PC.DEL/887/22
16 June 2022

Original: RUSSIAN

1378th Meeting of the Permanent Council
16 June 2022
Russian Federation on large-scale cyberattacks against Russia

**ПОСТОЯННОЕ ПРЕДСТАВИТЕЛЬСТВО
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРИ ОРГАНИЗАЦИИ ПО БЕЗОПАСНОСТИ
И СОТРУДНИЧЕСТВУ В ЕВРОПЕ**

**PERMANENT MISSION
OF THE RUSSIAN FEDERATION
TO THE ORGANIZATION FOR SECURITY
AND CO-OPERATION IN EUROPE**

Выступление заместителя Постоянного представителя Российской Федерации М.В.БУЯКЕВИЧА на заседании Постоянного совета ОБСЕ 16 июня 2022 года

О массированных кибератаках на Россию

Господин Председатель,

Тематика международной информационной безопасности с самого начала ее появления на международной арене являлась объединительной темой. Первая резолюция на этот счет, принятая в 1998 году по инициативе России, обратила внимание мирового сообщества на угрозы, исходящие из виртуального пространства. По предложению Москвы был создан первый профильный дискуссионный механизм – Группа правительственных экспертов ООН. Широкий интерес стран к проблематике безопасности в сфере использования ИКТ обусловил запуск в 2018 году – опять же по инициативе российской стороны – Рабочей группы ООН открытого состава, которая расширила состав стран-участниц, а также привлекла к своей работе представителей бизнеса, научно-академических кругов. Удалось реализовать и другую нашу идею – запустить Спецкомитет ООН по разработке универсальной конвенции по борьбе с информационной преступностью. Разумеется, важной вехой стало и формирование здесь, в ОБСЕ по нашему настоянию комплекса мер доверия с целью наращивания межгосударственного сотрудничества, транспарентности, предсказуемости и уменьшения рисков ошибочного восприятия, эскалации и конфликтов, которые могут возникать в результате использования ИКТ. Все это позволило мировому сообществу двигаться навстречу единому пониманию правил поведения в данной сфере и преодолению возникающих угроз.

Однако вот уже более 20 лет, особенно это заметно в последние месяцы, главной преградой на пути успеха международных переговоров и достижения реального прогресса по формированию справедливого международно-правового режима регулирования информпространства является позиция стран Запада. США и их союзники изначально выбрали путь утверждения права сильного, насаждения односторонних правил, которые не только не нацелены на предотвращение конфликтов

и преступных деяний, но и фактически всячески их поощряют, чтобы скрыть свои наступательные операции и закрепить всеми правдами и неправдами доминирование в области международной информационной безопасности. Вместо фактов и конструктивных переговоров американская сторона выбрала язык необоснованных и ничем не подкрепленных обвинений, грубейших фальсификаций и односторонних санкций.

Господин Председатель,

Мы обеспокоены продолжающимся экспонентным ростом компьютерных атак на информационную инфраструктуру России с территории отдельных государств-участников, прежде всего США, Украины и ряда стран-членов ЕС. Ведется методичная работа по милитаризации виртуального пространства, предпринимаются безответственные попытки превратить его в арену межгосударственного противостояния, многократно увеличивая угрозу масштабной конфронтации с непредсказуемыми последствиями.

Этому способствует разработка западными странами, прежде всего США, инструментов проведения кибернападений на критически важную инфраструктуру других государств. Примеры их прикладного использования, к сожалению, многочисленны. Мощнейшим атакам наша страна подвергалась при проведении таких знаковых мероприятий, как Зимняя Олимпиада в Сочи в 2014 году, Чемпионат мира по футболу в 2018 году, в ходе выборных процессов, в частности в Государственную Думу Российской Федерации в 2021 году. Подавляющая часть нападений совершалась, по имеющейся информации, с территории США. Важен и тот факт, что к этим незаконным и опасным акциям привлекались и хакерские группировки из других стран.

С февраля 2022 года проводятся скоординированные массированные DDoS-атаки на Россию, в которых на регулярной основе принимают участие свыше 65 тысяч «доморощенных хакеров» из США, Украины, Польши, Германии, Грузии и других стран. В противоправных операциях задействованы 22 хакерские группировки, наиболее активные – IT-army of Ukraine (Украина), GhostClan (США), GNG (Грузия), Squad303 (Польша). В этих целях активно задействуется программное обеспечение на базе серверов компаний-поставщиков Hetzner (ФРГ) и DigitalOcean (США), специализированные платформы War.Apexi.Tech, Ben-Dera.com, онлайн-мощности серверов IPstress.in и Google. Под ударом оказались не только информационные ресурсы российских госорганов, но и многочисленных компаний, в т.ч. «Яндекса», «Сбербанка», «Газпрома», «Лукойла», авиакомпаний «Россия», «Аврора», «Ямал», NordStar, Smartavia, «Якутия».

Отдельного упоминания заслуживает недавнее высказывание вице-премьера, министра цифровой трансформации Украины Михаила Федорова в интервью испанской газете «El Pais». Он с помпой объявил о создании первой в мире «киберармии из 300 тысяч хакеров». Иными словами, происходит массовая мобилизация киберпреступников под задачу подрыва работы критической и социальной инфраструктуры России. Такого рода «цифровые интервенции» могут привести к нарушению функционирования государственных учреждений, предприятий сферы здравоохранения, транспорта, финансовых и энергетических секторов и иметь пагубные последствия для граждан нашей страны. Фактически речь идет о поощрении «технологического терроризма». Убеждены, что подобный киберфронт невозможно «поставить под ружье» сиюминутно и собственными силами – очевидно, его подготовка при внешнем техсодействии велась уже длительное время. Не вызывает сомнений, что этих хакеров не удастся демобилизовать по команде, а полученные ими навыки боевого применения ИКТ приведут к еще большей дестабилизации и разрастанию хакерской угрозы в Европе и по всему миру.

В завершение хотелось бы напомнить, что мы выступаем за сохранение мира и безопасности в информационном пространстве в полном соответствии с общепризнанными принципами и нормами международного права, закрепленными в Уставе ООН, в частности, неприменения силы или угрозы силой, невмешательства во внутренние дела других государств, уважения государственного суверенитета и другими. По-прежнему считаем важной разработку правил, норм и принципов ответственного поведения государств в сфере использования ИКТ и придания им юридически обязывающего характера с целью предотвращения межгосударственных конфликтов в цифровой сфере. Следует активнее задействовать имеющийся в ОБСЕ инструментарий мер доверия по нивелированию возникающих угроз – даже в условиях, когда усилиями отдельных западных стран это доверие сильно подорвано.

Благодарю за внимание