

[А.И. Смирнов](#) Президент Национального института исследований глобальной безопасности, Генеральный директор Национальной Ассоциации международной информационной безопасности, д.ист.н., профессор МГИМО МИД России, Чрезвычайный и Полномочный Посланник РФ в отставке

Человечество переживает тотальную ломку миропорядка. Подрывную роль в данном процессе и десоверенизации государств играют информационно-коммуникационные технологии (ИКТ) и инфогенный нарратив в целом¹. При этом пандемия COVID-19 стала триггером как многих преимуществ цифровизации, так и угроз, сопоставимых с Великой депрессией и даже с вызовами времен Второй мировой войны.

На смену пятому технологическому укладу – микроэлектронике – драйвером цифровизации пришел шестой уклад: нано, -био, -инфо – и когнитивные технологии, вызвавшие поистине тектонические сдвиги в развитии цивилизации. По сути, человечество вступило в новый фазовый переход, сравнимый по значению, например, с созданием письменности.

На основе шестого уклада, или Industry IV стремительно развивается цифровая экономика, киберфизические системы, искусственный интеллект, квантовые вычисления, блокчейн, связь поколения 5G и иные прорывные технологии, кардинально меняющие мир.

В данном контексте приобретает особый смысл выражение «история войн – это история технологических прорывов». В этих условиях ведущие страны разрабатывают и реализуют разнообразные доктрины и стратегии по внедрению данных технологий с целью получения решающего геополитического доминирования и десоверенизации противника.

Рассмотрим так называемое когнитивное оружие.

В силу этого неопределимое значение в обеспечении стратегической стабильности имеют

новые «Основы государственной политики в области международной информационной безопасности»[

2].
Данный документ направлен на продвижение российских подходов к формированию системы обеспечения международной информационной безопасности (МИБ) и российских инициатив в этой сфере, на содействие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве.

Мне очень приятно и вместе с тем ответственно сообщить, что Президент В. Путин при рассмотрении проекта «Основ...» на заседании Совета Безопасности России 26 марта 2021 г. отметил роль нашей Ассоциации: «...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.»

Подчеркну, что согласно Уставу Ассоциации, созданной в 2018 г., одной из важнейших задач является проработка в упреждающем режиме проблемных вопросов обеспечения

МИБ в интересах формирования переговорных позиций государственных органов[3].

Наряду со многими международными конференциями по проблематике МИБ члены НАМИБ сделали сотни докладов, опубликовали десятки статей, приняли участие в выпуске учебника «Международная информационная безопасность: теория и практика» в трех томах, который переиздан в 2021 г. и т.д.

Вернемся к Основам госполитики в области МИБ. В Основах 2013 г. на период до 2020 г. основными угрозами использования ИКТ для МИБ были определены следующие четыре⁴
:

а) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной

целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

б) в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привле-

чения к террористической деятельности новых сторонников;

в) для вмешательства во внутренние дела

суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

г) для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ.

В «Основах», утвержденных указом Президента России 12 апреля 2021 г. No 213, вышеупомянутые угрозы были уточнены и дополнены еще двумя[5]:

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

- использование ИКТ для проведения

компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру.

Особое агрессивное воздействие на Россию и её союзников оказывается со стороны США и их сателлитов. Данный постулат подтверждается, в частности, недавним докладом «НАТО 2030: сделать сильный альянс еще сильнее»⁶, который на июньском саммите альянса был нацелен на усиление гибридного воздействия на Россию и её союзников: политико-дипломатического, экономического, военного и информационного. Как уже отмечалось, ключевую роль в манипулировании массовым сознанием в так называемой «ментальной войне» играют центры НАТО в Риге, Таллине, Варшаве. Рассмотрим как данную проблему видит Европейский центр передового опыта по противодействию гибридным угрозам, базирующийся в Хельсинки. Это межпра-

[6] URL: <https://www.nato.int/nato2030/> (дата обращения 23.08.2021)

вительственный аналитический центр, который занимается анализом реагирования на гибридные угрозы под эгидой Европейского союза и НАТО.

Сами за себя говорят и названия последних «трудов» Центра стратегических коммуникаций НАТО в Риге.

Резюмируя, приходится констатировать, что резко вырос подрывной потенциал прорывных технологий для глобальной стабильности и особенно на треке ментальных войн.

Спасибо за внимание!

