А.И. Смирнов,
Национальная Ассоциация международной информационной безопасности, Национальный институт исследований глобальной безопасности, Россия

НОВЕЙШИЕ ИКТ КАК ФАКТОР ГЛОБАЛЬНОЙ НЕСТАБИЛЬНОСТИ: КАК ДОСТИЧЬ КИБЕР МОДУС ВИВЕНДИ[1]?

Уважаемые коллеги!

Человечество входит в зону тотальной ломки миропорядка. По оценкам многих экспертов, подрывную роль в этой, столь важной для цивилизации проблеме играет инфогенный нарратив. Осознав данную угрозу, Россия еще в 1998 году инициативно внесла в ООН свои предложения, которые были приняты Генассамблеей в резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Об этом вчера убедительно прозвучало в выступлениях В.П. Шерстюка, А.В. Крутских, С.М. Бойко и других ораторов.

В действующей Стратегии национальной безопасности подчеркнуто, что проведение Россией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее гибридного воздействия: политического, экономического, военного и информационного.

Рассмотрим информационный фактор. Только за последние два года можно привести целый ряд действий США и их партнеров по использованию ИКТ в силовом сценарии воздействия на Россию. Приведу лишь наиболее известные:

- отказ от взаимодействия с Россией по предотвращению инцидентов в ИКТ-среде, предусмотренного совместным заявлением президентов России и США (2013 год);
- записка Б.Обамы Д.Трампу о закладке в объекты критической информационной инфраструктуры России так называемых кибербомб для подрыва экономической и социальной стабильности российского общества;
- разработка ЦРУ маскировочных программных средств проведения компьютерных атак, в том числе под «чужим флагом»;
- указание в Стратегии национальной безопасности США (2017 год) на Китай и Россию как ревизионистские силы, которые используют технологии, пропаганду и принуждение, чтобы сформировать мир, противоречащий интересам и ценностям США;
- принятие 23 марта 2018 г. закона Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (Закон о разъяснении законного использования данных за рубежом), который упростил спецслужбам США получение данных с оборудования, поставленного фирмами США в любую страну;
- отмена 16 августа 2018 г. Д. Трампом правил по кибератакам, утвержденных директивой Б. Обамы;
- принятие в сентябре 2018 г. Национальной киберстратегии США и киберстратегии Пентагона, позволяющих кибераграссию и названных экспертами «преамбулой войны»;
- разработка в начале 2019 г. Пентагоном новой стратегии «Троянский конь»,

1 Модус вивенди (лат., англ. Modus vivendi — образ жизни, способ существования) — дипломатический термин, применяемый для обозначения временных или предварительных соглашений

сутью которой является инспирирование протестов «пятой колонны» в целях дестабилизации обстановки с одновременным нанесением ударов высокоточного и кибероружия по наиболее важным объектам.

Анализ эволюции войн показывает, что вместо оружия все чаще используются небоевые средства, в том числе ИКТ и информресурсы, как главные компоненты современных «гибридных войн». Причина распространения «гибридных войн» понятна – они не требуют объявления войны. При этом США и их сателлиты безуспешно пытаются обвинить Россию и ее союзников в хакерских атаках, дезинформации и пропаганде. Для придания легитимности надуманным обвинениям в проведении кибератак США продвигают новую концепцию «Выяви и Пристыди» (Name and Shame) и настаивают, что группа стран может вынести вердикт виновности в совершении кибератаки. При таком подходе доказательной базой становится «коллективная атрибуция», то есть совместное назначение виновника. Однако технология такой атрибуции не раскрывается и, значит, о достоверности речь не идет. Основным фактором в определении виновного является политический контекст, а аргументом – известный тезис «Хайли лайкли» (Highly likely) – «с высокой вероятностью».

Согласно данным Национального координационного центра по компьютерным инцидентам, на критическую информационную инфраструктуру (КИИ) России в 2018 году было совершено более 4,3 млрд. информационных воздействий.

Общее количество кибератак на КИИ за 6 лет выросло на 57% (число атак резко возрастало при проведении Олимпиады 2014 года в Сочи, чемпионата мира по футболу 2018 года и выборов президента России 2018 года). Согласно анализу зарубежных компаний, основным источником распространения вредоносных программ являются интернет-ресурсы на территории США. При этом способы использования ИКТ для «силового» воздействия на противника стремительно развиваются: все активнее применяется искусственный интеллект, в том числе в смертоносных автономных системах вооружения и военной технике в целом.

К сожалению, в декабре 2018 г. мировое сообщество в ООН при выработке норм и правил ответственного поведения государств в информационном пространстве раскололось. Как подчеркнул вчера при открытии Форума президент НАМИБ В.П.Шерстюк, «когда перестает работать сила права, начинает работать право силы». Россия и другие государства-члены ШОС на 73-й сессии ГА ООН выступили с проектом резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Резолюцию поддержали 119 стран, из которых 32 стали ее соавторами, против проголосовали 46, 14 – воздержались. Именно США и те страны, которые бездоказательно обвиняют Россию в противоправном использовании ИКТ, выступили против, предложив свою резолюцию.

Российская резолюция содержит 13 конкретных норм и правил ответственного проведения государств в ИКТ-среде. Среди правил особого внимания заслуживает п.2: «…Обвинения в организации и совершении противоправных деяний, выдвигаемые против государств, должны быть обоснованными…». От-

сутствие механизмов определения атрибуции кибератаки, то есть «кто стоит за кибератакой», не позволяет применять международное право, что само по себе создает дополнительную угрозу сохранению стратегической стабильности. По мнению ряда экспертов, решение этой проблемы лежит в снижении анонимности ИКТ-сферы, т.е. к обязательной идентификации устройств в мировой сети, в том числе с помощью нового интернет-протокола IPv6. Это позволит уполномоченным структурам государства эффективнее бороться с противоправными деяниями в ИКТ-сфере. Напрашивается вопрос: случайно ли ICANN (институт находится под юрисдикцией штата США) тормозит его внедрение?

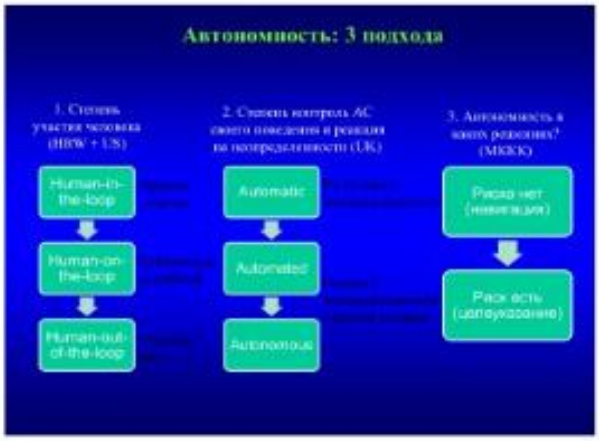
В этих условиях Россия была вынуждена в целях обеспечения безопасного и устойчивого функционирования интернета на своей территории подготовить соответствующий законопроект, вступление в силу которого намечено на 1 ноября 2019 г.

Опасной угрозой является использование глобальной медиасферы для оправдания силовых подходов к разрешению межгосударственных споров и вмешательства во внутренние дела суверенных государств. В последнее время проблема злоупотребления государствами средствами массовой коммуникации для пропаганды идеологического превосходства, особой исторической миссии становится все более угрожающей. Достоверная информация, распространяемая этими странами, активно перемешивается с ложной информацией («фейками»).

Как это видно на примере мифического российского следа в так называемом «деле Скрипалей», заинтересованные государства создают цепочки фейковых новостей, образуя своеобразный «фейк-чэйн». Создание «фейк-чэйнов» имеет целью активное манипулирование международным и национальным общественными мнениями, что создает угрозу международному миру и безопасности. В этом контексте уместно привести слова С.В. Лаврова на конференции в Мюнхене (2017 год) «…мы смогли бы быстро преодолеть период «post-truth», отбросить навязываемые международному сообществу истеричные информационные войны и перейти к честной работе, не отвлекаясь на ложь и вымыслы. Пусть это будет эпоха «post-fake».

В настоящее время у России с НАТО практически нет совпадающей повестки дня в сфере безопасности. НАТО устроено таким образом, что его генетический код постоянно проявляет себя. Эти проявления мы видим и сегодня – поиск врага на Востоке, от которого надо обороняться. На самом деле это абсолютно тупиковый путь.

НАТО, ведомое США, активно применяет гибридные угрозы, в том числе информационные. Центры передового опыта НАТО в Таллинне (киберзащиты), в Риге (стратком) и в Хельсинки (совместно с ЕС – противодействие гибридным угрозам) – тому убедительное подтверждение. Более того, для координации этой работы в НАТО в 2019 году создается Центр кибероперация в г.Монсе (Бельгия). При открытии Центра в Риге в 2015 году отмечалось, что в его арсенале есть средства (армия «умных» ботнетов, роботроллинг, инспирирование «кибербунтов» и т.д.), способные заставить врагов потерять волю к борьбе, возненавидеть собственную страну, и это обеспечит бескровную победу.



Особую роль в НАТО играет Великобритания, где создан новый Центр не только для противодействия киберугрозам, но и проведения наступательных операций. В ноябре 2018 г. хакеры из группировки Anonymous выложили документы о деятельности Института государственного управления Integrity Initiative, который Великобритания использовала для вмешательства во внутренние дела других стран, в том числе для информационной войны против России. Примечательно, что после публикации проекта «противостояние России» в ответ на ноту посольства России, он был признан Форин Офисом. Судя по всему, Великобритания не сделала выводов из скандала (2018 год) с компанией Cambridge Analytica, которая использовала технологии глубинного анализа, в том числе данных соцсетей, взятки и компромат, вмешиваясь в ход выборов в десятках стран мира.

Североатлантический альянс активизировал координацию своих мероприятий с киберпроектами ЕС. По аналогии с центром «Стратком» НАТО в Риге ЕС в 2015 году создал Оперативную рабочую группу по стратегическим коммуникациям. Группа (400 экспертов из 30 стран) выпускает еженедельно по сути русофобский «Обзор дезинформации» с оговоркой, что он не отражает позиции ЕС. Анализ обзоров показывает их примитивно фейковый уровень и политизированную «охоту на киберведьм».

Резюмируя, приходится констатировать, что дальнейшее промедление с разработкой и принятием Модуса вивенди – временного или предварительного соглашения по правилам ответственного поведения государств в ИКТ-сфере – смерти подобно.

Потомки нам этого не простят!

Спасибо за внимание!