NHỮNG KHÍA CẠNH PHÁP LÝ VỀ CẤM SỬ DỤNG VŨ LỰC, ĐE DỌA SỬ DỤNG VŨ LỰC VÀ QUYỀN TỰ VỆ CỦA QUỐC GIA TRÊN KHÔNG GIAN MẠNG TRONG LUẬT QUỐC TẾ

ĐỖ THỊ HÀ*

Cuộc cách mạng công nghiệp lần thứ tư mang lại những cơ hội chưa từng có trong lịch sử nhân loại, đồng thời cũng mang đến những thách thức không nhỏ trong việc giữ gìn hòa bình, an ninh, chủ quyền quốc gia. Để phòng, tránh, và đối phó với các nguy cơ mất an ninh, đặc biệt là tấn công mạng, pháp luật quốc gia cũng như pháp luật quốc tế cần thống nhất cách tiếp cận các khía cạnh pháp lý về vũ lực và sử dụng vũ lực trên không gian mạng, áp dụng quyền tự vệ quốc gia nhằm bảo vệ có hiệu quả chủ quyền quốc gia trên không gian mạng. Bài viết nghiên cứu các khía cạnh pháp lý về việc cấm dùng vũ lực, đe dọa sử dụng vũ lực và quyền từ vệ của quốc gia trên không gian mạng cũng như đề cập đến những khó khăn thách thức khi xác định những yếu tố này.

Từ khóa: Không gian mạng, tấn công mạng, sử dụng vũ lực, quyền tự vệ quốc gia, an ninh mạng, luật quốc tế.

The 4th industrial revolution brings both unprecedented opportunities and significant challenges in peacekeeping, security and national sovereignty. In order to prevent and deal with insecurity risks, especially cyber attacks, national laws and international law need to agree on an approach to the legal aspects of force and the use of force in cyberspace, to apply national self-defense to effectively protect national sovereignty on cyberspace. The paper studies the legal aspects of the prohibition of force, threats to use force and national self-defense on cyberspace as well as the difficulties and challenges in identifying these factors.

Keywords: Cyberspace, cyber-attacks, use of force, national self-defense, cyber security, international law.

Không gian mạng vốn được cho là "*không có giới hạn không gian và thời gian*"[1], tuy nhiên môi trường này không phải là nơi *"không có luật lệ"* để bất kỳ ai cũng có thể tiến hành các hoạt động thù địch mà không bị kiểm soát. Trong khi mọi quốc gia đang nỗ lực để kiểm soát tình hình an ninh trật tự xã hội trong thế giới thực thì không gian mạng lại mở ra một thế giới ảo rất khác, làm dấy lên hàng loạt các vấn đề liên quan đến hoạt động tấn công mạng, kích động biểu tình, nổi dậy, tiếp tay cho hoạt động tuyên truyền xuyên tạc sự thật lịch sử, gây bất ổn hoặc căng thẳng trong quan hệ quốc tế. Đảm bảo an toàn, an ninh trên không gian mạng không còn là vấn đề mang tính quốc gia mà mang tính quốc tế toàn cầu bởi tính "không giới hạn" của không gian mạng. Để giải quyết thực tế đó, nhiều quốc gia có thể trông đợi vào việc kí kết, tham gia vào các điều ước quốc tế điều

[1] Khoản 3 Điều 2 Luật An ninh mạng năm 2018: "*Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.*"

** Thạc sĩ, Giảng viên Luật quốc tế, Học viện An ninh nhân dân.*

chỉnh lĩnh vực không gian mạng trên cơ sở các nguyên tắc cơ bản của luật quốc tế, phù hợp với thực tiễn tập quán quốc tế nhằm duy trì hòa bình, bảo đảm an ninh cho các thế hệ tương lai.[2]

1. Cấm dùng vũ lực, đe dọa sử dụng vũ lực và quyền tự vệ quốc gia trên không gian mạng

1.1. Các hành vi sử dụng vũ lực, đe dọa sử dụng vũ lực trên không gian mạng

Cấm dùng vũ lực, đe dọa sử dụng vũ lực trong luật quốc tế hiện đại là một trong những nguyên tắc giữ vị trí trung tâm trong hệ thống nguyên tắc cơ bản của luật quốc tế có tính Jus Cogens. Việc nhận diện các hành vi dùng vũ lực và đe dọa sử dụng vũ lực trong quan hệ quốc tế không phải bao giờ cũng dễ dàng xuất phát từ nhiều nguyên nhân khác nhau. Trên không gian mạng, việc xác định được đâu là hành vi dung vũ lực, đâu là hành vi đe dọa sử dụng vũ lực càng trở nên khó khăn hơn. Hành vi "*tấn công vũ lực*" hay "*đe dọa dùng vũ lực*" trên không gian mạng được xác định không chỉ bởi các hành vi mà bằng cách đánh giá *chuỗi các hậu quả* gây ra bởi các hành vi cụ thể trên không gian mạng[3]. Biểu hiện của chuỗi các hậu quả này rất đa dạng. Đó có thể là những tổn hại về người, tài sản, cơ sở vật chất trên thực tế nhưng có nguồn gốc từ hành vi tác động của chủ thể trên không gian mạng, nghĩa là hậu quả từ hành vi "ảo" nhưng có tác động "thật" giống như các hành vi sử dụng vũ lực thông thường. Ví dụ, hành vi diễn ra trên không gian mạng lại gây ra các hậu quả làm kích động bạo lực, gây thương vong, phá hủy cơ sở vật chất, hạ tầng, phương tiện, vv… đều được xem như là sử dụng vũ lực.

Trong việc xem xét hành vi có sử dụng vũ lực hay không, phải đánh giá các yếu tố tác động bao gồm bối cảnh sự kiện, nhân tố gây ra hoạt động thù địch (để nhận diện những vấn đề khó khăn trong việc quy kết cho hoạt động trên không gian mạng), mục tiêu, địa điểm, ý định và hệ quả, những vấn đề khác có khả năng xảy ra. Các hoạt động thường được dẫn chiếu làm ví dụ điển hình cho việc quy kết hành vi sử dụng vũ lực trên không gian mạng là: (1) tổ chức kích động chương trình vũ khí hạt nhân; (2) tổ chức kích động phá hủy các con đập (hồ chứa nước), mạng lưới điện, gây nguy hại cho khu vực dân cư trong phạm vi lưu vực ảnh hưởng, hoặc hành vi tổ chức các hoạt động vô hiệu hóa hoạt động kiểm soát không lưu dẫn đến làm rơi máy bay và các hậu quả nặng nề khác. Những hành vi sử dụng vũ lực trong thực tế như bắn phá các mục tiêu, thả bom, tấn công bạo lực,… trong thực tế gây ra hậu quả vật chất như thế nào thì hành vi bạo lực trên không gian mạng cũng có thể dẫn đến hậu quả nguy hại như vậy. Hành vi tấn công trên không gian mạng còn nhắm đến các trung tâm điều khiển một cách có hệ thống hơn cả hành vi bạo lực đơn thuần diễn ra ngoài xã hội, dẫn đến hậu quả khôn lường và khó khắc phục. Thực tiễn cho thấy, trong nhiều trường hợp, các hoạt động trên không gian mạng đã cấu thành hành vi đe dọa sử dụng hoặc sử dụng vũ lực theo quy định của Điều 2(4) Hiến chương Liên hợp quốc năm 1945.

Năm 2010, sâu máy tính Stuxnet là một loại mã độc lây lan qua phần cứng

[2] Lời mở đầu, Hiến chương Liên hợp quốc năm 1945.

[3] Hongju Koh, Harold, "International Law in Cyberspace" (2012). Faculty Scholarship Series. 4854. https://digitalcommons.law.yale.edu/fss_papers/4854

của hệ thống máy tính điều hành, tấn công vào ít nhất 14 cơ sở công nghiệp của Iran, trong đó có cả một nhà máy làm giàu uranium, gây ra hậu quả thiệt hại nghiêm trọng làm cho công tác khắc phục kéo dài hàng năm sau đó.[4] Quá trình điều tra, truy tìm hành vi phát hiện mã độc Stuxnet liên hệ với hai máy chủ ở Malaysia và Đan Mạch. Năm 2011, hãng phim ảnh Sony Pictures của Nhật Bản đối mặt với vụ tấn công mạng gây hậu quả thiệt hại chưa từng có trong lịch sử kinh doanh gây ra bởi nhóm hacker #GOP được cho là từ Bắc Triều Tiên[5]. Năm 2014, Hàn Quốc phát hiện khoảng 100 triệu tài khoản ngân hàng đã bị đánh cắp thông tin trong vài năm trước đó, 20 triệu tài khoản khách hàng bị "hack", hậu quả gây xáo trộn tình hình kinh doanh của hệ thống ngân hàng, hơn hai triệu chủ thẻ đã chấm dứt hoạt động hoặc thay thế tài khoản tín dụng.[6] Năm 2017, công ty Equifax – một trong những trung tâm thông tin tín dụng lớn nhất nước Mỹ để lộ thông tin cá nhân của 147,9 triệu người do lỗ hổng bảo mật. Ở Việt Nam, các công ty truyền thông và công nghệ lớn như VCCorp, Bkav, VNG đều đã bị tấn công mạng, gây ảnh hưởng hàng chục tỷ đồng. Vụ việc nghiêm trọng nhất tính đến nay xảy ra vào năm 2015 khi hệ thống thông báo sân bay bị hacker nước ngoài chiếm đoạt, một số màn hình hiển thị thông tin chuyến bay của các Sân bay quốc tế bị chèn những nội dung xuyên tạc về Việt Nam, dữ liệu của 411.000 thành viên là các lãnh đạo, quản lý cơ quan Nhà nước, ngân hàng, doanh nghiệp lớn bị đánh cắp.[7] Theo thống kê của Cục An toàn thông tin (Bộ Thông tin và Truyền thông), Việt Nam ghi nhận hơn 1000 cuộc tấn công mạng trong khoảng 4 tháng đầu năm 2020 vào hệ thống thông tin[8].

Hàng loạt các cuộc tấn công mạng lớn, nhỏ trên thế giới hiện nay làm dấy lên mối lo ngại rất lớn là các mã độc/sâu máy tính giờ đây có thể được sử dụng để phá hoại nền an ninh, trật tự quản lý nhà nước, hoạt động kinh doanh sản xuất chứ không chỉ dùng cho mục đích thăm dò hay đánh cắp thông tin như trước đây.

1.2. Quyền tự vệ quốc gia (national self-defense) trên không gian mạng trong Luật quốc tế

Quyền tự vệ của quốc gia được ghi nhận tại Điều 51 Hiến chương Liên hợp quốc. Quyền này được quốc gia áp dụng khi có đủ điều kiện về về việc tồn tại các hoạt động tấn công mạng máy tính đạt đến mức cấu thành hành vi tấn công hoặc đe dọa tấn công mạng. Ví dụ, năm 2011, Hoa Kỳ đã ban bố Chiến lược Quốc tế về Không gian mạng năm và khẳng định vấn đề tự vệ theo quy chế Điều 51: "*Khi được cho phép, Hoa Kỳ sẽ phản ứng lại hành động tấn công thù địch trên không gian mạng giống như bất*

[4] Xem Câu chuyện về mã độc Stuxnet – vũ khí nguy hiểm trong thế giới mạng - <https://securitydaily.net/cau-chuyen-xung-quanh-stuxnet-vu-khi-nguy-hiem-trong-the-gioi-mang/> truy nhập ngày 13 tháng 11 năm 2020.

[5] Xem "Toàn cảnh vụ tấn công Sony Pictures"

6 Xem "Nửa số dân Hàn Quốc bị trộm thông tin thẻ tín dụng" <https://infonet.vietnamnet.vn/the-gioi/nua-so-dan-han-quoc-bi-trom-thong-tin-the-tin-dung-122927.html> truy nhập ngày 13 tháng 11 năm 2020.

[7] Xem "Thông cáo báo chí về vụ hacker tấn công vào hệ thống Vietnam Airlines" < https://vnisa.org.vn/thong-cao-bao-chi-ve-vu-hacker-tan-cong-vao-he-thong-vietnam-airlines/> truy nhập ngày 13 tháng 11 năm 2020.

[8] Xem "http://tapchitaichinh.vn/tai-chinh-phap-luat/viet-nam-ghi-nhan-hon-1000-cuoc-tan-cong-mang-trong-4-thang-dau-nam-322683.html"

trước bất kỳ đe dọa nào khác đối với quốc gia".

Trong đó, hành vi tự vệ quốc gia tại Điều 51 Hiến chương Liên hợp quốc có liên hệ chặt chẽ đến nguyên tắc *jus in bello* – công lý trong chiến tranh, yêu cầu các quốc gia phải tuân thủ nghiêm ngặt trong hoạt động sử dụng vũ lực để tự vệ. *Jus in bello* được giải thích là một trong hai nhóm quy tắc trong Luật chiến tranh, do học giả kiệt xuất người Hà Lan *Hugo Grotius* (1583-1645) khởi xướng. Ông là một trong những người quan trọng đóng góp nền móng lý luận xây dựng học thuyết phát triển Luật quốc tế trên thế giới. Để ngăn cản các cuộc chiến tranh phi nghĩa trong thời kỳ trung đại, ông dựa trên lý thuyết và thực tiễn lịch sử cổ đại và trung đại để xây dựng nên hai nhóm quy tắc: *jus ad bellum* (quyền gây chiến tranh) và *jus in bello* (công lý trong chiến tranh). Quy tắc *jus ad bellum* đặt ra những chuẩn mực mà theo đó, một nhà lãnh đạo chính trị có thể quyết định một cuộc chiến tranh có chính nghĩa hay không. Quy tắc *jus in bello* miêu tả những hành động quân sự nào được phép từ phương diện niềm tin chính nghĩa và hợp pháp từ phương diện pháp lý quốc tế khi xảy ra các cuộc chiến tranh, đặc biệt là các cuộc chiến phản công tự vệ.

Như vậy, đối chiếu với quy định Luật quốc tế hiện đại ngày nay, học thuyết các về nguyên tắc *jus in bello* còn nguyên giá trị trong vấn đề định đoạt những trường hợp ngoại lệ nào được sử dụng vũ lực trong quan hệ quốc tế. Trong bối cảnh của một cuộc xung đột vũ trang, pháp luật quốc tế được áp dụng để điều chỉnh phạm vi sử dụng vũ lực (trong một số hệ thống luật khác còn gọi là luật chiến tranh – *the law of war/armed conflict*) trên không gian mạng khi gây ra các hoạt động thù địch, giống như các phương thức phổ biến khác. Trong bất kỳ hoàn cảnh xung đột nào, pháp luật quốc tế cho phép nguyên tắc giới hạn hợp pháp về tính cần thiết và hợp lý trong sử dụng vũ lực để tự vệ. Thực tế, luật quốc tế không có quy định pháp lý nào yêu cầu hành vi phản ứng lại tấn công mạng cũng phải tương ứng là một hành vi trên không gian mạng, chỉ cần thực hiện đúng nguyên tắc cần thiết và hợp lý trong tự vệ (*necessity and proportionality*).

Nguyên tắc *jus in bello* về phân biệt mục tiêu áp dụng cả trong cuộc xung đột vũ trang dùng đến phương thức tấn công mạng máy tính. Với bất kỳ hình thức xung đột vũ trang nào thì nguyên tắc phân biệt mục tiêu đòi hỏi hành vi tấn công đó chỉ nhằm vào mục tiêu quân sự, và truy cứu trách nhiệm đối với những khu vực phục vụ cho quân sự hoặc khu vực nếu bị phá hủy sẽ có lợi cho mục đích quân sự bao gồm cả mục tiêu dân sự. Về nguyên tắc, pháp luật quốc tế bảo vệ hoàn toàn các khu vực dân sinh khỏi mọi hoạt động tấn công vũ lực. Nguyên tắc *jus in bello* về tính hợp lý của hành vi tấn công chống trả áp dụng trên không gian mạng máy tính trong mọi trường hợp tấn công chống trả để tự vệ. Nguyên tắc này cấm hành vi tấn công đe dọa gây ra thiệt hại ngẫu nhiên ảnh hưởng đến đời sống dân cư, thương vong hoặc phá hủy các mục tiêu dân sự mà sự thiệt hại đó có liên quan đến khả năng mang lại lợi ích cho hoạt động tấn công quân sự, ví dụ tấn công vào khu vực dân cư sản xuất lương thực, phương tiện hậu cần phục vụ quân đội,… Các bên tham chiến được yêu cầu phải đánh giá kỹ lưỡng nguy cơ ảnh hưởng hoặc gây thiệt hại đến các mục tiêu dân sự[9].

[9] Trên không gian mạng, trước khi tiến hành tấn

1.3. Trách nhiệm pháp lý quốc tế của quốc gia đối với hành vi tấn công mạng thực hiện thông qua máy chủ ủy nhiệm (proxy server)

Các quốc gia phải chịu trách nhiệm pháp lý cho mọi hoạt động diễn ra thông qua các máy chủ ủy nhiệm (proxy actors), chịu trách nhiệm do những cá nhân, tổ chức hành động dưới sự điều khiển của quốc gia đó. Không gian mạng tạo ra khả năng ngụy tạo tài khoản giả, địa điểm ảo gây khó khăn cho việc phát hiện, nhận dạng, đánh giá các nguy cơ tấn công mạng. Tuy nhiên, trong phạm vi điều chỉnh của mình, pháp luật quốc tế cho phép cơ chế truy cứu trách nhiệm pháp lý quốc tế khi tồn tại các tổ chức tư nhân (*private actors*) của quốc gia gây ảnh hưởng đến hòa bình và an ninh thế giới. Quy định về trách nhiệm pháp lý quốc tế của quốc gia về hành vi sai phạm của các yếu tố tư nhân hoạt động dưới sự chỉ đạo, hỗ trợ, khống chế của quốc gia. Nếu hành vi sai trái gây ra trên không gian mạng được chứng minh là có liên quan đến sự chỉ đạo, khống chế của một quốc gia thì quốc gia đó sẽ phải chịu trách nhiệm pháp lý quốc tế giống với trách nhiệm cho hành vi gây ra bởi các cơ quan, tổ chức của Nhà nước được quy định trong Điều 8, *Các điều khoản về trách nhiệm quốc tế của quốc gia cho hành vi sai phạm quốc tế* - Phụ lục của Nghị quyết Hội đồng Liên hợp quốc số 56/83 ngày 12/12/2001, và trong án lệ *Bosnia and Herzegovina v. Serbia and Montenegro* (Merits) 2007 của Tòa công lý quốc tế số I.C.J. 43, 207–08 (Feb. 26, 2007) về áp dụng Công ước ngăn ngừa và trừng phạt tội phạm diệt chủng của Liên hợp quốc. Theo đó, các quy định pháp luật quốc tế này nhằm mục đích điều chỉnh hành vi che giấu sai phạm quốc tế thực hiện bởi các tổ chức tư nhân (thuộc quốc gia) gây ra hậu quả thiệt hại đến cộng đồng quốc tế.

2. Những khó khăn, thách thức trong việc áp dụng nguyên tắc cấm sử dụng hoặc đe dọa sử dụng vũ lực trên không gian mạng trong Luật quốc tế

2.1. Khó khăn trong nhận diện hành vi dùng vũ lực (use of force) trên không gian mạng

Hành vi sử dụng vũ lực trong quan hệ quốc tế cần được mở rộng nội hàm với các dấu hiệu mới. Trên không gian mạng, hành vi có thể là một cú nhấp chuột hoặc bấm nút. Hành vi ảo trên mạng hoàn toàn có thể gây ra hậu quả thiệt hại vật chất nghiêm trọng giống như hành vi cơ học thông thường, ví dụ như phương thức tấn công truyền thống bằng bom phá hủy được cả mạng lưới hoặc một công trình trọng điểm quốc gia, gây hậu quả nghiêm trọng thì việc thêm mã độc vào phần mềm vận hành từ một máy tính từ xa cũng gây ra hậu quả nguy hại tương tự. Trong thực tế, có nhiều dạng hành vi trong không gian mạng không xác định được yếu tố "cơ học" để tác động lên mục tiêu ví dụ như việc lây lan mã độc, virus, cài cắm phần mềm phá hoại hệ thống mạng, tấn công chương trình điều khiển hệ thống không lưu của sân bay quốc tế,… Điều này làm dấy lên

công (chống trả hoặc tự vệ), các bên thường đánh giá các yếu tố:

i) hậu quả ảnh hưởng của công cụ vũ khí trên không gian mạng đến các mục tiêu quân sự và hệ thống cơ sở hạ tầng dân sinh, gồm cả hạ tầng dùng chung ví dụ như đập thủy điện hoặc mạng lưới năng lượng,…;

ii) khả năng gây ra hậu quả thiệt hại vật chất mà cuộc tấn công mạng đem lại, số lượng thương vong ước tính;

iii) thiệt hại riêng đối với mục tiêu là các hệ thống mạng máy tính dân sự, không có tầm quan trọng phục vụ quân sự, quốc phòng nhưng lại có kết nối với mục tiêu quân sự.

câu hỏi về phạm vi nhận thức thuật ngữ "*vũ lực*" trong giai đoạn mới.

Rõ ràng, vũ lực phải được hiểu theo nghĩa rộng và thống nhất một thuật ngữ pháp lý được chấp thuận rộng rãi giữa các quốc gia. Bất kỳ hành vi gây hấn mang tính thù địch, ảnh hưởng đến quan hệ thân thiện giữa các quốc gia và trong mọi lĩnh vực của đời sống quốc tế, kể cả trên không gian mạng, gây ra hậu quả nghiêm trọng hoặc đe dọa gây ra hậu quả đều sẽ được hiểu là hoạt động sử dụng vũ lực – *use of force*. Trong trường hợp hành vi tấn công mạng cấu thành hành vi sử dụng vũ lực thì quốc gia chịu thiệt hại có thể dẫn chiếu để áp dụng mà không nhất thiết phải xây dựng một khung pháp lý mới điều chỉnh vấn đề sử dụng vũ lực trên không gian mạng. Muốn thực hiện được điều này, công tác tuyên truyền phổ biến kiến thức về nguyên tắc cấm sử dụng vũ lực, nhận thức về hành vi sử dụng vũ lực trên không gian mạng, trách nhiệm pháp lý quốc tế của quốc gia trong việc quản lý các cơ sở, tổ chức hoạt động trên không gian mạng nhằm tránh gây ra các hoạt động thù địch dẫn đến hậu quả nghiêm trọng ảnh hưởng đến quan hệ quốc tế phải được thực hiện có hiệu quả hơn là tình trạng buông lỏng như hiện nay. Việc sử dụng truyền thông trong nước và quốc tế để tuyên truyền xây dựng nhận thức chung về vấn để bảo đảm an n inh trên không gian mạng có thể tạo ra những tập quán quốc tế mới giữa các quốc gia, được chấp thuận, thực hành và nhân rộng thường xuyên giữa các nước sẽ trở thành công cụ chống lại hành vi vũ lực trên không gian mạng có hiệu quả.

2.2. Khó khăn trong xác định trách nhiệm pháp lý quốc tế trên không gian mạng

Không gian mạng là nơi cho phép tạo ra công cụ để hợp lý hóa các nguồn phát sinh hành vi của các chủ thể thực hiện, che giấu, làm giả, thậm chí làm cho lực lượng điều tra mạng không thể truy xuất được chính xác nguồn tấn công đến từ đâu, thông qua hệ thống máy chủ ủy nhiệm proxies. Mặc dù luật quốc tế có các công cụ pháp lý để quy kết hành vi vi phạm pháp luật quốc tế đã gây ra hậu quả sai trái, chứng minh sự tồn tại của hành vi đó thông qua hậu quả vi phạm gây ra trên thực tế, tuy nhiên, vấn đề đặt ra trong tình huống này không phải là quy định pháp luật về bản chất mà là *quy trình kỹ thuật* để quy kết được cho chủ thể hành vi thực hiện qua không gian mạng, nơi mà các quy định pháp lý chưa đầy đủ, chưa theo kịp sự phát triển của công nghệ. Ví dụ như vấn đề chủ quyền quốc gia trên không gian mạng thực sự tồn tại theo quy định của luật quốc tế, được các quốc gia thừa nhận. Tuy nhiên, phạm vi chủ quyền đó đến đâu vẫn là câu hỏi bỏ ngỏ, vấn đề áp dụng biện pháp cưỡng chế của pháp luật quốc tế, vấn đề trách nhiệm của quốc gia liên quan đến các nhóm theo chủ nghĩa tin tặc (*hacktivists*) trên lãnh thổ quốc gia mình, vv… Đây chính là các câu hỏi chưa có lời giải thỏa đáng mà không chỉ riêng các nước phát triển hơn về công nghệ như Hoa Kỳ, Nhật Bản, Trung Quốc đang nghiên cứu mà các quốc gia đang phát triển như Việt Nam, Ấn Độ,… cũng cần phải khởi động các cuộc thảo luận, dự kiến chương trình bồi dưỡng, đào tạo chuyên viên pháp lý quốc tế, cán bộ chuyên trách về tổ chức, thi hành, các nhà hoạch định chính sách liên quan đến vấn đề hoạt động trên không gian mạng. Đối với chiến lược quốc gia, muốn tạo ra được môi trường hòa bình ổn định trên không gian mạng, quốc gia đó phải có sẵn các chính sách và phương án tiếp cận, đối phó với các hình thức xung đột sẽ xảy ra - điều được dự báo là khó tránh khỏi trong giai đoạn mới.

2.3. Khó khăn từ yếu tố lưỡng dụng (dual-use infrastructure) của cơ sở hạ tầng trên không gian mạng

Ngày nay, cơ sở hạ tầng về công nghệ thông tin và truyền thông thường được sử dụng kết hợp giữa mục đích quân sự - quốc phòng và dân sự. Trong quy định của pháp luật quốc tế, các hạ tầng dân sự phải được phân biệt rõ để không trở thành mục tiêu tấn công trong các cuộc chiến tranh, kể cả các cuộc chiến tranh thông tin trên không gian mạng. Nguyên tắc chiến tranh chính nghĩa – *jus in bello* phân biệt các mục tiêu quân sự và dân sự sẽ được áp dụng như thế nào trong các cuộc chiến tranh mạng? Các quốc gia phải đánh giá được một cách tỉ mỉ về các nguy cơ ảnh hưởng của các vụ tấn công mạng lên hệ thống máy tính phục vụ quản lý dân sinh, không phải mục tiêu quân sự nhưng lại có sự liên kết đến yếu tố quân sự, ví dụ hệ thống mạng thông tin truyền thông phục vụ dân sự nhưng lại được cung cấp bởi công ty của Bộ quốc phòng, các sân bay, cảng hàng không dân dụng được vận hành bởi hệ thống mạng máy tính của quân đội, vv… Các quốc gia cũng cần đánh giá mức độ và tính hợp lý của nguyên tắc *jus in bello* ảnh hưởng đến cơ sở hạ tầng dùng chung cho cả dân sự và quân sự trong mỗi tình huống viễn cảnh tấn công mạng xảy ra.

Tóm lại, các khía cạnh pháp lý về sử dụng vũ lực, đe dọa sử dụng vũ lực và quyền tự vệ của quốc gia trên không gian mạng trong luật quốc tế vẫn còn là vấn đề mới mẻ đối với nhiều quốc gia, trong đó có Việt Nam. Nghiên cứu vấn đề này cho thấy những rào cản, khó khăn trong việc nhận diện hành vi, xác định trách nhiệm trong việc sử dụng vũ lực, đe dọa sử dụng vũ lực và quyền tự vệ của quốc gia trên không gian mạng. Cần khẳng định rằng những nội dung này sẽ luôn biến đổi cùng với sự thay đổi nhanh chóng của nền tảng công nghệ trong thời đại cách mạng 4.0. Do đó, càng làm rõ được nội hàm của việc sử dụng vũ lực, đe dọa sử dụng vũ lực cũng như xác định rõ giới hạn quyền tự vệ trên không gian mạng là cơ sở pháp lý quan trọng để các nước có thể bảo vệ tốt hơn chủ quyền quốc gia./.

TÀI LIỆU THAM KHẢO

1. LegalMatch, What is Cyberspace Law? <https://www.legalmatch.com/law-library/article/cyberspace-law.html> truy cập ngày 12 tháng 11 năm 2020.

2. Nghị quyết số A/70/455 của Đại hội đồng Liên hợp quốc ngày 30/12/2015. Truy cập tại: <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf> truy cập ngày 12 tháng 11 năm 2020.

3. Quy chế Tòa án Công lý quốc tế 1945.

4. Hiến chương Liên hợp quốc 1945.

5. Quốc hội, Luật quốc phòng năm 2018.

6. Quốc hội, Luật An ninh mạng năm 2018.

7. Câu chuyện về mã độc Stuxnet – vũ khí nguy hiểm trong thế giới mạng - <https://securitydaily.net/cau-chuyen-xung-quanh-stuxnet-vu-khi-nguy-hiem-trong-the-gioi-mang/> truy nhập ngày 13 tháng 11 năm 2020.

8. "Nửa số dân Hàn Quốc bị trộm thông tin thẻ tín dụng" <https://infonet.vietnamnet.vn/the-gioi/nua-so-dan-han-quoc-bi-trom-thong-tin-the-tin-dung-122927.html> truy nhập ngày 13 tháng 11 năm 2020.

9. "Thông cáo báo chí về vụ hacker tấn công vào hệ thống Vietnam Airlines" <https://vnisa.org.vn/thong-cao-bao-chi-ve-vu-hacker-tan-cong-vao-he-thong-vietnam-airlines/> truy nhập ngày 13 tháng 11 năm 2020.

10. Hongju Koh, Harold, "International Law in Cyberspace" (2012). Faculty Scholarship Series. 4854. <https://digitalcommons.law.yale.edu/fss_papers/4854>