**1.Что такое кибертерроризм?**

Определить понятие «компьютерный терроризм» – достаточно трудная задача, поскольку нелегко установить четкую границу для отличия его от информационной войны и информационного криминала. Еще одна трудность состоит в том, что необходимо выделить специфику именно этой формы терроризма.

Само понятие «кибертерроризм» образовано слиянием двух слов: «кибер» («киберпространство») и «терроризм». В русскоязычной литературе все чаще встречаются термины «виртуальное пространство», «виртуальный мир», что обозначает моделируемое с помощью компьютера информационное пространство, в котором существуют определенного рода объекты или символьное представление информации – место, в котором действуют компьютерные программы и перемещаются данные.

Исходя из основного понятия терроризма и сочетания его с виртуальным пространством, можно вывести следующее определение.

Кибертерроризм – это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта. Одним из способов кибертерроризма является политически мотивированная атака на информацию. Она заключается в непосредственном управлении социумом с помощью превентивного устрашения. Это проявляется в угрозе насилия, поддержании состояния постоянного страха с целью достижения определенных политических или иных целей, принуждении к определенным действиям, привлечении внимания к личности кибертеррориста или террористической организации, которую он представляет .Казалось бы, кибертерроризм угрожает в большей мере высокоразвитым в технологическом плане странам, например США. Но это только на первый взгляд. Мы уже могли наблюдать, как интенсивно развивается всемирная сеть Интернет, и какова динамика у компьютерной преступности. Ни в коем случае нельзя умолять его значения и для России.

Террористы поддерживают свою деятельность другими преступлениями, совершенными через Интернет, например, получают доступ к базам кредитных карт или совершают различные формы прибыльного мошенничества. Информационные технологии также облегчают множество действий террористов и транснациональных преступных групп – от финансирования до создания необходимых документов. С помощью компьютерных технологий организованные преступные группы способны создать подложные документы, удостоверяющие личность, документы, свидетельствующие о ведении какой-либо деятельности, служащей прикрытием для их операций. Использование информационных технологий преступниками и террористами происходило одновременно с ростом их легального использования международным сообществом..

**2. Проявление кибертерроризма и его отличия от терроризма**

Терроризм, террористы, террористическая деятельность – эти понятия практически ежедневно появляются в средствах массовой информации и наводят страх и ужас на население. Терроризм противоречит основным положениям Всеобщей декларации прав человека 1948 г. и Европейской конвенции по правам человека 1950 г. Однако до сих пор ученые спорят по поводу теоретической сущности этого явления. Проблема теоретического осмысления терроризма стоит буквально со времени проявления этого феномена в общественно-политической жизни. Так, по мнению американского политолога А. Кассиса, существует более ста определений терроризма. Анализ существующих подходов к определению сущности терроризма показывает, что большинство ученых мира видят этот феномен как выражение недовольства существующим социально-политическим положением, нарушающее правовые основы жизнедеятельности и связанное с идеологическим и психологическим самовыражением. При этом каждый из исследователей в соответствии со своей научной приверженностью делает главный акцент на одном из этих оснований. Так, терроризм в качестве особой формы насилия определяется как сознательное и целенаправленное использование кем-либо насилия или угрозы насилия для принуждения политического руководства страны к реализации политических, экономических, религиозных или идеологических целей террористической организации.

Важным фактором природы и мотивации терроризма является то, что акт терроризма предполагает эмоциональное воздействие на общественное мнение, порождает в обществе страх, панические настроения, ведет к потере доверия к власти и в конечном счете вызывает политическую нестабильность. Однако не любой акт терроризма можно классифицировать как политический. Применение экстремистского насилия может наблюдаться и в криминально-экономическом мире: разборки бандитских группировок, запугивание конкурентов, вооруженное ограбление в целях обогащения и т.д. Ограбление же с использованием методов терроризма, имеющее конечной целью финансирование деятельности какого-либо политического движения, также может рассматриваться как политический терроризм.

В настоящее время практически для всех стран возросла угроза новой формы терроризма – кибертерроризма. Казалось бы, почему мы не можем квалифицировать действия террористов по существующей статье УК?

В Законе о борьбе с терроризмом приведено понятие терроризма. Что касается природы кибертерроризма, то он качественно отличается от общепринятого понятия терроризма, сохраняя лишь стержень этого явления и признаки. Однако имеются примеры кибератак, находящихся на грани с реальным терроризмом. Например, случай использования программных средств для произведения взрыва на Ингналинской АЭС. По сути, это и есть акт кибертерроризма, поскольку он реализован через информационную систему и информационными средствами. Но этот факт наглядно показывает потенциальные возможности терроризма вообще, формы его проявления.

Действительно, гораздо легче нанести большой вред, используя в преступном арсенале клавиатуру и мышь, нежели взрывное устройство, например бомбу. Трудности состоят лишь в определении его понятия. Порой очень сложно отделить сам кибертерроризм от акций информационной войны, информационного оружия, информационного криминала или преступлений в сфере компьютерной информации. Дополнительные трудности могут возникнуть при попытке выявить специфику этой формы терроризма. Так, психологический и экономический аспекты кибертерроризма тесно переплетены, и невозможно определить, какой из них имеет большее значение. Эта неопределенность говорит о новизне явления.

Информационный криминал – это действия отдельных лиц или групп, направленные на взлом системы защиты, на хищение или разрушение информации в корыстных или хулиганских целях. Это, как правило, разовые преступления против конкретного объекта киберпространства.

Информационный терроризм отличается от этих форм воздействия на киберпространство прежде всего своими целями, которые остаются свойственными политическому терроризму. Средства осуществления информационно-террористических действий могут варьироваться и включать все виды современного информационного оружия. В то же время тактика и приемы его применения существенно отличаются от тактики информационной войны и приемов информационного криминала. Главное в тактике информационного терроризма состоит в том, чтобы акт Терроризма имел опасные последствия, стал широко известен населению и получил большой общественный резонанс. Как правило, требования сопровождаются угрозой повторения акта без указания конкретного объекта.

Основной формой кибертерроризма является информационная атака на компьютерную информацию, вычислительные системы, аппаратуру передачи данных, иные составляющие информационной инфраструктуры, совершаемая группировками или отдельными лицами. Такая атака позволяет проникать в атакуемую систему, перехватывать управление или подавлять средства сетевого информационного обмена, осуществлять иные деструктивные воздействия. Эффективность же форм и методов кибертерроризма зависит от особенностей информационной инфраструктуры и степени ее защищенности. Но в чем проявляется кибертерроризм или какова его тактика воздействия в глобальной сети Интернет? Если говорить о видах воздействия или о различных приемах кибертерроризма, то к ним можно отнести:

- нанесение ущерба отдельным физическим элементам информационного пространства (разрушение сетей электропитания, наведение помех, использование химических средств для разрушения элементной базы и др.);

- кражу или уничтожение информационного, программного и технического ресурсов, имеющих общественную значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок и т.п.;

- воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления;

-раскрытие и угрозу опубликования или само опубликование закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодах шифрования, принципах работы систем шифрования, успешном опыте ведения информационного терроризма и др.;

-захват каналов средств массовой информации с целью распространить дезинформацию, слухи, продемонстрировать мощь террористической организации и объявить свои требования;

-уничтожение или активное подавление линий связи, неправильную адресацию, искусственную перегрузку узлов коммутации;

-проведение информационно-психологических операций;

-ложную угрозу акта кибертерроризма, влекущую за собой серьезные экономические последствия;

-уничтожение или активное подавление линий связи, неправильное адресование, искусственную перегрузку узлов коммутации и др.;

- воздействие на операторов, разработчиков информационных и телекоммуникационных сетей и систем путем насилия или угрозы насилия, шантаж, подкуп, использование нейролингвистического программирования, гипноза, средств создания иллюзий, мультимедийных средств для ввода информации в подсознание или ухудшения здоровья человека и др.

Теоретически можно блокировать работу, например, метрополитена любого крупного города. Учитывая то, что основная масса населения добирается до места работы на метро, на некоторое время город будет попросту парализован. Повсеместное отключение электроэнергии и, как следствие, отключение компьютерных систем – также вполне реальная угроза.

Вполне возможно и проникновение в локальные сети, изменение или уничтожение информации, блокирование работы компьютеров, какого-либо государственного учреждения.

Все это позволяет сегодня говорить, что террористическая плоскость переходит из реального пространства в пространство виртуальное.

**3. Кто и почему совершает акты кибертеррора**

Рост информационных технологий дает террористам возможность получить существенную прибыль при относительно низком риске. Они могут финансировать свою деятельность, не обращаясь к силовым нападениям или грабежам банков, которые увеличили бы риск обнаружения. Террористы весьма активно используют информационные ресурсы для решения организационных и финансовых вопросов, обеспечения связи, планирования актов терроризма и осуществления контроля над их проведением.

Сеть Интернет может быть использована транснациональными террористическими организациями для тщательного изучения своих новых кандидатов, ведения пропаганды, минуя контроль со стороны государственных органов, вывода из строя правительственных компьютерных сетей и пр. В настоящее время практически все более или менее крупные исламистские организации, в том числе радикального толка, имеют свои сайты в Интернете. В сети существует масса сайтов, на которых детально излагаются рецепты и схемы изготовления оружия и взрывчатых веществ из подручных материалов, способы их использования и т.д. Многочисленные чаты и форумы, существующие в Интернете, идеально приспособлены для передачи зашифрованных посланий, а современные технологии позволяют легко распространять в сети карты и фотографии.

Для кибертерроризма характерно и то, что все известные сегодня хакерские группы и отдельные лица не стремятся афишировать свои данные и выступают исключительно под псевдонимом. При этом следует отличать хакера-террориста от простого хакера, компьютерного хулигана или компьютерного вора, который действует в корыстных или хулиганских целях. Но если действия членов этой организации приведут к тяжким последствиям, например, к гибели людей, то подобного рода хулиганство нельзя расценивать иначе как терроризм. Главное в тактике кибертерроризма состоит в том, чтобы это киберпреступление имело опасные последствия, стало широко известно населению, получило большой общественный резонанс и создавало атмосферу угрозы повторения акта без указания конкретного объекта. Так, руководители ряда радикальных мусульманских организаций Ближнего Востока придают все большее значение использованию в своей деятельности именно современных информационных технологий, рассматривая их в качестве эффективного оружия в борьбе с режимами Израиля, Саудовской Аравии и поддерживающими их западными странами. Это, во-первых, достаточно недорогое средство совершения акта терроризма (поэтому к кибертерроризму прибегают в основном страны с неразвитой экономикой страны), а во-вторых – сложное пространство для выявления самого террориста. Наиболее активно методы информационного воздействия применяет террористическое движение «Хезболла», руководство которой рассчитывает таким образом нанести Израилю больший ущерб, чем при проведении обычных боевых операций. В структуре «Хезболлы» выделена группа программистов, в задачи которой входит создание и обновление веб-страницы в Интернете для пропаганды проводимых организацией акций и доведения направленной информации до израильтян.

Большое внимание «Хезболла» придает таким традиционным методам, как воздействие на аудиторию через средства массовой информации. Для вещания на территории Южного Ливана и Северного Израиля задействованы принадлежащие организации радио- и телевизионный каналы. Помимо материалов агитационного характера по ним регулярно демонстрируются записи, сделанные при проведении боевых операций против израильских войск и армии Южного Ливана. По оценке специалистов «Хезболлы», трансляция подобных передач способствует снижению боевого духа военнослужащих противника, появлению у них упаднических настроений.

По мнению аналитиков, большинство транснациональных террористических организаций придерживаются рационального подхода, добиваясь прежде всего политических целей и используя тактику террора в надежде на общественное признание законности своей борьбы. К ним применимы превентивные меры информационно-психологического и пропагандистского воздействия. Так, известная экстремистская организация «Хамас» приостановила проведение актов терр

Но существуют организации, которые действуют по совершенно иной логике. К ним, в частности, относятся Аум Синрике и «Аль-каида». Руководители этих организаций, обладая так называемой манией величия и являясь (мягко говоря) безжалостными людьми, действуют исключительно со своими собственными убеждениями и верят, что проводимые ими акты терроризма либо радикально изменят ход истории, либо их позднее оправдает сама история. По мнению экспертов, на таких террористов не оказывают какого-либо воздействия пропагандистская и психологическая составляющие информационных мер противодействия. Здесь потребуется использовать весь арсенал имеющихся сил и средств, консолидировать государственные и общественные структуры для выявления и пресечения террористической деятельности.

В 2006 году по решению Кунцевского суда была депортирована из России гражданка США М. МаКри, которая, по представленным материалам ФСБ России, разрабатывала конкретные планы по взрывам Голливуда и ряда государственных учреждений США, активно пыталась вступить в контакт посредством Интернета с лидерами известных мусульманских террористических организаций. Для организации подобных кибератак необходима значительно большая квалификация их исполнителей, так как в ряде случаев кибертеррористические действия могут оказаться более предпочтительными, чем акты обычного терроризма. Проведение кибератак обеспечивает высокую степень анонимности и требует большего времени реагирования. Выработка методов антитеррористической борьбы лежит прежде всего в области противодействия обычному терроризму. Осуществление атаки через информационные системы вообще может оказаться нераспознанным как акт терроризма, а будет воспринято, например, как случайный сбой системы.

Таким образом, угроза кибертерроризма в настоящее время является очень серьезной проблемой. Ее актуальность будет возрастать по мере развития и распространения информационно-телекоммуникационных технологий.

Примерами таких кибератак являются:

-Армения – Азербайджан. В феврале 2000 г. армянские хакерские группы Liazor (уполномоченные), предприняли компьютерную диверсию против 20 сайтов правительственных организаций и средств массовой информации Азербайджана в системе Интернет (действия осуществлялись с территории Армении, России, США). Армянские хакеры США создали и внедрили специальную компьютерную программу «Synergy Internet Systems» обеспечивающую негласный перехват и снятие информации с компьютеров. Одна из групп в составе трех человек была вскрыта и задержана 4 февраля 2000 г. полицией в Лос-Анджелесе.

-Россия – Чечня. С 1999 г. предпринимаются усилия по блокированию и подавлению работы зарубежных порталов чеченского сепаратистского движения. Только в течение одной недели в конце апреля – начале мая 2002 г. портал «Кавказ» подвергся 140 атакам (в том числе массированным DOS – атакам).

-Югославия – США (НАТО). Весной 1999 г. в период боевых действий зафиксированы скоординированные действия югославских хакеров, направленные на блокирование компьютерных сетей управления группировки ОВС НАТО в Италии, а также политически мотивированные вторжения в сетевые порталы штаб-квартиры НАТО, Минобороны США, ряда других структур. Отслеживались также действия третьих сторон в контексте конфликта вокруг Косово (греческие хакерские группы студентов университетов г. Афины, Салоники, Кания согласованными действиями проникли в систему компьютерного центра ВС США на военном объекте в штате Аризона).

**4.Направления актов кибертерроризма**

Нет общего мнения по поводу определения объекта актов терроризма. Причем мнение колеблется от межгосударственной направленности, когда объектом становятся не только отдельные международные организации, но и целые государства, народы, до узкогрупповой, даже личностной, когда объектом становится конкретное лицо (политический или государственный деятель) либо случайное лицо. Действия кибертеррористов могут быть направлены как на гражданские, так и на военные объекты.

По мнению американских экспертов, наиболее уязвимыми точками инфраструктуры являются энергетика, телекоммуникации, авиационные диспетчерские, финансовые электронные и правительственные информационные системы, а также автоматизированные системы управления войсками и оружием. Так, в атомной энергетике изменение информации или блокирование информационных центров может повлечь за собой ядерную катастрофу или прекращение подачи электроэнергии в города и на военные объекты. Искажение информации или блокирование работы информационных систем в финансовой сфере может иметь следствием экономический кризис, а выход из строя, скажем, электронно-вычислительных систем управления войсками и оружием – непредсказуемые необратимые последствия. Так, цели, на которые направлены атаки кибертеррористов, соответствуют национальной информационной инфраструктуре. Это:

-оборудование, включая компьютеры, периферийное, коммуникационное, теле, видео и аудиооборудование;

-программное обеспечение;

-сетевые стандарты и коды передачи данных;

-информация как таковая, которая может быть представлена в виде баз данных, аудио-, видеозаписей, архивов и др.;

- люди, задействованные в информационной сфере.

Следует выделить первые три цели, так как они взаимосвязаны и едва ли могут рассматриваться отдельно. Физические компоненты инфраструктуры представляют собой комплекс аппаратных средств (оборудования) и программного обеспечения, работающий по согласованным и унифицированным стандартам. Таким образом, эти объекты можно рассматривать как своего рода служебную структуру, обеспечивающую работоспособность всей информационной структуры. Мишенями кибертеррористов могут стать как гражданские, так и военные объекты.

Возможность захвата систем управления военными спутниками, наведения и запуска ракет, а также комплексами противовоздушной обороны уже давно существует. Примером может служить вывод из строя комплексов противовоздушной обороны Ирака во время операции «Буря в пустыне». Закладки, заложенные в комплексах противовоздушной обороны, стоявших на вооружении Ирака и купленных в основном в Европе, блокировали нормальную работу систем, и американские воздушные силы смогли практически беспрепятственно проникнуть в воздушное пространство этой ближневосточной страны.

Целью кибертеррористов может стать как выведение из строя информационных систем, так и разрушение объектов информационных систем. Выведение из строя информационных систем характеризуется прежде всего тем, что именно такие атаки наиболее распространены. Они направлены на выведение из строя отдельных интернет-служб или переадресацию информации. Такие кампании осуществляются чаще всего так называемыми временными кибертеррористами – частными лицами, не связанными напрямую с террористическими группами, однако разделяющими их идеи.

Еще одна цель кибертеррористических атак – разрушение объектов информационных систем. Это может привести к уничтожению информационных ресурсов и линий коммуникаций либо к физическому уничтожению структур, в которые включаются информационные системы. Если же системы задействованы в критических инфраструктурах, то при наихудшем развитии событий сетевые информационные атаки могут привести к столь же масштабным последствиям с жертвами, что и традиционные акты терроризма.

**5.Воздействие кибертерроризма на международную информационную безопасность**

Информация, играющая решающую роль в функционировании как государственной власти, так и общественных институтов, становится самым слабым звеном национальной инфраструктуры государства на современном этапе развития, поэтому проблема международного терроризма приобретает в условиях информационного противостояния новое звучание. Это связано прежде всего с двумя аспектами: 1) с использованием террористами информационной инфраструктуры для развития так называемых сетевых способов собственной организации и 2) с прямым террористическим воздействием на объекты информационных инфраструктур.

В сфере международных отношений терроризм представляет прежде всего острую угрозу для международной безопасности, поскольку подвергает опасности стабильность и мирный характер во взаимоотношениях между отдельными государствами, а также группами государств, провоцирует напряженность в отношениях между ними, нередко способствует разжиганию опасных международных конфликтов, препятствует их разрешению. Терроризм на международной арене выступает и как инструмент вмешательства во внутренние дела государств, дезорганизует международные связи, грубо нарушает права человека, международный правопорядок. Вот почему следует проблему терроризма рассматривать на международном уровне как прямую угрозу международной безопасности, а угрозу кибертерроризма – как вторую составляющую такого рода угроз.

Что же касается международной информационной безопасности («состояние международных отношений, препятствующее нарушению международной стабильности и возникновению угрозы безопасности государств и международного сообщества в сфере информации») и прямой угрозы ей со стороны кибертерроризма, то тут следует говорить прежде всего о трансграничности виртуального пространства. Как мы можем наблюдать, инфраструктура телекоммуникаций является полем для международного общения и международных отношений. Экономическая и научно-техническая политика подключения государства к мировым открытым сетям должна предусматривать защиту национальных информационных сетей от кибертерроризма. Понимание государствами важности этого вопроса можно проследить и в сфере международного права. Восемь ведущих государств мира, включая Россию, приняли Окинавскую хартию глобального информационного общества от 22 июля 2000 г., по которой в целях развития глобального информационного общества предлагается предпринять «согласованные действия по созданию безопасного и свободного от преступности киберпространства». Глобализация инфосферы с развитием средств трансграничной передачи информации является предпосылкой к увеличению роли международного права в регулировании информационного обмена, поэтому угроза международной информационной безопасности в лице кибертерроризма приобретает все больший размах.

Разрешение проблемы кибертерроризма важно при международной информационной безопасности. Существует трудность создания и сохранения коалиций при международном сотрудничестве. Так, с началом серьезного информационного акта терроризма прочность коалиций государств подвергается большому испытанию, поскольку все союзники окунутся в «информационный туман». Могут возникнуть и острые проблемы с реализацией совместных планов действий против транснациональной криминальной или террористической организации.

Страны с высокой производительностью в сфере информационных технологий и с низкой способностью противостоять преступлениям, совершенным с помощью компьютеров и телекоммуникационных технологий, становятся приютом для транснациональной преступности и терроризма. Понятие зоны безопасности приобретает иное значение, когда вместо обычного оружия используются информационные технологии, позволяющие организовать заговор, финансировать и, возможно, даже исполнять серьезные преступления.

Действительно, международный терроризм, перешедший в сферу информационно-коммуникационного поля, не знает границ. Он не имеет ни национальной, ни религиозной принадлежности. Террористы и кибертеррористы – это бросившие вызов культуре, цивилизации, обществу преступники, компромисс с которыми невозможен и которые должны предстать перед судом.

Долг мирового сообщества государств – защитить общество, защитить мир. Вопрос обеспечения информационной безопасности как одной из важных составляющих национальной безопасности государства особенно остро возникает в контексте появления транснациональной трансграничной компьютерной преступности и кибертерроризма.

6**. Основные источники киберугроза**

Россия и Китай – два государства, которые в настоящее время выделяются экспертами стран Запада в качестве основных источников киберугроз. Так, доклад «НАТО и киберзащита» упоминает несколько эпизодов компьютерных атак со стороны России: в апреле 2007 г. состоялась атака на сайты госучреждений Эстонии, в июле 2008 г. – атака литовских сайтов в результате принятия Сеймом закона о запрещении к употреблению на собраниях и митингах на всей территории Литвы символики СССР и приравнивание ее к символике Третьего Рейха, в августе 2008 г. в ходе Южноосетинского конфликта была проведена атака на сайты правительственных структур Грузии, и в ноябре 2008 г. – атака компьютерных сетей Центрального командования США . Что касается Китая, то авторы секретного доклада ФБР, переданного в конгресс США в марте 2010 г., утверждают, что в последние годы Китаю удалось подготовить не менее 180 тысяч кибершпионов (30 тысяч военнослужащих Народной армии и 150 тысяч гражданских специалистов), основной задачей которых является получение оборонной информации. Только в 2009 г. китайские хакеры предприняли около 90 тыс. попыток взлома базы данных военного ведомства США. Кроме того, Китай намерен создать к 2020 г. году «лучшие в мире информационные войска» и пока нет никаких поводов сомневаться в этом утверждении. Самыми известными кибератаками, которые, как считается, были проведены китайцами, являются «Титановый дождь» (атака на базу данных Пентагона) и попытка взлома (насколько она удалась – неизвестно) в 2009 г. самого дорогого проекта Пентагона Joint Strike Fighter .

Кроме того, по мнению аналитиков американской контрразведки, этаким «Троянским конем» являются компьютерные микросхемы китайского производства, которые могут содержать шпионские программы, позволяющие не только копировать, но и отсылать информацию «заказчику». Подобные попытки были зафиксированы в компьютерных сетях Госдепартамента, Министерства торговли, Министерства внутренней безопасности..

**7.Киберугроза и Новая стратегическая концепция НАТО**

Сложность определения настоящего заказчика кибератаки не позволила государствам – членам НАТО в ходе Лиссабонского саммита в ноябре 2010 г. признать кибератаку действием, подпадающим под положения статьи 5, хотя еще в середине 2010 г. группа экспертов НАТО во главе с бывшим госсекретарем США М.Олбрайт в своем докладе пришли к заключению, что компьютерная атака против жизненно важных инфраструктур стран Альянса должна приравниваться к вооруженному нападению, и, тем самым, оправдывает ответный удар военными средствами . Если в концепции 1999 г., не говоря уже о концепции 1991 г. нет ни слова о киберугрозе, то в Новой стратегической концепции НАТО поставила кибертерроризм в число основных угроз, с которыми Альянс может столкнуться уже в ближайшем будущем . Понятие «кибератака» встречается в Новой концепции два раза: в разделе «безопасность», где признается, что «Кибератаки становятся все более частыми, более организованными и более дорогостоящими по размерам ущерба… и могут достичь уровня, который угрожает национальному и евро-атлантическому процветанию, безопасности и стабильности», а также в разделе «Оборона и сдерживание», в котором заявляется, что Альянс «имеет полный набор возможностей, необходимых для сдерживания и защиты от любой угрозы безопасности нашего населения» и будет и дальше «развивать способность предупреждать, выявлять, защищаться и восстанавливаться от кибератак, в том числе с помощью процесса планирования по укреплению и координации национальных возможностей киберзащиты, в результате чего все органы НАТО будут находиться под централизованной киберзащитой…» .

Проблема заключается в том, что создать полностью защищенную и централизованную систему пока не удалось, а уровень опасности и организации кибератак постоянно растет. Тем не менее, члены Альянса продолжают активно разрабатывать эту проблематику, для чего была создана специальная система институтов