ĐIỀU ƯỚC QUỐC TẾ

BỘ NGOẠI GIAO

BỘ NGOẠI GIAO	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 15/2019/TB-LPQT	*Hà Nội, ngày 10 tháng 5 năm 2019*

THÔNG BÁO

Về hiệu lực của điều ước quốc tế

Thực hiện quy định tại Điều 56 của Luật Điều ước quốc tế năm 2016, Bộ Ngoại giao trân trọng thông báo:

Hiệp định giữa Chính phủ nước Cộng hòa xã hội Việt Nam và Chính phủ Liên bang Nga về hợp tác trong lĩnh vực bảo đảm an ninh thông tin quốc tế, ký tại Sochi, Liên bang Nga, ngày 06 tháng 9 năm 2018, có hiệu lực từ ngày 27 tháng 4 năm 2019.

Bộ Ngoại giao trân trọng gửi bản sao Hiệp định theo quy định tại Điều 59 của Luật nêu trên./.

TL. BỘ TRƯỞNG
KT. VỤ TRƯỞNG
VỤ LUẬT PHÁP VÀ ĐIỀU ƯỚC QUỐC TẾ
PHÓ VỤ TRƯỞNG

Lê Đức Hạnh

HIỆP ĐỊNH

GIỮA CHÍNH PHỦ NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM VÀ CHÍNH PHỦ LIÊN BANG NGA VỀ HỢP TÁC TRONG LĨNH VỰC BẢO ĐẢM AN NINH THÔNG TIN QUỐC TẾ

Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam và Chính phủ Liên bang Nga, sau đây được gọi là hai Bên,

Nhận thấy những tiến bộ đáng kể trong việc phát triển và áp dụng công nghệ thông tin và truyền thông mới nhất tạo ra tác động đáng kể tới hoạt động bảo đảm an ninh thông tin quốc tế,

Hiểu được tầm quan trọng to lớn của công nghệ thông tin và truyền thông với sự phát triển kinh tế xã hội, phục vụ lợi ích của con người và duy trì nền hòa bình, an ninh và ổn định quốc tế trong bối cảnh hiện nay,

Thể hiện sự quan ngại đối với các mối đe dọa liên quan đến việc có thể sử dụng công nghệ thông tin và truyền thông xâm hại đến chủ quyền và an ninh các quốc gia, can thiệp vào công việc nội bộ của nhau, xâm phạm đời sống cá nhân của công dân, gây mất ổn định chính trị, xã hội, kinh tế trong nước, kích động các cuộc tranh chấp liên sắc tộc và liên tôn giáo... mâu thuẫn với mục đích bảo đảm hòa bình, an ninh và ổn định quốc tế,

Hiểu được tầm quan trọng của an ninh thông tin quốc tế là một trong những nhân tố then chốt của hệ thống an ninh quốc tế,

Ủng hộ việc xây dựng và thông qua dưới sự bảo trợ của Liên hợp quốc các tiêu chuẩn, quy tắc hoặc nguyên tắc ứng xử có trách nhiệm của các quốc gia trên không gian mạng để có thể thúc đẩy việc bảo đảm an ninh công bằng cho các quốc gia,

Khẳng định chủ quyền quốc gia và các quy tắc, quy định quốc tế được xuất phát từ chủ quyền quốc gia áp dụng cho hoạt động của các quốc gia liên quan tới công nghệ thông tin và truyền thông, và áp dụng với thẩm quyền quốc gia đối với cơ sở hạ tầng công nghệ thông tin và truyền thông trong lãnh thổ quốc gia đó, cũng như quyền tự quyết định và thực hiện chính sách quốc gia về vấn đề liên quan tới mạng lưới thông tin và truyền thông của mình, bao gồm bảo đảm an ninh,

Tin tưởng rằng, việc củng cố sự tin cậy và phối hợp giữa hai Bên trong việc sử dụng công nghệ thông tin và truyền thông là vấn đề cấp bách và đáp ứng lợi ích của hai Bên,

Hiểu được tầm quan trọng đặc biệt về sự cân bằng giữa bảo đảm an ninh và tôn trọng quyền con người trong lĩnh vực công nghệ thông tin và truyền thông,

Nhằm mục đích ngăn chặn các mối đe dọa tới an ninh thông tin quốc tế, bảo vệ lợi ích an ninh thông tin của nhà nước mỗi Bên để phát triển môi trường

thông tin quốc tế, từ đó tạo điều kiện cho việc bảo đảm hòa bình, an ninh, sự minh bạch và hợp tác,

Mong muốn thiết lập cơ sở về pháp lý và cơ chế cho sự hợp tác giữa hai Bên trong lĩnh vực an ninh thông tin quốc tế trên cơ sở tôn trọng độc lập, chủ quyền, lợi ích và toàn vẹn lãnh thổ của nhau và không nhằm phương hại đến lợi ích của bên thứ ba,

Đã thống nhất như sau:

Điều 1
Các mối đe dọa chính trong lĩnh vực an ninh thông tin quốc tế

Hợp tác trong việc thực thi Hiệp định này, hai Bên đánh giá các mối đe dọa chính tới an ninh thông tin quốc tế là việc sử dụng công nghệ thông tin và truyền thông:

1. Để thực hiện các hành động nhằm đe dọa tới chủ quyền, an ninh và toàn vẹn lãnh thổ của quốc gia;

2. Gây hại đến kinh tế và các mối nguy hại khác bao gồm ảnh hưởng tiêu cực đến các yếu tố về cơ sở hạ tầng thông tin;

3. Vì mục đích khủng bố cũng như truyền bá tư tưởng khủng bố và tham gia hoạt động khủng bố;

4. Thực hiện tội phạm bao gồm các tội phạm liên quan tới việc truy cập bất hợp pháp thông tin máy tính, mạng máy tính và mạng Internet;

5. Can thiệp vào các công việc nội bộ của nhà nước, vi phạm trật tự xã hội, xúi giục xung đột liên sắc tộc, chủng tộc và tôn giáo, ủng hộ cho các ý tưởng, luận thuyết phân biệt chủng tộc và bài xích người nước ngoài dẫn đến việc châm ngòi cho lòng hận thù, phân biệt đối xử và kích động gây bạo loạn, gây mất ổn định tình hình kinh tế, xã hội, chính trị nội bộ, vi phạm quản lý nhà nước;

6. Truyền bá các thông tin gây hại đến hệ thống chính trị công và kinh tế xã hội, môi trường văn hóa, đạo đức tinh thần của nhà nước mỗi Bên.

Điều 2
Nguyên tắc chung về hợp tác

1. Hai Bên hợp tác trong lĩnh vực bảo đảm an ninh thông tin quốc tế trong khuôn khổ Hiệp định này nhằm thúc đẩy phát triển kinh tế - xã hội, phù hợp với mục tiêu duy trì hòa bình, an ninh và ổn định quốc tế và các nguyên tắc, quy phạm của luật pháp quốc tế được công nhận rộng rãi, bao gồm các nguyên tắc tôn trọng chủ quyền và toàn vẹn lãnh thổ của nhau, giải quyết hòa bình các xung đột và tranh chấp, không sử dụng vũ lực và đe dọa vũ lực, không can thiệp vào công việc nội bộ, tôn trọng quyền con người và các quyền tự do

cơ bản, cũng như nguyên tắc hợp tác song phương và không can thiệp vào nguồn thông tin của Nhà nước mỗi Bên.

2. Hoạt động của hai Bên trong khuôn khổ Hiệp định này phải tuân thủ các quy định pháp luật của mỗi Bên. Các Bên không can thiệp vào công việc nội bộ của nhau, tôn trọng quyền con người và các quyền tự do cơ bản, cũng như nguyên tắc hợp tác song phương và không can thiệp vào các nguồn thông tin của Nhà nước Bên kia.

3. Mỗi Bên có quyền như nhau trong bảo mật các nguồn thông tin của nước mình khỏi sử dụng và can thiệp trái phép, bao gồm cả hoạt động tấn công máy tính. Các Bên không tiến hành các hoạt động chống lại Bên kia và hỗ trợ Bên kia trong việc thực hiện các quyền nêu trên.

4. Tôn trọng chủ quyền và toàn vẹn lãnh thổ, giải quyết một cách hòa bình các tranh chấp và xung đột, không sử dụng vũ lực hay đe dọa sử dụng vũ lực; nỗ lực để cơ sở hạ tầng thông tin, tài nguyên thông tin của các Bên không bị Bên thứ ba lợi dụng gây thiệt hại cho Nhà nước mỗi Bên.

Điều 3
Các hoạt động hợp tác chính

1. Xem xét mối đe dọa chính thức được nêu tại Điều 1 của Hiệp định này, hai Bên, đại diện được ủy quyền và cơ quan có thẩm quyền của hai Bên được chỉ định theo Điều 5 của Hiệp định này, hợp tác bảo đảm an ninh thông tin quốc tế trên các lĩnh vực chính sau:

1) Tham gia xây dựng, thúc đẩy các quy chuẩn luật pháp quốc tế về bảo đảm an ninh thông tin quốc gia và quốc tế;

2) Phối hợp đấu tranh phòng, chống các mối đe dọa trong lĩnh vực bảo đảm an ninh thông tin quốc tế được nêu tại Điều 1 của Hiệp định này;

3) Trao đổi thông tin trên lĩnh vực thực thi pháp luật phục vụ điều tra các vụ việc liên quan đến sử dụng công nghệ thông tin và truyền thông vào mục đích khủng bố và tội phạm;

4) Đàm phán thống nhất và thực hiện các biện pháp xây dựng lòng tin cần thiết góp phần bảo đảm an ninh thông tin quốc tế;

5) Trao đổi thông tin giữa các cơ quan có thẩm quyền hai Bên về vấn đề bảo đảm an ninh, bao gồm hợp tác giữa các cơ quan có thẩm quyền của hai Bên trong lĩnh vực ứng phó với các sự cố máy tính;

6) Trao đổi thông tin về luật pháp của hai Bên liên quan đến bảo đảm an ninh thông tin;

7) Hỗ trợ hoàn thiện cơ sở pháp lý song phương và cơ chế thực tiễn hợp tác hai Bên trong bảo đảm an ninh thông tin quốc tế;

8) Tăng cường hợp tác và phối hợp hành động giữa hai Bên liên quan đến bảo đảm an ninh thông tin quốc tế trong các tổ chức và diễn đàn quốc tế (bao gồm Liên hợp quốc, Liên minh Viễn thông quốc tế, Tổ chức Tiêu chuẩn hóa quốc tế và các tổ chức khác);

9) Tổ chức các buổi làm việc, hội nghị, hội thảo và các diễn đàn khác của đại diện và chuyên gia được ủy quyền của hai Bên trong lĩnh vực an ninh thông tin quốc tế;

10) Tăng cường hợp tác đào tạo, tập huấn, trao đổi chuyên gia trong lĩnh vực an ninh thông tin giữa hai Bên;

11) Hợp tác chuyển giao công nghệ trong lĩnh vực an ninh thông tin theo quy định của luật pháp mỗi Bên;

12) Tạo điều kiện để các cơ quan có thẩm quyền của mỗi Bên phối hợp thực hiện Hiệp định này

2. Hai Bên và cơ quan có thẩm quyền của hai Bên có thể xác định các hướng hợp tác khác bằng văn bản thỏa thuận cụ thể.

Điều 4
Cơ quan điều phối

Nhằm tạo điều kiện thực hiện hiệu quả các điều khoản của Hiệp định và thiết lập kênh phối hợp trực tiếp giữa nước Cộng hòa xã hội chủ nghĩa Việt Nam và Liên bang Nga trong khuôn khổ Hiệp định, hai bên xác định cơ quan điều phối:

- Về phía nước Cộng hòa xã hội chủ nghĩa Việt Nam - Bộ Công an;

- Về phía Liên bang Nga - Văn phòng Hội đồng An ninh Liên bang Nga.

Trong trường hợp cần thiết, hai Bên có thể thay đổi cơ quan điều phối và kịp thời thông báo bằng văn bản cho phía Bên kia thông qua kênh ngoại giao.

Điều 5
Hình thức và cơ chế hợp tác

1. Hai Bên tiến hành hoạt động phối hợp theo phương hướng hợp tác cụ thể được quy định trong Hiệp định thông qua cơ quan có thẩm quyền của hai Bên có trách nhiệm thi hành Hiệp định này. Trong vòng 60 ngày kể từ ngày Hiệp định có hiệu lực, hai Bên trao đổi thông tin qua kênh ngoại giao về cơ quan có thẩm quyền của hai Bên chịu trách nhiệm thi hành Hiệp định này.

2. Nhằm mục đích tạo cơ sở pháp lý và tổ chức cho việc hợp tác trong các lĩnh vực cụ thể, cơ quan có thẩm quyền của Chính phủ hai Bên có thể ký kết các thỏa thuận liên ngành liên quan.

3. Hai Bên tổ chức tham vấn thường xuyên giữa các cơ quan được ủy quyền và cơ quan có thẩm quyền của hai Bên nhằm rà soát công tác triển khai Hiệp định, trao đổi thông tin, phân tích đánh giá các mối đe dọa đang nổi lên đối với an ninh thông tin quốc tế, cũng như nhằm xác định, thống nhất và phối hợp triển khai các biện pháp ứng phó chung đối với các nguy cơ này.

Trên cơ sở nhất trí của hai Bên, các buổi tham vấn trên sẽ được tổ chức 02 lần mỗi năm luân phiên tại nước Cộng hòa xã hội chủ nghĩa Việt Nam và Liên bang Nga.

Mỗi Bên có thể đề nghị tổ chức thêm các buổi tham vấn và đề xuất thời gian, địa điểm và chương trình nghị sự.

Điều 6
Bảo mật thông tin

Hai Bên tiến hành các biện pháp cần thiết bảo mật các thông tin được chuyển giao hoặc phát sinh trong quá trình hợp tác trong khuôn khổ Hiệp định này. Việc tiếp cận thông tin bị giới hạn do pháp luật nhà nước của hai Bên quy định.

Các thông tin được bảo mật theo pháp luật và các văn bản quy phạm pháp luật có liên quan của Nhà nước Bên tiếp nhận thông tin. Thông tin này sẽ không được tiết lộ hoặc chuyển giao mà không có sự đồng ý bằng văn bản của Bên chuyển giao thông tin.

Thông tin sẽ được phân loại theo đúng quy định của pháp luật của Nhà nước mỗi Bên.

Trình tự trao đổi, bảo mật thông tin bí mật quốc gia Liên bang Nga hay tài liệu mật của nước Cộng hòa xã hội chủ nghĩa Việt Nam được xác định theo Hiệp định giữa Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam và Chính phủ Liên bang Nga về bảo vệ thông tin mật ký ngày 27/3/2002.

Điều 7
Tài chính

1. Hai Bên sẽ chịu các chi phí cho đại diện và chuyên gia của mình khi tham gia các hoạt động diễn ra trong quá trình thực thi Hiệp định.

2. Về các chi phí khác liên quan đến việc thực thi Hiệp định, trong từng trường hợp cụ thể hai Bên có thể thống nhất các thủ tục tài chính khác tuân theo luật pháp của nhà nước mình.

Điều 8
Mối liên hệ với các Điều ước quốc tế khác

Hiệp định này không ảnh hưởng đến các quyền lợi và nghĩa vụ của mỗi Bên phát sinh từ các điều ước quốc tế khác mà nhà nước Bên đó đang tham gia.

Điều 9
Giải quyết các tranh chấp

Hai Bên sẽ giải quyết các tranh chấp phát sinh do giải thích hoặc áp dụng các điều khoản của Hiệp định này thông qua tham vấn và đàm phán giữa các cơ quan có thẩm quyền hai Bên và thông qua kênh ngoại giao nếu cần thiết.

Điều 10
Điều khoản thực thi

1. Hiệp định này có hiệu lực từ ngày 30 (ba mươi) kể từ khi nhận được thông báo sau cùng của hai Bên thông qua đường ngoại giao về việc hoàn tất các thủ tục nội bộ cần thiết để Hiệp định có hiệu lực.

2. Theo thỏa thuận hai Bên có thể sửa đổi Hiệp định này. Các chỉnh sửa là một phần không thể tách rời của Hiệp định và sẽ được thể hiện thành nghị định thư riêng.

3. Hiệp định này sẽ chấm dứt hiệu lực sau 90 ngày kể từ khi một Bên nhận được thông báo bằng văn bản qua đường ngoại giao của Bên kia về ý định chấm dứt hiệu lực Hiệp định. Việc chấm dứt hiệu lực của Hiệp định này không làm ảnh hưởng đến hoạt động hợp tác đang được hai Bên thực hiện hoặc thống nhất triển khai trước đó.

4. Trong trường hợp chấm dứt hiệu lực Hiệp định này, hai Bên phải có biện pháp nhằm hoàn thành nghĩa vụ của mình trong bảo mật thông tin cũng như hoàn thành các hoạt động, dự án, sự kiện chung đã thống nhất trước đó, đang được triển khai trong khuôn khổ Hiệp định này nhưng chưa kết thúc khi Hiệp định chấm dứt hiệu lực.

Hiệp định được làm tại Sochi vào ngày 06 tháng 9 năm 2018 thành hai bản, mỗi bản bằng tiếng Việt, tiếng Nga và tiếng Anh, các văn bản có giá trị như nhau. Trong trường hợp có khác biệt về cách hiểu, văn bản tiếng Anh sẽ được sử dụng.

THAY MẶT CHÍNH PHỦ NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM	THAY MẶT CHÍNH PHỦ LIÊN BANG NGA
Bùi Văn Nam	Sergey Lavrov
Thứ trưởng Bộ Công an	Bộ trưởng Bộ Ngoại giao

СОГЛАШЕНИЕ
МЕЖДУ ПРАВИТЕЛЬСТВОМ СОЦИАЛИСТИЧЕСКОЙ РЕСПУБЛИКИ ВЬЕТНАМ И ПРАВИТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Правительство Социалистической Республики Вьетнам и Правительство Российской Федерации, далее именуемые Сторонами,

Отмечая значительный прогресс в развитии и внедрении новейших информационно-коммуникационных технологий, оказывающих существенное влияние на обеспечение международной информационной безопасности,

Отмечая большое значение информационно-коммуникационных технологий для социально-экономического развития на благо всего человечества, а также для поддержания в современных условиях международного мира, безопасности и стабильности,

Выражая озабоченность угрозами, связанными с возможностями использования информационно-коммуникационных технологий в целях, не совместимых с задачами обеспечения международного мира, безопасности и стабильности, для подрыва суверенитета и безопасности государств и вмешательства в их внутренние дела, нарушения неприкосновенности частной жизни граждан, дестабилизации внутриполитической и социально-экономической обстановки, разжигания межнациональной и межконфессиональной вражды,

Придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности,

Поддерживая разработку и принятие под эгидой ООН норм, правил, принципов ответственного поведения государств в информационном пространстве для содействия обеспечению равной безопасности для всех стран,

Подтверждая то, что государственный суверенитет и международные нормы и принципы, вытекающие из государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием информационно-коммуникационных технологий, и юрисдикцию государств над информационной инфраструктурой на их территории, а также то, что государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-

телекоммуникационной сетью «Интернет», включая обеспечение безопасности,

Будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия Сторон в области использования информационно-коммуникационных технологий являются настоятельной необходимостью и отвечают их интересам,

Придавая важное значение балансу между обеспечением безопасности и соблюдением прав человека в области использования информационно-коммуникационных технологий,

Стремясь предотвращать угрозы международной информационной безопасности, обеспечить интересы информационной безопасности государств Сторон в целях формирования международной информационной среды, для которой характерны мир, безопасность, открытость и сотрудничество,

Желая создать правовые и организационные основы сотрудничества Сторон в области обеспечения международной информационной безопасности, исходя из взаимного уважения независимости, суверенитета, интересов и территориальной целостности, и которое не направлено на причинение вреда интересам третьей стороны,

Согласились о нижеследующем:

Статья 1
Основные угрозы в области обеспечения международной информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами в области обеспечения международной информационной безопасности является использование информационно-коммуникационных технологий:

1) для осуществления актов, направленных на нарушение суверенитета, безопасности и территориальной целостности государств;

2) для нанесения экономического и другого ущерба, в том числе путем оказания деструктивного воздействия на объекты информационной инфраструктуры;

3) в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности;

4) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, компьютерным сетям, сети «Интернет»;

5) для вмешательства во внутренние дела государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутриполитической и социально-экономической обстановки, нарушения управления государством;

6) для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Статья 2
Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в области обеспечения международной информационной безопасности в рамках настоящего Соглашения таким образом, чтобы такое сотрудничество способствовало социальному и экономическому развитию, было совместимо с задачами поддержания международного мира, безопасности и стабильности и соответствовало общепризнанным принципам и нормам международного права, включая принципы взаимного уважения суверенитета и территориальной целостности, мирного урегулирования споров и конфликтов, неприменения силы и угрозы силой, невмешательства во внутренние дела, уважения прав и основных свобод человека, а также принципам двустороннего сотрудничества и невмешательства в информационные ресурсы государств Сторон.

2. Деятельность Сторон в рамках настоящего Соглашения должна быть совместимой с законодательством государств Сторон. Стороны не вмешиваются во внутренние дела друг друга, уважают права и основные свободы человека, а также принципы двустороннего сотрудничества и невмешательства в информационные ресурсы государства Сторон.

3. Каждая Сторона имеет равные права на защиту информационных ресурсов своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от компьютерных атак на них. Каждая Сторона не осуществляет по отношению к другой Стороне подобных действий и оказывает содействие другой Стороне в реализации указанных прав.

4. Стороны уважают суверенитет и территориальную целостность, урегулируют споры и конфликты мирными способами, не используют силу или угрозу применения силы; прилагают усилия к тому, чтобы информационная инфраструктура и ресурсы государств Сторон не

использовались третьей стороной для нанесения ущерба государствам Сторон.

Статья 3
Основные направления сотрудничества

1. С учетом основных угроз, указанных в статье 1 настоящего Соглашения, Стороны, уполномоченные представители и компетентные органы государств Сторон, которые определяются в соответствии со статьей 5 настоящего Соглашения, осуществляют сотрудничество в области обеспечения международной информационной безопасности по следующим основным направлениям:

1) участие в разработке и продвижении норм международного права в целях обеспечения национальной и международной информационной безопасности;

2) координация противодействия угрозам в области обеспечения международной информационной безопасности, указанным в статье 1 настоящего Соглашения;

3) обмен информацией в правоохранительной области в целях расследования дел, связанных с использованием информационно-коммуникационных технологий в террористических и криминальных целях;

4) согласование путем переговоров и осуществление необходимых мер доверия, способствующих обеспечению международной информационной безопасности;

5) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения безопасности, включая сотрудничество между уполномоченными органами государств Сторон в области реагирования на компьютерные инциденты;

6) обмен информацией о законодательстве государств Сторон по вопросам обеспечения информационной безопасности;

7) содействие совершенствованию двусторонней нормативно-правовой базы и практических механизмов сотрудничества государств Сторон в обеспечении международной информационной безопасности;

8) углубление взаимодействия и координации деятельности государств Сторон по проблемам обеспечения международной информационной безопасности в рамках международных организаций и форумов (включая Организациб Объединенных Наций, Международный союз электросвязи, Международную организацию по стандартизации и другие);

9) проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов государств Сторон в сфере международной информационной безопасности.

10) укрепление взаимодействия в области подготовки кадров, стажировок, обмен специалистами в сфере международной информационной безопасности;

11) взаимодействие в области передачи технологий в сфере информационной безопасности в соответствии с законодательством государств Сторон;

12) создание условий для взаимодействия компетентных органов государств Сторон в целях реализации настоящего Соглашения.

2. Стороны или компетентные органы государств Сторон могут определять другие направления сотрудничества путем письменной договоренности.

Статья 4
Координирующие органы

В целях содействия эффективной реализации положений настоящего Соглашения и установления непосредственного взаимодействия между Социалистической Республикой Вьетнам и Российской Федерацией в рамках настоящего Соглашения Координирующими органами определены:

от Социалистической Республики Вьетнам - Министерство общественной безопасности;

от Российской Федерации - аппарат Совет Безопасности Российской Федерации.

При необходимости Стороны могут заменить координирующий орган, незамедлительно оповестив в письменной форме о таких изменениях другую Сторону по дипломатическим каналам.

Статья 5
Формы и механизмы сотрудничества

1. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии компетентных органов государств Сторон, ответственных за реализацию настоящего Соглашения, в течение 60 дней со дня вступления настоящего Соглашения в силу Стороны обменяются по дипломатическим каналам данными о компетентных органах

государств Сторон, ответственных за реализацию настоящего Соглашения.

2. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы государств Сторон могут заключать соответствующие договоры межведомственного характера.

3. С целью рассмотрения хода реализации настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз международной информационной безопасности, а также определения, согласования и координации совместных мер реагирования на такие угрозы Стороны проводят на регулярной основе консультации уполномоченных и компетентных органов государств Сторон.

Указанные консультации проводятся по согласованию Сторон, 2 раза в год, попеременно в Социалистической Республике Вьетнам и Российской Федерации.

Каждая из Сторон может инициировать проведение дополнительных консультаций, предлагая время и место их проведения, а также повестку дня.

Статья 6
Защита информации

Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, доступ к которой ограничен в соответствии с законодательством государств Сторон.

Защита такой информации осуществляется в соответствии с законодательством и (или) соответствующими нормативными правовыми актами государства получающей Стороны. Такая информация не раскрывается и не передается без письменного согласия Стороны, являющейся источником этой информации.

Такая информация обозначается в соответствии с законодательством государств Сторон.

Порядок обмена информацией, содержащей сведения, составляющие государственную тайну Российской Федерации или секретные материалы Социалистической Республики Вьетнам, порядок защиты такой информации определяются Соглашением между Правительством Социалистической Республики Вьетнам и Правительством Российской Федерации о взаимном обеспечении защиты секретных материалов от 27 марта 2002 года.

Статья 7
Финансирование

1. Стороны самостоятельно несут расходы, связанные с участием их представителей и экспертов в соответствующих мероприятиях по выполнению настоящего Соглашения.

2. В отношении прочих расходов, связанных с выполнением настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с законодательством государств Сторон.

Статья 8
Отношение к другим международным договорам

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон по другим международным договорам, участником которых является ее государство.

Статья 9
Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем консультаций и переговоров между компетентными органами государств Сторон и в случае необходимости по дипломатическим каналам.

Статья 10
Заключительные положения

1. Настоящее Соглашение вступает в силу на 30-й день со дня получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

2. По согласию Сторон в настоящее Соглашение могут вноситься изменения, являющиеся неотъемлемой частью настоящего Соглашения и оформляемые отдельными протоколами.

3. Действие настоящего Соглашения может быть прекращено по истечении 90 дней со дня получения одной из Сторон по дипломатическим каналам письменного уведомления другой Стороны о ее намерении прекратить действие настоящего Соглашения. Прекращение действия настоящего Соглашения не затрагивает мероприятия,

осуществляемые в рамках сотрудничества Сторон, или согласованные ранее.

4. В случае прекращения действия настоящего Соглашения Стороны принимают меры для полного выполнения обязательств по защите информации, а также обеспечивают выполнение ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках настоящего Соглашения и не завершенных к моменту прекращения действия настоящего Соглашения.

Совершено в г. Сочи «06» сентября 2018 г. в двух экземплярах, каждый экземпляр на вьетнамском, русском и английском языках, причем все тексты имеют одинаковую силу. В случае возникновения расхождений в толковании используется текст на английском языке.

ЗА ПРАВИТЕЛЬСТВО СОЦИАЛИСТИЧЕСКОЙ РЕСПУБЛИКИ ВЬЕТНАМ	ЗА ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
БУЙ ВАН НАМ	СЕРГЕЙ ЛАВРОВ
Заместитель Министра Общественной Безопасности	Министр Иностранных Дел

AGREEMENT
BETWEEN THE GOVERNMENT OF THE SOCIALIST REPUBLIC OF VIET NAM AND THE GOVERNMENT OF THE RUSSIAN FEDERATION ON COOPERATION IN THE FIELD OF INTERNATIONAL INFORMATION SECURITY

The Government of the Socialist Republic of Viet Nam and the Government of the Russian Federation, hereinafter referred to as the Parties,

Noting that considerable progress has been achieved in the development and implementation of the latest information and communication technologies that have a considerable impact on ensuring international information security,

Noting great importance of information and communication technologies in social and economic development for the benefit of the entire humanity and in maintaining international peace, security and stability in modern-day conditions,

Expressing concern over the threats linked to the possibilities of the use of information and communication technologies for purposes inconsistent with the tasks of ensuring international peace, security and stability, for the purposes of undermining sovereignty and security of States and interference in their internal affairs, violation of the citizens' private life, destabilization of domestic political, social and economic situation, fomenting of interethnic and interconfessional strife,

Attaching great importance to international information security as one of the key elements of the international security system,

Supporting the development and adoption under the auspices of the UN of norms, rules and principles of responsible behavior of States in information space in order to promote equal security for all countries,

Affirming, that state sovereignty and international norms and principles, which flow from state sovereignty, apply to behavior of States within the framework of activities related to the use of information and communication technologies, and to their jurisdiction over information infrastructure within their territory, and that a State has a sovereign right to determine and implement public policy on matters related to the Internet information and telecommunication network, including ensuring security,

Convinced that further build-up of trust and interaction between the Parties in the field of the use of information and communication technologies is an urgent necessity and corresponds with their interests,

Attaching major importance to the balance between ensuring security, and respecting human rights in the field of the use of information and communication technologies,

Seeking to prevent threats to international information security, to protect the interests of information security of the States of the Parties in order to form international information environment, for which peace, security, transparency and cooperation are inherent,

Wishing to establish legal and organizational foundation for cooperation between the Parties in the field of international information security on the basis of mutual respect for independence, sovereignty, interests and territorial integrity and without intention to cause damage to the interests of any third Party,

Have agreed as follows:

Article 1
Major Threats in the Field of International Information Security

In cooperating in accordance with this Agreement, the Parties shall act on the premise that the major threats in the field of international information security are posed by the use of information and communication technologies:

1) for committing acts aimed at undermining sovereignty, security and territorial integrity of States;

2) for causing economic and other damage, including through destructive impact on elements of information infrastructure;

3) for terrorist purposes, including for terrorist propaganda and engagement in terrorist activities;

4) for committing crimes, including those connected with unauthorized access to computer information, computer networks and the Internet network;

5) for interference into the domestic affairs of States, violation of public order, incitement of interethnic, interracial and interconfessional strife, advocacy of racist and xenophobic ideas and theories that ignite hatred and discrimination and foment violence and instability and also for destabilizing domestic political, social and economic situation and disturbance to state governance;

6) for dissemination of information harmful to socio-political and socio-economic systems, spiritual, moral, and cultural environment in the States of the Parties.

Article 2
General Principles of Cooperation

1. The Parties shall cooperate in the field of ensuring international information security within the framework of this Agreement in such a way that

such cooperation promotes social and economic development and is compatible with the objectives of maintaining international peace, security, and stability and corresponds with the universally accepted principles and norms of international law, including the principles of mutual respect of sovereignty and territorial integrity, peaceful settlement of disputes and conflicts, non-use of force or threat of force, non-interference in internal affairs, respect for human rights and fundamental freedoms, as well as the principles of bilateral cooperation and non-interference in information resources of the States of the Parties.

2. The activities of the Parties within the framework of this Agreement shall be compatible with legislation of the State of the Parties. The Parties shall not interfere in each other's domestic affairs and shall respect human rights and fundamental freedoms, as well as the principles of bilateral cooperation and non-interference in information resources of the States of the Parties.

3. Each Party shall have equal rights to protect information resources of its State from unlawful use and unauthorized interference, including from computer attacks against them. Each of the Parties shall not take such action against the other Party and shall assist other Parties in fulfilling the specified rights.

4. The Parties shall respect sovereignty and territorial integrity, settle disputes and conflicts by peaceful means, not use force or threat of force; make efforts in order to prevent the use of information infrastructure and resources of the State Parties by a third party in order to cause damage to the States of the Parties .

Article 3
Major Areas of Cooperation

1. Taiking into account the major threats listed in Article 1 of this Agreement, the Parties, their authorized representatives and the competent state authorities of the States of the Parties assigned in accordance with Article 5 of this Agreement, shall cooperate in the field of ensuring international information security in the following major areas:

1) participation in development and promotion of the norms of international law to ensure national and international information security;

2) coordination of countering threats in the field of international information security listed in Article 1 of this Agreement;

3) information exchange in the field of law enforcement in order to investigate cases connected with the use of information and communication technologies for terrorist and criminal purposes;

4) harmonization by way of negotiations and implementation of necessary confidence-building measures contributing to ensuring international information security;

5) information exchange between competent authorities of the States of the Parties on the issues of ensuring security, including cooperation between competent authorities of the States of the Parties in the field of response to computer incidents;

6) information exchange on the legislation of the States of the Parties related to ensuring information security;

7) assistance in improving bilateral legal and policy framework and practical mechanisms of cooperation between the States of the Parties in ensuring international information security;

8) intensifying cooperation and coordination of activities of the States of the Parties with regard to ensuring international information security within the framework of international organizations and fora (including the United Nation, International Telecommunication Union, International Standardization Organization, etc.);

9) holding working meetings, conferences, workshops and other forums of authorized representatives and experts of the States of the Parties in the field of international information security;

10) strengthening interaction in the area of personnel training, internship, exchange of specialists in the field of international information security;

11) cooperating to transfer technology in the field of information security in accordance with the legislation of the States of the Parties;

12) creating conditions for interaction between competent authorities of the States of the Parties for the purpose of implementing this Agreement.

2. The Parties and competent authorities of the States of the Parties may, by written agreement, determine other areas of cooperation.

Article 4
Coordinating Authorities

In order to facilitate effective implementation of the provisions of this Agreement and establishment of direct interaction between the Socialist Republic of Viet Nam and the Russian Federation, the coordinating authorities within the framework of this Agreement shall be determined as follows:

from the Socialist Republic of Viet Nam - the Ministry of Public Security;

from the Russian Federation - office of the Security Council of the Russian Federation.

If necessary, the Parties may change the coordinating authority by immediately providing a written notification of such changes to another Party through diplomatic channels.

Article 5
Forms and Mechanisms of Cooperation

1. The Parties may ensure practical interaction in specific areas of cooperation provided for by this Agreement through the competent authorities of the States of the Parties responsible for the implementation of this Agreement; within 60 days after the date of entry into force of this Agreement, the Parties shall, through diplomatic channels, exchange data on the competent authorities of the States of the Parties responsible for the implementation of this Agreement.

2. In order to lay the legal and organizational foundation for the cooperation in specific areas, the competent authorities of the States of the Parties may conclude relevant inter-agency agreements.

3. In order to review the implementation of this Agreement, to exchange information, analyze and jointly assess arising threats to international information security, as well as to determine, agree upon and coordinate joint response measures against such threats, the Parties shall hold regular consultations of designated and competent authorities of the States of the Parties.

The mentioned consultations shall be held, upon agreement between the Parties, two times a year, in the Socialist Republic of Viet Nam and the Russian Federation on a rotating basis.

Each Party may initiate additional consultations and suggest their dates, venue and agenda.

Article 6
Protection of Information

The Parties shall provide appropriate protection of the information transferred or generated in the course of cooperation under this Agreement, access to which is limited by the legislation of the States of the Parties.

Such information shall be protected in accordance with the legislation and/or relevant normative legal acts of the State of the receiving Party. Such information shall not be disclosed or transferred without a written consent of the Party transferring this information.

Such information shall be duly marked in accordance with the legislation of the States of the Parties.

The exchange of information containing data constituting a State secret of the Russian Federation or classified materials of the Socialist Republic of Vietnam, as well as the procedures for protection of such information shall be determined by the Agreement between the Government of the Socialist Republic of Viet Nam and the Government of the Russian Federation on mutual protection of classified information of 27 March 2002.

Article 7
Financing

1. The Parties shall independently bear the costs of the participation of their representatives and experts in the relevant activities to implement this Agreement.

2. With regard to other costs related to the implementation of this Agreement, the Parties may agree upon other financial procedures in each particular case in accordance with the legislation of the States of the Parties.

Article 8
Relation to Other International Treaties

This Agreement shall not affect the rights and obligations of each Party deriving from other international treaties to which its State is Party.

Article 9
Settlement of Disputes

The Parties shall settle the disputes that may arise with regard to the interpretation or application of the provisions of this Agreement through consultations and negotiations between competent authorities of the States of the Parties and, if necessary, through diplomatic channels.

Article 10
Final Provisions

1. This Agreement shall enter into force on the 30th day following the date of the receipt, through diplomatic channels, of the last written notification on the completion by the Parties of their domestic procedures necessary for its entry into force.

2. By mutual consent of the Parties, amendments may be made to this Agreement, which shall be considered an integral part of this Agreement and formalized as a separate protocols.

3. This Agreement may be terminated 90 days after the receipt by either of the Parties, through diplomatic channels, of a written notification from the other Party of its intention to terminate this Agreement. The termination of this Agreement shall not affect activities undertaken as part of the cooperation between the Parties of formerly agreed.

4. In case of termination of this Agreement, the Parties shall take measures to fulfill their obligations in the field of protecting information as well as to implement formerly agreed joint activities, projects and other measures carried out under this Agreement and not completed upon termination of this Agreement.

Done at Sochi on "06" September 2018, in two copies, in the Vietnamese, Russian and English languages, all of them being equally authentic. In case of any discrepancies in interpretation the English text shall be used.

FOR THE GOVERNMENT OF THE SOCIALIST REPUBLIC OF VIET NAM	FOR THE GOVERNMENT OF THE RUSSIAN FEDERATION
Bui Van Nam Deputy Minister of Public Security	Sergey Lavrov Minister