SECRETARIAT OF THE CONFERENCE ON INTERACTION AND CONFIDENCE BUILDING MEASURES IN ASIA

СЕКРЕТАРИАТ СОВЕЩАНИЯ ПО ВЗАИМОДЕЙСТВИЮ И МЕРАМ ДОВЕРИЯ В АЗИИ

№ 17-1/308

The Secretariat of the Conference on Interaction and Confidence Building Measures in Asia (CICA) presents its compliments to the CICA Member States and has the honour to forward herewith the information of Russian delegation on proposed CBM "Security of and in the use of ICTs" to the CICA Catalogue of Confidence Building Measures, presented at the SWG meeting on May 27, 2021.

Enclosure: as stated, on 4 p.

The Secretariat avails itself of this opportunity to renew to the CICA Member States the assurances of its highest consideration.

Nur-Sultan, 1 June 2021

MEMBER STATES OF THE CONFERENCE ON INTERACTION AND CONFIDENCE BUILDING MEASURES IN ASIA

SECRETARIAT OF THE CONFERENCE ON INTERACTION AND CONFIDENCE BUILDING MEASURES IN ASIA

СЕКРЕТАРИАТ СОВЕЩАНИЯ ПО ВЗАИМОДЕЙСТВИЮ И МЕРАМ ДОВЕРИЯ В АЗИИ

№ 17-1/308

Приложение:
упомянутое, на 4 л.

Секретариат Совещания по взаимодействию и мерам доверия в Азии (СВМДА) свидетельствует свое уважение государствам-членам СВМДА и имеет честь препроводить информацию российской делегации по включению в Каталог мер доверия нового направления сотрудничества – безопасность в сфере использования ИКТ, представленную на заседании СРГ СВМДА 27 мая 2021 года.

Секретариат пользуется случаем, чтобы возобновить государствам-членам СВМДА уверения в своем высоком уважении.

город Нур-Султан, 1 июня 2021 года

ГОСУДАРСТВА-ЧЛЕНЫ
СОВЕЩАНИЯ ПО ВЗАИМОДЕЙСТВИЮ И
МЕРАМ ДОВЕРИЯ В АЗИИ

бейресми аударма

Азиядағы өзара іс-қимыл және сенім шаралары кеңесінің (АӨСШК) Хатшылығы АӨСШК мүше мемлекеттеріне өзінің зор ілтипатын білдіре отырып ү.ж. 27 мамырда Сенім шаралар каталогына АКТ-іні қолдану аясындағы қауіпсіздік бойынша ынтымақтастықтың жаңа бағыты ретінде қосуға қатысты Арнайы жұмыс тобы отырысында ресей делегациясының ұсынған информацияны жолдап отыр.

Қосымша: аталған, 4 п.

Хатшылық осы мүмкіндікті пайдалана отырып, АӨСШК мүше мемлекеттеріне өзінің зор ілтипатын тағы да растайды.

Нұр-Сұлтан қаласы, 2021 жылғы 1 маусым

АЗИЯДАҒЫ ӨЗАРА ІС-ҚИМЫЛ ЖӘНЕ СЕНІМ ШАРАЛАРЫ КЕҢЕСІНІҢ МҮШЕ МЕМЛЕКЕТТЕРІ

Позиция по пунктам
2.2.4, 2.2.7-2.2.9 обновленного
Каталога мер доверия СВМДА

(27 мая 2021 г.)

Пункт 2.2.4

1. Нецелесообразно объединять экономические преступления и преступления в области безопасности в сфере использования ИКТ и самих ИКТ в одном подпункте 2.2.4, так как **проблема информпреступности больше связана с безопасностью, чем с экономикой**.

2. Предложенные в подпункте 2.2.4 формулировки частично дублируют подпункты 2.2.5 и 2.2.6, а потому представляются излишними.

3. При разработке раздела по безопасности в сфере использования ИКТ и самих ИКТ Каталога мер доверия СВМДА считаем необходимым ориентироваться на **терминологию, закрепленную в ключевых профильных документах ООН**, в частности в резолюции Генеральной Ассамблеи ООН 75/240 от 31 декабря 2020 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», и отказаться от использования «кибер»-лексики в пользу ИКТ-формулировок.

Пункты 2.2.7-2.2.9

1. Вопросы **предотвращения конфликтов и кризисов**, связанных с использованием ИКТ и самих ИКТ, и **укрепления доверия** в этой области в течение более чем двадцати лет являются важной частью дискуссии в рамках ООН. Ее достижения отражены в резолюции 75/240 и в принятом 12 марта с.г. докладе рабочей группы открытого состава ООН по международной информационной безопасности.

2. Дискуссия по вопросу о **профильной терминологии** ведется в рамках различных региональных площадок, таких как Организация по безопасности и сотрудничеству в Европе (ОБСЕ) и Региональный форум АСЕАН по безопасности (АРФ). Упомянутая тема, как ожидается, станет одной из центральных в деятельности новой рабочей группы открытого состава ООН.

3. Продвижение сотрудничества по **противодействию преступности в сфере использования ИКТ** и самих ИКТ (подпункт 2.2.9). Граждане, предприятия и государственные структуры все более уязвимы перед лицом информпреступности, а ее последствия становятся все разрушительнее. В силу трансграничного характера и масштаба этих вызовов государства не могут бороться с ними в одиночку. Кроме того, ряд стран сталкивается с недостатком технических возможностей и опыта для противодействия им.

На глобальном уровне на эти проблемы давно обратили внимание. В 2019 г. принята резолюция Генассамблеи ООН №74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». 26 мая с.г. одобрена резолюция ГА ООН, запускающая работу специального межправительственного комитета открытого состава для разработки всеобъемлющей конвенции о противодействии использованию ИКТ в преступных целях.

К вопросу израильской стороны (о «совместимости» с Будапештской конвенцией)

Сотрудничество по вопросам противодействия информпреступности осуществляется в рамках различных региональных объединений, например в АРФ, куда входят в том числе страны, присоединившиеся к Конвенции Совета Европы по киберпреступности (Будапештской конвенции).

В частности, в состоявшемся в этом году семинаре АРФ по противодействию информпреступности (организаторы – Россия, Вьетнам, Китай) в качестве слушателей приняли участие представители США, ЕС и Канады.

Unofficial translation

Talking Points for the CICA
Special Working Group Meeting
(May 27, 2021, online)

Paragraph 2.2.4

1. It is inappropriate to combine economic crimes and ICT-related crimes in one subparagraph 2.2.4 since **the problem of the use of ICTs for criminal purposes has more to do with security rather than with economics**.

2. The wording proposed in subparagraph 2.2.4 overlaps with subparagraphs 2.2.5 and 2.2.6 and therefore seems redundant.

3. In developing the section on security of and in the use of ICTs of the CICA Catalogue of Confidence Building Measures **the terminology enshrined in the relevant key UN documents**, in particular, UN General Assembly resolution 75/240 of December 31, 2020, entitled "Developments in the field of information and telecommunications in the context of international security" should be followed. Thus, the use of "cyber" vocabulary should be abandoned in favor of ICT language.

Paragraphs 2.2.7-2.2.9

1. Issues of **conflict and crisis prevention** related to the security of and in the use of ICTs and **confidence-building** in this area have been an important part of the discussion within the UN for more than twenty years. The achievements are reflected, *inter alia*, in Resolution 75/240 mentioned above and in the report by the UN Open-Ended Working Group on international information security adopted on March 12 this year.

2. Discussions on **ICT-related terminology** are underway within various regional platforms, such as the Organization for Security and Cooperation in Europe (OSCE) and the ASEAN Regional Forum on Security (ARF). This topic is expected to become one of the focal points in the work of a new UN open-ended working group.

3. Promoting cooperation to **respond to the criminal use of ICTs** (subparagraph 2.2.9). Individuals, businesses and governmental structures are increasingly vulnerable to ICT-related crimes with their impact becoming more devastating. Due to transborder nature and scale of these challenges, no State can cope with them alone. Besides, a number of countries lack technical capacity and experience to counter them.

At the global level, these challenges have long been of concern. In 2019, UN General Assembly Resolution No. 74/247 entitled "Countering the use of information and communications technologies for criminal purposes" was adopted. The UN General Assembly resolution that establishes an open-ended ad hoc intergovernmental committee to elaborate a comprehensive convention on countering the use of ICTs for criminal purposes was adopted on May 26, 2021.

Regarding the question of Israel (on "compatibility" with Budapest Convention)

Cooperation on combating the use of ICTs for criminal purposes has been developed within other regional organizations, such as the ARF which includes, *inter alia*, the countries that have acceded to the Council of Europe Convention on Cybercrime (Budapest Convention).

In particular, this year the United States, the EU and Canada attended an ARF workshop on countering the use of ICTs for criminal purposes organized by Russia, Vietnam and China.