ĐẤU TRANH PHÒNG, CHỐNG TỘI PHẠM MẠNG: THỰC TIỄN Ở NGA VÀ TRIỂN VỌNG CỦA SỰ HỢP TÁC QUỐC TẾ[1]

PLOKHOV SERGEY VLADIMIROVICH*

Ngày nay, chung tay đối phó với các thách thức toàn cầu và các mối đe dọa đối với an ninh thế giới là nhiệm vụ vô cùng quan trọng của tất cả các quốc gia. Một trong những mối đe dọa nguy hiểm nhất chính là tội phạm mạng và công nghệ cao. Do ảnh hưởng của đại dịch Covid-19 những năm gần đây, tội phạm này đã mở rộng quy mô lên cấp độ mới với quá trình số hóa rộng rãi, tài sản ảo trở nên phổ biến hơn và sự di chuyển ẩn danh xuyên biên giới của chúng. Giới tội phạm sử dụng Darknet[2] rộng rãi với mục đích buôn bán bất hợp pháp thông tin và các mặt hàng bị cấm. Internet bị lợi dụng để thực hiện các hành vi khủng bố và cực đoan, tác động tiêu cực đến thế hệ trẻ, lôi kéo và kích động thanh thiếu niên thực hiện hành vi phạm tội. Liên bang Nga cũng không đứng ngoài sự ảnh hưởng tiêu cực của việc gia tăng bùng nổ các loại tội phạm mạng và công nghệ thông tin. Bài viết thông tin về những thách thức trong đấu tranh phòng, chống tội phạm mạng và công nghệ thông tin ở Liên bang Nga; thực tiễn hoạt động về thực thi, hoàn thiện pháp luật, xây dựng thể chế và hợp tác quốc tế của Nhóm công tác liên ngành của Tổng Viện kiểm sát Liên bang Nga trong bối cảnh gia tăng về số lượng, tính chất, quy mô của tội phạm tội phạm mạng và công nghệ thông tin.

Từ khóa: Tội phạm mạng, tội phạm công nghệ thông tin, hợp tác quốc tế, Liên bang Nga.

Ngày nhận bài: 09/12/2022; Biên tập xong: 12/12/2022; Duyệt đăng: 12/12/2022

Every nation can not underestimate the importance of joint actions against modern challenges and threats to global security which one of the most dangerous threats is ICT-related crime (also called Cybercrime or High-tech Crime). Due to the impact of the Covid-19 pandemic, it has acquired new dimensions with the extensive digitization process, the spreading of virtual assets and its anonymous trans-border movement. Criminals actively use Darknet for illegal trade of information and prohibited items. Internet becomes a tool for perpetration of acts of terrorism and extremism. It also has negative influence upon the youth, involvement and inclination them to commit crimes. The Russian Federation is no exception to the negative influence of the explosive global growth of ICT-related crimes. The articles informs the challenges in preventing and fighting against ICT-related crime in the Russia, the practice of implementing and perfecting legal regulations as well as international cooperation of Interdisciplinary group of Prosecutor General's Office of the Russian Federation in the context of increasing number, nature and scale of cybercrime.

Keywords: ICT-related crime, cybercrime, international cooperation, the Russian Federation.

1. Nhận diện các thách thức trong đấu tranh chống tội phạm mạng ở Liên bang Nga

Theo thống kê, trong năm 2021, Nga đã ghi nhận hơn 517.000 tội phạm sử dụng công nghệ thông tin, chiếm hơn một phần tư tổng số các hành vi phạm tội được ghi nhận ở nước này[3]. Vấn đề quan trọng nhất trong quá trình điều tra các loại tội phạm trên thường liên quan đến bảo mật sơ bộ các dấu vết điện tử, sự phối hợp với các nhà cung cấp dịch vụ trong lĩnh vực công nghệ thông tin và truyền thông, mã hóa (đặc biệt là mã hóa đầu cuối (End-to-End) trong tin nhắn tức thời, các mạng ngang hàng, Darknet), ẩn danh và quy kết trong tấn công mạng.

Khác với tội phạm truyền thống, việc phát hiện, phòng ngừa, đấu tranh, chống loại tội phạm sử dụng công nghệ thông tin và truyền thông trở nên khó khăn do những đặc thù của loại tội phạm này. Trong thực tế, các nhóm tin tặc không bị giới hạn bởi biên giới quốc gia truyền thống mà mang tính chất xuyên quốc gia. Việc chuẩn bị và thực hiện tội phạm có thể được tiến hành ở một quốc gia hoặc một châu lục khác. Chính điều này đã gây ra những khó khăn nhất định cho các cơ quan thực thi pháp luật trong quá trình điều tra cũng như thu thập chứng cứ. Đồng thời, thực tế cũng cho thấy loại tội phạm này đã có sự thay đổi nhanh chóng về cấu trúc và thủ đoạn, sự gia tăng về tần suất và phương thức phạm tội so với các biện pháp bảo đảm an ninh và quy định pháp luật. Điều này đòi hỏi các nhà lập pháp và những người thực thi pháp luật phải kịp thời áp dụng các biện pháp, phối hợp công tác, tăng cường hợp tác quốc tế để hình thành hệ thống bảo đảm an toàn thông tin, đấu tranh có hiệu quả với tội phạm mạng.

2. Thực tiễn và những triển vọng trong hoạt động đấu tranh chống tội phạm mạng của Liên bang Nga

Với mục đích đấu tranh với tội phạm mạng và công nghệ thông tin, từ hai năm trước, Viện trưởng Tổng Viện kiểm sát Liên bang Nga Igor Viktorovich Krasnov đã thành lập Nhóm công tác liên ngành là đại diện các cơ quan có thẩm quyền của Nga, bao gồm Bộ Ngoại giao, Bộ Tư pháp, Bộ Nội vụ, Cơ quan An ninh liên bang (FSB) và Ủy ban điều tra. Chức năng chính của Nhóm là điều phối hoạt động của các cơ quan thực thi pháp luật về chống tội phạm mạng và công nghệ thông tin. Đây là một trong những nhiệm vụ then chốt của cơ quan công tố Liên bang Nga trong bối cảnh Chiến lược an ninh quốc gia và Các nguyên tắc cơ bản của chính sách nhà nước Liên bang Nga trong lĩnh vực an toàn thông tin quốc tế đã được Tổng thống Liên bang Nga phê duyệt.

Để phòng, chống tội phạm mạng,

** Phó Tổng Cục trưởng Tổng Cục Hợp tác pháp luật quốc tế, Tổng Viện kiểm sát Liên bang Nga*

[1] Bài viết là bản trình bày của Tác giả tại buổi làm việc và giảng bài tại Trường Đại học Kiểm sát Hà Nội ngày 03/10/2022. Tựa đề và các tiểu mục do Ban biên tập đặt. Bài viết phản ánh quan điểm của Tác giả.

[2] Đây là mạng của các trang web không thể truy cập từ công cụ tìm kiếm, bao gồm một tập hợp con của các trang web bí mật tồn tại trên một mạng được mã hóa.

[3] Đáng lưu ý, trong 6-7 năm trước, các hành vi phạm tội trong lĩnh vực này chỉ chiếm 2% trong tổng số các vụ phạm tội.

các cơ quan thực thi pháp luật vẫn tiếp tục hình thành các đơn vị chuyên trách và thường xuyên nâng cao trình độ chuyên môn nghiệp vụ cho cán bộ, nhân viên. Máy tính, các công cụ điều tra hình sự và hệ thống tìm kiếm tự động đang được đưa vào hoạt động để ngăn chặn tội phạm mạng và công nghệ thông tin, cũng như ngăn chặn việc lưu hành trái phép các chất ma túy, phổ biến thông tin bị cấm và các hành vi khác. Ví dụ, trong một năm kể từ khi vận hành hệ thống máy tính "Gian lận từ xa"[4], Nga đã xác định được hơn 600.000 dấu hiệu của tội phạm hàng loạt, trong đó có những dấu hiệu của hành vi phạm tội thuộc nhiều vùng miền khác nhau của đất nước. Sự phối hợp công tác giữa các cơ quan thực thi pháp luật trong cơ chế hoạt động của Nhóm công tác liên ngành cho thấy những kết quả tích cực theo từng năm. Chỉ tính riêng 6 tháng đầu năm 2022, tội phạm mạng và công nghệ thông tin đã giảm 8% so với trước đây.

Trong khuôn khổ hoạt động của mình, nhóm công tác đã soạn thảo và phê duyệt danh sách các loại tội phạm được thực hiện trong lĩnh vực công nghệ thông tin và truyền thông. Điều này đã hỗ trợ công tác thống kê trong lĩnh vực này để kịp thời đối phó với các mối đe dọa đang hình thành và phát triển trong môi trường kỹ thuật số. Nhóm cũng tập trung hoàn thiện luật pháp của Nga và thực tiễn áp dụng luật cùng các vấn đề hợp tác quốc tế trong lĩnh vực chống tội phạm mạng, bao gồm việc hình thành các cơ chế quốc tế tương ứng.

Có thể kể đến một kết quả nổi bật là bản dự thảo của Liên bang Nga về Công ước của Liên hợp quốc về chống sử dụng công nghệ thông tin và truyền thông vào mục đích tội phạm do các chuyên gia của nhóm công tác liên ngành biên soạn. Bản dự thảo này đã được chính thức đệ trình lên Ủy ban liên chính phủ đặc biệt của Liên hợp quốc vào tháng 7/2021. Trái ngược với cách tiếp cận khá hẹp trong việc soạn thảo văn kiện quốc tế chỉ nhằm chống lại tội phạm mạng ở một số quốc gia, Liên bang Nga coi dự thảo Công ước này là một cơ chế toàn diện để phòng, chống các hành vi phạm tội có sử dụng công nghệ thông tin và truyền thông một cách rộng rãi nhất[5].

Bản dự thảo thể hiện 23 hành vi phạm tội, bao gồm truy cập trái phép vào dữ liệu cá nhân, phân phối bất hợp pháp thuốc giả và thiết bị y tế (vấn đề đặc biệt thiết thực trong thời kỳ đại dịch COVID-19), chủ nghĩa khủng bố, chủ nghĩa cực đoan, phục hồi chủ nghĩa phát xít, buôn bán trái phép ma túy và vũ khí, lôi kéo trẻ vị thành niên vào các hoạt động bất hợp pháp và nhiều tội phạm

[4] Đây là phần mềm giúp thu thập, tổ chức, xử lý và phân tích thông tin nhận được trong quá trình điều tra các vụ án hình sự về tội phạm sử dụng công nghệ thông tin và viễn thông từ xa của Liên bang Nga, cho phép ghi lại những thông tin cần thiết kể từ thời điểm đăng ký báo cáo về những tội phạm này.

[5] Cụ thể, trong nửa đầu năm 2022, Nga đã chính thức ghi nhận gần 249.000 tội phạm công nghệ thông tin và truyền thông, trong đó chỉ có hơn 4.000 tội phạm máy tính (chủ yếu là truy cập bất hợp pháp vào thông tin máy tính; tạo ra, sử dụng và lan truyền các chương trình máy tính độc hại). Điều này có nghĩa là tội phạm máy tính trong lĩnh vực tội phạm công nghệ thông tin và truyền thông chỉ chiếm khoảng 1,5%. Trong khi đó, các nước phương Tây thực chất chỉ ghi nhận và xử lý một phần nhỏ các hành vi phạm tội này.

khác nữa. Đây đều là những vấn đề nhức nhối trong thế giới tội phạm mạng.

Đồng thời, bản dự thảo cũng tập trung vào trình tự tố tụng. Hoạt động hợp tác quốc tế và các cơ chế tương trợ cấp bách là rất quan trọng và cần thiết để nâng cao hiệu quả điều tra các loại tội phạm có tính chất xuyên biên giới của các cơ quan thực thi pháp luật. Trong tương lai, Công ước sẽ là cơ sở để các quốc gia thành viên Liên hợp quốc hoàn thiện luật pháp trong việc bảo vệ con người, xã hội và doanh nghiệp. Dự thảo Công ước cũng cố gắng cân bằng giữa việc bảo vệ dữ liệu cá nhân, tôn trọng chủ quyền quốc gia và quyền con người. Một loạt các biện pháp đã được thực hiện để bảo vệ nhân chứng cũng như việc áp dụng tích cực các công nghệ hiện đại, trong đó có các hệ thống trực tuyến để thẩm vấn nhân chứng cũng như các tác vụ thủ tục pháp lý khác.

Có thể thấy, Công ước toàn diện của Liên hợp quốc về chống tội phạm mạng và công nghệ thông tin là sự bổ khuyết cần thiết cho các công cụ hiện có, khỏa lấp những khoảng trống trong thực tiễn hợp tác quốc tế trong đấu tranh phòng chống loại tội phạm này. Thật vậy, đối với các văn bản pháp luật ở cấp khu vực, ví dụ như Công ước Budapest về tội phạm mạng của Hội đồng châu Âu đã được soạn thảo cách đây 20 năm khi nhân loại còn chưa biết đến các vấn đề hiện đại như Darknet, Phishing, phần mềm lừa đảo, tấn công DDos, SPAM… Tuy nhiên, trong hai thập kỷ vừa qua, thế giới đã thay đổi nhanh chóng và các đối tượng phạm tội cũng đã trang bị những công nghệ đó sử dụng cho các mục đích phạm tội. Do đó, Công ước toàn diện của Liên hợp quốc cung cấp cho các cơ quan thực thi pháp luật những công cụ cần thiết mà không làm tổn hại đến các cơ chế hiện có.

Đáng lưu ý, Liên bang Nga và một số lượng đáng kể các quốc gia không tham gia vào Công ước Budapest về tội phạm mạng. Nguyên nhân là bởi khoản b Điều 32 của Công ước cho phép một quốc gia thành viên có quyền truy cập xuyên biên giới hầu như không giới hạn vào thông tin có nguồn nằm ở một quốc khác mà không cần thông báo cho các cơ quan có thẩm quyền của quốc gia đó[6]. Trên thực tế, điều này được hiểu là một quốc gia có thể viện dẫn lý do là nhằm phòng, chống tội phạm mạng mà tự do xâm nhập một cách không hạn chế vào không gian mạng của các quốc gia khác, vi phạm nguyên tắc độc lập chủ quyền quốc gia và các quyền tự do cơ bản của con người, đặc biệt là quyền riêng tư. Một nhược điểm khác của Công ước Budapest là tính chất khu vực của nó, bởi Công ước này được soạn thảo cho các quốc gia thuộc Hội đồng châu Âu. Trong khi đó, bản dự thảo về Công ước của Liên hợp quốc về chống sử dụng công nghệ thông tin và truyền thông vào mục đích tội phạm là một văn

[6] Nguyên gốc:
Article 32 – Trans-border access to stored computer data with consent or where publicly available
A Party may, without the authorisation of another Party:
...
b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

bản toàn diện và phổ quát hơn.

Thực tế, sẽ mất nhiều thời gian để có thể xây dựng, ban hành và thông qua Công ước này, trong khi những vấn đề cấp bách nhằm đấu tranh phòng, chống tội phạm mạng thì phải được quan tâm giải quyết sớm nhất có thể. Do đó, Liên bang Nga đang thực hiện việc ký kết các thỏa thuận và chương trình hợp tác về phòng, chống tội phạm mạng và công nghệ thông tin với các cơ quan có thẩm quyền của các quốc gia khác. Trong gần 02 năm qua, Tổng Viện kiểm sát Liên bang Nga đã ký hơn 20 văn bản hợp tác như vậy. Điều này cho phép Nga tăng cường hợp tác quốc tế và có tác dụng tích cực trong việc xem xét các yêu cầu hỗ trợ pháp lý – công cụ hợp tác quốc tế chính của Liên bang Nga trong các vụ án hình sự. Chỉ tính riêng trong 8 tháng đầu năm 2022, Tổng Viện kiểm sát Liên bang Nga đã tổ chức thực hiện hơn 3.000 yêu cầu của các cơ quan có thẩm quyền của các nước ngoài về hỗ trợ tư pháp trong các vụ án hình sự thuộc loại này; trong đó có hơn 2.000 yêu cầu đã được thực hiện xong[7]. Nội dung các yêu cầu hỗ trợ pháp lý (các yêu cầu gửi đến và gửi đi) chủ yếu tập trung vào các hành vi gian lận máy tính, tống tiền và bóc lột tình dục trẻ em qua mạng Internet.

Trong quá trình xem xét và thực hiện yêu cầu của nước ngoài, nếu các cơ quan chức năng của Nga phát hiện thấy các dấu hiệu của tội phạm thuộc khu vực pháp lý của Liên bang Nga, đặc biệt là có thông tin về sự hiện diện của người liên quan đến tội phạm đó trên lãnh thổ của Liên bang Nga, thì Nga sẽ đề nghị nước ngoài chuyển cho mình các bản sao hồ sơ tài liệu về trình tự tố tụng hình sự tương ứng ở nước đó. Hồ sơ gồm công văn yêu cầu hoặc các thông báo khác về tội phạm theo hình thức hỗ trợ tư pháp hoặc hỗ trợ thực thi pháp luật để giải quyết vụ án hình sự hoặc lập hồ sơ nghiệp vụ. Trong trường hợp quốc gia nước ngoài từ chối dẫn độ bị can thì Liên bang Nga đề nghị chuyển hồ sơ kết quả truy cứu trách nhiệm hình sự của người đó cho Liên bang Nga theo nguyên tắc "không dẫn độ thì truy tố"[8].

Mặc dù tình hình thế giới và khu vực vẫn còn những diễn biến phức tạp nhưng sự hợp tác trong lĩnh vực thực thi pháp luật trong phòng, chống tội phạm mạng và công nghệ thông tin vẫn đang tiếp tục. Điều này đòi hỏi các quốc gia, các khu vực pháp lý phải nâng cao hợp tác, trao đổi dữ liệu cho các mục đích thực thi pháp luật. Việc thiếu thiện chí giữa các quốc gia chỉ tạo điều kiện thuận lợi hơn cho các băng nhóm tội phạm. Do đó, Liên bang Nga tiếp tục thực hiện các nghĩa vụ quốc tế của mình và sẵn sàng đối thoại trung thực và đôi bên cùng có lợi với các quốc gia trên thế giới để cùng nhau chống lại những thách thức và mối đe dọa của một trong những tội phạm nguy hiểm nhất thời hiện đại - tội phạm sử dụng công nghệ thông tin và truyền thông./.

[7] Hợp tác của Liên bang Nga chủ yếu với Belarus, Armenia, Hàn Quốc, Ba Lan, Thổ Nhĩ Kỳ và Pháp.

[8] Đáng chú ý là từ tháng 3 đến tháng 8 năm 2022 Liên bang Nga đã nhận được hơn 70 công văn từ chối yêu cầu dẫn độ công dân, một phần đáng kể trong số đó được các quốc gia này cho là vì lý do chính trị.