В.П.Шерстюк – Президент

Национальной Ассоциации
международной информационной
безопасности

Актуальные проблемы международной информационной безопасности

– взгляд из России

Человечество вошло в зону обострения геополитической напряженности. Об этом емко и четко говорится в п.17 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 2 июля 2021 г. N 400, «Рост геополитической нестабильности и конфликтности, усиление межгосударственных противоречий сопровождаются повышением угрозы использования военной силы. Расшатывание общепризнанных норм и принципов международного права, ослабление и разрушение существующих международных правовых институтов, продолжающийся демонтаж системы договоров и соглашений в области контроля над вооружениями ведут к нарастанию напряженности и обострению военно-политической обстановки, в том числе вблизи государственной границы Российской Федерации. Действия некоторых стран направлены на инспирирование в Содружестве Независимых Государств (СНГ) дезинтеграционных процессов в целях разрушения связей России с ее традиционными союзниками. Ряд государств называет Россию угрозой и даже военным противником. Увеличивается опасность перерастания вооруженных конфликтов в локальные и региональные войны, в том числе с участием ядерных держав. Космическое и информационное пространства активно осваиваются как новые сферы ведения военных действий.[1)]

По мнению ведущих экспертов, всё большую подрывную роль в данном процессе и процессе десуверенизации национальных государств играют информационно-коммуникационные технологии (ИКТ). Действительно, планета охвачена беспрецедентной цифровой трансформацией. Её драйвером стали интернет-технологии, которые вызвали и продолжают вызывать тектонические сдвиги в развитии цивилизации. По сути, человечество вступило не только в новый технологический уклад, но и в новый фазовый переход, сравнимый по значению, например, с созданием электричества. Это означает, что на смену микроэлектронике пришли нано-, био-, инфо- и когнитивные технологии, а на основе принципов Industry IV стремительно развивается цифровая экономика, киберфизические системы, искусственный интеллект, квантовые вычисления, блокчейн, связь поколения 5G и иные технологии, кардинально меняющие современный мир.

В этих условиях ведущие страны мира разрабатывают и реализуют разнообразные

концептуальные и доктринальные стратегии по внедрению новейших технологий с целью достижения геополитического доминирования, что привело к резкому обострению геополитического противоборства. Тем самым подтверждается хорошо известный постулат: история войн – это история технологических открытий.

В силу этого неоценимое значение и стратегическую важность в создании безопасного глобального информационного пространства имеют утвержденные Указом Президента Российской Федерации от 12 апреля 2021 г. № 213 «Основы государственной политики в области международной информационной безопасности»[2] (далее - Основы). Данный документ направлен на продвижение российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в этой сфере, на содействие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве и на организацию межведомственного взаимодействия.

Среди угроз международной информационной безопасности в Основах выделены следующие:

а) использование ИКТ в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

б) использование ИКТ в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) использование ИКТ в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

г) использование ИКТ в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;

д) использование ИКТ для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

е) использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка ИКТ, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

В сравнении с Основами 2013 года в документе в качестве одних из основных угроз международной информационной безопасности впервые представлены угрозы использования ИКТ для проведения компьютерных атак на информационные ресурсы государств.

Трансграничный характер перечисленных угроз и масштабы их возможных последствий объективно свидетельствуют о невозможности противодействия им в одиночку. Данное обстоятельство диктует необходимость развития на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской

Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности.

Реализация государственной политики в области международной информационной безопасности предусматривается по следующим основным направлениям:

- развитие на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности;
- противодействие угрозе использования ИКТ в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;
- формирование механизмов международного сотрудничества в сфере противодействия угрозе использования ИКТ в террористических целях;
- содействие разработке и реализации на глобальном, региональном, многостороннем и двустороннем уровнях комплекса мер, направленных на противодействие угрозе использования ИКТ в экстремистских целях;
- создание условий для противодействия угрозе использования ИКТ в экстремистских целях, а также в целях вмешательства во внутренние дела суверенных государств;
- повышение эффективности международного сотрудничества, направленного на противодействие угрозе использования ИКТ в преступных целях, и по созданию необходимого для этого международно-правового режима;
- совершенствование межгосударственного взаимодействия, направленного на противодействие угрозе использования ИКТ для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также межгосударственного взаимодействия в области реагирования на компьютерные инциденты;
- создание условий для обеспечения технологического суверенитета государств в области ИКТ и преодоления информационного неравенства между развитыми и развивающимися странами.

По сути, каждое направление реализации государственной политики увязано с решением задач по противодействию угрозам международной информационной безопасности.

Хотелось бы подробнее остановиться на конкретных идеях и инициативах России в рамках указанных направлений.

Содействие формированию системы обеспечения международной информационной безопасности вот уже более 20 лет является приоритетной линией российской внешнеполитической деятельности, реализуемой на различных международных площадках.

Старт работе на данном направлении был дан принятием в декабре 1998 года по инициативе России резолюции Генеральной Ассамблеи ООН 53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[3)], впервые отметившей необходимость широкого международного взаимодействия в

борьбе с угрозами неправомерного использования ИКТ.

Поэтому логичным и последовательным представляется обозначенный в новых Основах курс на развитие на всех уровнях сотрудничества с зарубежными партнерами в интересах формирования системы обеспечения международной информационной безопасности.

В качестве приоритетного направления на заседании Совета безопасности 26 марта 2021 года Президентом Российской Федерации В.В.Путиным обозначен диалог с нашими ближайшими партнерами по ОДКБ, СНГ, ШОС и БРИКС[4)].

Как отметил глава государства, «Россия, как и прежде, открыта для диалога и конструктивного взаимодействия со всеми партнерами, причем как в двустороннем формате, так и на площадках международных структур и форумов, прежде всего, конечно, в Организации Объединенных Наций»[5)].

В Основах сформулированы инициативы России, которые нашли поддержку большинства государств - членов мирового сообщества.

Во-первых, это создание условий для принятия Конвенции ООН об обеспечении международной информационной безопасности. Впервые данная инициатива была озвучена секретарем Совета безопасности Российской Федерации Н.П.Патрушевым в сентябре 2011 года в Екатеринбурге на международной встрече высоких представителей, курирующих вопросы безопасности. Участникам встречи была представлена концепция такой конвенции. В настоящее время имеется обновленная редакция этой концепции[6)]. Потребность в юридически обязательном документе, регулирующем деятельность государств в глобальном информационном пространстве, давно назрела. Предложения о его принятии неоднократно звучали в 2019-2021 годах в ходе заседаний профильной Рабочей группы открытого состава (РГОС) ООН.

Создание новой группы на период 2021-2025 годов стало еще одной инициативой России, зафиксированной в резолюции Генеральной Ассамблеи ООН 75/240, принятой большинством голосов государств - членов Организации 31 декабря 2020 года[7)].

Это вторая российская инициатива, нашедшая отражение в новых Основах и нацеленная на содействие организации под эгидой ООН регулярного институционального диалога с участием всех государств - членов ООН для обеспечения демократического, инклюзивного и транспарентного переговорного процесса по вопросам безопасности в сфере использования ИКТ.

Третьей инициативой, поддержанной большинством при голосовании по российскому проекту резолюции Генеральной Ассамблеи ООН 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях»[8)], стало создание в ООН Специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.

Содействие деятельности Специального комитета, а также создание условий для последующего принятия государствами - членами ООН упомянутой конвенции отнесены к одному из основных направлений реализации государственной политики Российской Федерации в области международной информационной безопасности.

Принятие вышеуказанных конвенций станет наиболее весомым вкладом в

построение системы обеспечения международной информационной безопасности на ее высшем, глобальном уровне.

Однако новые Основы ориентируют на достижение и выполнение двусторонних и многосторонних договоренностей международно-правового и иного характера между Российской Федерацией и иностранными государствами о сотрудничестве в рассматриваемой области.

Достижению этих договоренностей будут способствовать проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и основных направлений сотрудничества в области обеспечения международной информационной безопасности с государствами - участниками СНГ, объединения БРИКС, государствами - членами ОДКБ, ШОС, АСЕАН, «Группы двадцати», другими государствами и международными организациями.

Для проведения подобных консультаций в многостороннем формате с ближайшими партнерами России потребуется активизировать деятельность уже созданных в этих целях профильных групп экспертов: Рабочей группы при Комитете секретарей советов безопасности ОДКБ по информационной политике и информационной безопасности, Группы экспертов государств - членов ШОС по международной информационной безопасности, Рабочей группы БРИКС по вопросам безопасности в сфере использования ИКТ.

Новый импульс получит сотрудничество с государствами - членами АСЕАН в рамках Диалога Россия - АСЕАН по вопросам, связанным с обеспечением безопасности информационно-коммуникационных технологий, концепция которого одобрена 26 января 2021 года Совещанием старших должностных лиц России и стран Ассоциации государств Юго-Восточной Азии на уровне заместителей министров иностранных дел[9)].

Следует отметить, что в практику взаимодействия России и ее партнеров давно вошли двусторонние межведомственные консультации, результатом которых стало подписание межправительственных соглашений о сотрудничестве в области обеспечения международной информационной безопасности с Бразилией, Беларусью, Кубой, Китаем, Индией, ЮАР, Вьетнамом, Туркменистаном, Ираном, Киргизией и др.

Одновременно ведется работа по подготовке проектов соглашений с полутора десятком государств. Сотрудничество России с ее иностранными партнерами будет нацелено прежде всего на совместное противодействие нарастающим вызовам и угрозам международной информационной безопасности, предотвращение (урегулирование) межгосударственных конфликтов в глобальном информационном пространстве.

Для этого к основным направлениям реализации российской государственной политики в рассматриваемой области отнесено содействие развитию региональных систем обеспечения международной информационной безопасности и формированию соответствующей глобальной системы на основе общепризнанных принципов и норм международного права с учетом специфики ИКТ, а также на основе новых принципов и норм международного права.

Единству подходов к практическому решению этих задач должна способствовать выработка на всех уровнях взаимодействия мер укрепления доверия в области

противодействия использованию ИКТ для осуществления в глобальном информационном пространстве действий, представляющих угрозу международному миру, безопасности и стабильности.

В целом, сохраняя преемственность стратегического курса России на предотвращение межгосударственных конфликтов в глобальном информационном пространстве и подтверждая приверженность нацеленности государственной политики на содействие формированию системы обеспечения международной информационной безопасности, Основы наглядно демонстрируют новые стратегические ориентиры государства с учетом национальных интересов Российской Федерации.

На необходимость совершенствования этой работы обратил внимание Президент Российской Федерации В.В.Путин в своем выступлении 26 марта 2021 года на заседании Совета безопасности: «Самое серьезное внимание следует уделить налаживанию механизмов практического сотрудничества в обеспечении безопасности глобальной информационной сферы»[10].

Мне, как президенту Национальной Ассоциации международной информационной безопасности (НАМИБ), приятно и ответственно отметить, что далее президент Путин подчеркнул «…в эффективной реализации государственной политики, обозначенной в новой редакции «Основ», надо активнее использовать возможности научных и экспертных кругов, делового сообщества, в том числе, конечно, Национальной ассоциации международной информационной безопасности».

В данном контексте несколько слов о НАМИБ. Ассоциация, как неправительственная организация, была создана в апреле 2018 года в целях содействия развитию государственно-частного партнерства в области безопасности использования ИКТ. Её учредителями стали ведущие вузы страны, бизнес-структуры, а также редакция журнала «Международная жизнь».

Согласно Уставу НАМИБ призвана, в том числе в упреждающем режиме проводить проработку проблемных вопросов обеспечения международной информационной безопасности в интересах формирования переговорных позиций государственных органов.

За 4 с половиной года Ассоциация приняла участие в десятках крупных международных форумах, в том числе в качестве организатора или соорганизатора. Так, проведены XIII, XIV и XV международные Форумы «Партнёрство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». XVI Форум состоится 19-21 сентября 2022 года в Дипломатической академии МИД России, на который приглашены сотни ведущих отечественных и зарубежных экспертов, а также представители ООН, ШОС, СНГ, ОДКБ, АСЕАН, ЛАГ и др.

Также были организованы форумы в Гватемале и на Кубе, медиафорумы в Братиславе, Праге, Нижнем Новгороде и др. Ассоциация участвовала VIII и IX Конференциях по интернет-безопасности в Пекине с приветствием председателя Наблюдательного совета НАМИБ, Зам. Секретаря Совбеза России О.В.Храмова и т.д. Члены НАМИБ сделали сотни докладов, опубликовали десятки статей, приняли участие в выпуске учебника «Международная информационная безопасность: теория и практика» в трех томах и т.д.

В июне 2022 года Ассоциация получила аккредитацию на площадке Рабочей группы ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ. Это открывает новое окно возможностей для продвижения сотрудничества по различным аспектам обеспечения международной информационной безопасности – одной из ключевых проблем современности.

Мы будем приветствовать взаимодействие и с нашими японскими коллегами.

1）URL: http://www.scrf.gov.ru/media/files/file/l4wGRPqJvETSkUTYmhepzRochb1j1jqh.pdf (Дата обращения 30.08.2022 г.)

2）«Основы государственной политики в области международной информационной безопасности», утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213
URL: http://kremlin.ru/acts/bank/46614 (дата обращения: 25.08.2022)

3）Резолюция 53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Принята Генеральной Ассамблеей ООН 4 декабря 1998 г. // URL: // https://undocs.org/ru/A/RES/53/70 (Дата обращения 30.08.2022 г.)

4）Выступление Президента Российской Федерации В.В.Путина на заседании Совета безопасности 26 марта 2021 г. // URL: // http://www.kremlin.ru/events/president/news/65231 (Дата обращения 30.08.2022 г.)

5）Там же

6）Конвенция ООН об обеспечении международной информационной безопасности (концепция) // URL: // http://www.scrf.gov.ru/security/information/document112/ (Дата обращения 30.08.2022 г.)

7）Резолюция A/75/240 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Принята Генеральной Ассамблеей ООН 31 декабря 2020 г. URL: // https://undocs.org/ru/A/RES/75/240

8）Резолюция A/74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Принята Генеральной Ассамблеей ООН 27 декабря 2019 г. // URL: // https://undocs.org/ru/A/RES/74/247

9）Об участии заместителя министра иностранных дел России И.В.Моргулова в Совещании старших должностных лиц Россия - АСЕАН. Сообщение для СМИ // URL: // https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4542722

10）Выступление Президента Российской Федерации В.В.Путина на заседании Совета безопасности 26 марта 2021 г. // URL: // http://www.kremlin.ru/events/president/news/65231 (Дата обращения 30.08.2022 г.)

V.P. シュルスチュク
国家国際情報セキュリティ協会会長

国際情報セキュリティ緊急の課題

――ロシアの視点――

人類は地政学的緊張が激化する領域に突入した。このことは、2021年７月２日付けのロシア連邦大統領令第400号によって承認された、ロシア連邦国家安全保障戦略の第17項で明確に示されている。「地政学的な不安定さと紛争の増加、国家間の対立の激化に伴い、軍事力行使の脅威が高まりを見せている。一般的に認められた国際法の規準と原則の不安定化、現存の国際的な法体系の弱体化と崩壊、止まることを知らない軍備管理分野における合意と協定システムの解体は、ロシア連邦の国境周辺を含めた軍事政治的情勢の緊張の高まりと激化を招いている。一部の国の行動は、ロシアとその伝統的な同盟国との関係を破壊させようと、独立国家共同体（CIS）内の崩壊プロセスを煽動することを目的としている。一連の国々がロシアを脅威であるとみなし、中には軍事的な敵と位置付けている国さえある。軍事紛争が、核大国が参加する形となる局地戦、地域戦争に発展する危険性が高まっている。宇宙空間、情報空間が、軍事行動[1)]を実施する新たな領域として積極的に開発されている。」

主要な専門家の見解によれば、このようなプロセス、また国家の非主権化プロセスにおいて、ますます大きな破壊的役割を果たしているのが、情報通信技術である。実際、地球は前例のないデジタルトランスフォーメーションに覆われている。その原動力となったのは、文明発展における地殻変動を呼び起こし、今も呼び起こし続けているインターネット技術である。実際、人類は新たな科学技術を基礎とした秩序に突入しただけでなく、たとえば電気の発明などと同等の価値を持つ新たな秩序のフェーズへ移行した。これは、マイクロエレクトロニクスに代わり、ナノ技術、バイオ技術、情報技術、そして認知技術が現れ、インダストリー4.0の原則を基礎として、デジタル経済、サイバーフィジカルシステム、人工知能、量子コンピュータ、ブロックチェーン、第５世代移動通信システム、そして、現代世界を根本的に変化させるその他の技術が劇的に発展していることを意味する。

こうした条件の下、世界の主要な国々は、地政学的支配の達成を目的とした最新技術の導入に向け、さまざまな概念的および教義的戦略を考案、実現しており、これが地政学的対立の著しい悪化を引き起こした。そしてこれにより、「戦争の歴史は技術的発展の歴史」であるという非常に有名な公理が正しいことが証明された。

こうしたことから、2021年４月12日付けのロシア連邦大統領令第213号で承認された

「国際情報セキュリティ分野における国家政策の原則」[2)]（以下、「原則」とする）は、安全なグローバル情報空間を創設する上で、極めて重要な意義と戦略的重要性を持っている。この文書は、国際情報セキュリティシステムの構築に向けたロシアのアプローチと、この分野におけるロシアのイニシアチブの推進、グローバルな情報空間における国家間の紛争防止および解決に向けた国際法メカニズムの構築の促進、そして省庁間の協力の構築を目的としたものである。

「原則」の中で挙げられている国際情報セキュリティに対する脅威は以下のようなものである。

a）主権破壊（侵害）、国家の領土保全の侵害、また、グローバルな情報空間での世界の平和、安全、安定の維持を妨害するその他の行為の実現を目的とした軍事、政治、および、その他の分野における情報通信技術の利用

b）テロの宣伝およびテロ活動への新たな支持者の勧誘を含むテロを目的とした情報通信技術の利用

c）過激主義的な目的を持つ情報通信技術の利用、主権国家の内政干渉のための情報通信技術の利用

d）コンピュータ情報分野での犯罪、あらゆる種類の詐欺行為を含む、犯罪を目的とした情報通信技術の利用

e）重要な情報インフラを含む、国家の情報リソースに対するサイバー攻撃実施のための情報通信技術の利用

f）情報通信技術市場の独占、最新の情報通信技術への他国からのアクセス制限、また、情報分野で支配的な立場にある国家への技術的依存、情報格差を拡大させるためグローバルな情報空間を技術的に支配する個別の国家を利用すること

2013年の「原則」と比較してみると、この文書では、国家の情報安全保障に対するサイバー攻撃は、国際情報セキュリティの主な脅威の一つとして初めて公式文書に取り上げられたことは特筆すべきことである。「原則」で提示した脅威の持つ国家の枠を超えた脅威とそれによって起こりうる被害は、それらの脅威に対して国家が単独では対抗できないことを客観的に証明している。このような状況は、ロシア連邦が国際情報セキュリティシステム構築の諸問題をめぐる諸外国との協力を国際的、地域的、多国間、また二国間レベルでそれぞれ発展させていく必要があることを示唆している。

国際情報セキュリティ分野における国家政策の実現は、以下の主な方向性で想定されている。

- 国際情報セキュリティシステム構築の諸問題をめぐるロシア連邦と諸外国との国際的、地域的、多国間、二国間レベルでの協力の発展

- 主権の破壊（侵害）、国家の領土保全の侵害、グローバルな情報空間において世界の平和、安全、安定の維持を妨害するようなその他の行為の実現を目的とした情報通信技術利用の脅威への対抗
- テロを目的とした情報通信技術の利用の脅威に対抗するための国際的な協力メカニズムの構築
- 過激主義的な目的を持つ情報通信技術利用の脅威に対抗するため国際的、地域的、多国間、二国間レベルでの複合的措置の考案とその実現に向けた協力
- 過激主義的な目的を持つ情報通信技術利用の脅威、また主権国家の内政干渉を目的とした情報通信技術利用の脅威に対抗するための条件策定
- 犯罪を目的とした情報通信技術利用の脅威への対抗、およびそれに必要な国際法体制の構築に向けた国際協力の有効性の向上
- 重要な情報インフラを含む国家の情報リソースへサイバー攻撃を行うために情報通信技術を利用する脅威に対抗するための国際協力の発展、情報セキュリティ事故へ即応可能な国家間協力の改善
- 情報通信技術分野における国家の技術的主権を保障するための条件策定、先進国と途上国間での情報格差の解消

事実、国家政策実現に向けたそれぞれの方向性は、国際情報セキュリティへの脅威に対抗するための課題の解決と直結している。

上述した方向性において、ロシアの具体的なアイデアとイニシアチブについて、もう少し詳細に述べたい。国際情報セキュリティシステム構築に対する対する国際協力は、すでに20年以上にわたり、さまざまな国際会議などで実現されつつあるが、ロシアの外交政策において優先順位の高いアジェンダとなっている。このような国際的な取り組みは、ロシア発案による国連総会決議53/70「国際安全保障の文脈における情報および電気通信分野の進歩」[3)]が1998年12月に採択されたことにより開始された。この決議で重要なことは、情報通信技術の不正利用の脅威との闘いにおいて幅広い国際協力が必要であることを初めて指摘した。そこで、新たな「原則」に記された、国際情報セキュリティシステム構築を目的とした外国のパートナーとのあらゆるレベルでの協力の発展に向けた基本方針は、理論的であり、筋の通ったものである。そして、2021年３月26日の安全保障会議で、ロシア連邦の V.V. プーチン大統領は、その優先的な方向性として、集団安全保障条約、独立国家共同体、上海協力機構、BRICS を通じた、ロシアにとってより近いパートナー国との対話を挙げた[4)]。また、大統領は「ロシアは、これまで同様、すべてのパートナーと対話し、建設的な協力を行う用意がある。しかも、二国間の形式でも、また何より国連を始めとする国際的な組織やフォーラムにおいてもそうである」[5)]と指摘した。「原則」では、

国連加盟国の大多数の支持を得たロシアのイニシアチブが策定されている。

まずそれは、国際情報セキュリティに関する国連条約を採択するための条件の策定である。一つ目のイニシアチブは、2011年９月にエカテリンブルグで開かれた安全保障問題を担当した高官による国際会議であり、ロシア連邦安全保障会議の N.P. パトルシェフ書記によって初めて発表された。会議の参加者らに対しては、こうした条約のコンセプトも発表された（現在、このコンセプト[6]は改訂されている）。グローバルな情報空間において国家活動を規制する法的拘束力を持つ文書策定の必要性については、すでに以前より指摘されてきた。その文書の採択提案に関しては、2019年から2021年にかけ、国連のオープン・エンド作業部会（OEWG）の会議でも、繰り返し発言がなされている。

二つ目のイニシアチブでは2021年から2025年にかけての新たな作業部会の創設は、ロシアのもう一つの発案となったが、これは国連総会決議75/240として策定され、2020年12月31日、国連加盟国の大多数の賛成によって採択された[7]。これは、新たな「原則」にも反映されているもので、情報通信技術をめぐる安全保障問題において民主的で包括的、かつ透明な協議プロセスを保障するため、国連主導の下、国連のすべての加盟国が参加する定期的な対話を制度化し、促進することを目的としている。これがロシアの２つ目のイニシアチブである。

三つ目のイニシアチブは、ロシアが提案した国連総会決議案74/247「犯罪目的での情報通信技術利用への対抗策」[8]の投票で、大多数の支持を得た３つ目のイニシアチブにより、国連内に、犯罪目的の情報通信技術利用に対抗するための包括的な国際条約の草案を取りまとめるオープン・エンド特別政府間専門家委員会が創設された。特別委員会への活動協力、また、それに続いて、先述した条約が採択されるための条件策定は、国際情報セキュリティ分野におけるロシア連邦の国家政策実現に向けた主な方向性の一つとなっている。上記の条約の採択は、もっとも高度な世界レベルの国際情報セキュリティシステムを構築するにあたり、もっとも意義深い貢献となる。

一方で、新たな「原則」は、検討されている分野でのロシア連邦と諸外国との協力に関する二国間および多国間での国際法上の合意の達成と遂行を目的としている。こうした合意の達成を促進するのが、二国間および多国間での定期的な専門家協議の実施、独立国家共同体、BRICS の加盟国、集団安全保障条約、上海協力機構（SCO）、ASEAN、G20の加盟国、その他の国々や国際組織などとの間での国際情報セキュリティ分野における立場の調整や主な方向性のすり合わせである。

ロシアと近い関係にあるパートナーとの間でこうした協議を多国間で行うためには、すでにこれを目的として創設された専門家作業部会の活動を活発化することが必要である。それは、集団安全保障条約安全保障会議書記委員会付属の情報政策・情報セキュリティ問

題作業部会、上海協力機構加盟国の国際情報セキュリティ問題専門家グループ、BRICSの情報通信技術利用分野での安全保障問題作業部会である。また2021年１月26日にロシアとASEAN加盟国の外務次官級の高官会議[9]でその構想が承認された、ロシア・ASEAN対話の枠内での情報通信技術の安全保障に関する諸問題をめぐるASEAN加盟国との協力は、新たな刺激を生むものとなるだろう。ロシアとそのパートナーとの協力は、かなり前から２カ国省庁間協議という形で実践されている。その結果、ブラジル、ベラルーシ、キューバ、中国、インド、南アフリカ共和国、ベトナム、トルクメニスタン、イラン、キルギスなどの間で、国際情報セキュリティ分野における二国間協力協定が締結されたことは、指摘しておく必要がある。それと同時に、15カ国以上の国家との合意文書案の準備作業が進められている。ロシアと外国のパートナーらとの協力は、まず何より、高まりつつある国際情報セキュリティに対する挑戦と脅威に共同で対抗すること、また、グローバルな情報空間での国家間の紛争を防止（解決）することを目的としている。そのために、検討される分野においてロシアの国家政策実現に向けた主な方向性とされているのが、国際情報セキュリティのための地域システム発展の促進、情報通信技術の特徴を考慮に入れた上での、一般に認められた国際法の原則と規準および新たな国際法の原則と規準を基礎とした然るべき国際的なシステムの構築である。世界の平和と安全および安定を脅威にさらすような行動を実施するためのグローバルな情報空間で、情報通信技術の利用に対抗する分野において、あらゆる協力レベルでの信頼強化措置の策定は、これらの課題解決に向けたアプローチの統合を促進するものとなるはずである。総じて、「原則」は、グローバルな情報空間における国家間紛争の防止に向けたロシアの戦略路線の継承性を保ち、かつ国際情報セキュリティシステム構築への協力に向けた国家政策の狙いに忠実であることを確認している。その上、ロシア連邦の国益を考慮に入れた国家の新たな戦略的目標も明確に示している。

ロシア連邦のV.V.プーチン大統領は、2021年３月26日に開かれた安全保障会議での演説の中で、この取り組みをさらに改善する必要があることに注意を向け、「世界の情報分野の安全保障における実際的な協力メカニズムの形成に、細心の注意を払う必要がある」[10]と述べた。「国家国際情報セキュリティ協会」（NAMIB）会長の私が、非常に喜ばしい気持ちで、責任感を持ちつつ指摘したいのは、プーチン大統領がそれに続いて、「改訂版の『原則』で示された国家政策を効果的に実現していくにあたっては、何より国家国際情報セキュリティ協会を含めた研究者、専門家、企業界が持つ可能性を積極的に利用する必要がある」と強調したことである。

この文脈において、「国家国際情報セキュリティ協会」について簡単に紹介する。協会は、情報通信技術利用の安全保障分野において、国家および民間のパートナーシップの発

展を促進することを目的としており、2018年４月に非政府組織として創設された。創設者はロシアの主要な高等教育機関、ビジネス団体、そして外交雑誌「国際生活」の編集局である。「国家国際情報セキュリティ協会」は、その憲章で謳われている通り、国家機関の交渉の場を形成するため、ときに先んじて、国際情報セキュリティに関する諸問題を詳細に研究する使命を担っている。

協会は、この４年半の間に、数十の大規模な国際フォーラムに参加してきたが、その中には、主催者として、また共同主催者として参加したものも含まれる。第13回、第14回、第15回国際フォーラム「国際情報セキュリティにおける国家、ビジネス、市民社会のパートナーシップ」も実施された。第16回フォーラムは2022年９月19日から21日にかけてロシア外務省外交アカデミーで開催される予定であり、数百人のロシアと外国の主要な専門家、そして国連、上海協力機構、独立国家共同体、集団安全保障条約、ASEAN、アラブ連盟などの代表が招待されている。またグアテマラ、キューバでもフォーラムが組織され、ブラチスラヴァ、プラハ、ニジニ・ノヴゴロドなどでメディアフォーラムが開催された。さらに協会は中国の北京で開かれた第８回、第９回インターネット・セキュリティ大会にも参加し、国家国際情報セキュリティ協会監査役会会長でもある、ロシア安全保障会議の O.V. フラモフ副書記が挨拶を行った。国家国際情報セキュリティ協会のメンバーらはこれまでに数百の報告を行い、数十の論文を発表し、３巻から成る書籍「国際情報セキュリティ：理論と実践」などの出版に携わってきた。また、2022年６月、協会は情報通信技術の利用および情報通信技術分野での安全保障問題に関する国連オープン・エンド作業部会で認定を受けた。これは、現代の最重要問題の一つである国際情報セキュリティにおいて、さまざまな局面での協力を促進させる新たな可能性の扉を開くものである。

私たちは（同じ分野で活動する）日本の同僚たちとの協力も歓迎する。

註

1）URL: http://www.scrf.gov.ru/media/files/file/l4wGRPqJvETSkUTYmhepzRochb1j1jqh.pdf（アクセス日、2022年８月30日）

2）「国際情報セキュリティ分野における国家政策の原則」、2021年４月12日付けロシア連邦大統領令第213号で承認。
URL: http://kremlin.ru/acts/bank/46614（アクセス日、2022年８月25日）

3）決議53/70「国際安全保障の文脈における情報および電気通信分野の進歩」。1998年12月４日に国連総会で採択。URL: https://undocs.org/ru/A/RES/53/70

4）2021年３月26日の安全保障会議での V.V. プーチン大統領の発言
URL: http://www.kremlin.ru/events/president/news/65231（アクセス日、2022年８月30日）

5）４に同じ

6）国際情報セキュリティ確保に関する国連条約（コンセプト） URL: http://www.scrf.gov.ru/security/information/document112/（アクセス日、2022年８月30日）

7）決議 A/75/240「国際安全保障の文脈における情報および電気通信分野の進歩」。2020年12月31日に国連総会で採択。URL:https://undocs.org/ru/A/RES/75/240
8）決議A /74/247「犯罪目的での情報通信技術の利用への対抗策」。2019年12月27日国連総会で採択。URL:https://undocs.org/ru/A/RES/74/247
9）ロシア・ASEAN 高官会議へのロシアの I.V. マルグロフ外務次官の参加について。メディア向けメッセージ。URL: www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4542722
10）2021年 3 月26日、安全保障会議における V.V. プーチン大統領の発言
URL: http://www.kremlin.ru/events/president/news/65231（アクセス日、2022年 8 月30日）