bé họng”. Các hoạt động chính trị đó được thực hiện bằng vũ trang, để: Pháp thâu tóm Đông Dương; Đức muốn khu vực Alsace; Mỹ muốn can thiệp vào vấn đề Triều Tiên; …

Nhưng trên lĩnh vực không gian mạng, quyền lực chính trị không phải là riêng của một quốc gia, một chính phủ nào cả. Bất kỳ một cá nhân, tổ chức, đến những kẻ khủng bố… đều có thể làm ảnh hưởng trực tiếp tới nền chính trị này.

Sự phổ biến của thông tin mạng làm quyền lực chính trị phân tán rộng hơn, hệ ý thức phát triển hơn, nó phá vỡ biên giới, phá vỡ thế độc quyền của những cơ quan nhà nước truyền thống.

Bản đồ chính trị thế giới đã cho thấy, một thế lực mới đã xuất hiện. Đó là những hoạt động của những nhóm hacker nổi tiếng. Anonymous đã thực hiện các cuộc tấn công vào tổ chức Hồi giáo cực đoan IS; Mỹ cáo buộc Tổng thống Vladimir Putin, đứng sau các vụ tấn công mạng nhằm vào cuộc bầu cử tổng thống Mỹ…

Các cuộc tấn công an ninh mạng hiện nay đều nằm ngoài sự kiểm soát quân sự các quốc gia

Nếu xét theo các nội dung trên thì hiện nay, ý thức hệ của nhân dân cả nước trong lĩnh vực không gian mạng ở Việt Nam, vẫn chưa được xác định và hình thành được hệ thống pháp luật quy định cụ thể.

Để các nguyên tắc đó vẫn bị các thế lực bên ngoài lãnh thổ xâm phạm, can thiệp và gây nên những tổn thất cho quốc gia.

Bởi tại Điều 1 Hiến pháp năm 2013 mới chỉ quy định: “Nước Cộng hoà xã hội chủ nghĩa Việt Nam là một nước độc lập, có chủ quyền, thống nhất và toàn vẹn lãnh thổ, bao gồm đất liền, hải đảo, vùng biển và vùng trời”.

Điều này cho thấy chúng ta phải nhanh chóng cập nhật, bổ sung khái niệm "chủ quyền quốc gia trên không gian mạng" vào trong nội dung bộ luật gốc này.

Các nước đang làm gì để chuẩn bị cho cuộc chiến trang không gian mạng?
Tháng 6/2016, Tổng thư ký NATO – Jens Stoltenberg cũng phải thừa nhận coi không gian mạng là mặt trận tác chiến mới.

Đến nay, hơn 200 quốc gia trên thế giới đã sử dụng mạng Internet một cách phổ biến, thì có khoảng 60 nước đã nghiên cứu các phương tiện gián điệp, tấn công và theo dõi mạng của các quốc gia khác. Có khoảng 60 quốc gia đã mua sắm các phần miền hacker chuyên dụng và theo dõi mạng.

Có khoảng 30 nước đã thành lập đơn vị quân đội chuyên trách, trở thành một đơn vị phòng thủ quốc gia như: Bộ chỉ huy mạng (Cybercom) của Mỹ; đội dân quân mạng Cossack của Nga; C4I Branch) của Israel; Đức thành lập bộ chỉ huy Không quân mạng và không gian thông tin (KdoCIR); Trung QUốc thành lập Tổng cục 3 trực thuộc Bộ Tổng tham mưu quân đội…

Về vấn đề an ninh mạng, các quốc gia lớn cũng đã ban bố hệ thống pháp luật, tình trạng an ninh không gian mạng quốc gia. Để ngăn ngừa các cuộc tấn công, xâm phạm đến chủ quyền quốc gia trên phạm vi không gian mạng.

Năm 2011, Bộ Quốc phòng Mỹ đã tuyên bố các cuộc tấn công trên mạng vào quốc gia này như “một hành động chiến tranh” và sẽ đáp trả bằng hành động quân sự. Năm 2013 Mỹ ban hành “học thuyết chiến tranh không gian mạng” và năm 2015, Mỹ đã thông qua dự luật an ninh mạng.

Năm 2012, Nhật Bản cũng đã công nhận không gian mạng “là khu vực thuộc về an ninh quốc gia, như vùng đất, biển, vùng trời và không gian ngoài vũ trụ”.

Cuối năm 2016, Trung Quốc ban hành chiến lược an ninh không gian mạng. Với phương châm và 9 nhiệm vụ chiến lược an ninh mạng quan trọng.

Lần đầu tiên Luật Quốc phòng sử dụng khái niệm “Chủ quyền quốc gia trên không gian mạng”

Thực tế hiện nay cho thấy, Việt Nam là một quốc gia có gần 50 triệu người sử dụng Internet, chiếm tỉ lệ 53% dân số, và cao hơn mức trung bình thế giới là 46,64%. Tuy nhiên, vấn đề an ninh mạng, theo báo cáo của Liên minh Viễn thông Quốc tế (ITU) dựa trên bảng xếp hạng Chỉ số An ninh mạng Toàn cầu (GCI). Thì Việt Nam chỉ xếp thứ 101 trên tổng số 193 nước thành viên về khả năng đảm bảo an ninh mạng.

Công ty CrowdStrike của Mỹ cũng có bảng báo cáo cho thấy, Việt Nam được xếp hạng số 1 trên thế giới về tỷ lệ lây nhiễm phần mềm độc hại thông qua các thiết bị di động lưu trữ với 70,83% các máy tính bị nhiễm phần mềm độc hại từ không gian mạng.

Công ty này cũng báo cáo Việt Nam đã trở thành mục tiêu tấn công xâm nhập, thu thập thông tin tình báo hàng đầu của các nhóm tin tặc trên không gian mạng và có thể tiếp tục là một trong những mục tiêu tấn công chủ đạo của các nhóm tin tặc liên quan tới vấn đề Biển Đông.

Hệ thống an ninh mạng ở sân bay Việt Nam đã bị tấn công bởi những đứa trẻ vào năm 2016

Thực tế hiện nay ở Việt Nam, việc chống lại các đợt tấn công mạng chỉ như là hoạt động riêng rẽ của doanh nghiệp. Các cá nhân, doanh nghiệp, cơ quan nhà nước thực hiện việc bảo vệ hệ thống an ninh của mình chỉ giống như hoạt động “sập đâu vá đó”, chứ chưa có biện pháp bảo vệ trực tiếp.

Chưa bao giờ, khái niệm không gian mạng và tầm quan trọng của an ninh quốc gia về không gian mạng lại được đưa ra bàn luận nhiều đến thế. Vấn đề an ninh mạng trên không gian mạng đã được các cơ quan nhà nước đưa ra bàn luận, rất nhiều cuộc hội thảo đã lấy chủ đề bàn luận, rất nhiều vấn về an ninh mạng làm nóng tới 2 nhiệm kỳ gần đây của Quốc hội.

Dự thảo luật An ninh mạng và những đóng góp của đại biểu Quốc hội trong phiên thảo luận về Dự án Luật Quốc phòng (sửa đổi) sẽ hoàn thiện tới đây. Đã cho thấy những bước đi mạnh mẽ của Đảng, Nhà nước về phạm vi chủ quyền mới.

Sáng 10/11, Đại tướng Ngô Xuân Lịch – Bộ trưởng Quốc phòng, thừa ủy quyền của Thủ tướng, trình bày với Quốc hội dự án Luật Quốc phòng (sửa đổi). Và đây cũng là lần đầu tiên khái niệm “Chủ quyền quốc gia trên không gian mạng” được đưa vào dự án sửa đổi.

Trong mục 7 phần “giải thích từ ngữ”, có nêu: “Chủ quyền quốc gia trên không gian mạng là tất cả các quyền của Nhà nước đối với không gian mạng theo quy định của pháp luật Việt Nam, phù hợp với quy định của luật pháp quốc tế”.

Khoản g, điều 8 đã coi chủ quyền quốc gia không gian mạng là nhiệm vụ quốc phòng toàn dân. Vì vậy, khoản g, điều 9 cũng yêu cầu nhiệm vụ xây dựng hệ thống phòng thủ quân khu.

“Xây dựng và tổ chức thực hiện kế hoạch, phương án, biện pháp phòng, chống chiến tranh thông tin, chiến tranh không gian mạng và bảo vệ chủ quyền quốc gia trên không gian mạng”.

Khoản g, điều 8. Quốc phòng toàn dân

“Xây dựng kế hoạch, phương án và chỉ đạo, hướng dẫn đơn vị thuộc quyền, phối hợp với cơ quan, tổ chức, địa phương liên quan thực hiện các biện pháp phòng, chống chiến tranh thông tin, chiến tranh không gian mạng và bảo vệ chủ quyền quốc gia trên không gian mạng theo nhiệm vụ được giao”.

Khoản g, điều 9. Phòng thủ quân khu

Sự ra đời của Luật An toàn thông tin mạng, hoàn thiện của Luật Quốc phòng và sắp tới là thông qua dự án luật An ninh mạng vào tháng 5/2018. Cho thấy tầm quan trọng và bước đi mạnh mẽ của Đảng và Nhà nước Việt Nam nhằm kiểm soát tình hình an ninh, lãnh thổ quốc gia ở lĩnh vực này.

Khoản 4, Điều 34 của luật An ninh mạng quy định: “Các doanh nghiệp nước ngoài khi cung cấp dịch vụ viễn thông, Internet tại Việt Nam phải tuân thủ pháp luật, tôn trọng chủ quyền, lợi ích, an ninh quốc gia Việt Nam, có giấy phép hoạt động, đặt cơ quan đại diện, máy chủ quản lý dữ liệu người sử dụng Việt Nam trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam…”.

Điều này đã gây phản ứng trái chiều trên dư luận, nhưng đây không chỉ là vấn đề trên lĩnh vực kinh tế, của số tiền 350 triệu USD, ở thị trường quảng cáo trực tuyến mà Facebook và Youtobe đã sở hữu ở Việt Nam. Mà còn góp phần giúp cơ quan chuyên trách của Việt Nam là Cục an ninh mạng ( Bộ công an), Vụ Công nghệ thông tin (Bộ Thông tin – Truyền thông)… kiểm soát được các cuộc tấn công an ninh mạng từ bên ngoài, các tình trạng phát tán thông tin xuyên tạc, bôi nhọ cá nhân…

Nếu đảm bảo được một nền an ninh ổn định, thì việc yêu cầu đặt máy chủ là cần thiết

Nếu cuộc chiến an ninh mạng bùng nổ, tạo ra thế chiến thứ 3, thì nó sẽ phức tạp hơn các thế chiến trước đó. Sẽ không chỉ có một trận Trân Châu cảng ác liệt nữa, mà thay vào đó hàng loạt các trận “Trân Châu Cảng điện tử” (electronic Pearl Harbor), sẽ diễn ra và quy mô thiệt hại thì gấp nhiều mức nào khó có thể dự báo trước được.

Mối nguy hại càng lớn, khẳng định tầm quan trọng của hệ thống phòng thủ càng cao. Minh chứng lịch sử, về bài học phòng thủ của An Dương Vương với thành Cổ Loa là bài học lớn cho dân tộc ta muôn đời nay. Nếu không chuẩn bị cho một cuộc chiến không gian an ninh mạng, thì sẽ ứng với câu nói: “Không chuẩn bị là chuẩn bị cho tất cả”.

Bảo vệ công dân của mình được an toàn trong quốc gia lãnh thổ của mình, là cách mà Chính phủ mỗi nước đang cố gắng thực hiện. Vì vậy bằng mọi biện pháp Việt Nam không thể đứng ngoài cuộc chiến “không tiếng súng, nhưng càng nhiều máu và nước mắt” này.

Nguồn: Độc lập dân tộc gắn liền với Chủ nghĩa xã hội.

Trích trang Cờ đỏ thành phố Hồ Chí Minh (codotphcm.com)

Duyệt đăng trên các Website của Quận

**TRƯỞNG BAN**

**Đặng Tấn Tuyên**