УДК 327 (430+510)

М.Ш. Губайдуллина, Д.Карипжанов

Казахский Национальный Университет имени аль-Фараби,
факультет международных отношений, Казахстан, г. Алматы
e-mail: maragu@mail.ru

Кибернетические и сетевые войны: подходы к информационному противодействию (опыт Германии и Китая)

В условиях системного разлома международных отношений информационное противоборство, в частности кибернетические и сетевые войны, приобретают особое значение, сравнимые с «традиционной» войной. Кибер-и сетевые операции направлены либо на защиту своих информационных систем, либо на атаку противной стороны с тем, чтобы затруднить или сделать вообще невозможным принятие им верных решений. Кибервойны не имеют четких национальных и географических границ. Объектом их воздействия оказываются как военные, так производственные и гражданские сети, равным образом политическое и государственное управление. Объектом их воздействия оказываются как военные, так производственные (сфера экономики, хозяйственные объекты) и гражданские сети, равным образом политическое и государственное управление. Специальные кибернетические подразделения, созданные в Германии и Китае, имеют общие и отличительные особенности. Признается, что неотложной задачей является разработка международного механизма, норм и правил информационного обмена, исключающих проявление сетевого доминирования, вторжения, кибернетических войн и конфликтов.

Ключевые слова: кибернетическая война, кибернетические подразделения, «Computer Network Operations» Германии, «синяя армия» Китая

М.Ш. Губайдуллина, Д. Карипжанов

Кибернетикалық және желілік соғыс: ақпараттық қарсы әрекеттердің ұстанымдары (Германия мен Қытай тәжірибесі)

Халықаралық қатынастардағы жүйелік құлдырау жағдайында ақпараттық қарсыластық, атап айтқанда кибернетикалық және желілік соғыстар «дәстүрлі» соғыспен тең келерлік маңызға ие болып отыр. Кибер және желілік әрекеттер ақпараттық жүйені қорғауға немесе қарсы тараптың жұмысына кедергі жасауға, тіпті дұрыс шешім қабылдау мүмкіндігіне тосқауыл болуға бағытталған. Киберсоғыстардың нақты, ұлттық және географиялық шекарасы жоқ. Олардың әсер ету объектілері әскери, тіпті өндірістік, азаматтық желілер, сонымен қатар саяси және мемлекеттік басқару салалары болуы мүмкін.
Германия мен Қытайда әдейі ұйымдастырылған кибернетикалық бөлімшелердің ұқсастықтары мен ерекшеліктері бар. Кибернетикалық соғыстар мен қақтығыстардың және жүйелік басымдылықтың алдын алу үшін ақпараттық алмасудың ережелері мен нормаларын, халықаралық механизмін жасау қажеттігі маңызды болып отыр.

Түйін сөздер: кибернетикалық соғыс, кибернетикалық бөлімшелер, Германияның «Computer Network Operations», Қытайдың «көк әскері»

M. Gubaidullina, D. Karipzhanov

Cyber and network war: approaches to information struggle (the experience of Germany and China)

In the context of international relations system fault information warfare, and in particular cyber network war, are of particular importance, comparable to the "traditional" war. Cyber and network operations are directed either to protect their information systems, or to attack the opposing party in order to make it difficult or even impossible to take them right decisions. Cyber wars do not have clear national and geographical boundaries. The objects of their impact are

military and production (economic sphere) and civic networks, likewise political and public administration sphere. Cybernetic special units established in Germany and China have common and distinctive features. It is recognized that urgent task is to develop an international mechanism, norms and rules information exchange network exclusive manifestation of domination, invasion, cyber wars and conflicts.
Key words: cyber war, cyber division, «Computer Network Operations» Germany, "blue army" of China

Введение

Информационные аспекты развития современного общества и IT-технологии напрямую связаны со сферой национальной безопасности, находятся в центре пристального внимания интересов различных стран, имеют механизмы идеологического воздействия на общественное сознание. В киберпространство втянута сегодня большая политика, правительственные, финансово-экономические, военные учреждения и многое другое. Особенную актуальность развитие данной темы получает в связи с событиями «арабской весны» на Востоке, Афганистане, в Украине и др.

Практически одновременно с Германией, официально сообщившей о создании особого киберподразделения – войск «нового поколения» (CNO), военное ведомство КНР подтвердило факт образования государственного формирования – «сетевой синей армии» с целью зашиты безопасности интернет–пространства.

Активное сотрудничество спецслужбГермании и Китая выражается, в частности в том, что министерство государственной безопасности (МГБ)КНР иФедеральная разведывательная служба (BND/БНД) Германии налаживают совместную деятельность, в первую очередь в Азии, официально обмениваются аккредитованными резидентами. Сотрудники китайской разведки проходят стажировки в центре Федеральной разведывательной службы (BND) г. Пуллах (Pullach), что недалеко от Мюнхена. Резидентурам БНД разрешена совместная работа с резидентурами МГБ Китая в государствах Южной и Восточной Азии. Одним из важных направлений приложения совместных усилий спецслужб Китая и Германии является работа в странах Центральной Азии. Это связано с озабоченностью Китая ростом пантюркистских и фундаменталистских настроений, во многом инспирируемых спецслужбами Турции [1].Казахстан оказывается под прямым или опосредованным «прицелом» пересекающихся в центральноазиатском регионе кибер–интересов.

Кибер – и сетевые войны: сфера действия

Войну в кибернетическом (виртуальном) пространстве относят к специфической, высшей форме информационной войны, где она принимает различные формы [2]. Кибер – и сетевые войны появились сравнительно недавно, их относят к войнам нового типа, так как традиционная цель войны – использование в своих интересах потенциала и ресурсов побежденных, достигается таким образом, что предполагаемый противник побеждается без открытого боя, не физически, а психологически или ментально.

В поле действия кибервойны (прежде всего это компьютерный терроризм) входит осуществление диверсий против гражданских объектов противной стороны. Ввод случайных ошибок в пересылку данных, ведение тайного мониторинга сетей, несанкционированный доступ к закрытым данным и др. действия, могут привести к тотальному параличу сетей, перебоям связи, беспорядкам, колоссальному материальному ущербу, катастрофам, человеческим жертвам. Кибернетическая война является кроме прочего определенной концепцией ведения войны с использованием моделей и имитации в реальном времени, в ходе которых апробируются различные сценарии боевых действий, новые тактические приемы на представленных моделях. Средством (оружием) проведения операций служат компьютерные вирусы и другое программное обеспечение. В целом, кибероружие в совокупности с иными угрозами увеличивает ряд вызовов международной безопасности.

Цель сетевых войн направлена на психологическое подавление социумов и армий противника. На бесконечном интернет-пространстве проводятся спецоперации, способные дезорганизовать и/или дестабилизировать энергетическую или транспортную систему крупного города, страны, группы государств. Так, серверы спецслужб, Пентагон, крупнейшие корпорациимира и т.д. довольно часто подвергаются хакерским атакам. Секретная информация, обнародованная ресурсом WikiLeaks, открыла до-

ступ к данным конкурентов (или противников). Наибольшее число взломов касается банковских счетов, финансовых и деловых центров. В результате значительно слабеют их позиции, особенно при взламывании сетей с целью экономического шпионажа.

Первые данные о деятельности кибервойск стали известны сравнительно недавно. В 1991 г. США применили ИВ в ходе войны в Персидском заливе, затем в военных действиях в Косово. Дезинформация, распространявшаяся с самолетов и спутников союзников и СМИ, искажала информационные потоки Ирака, вызывала чувство страха, панику у его населения. В интересах безопасности США используют различные формы воздействия на «противную» сторону, включая сеть Интернет в качестве психологической атаки и как систему раннего политического предупреждения. На случай возникновения конфликтных ситуаций в разведывательном управлении минобороны США подготовлен план возможных действий по распространению среди населения дезинформации и направленных сведений с целью провоцирования выгодных для США изменений [3].

Кибернетические подразделения для специальных сетевых операций

Планы, обосновывающие создание в структуре военных ведомств специальных кибернетических подразделений с целью слежения за информационными сетями и другой электронной инфраструктурой, впервые появились в западных странах в конце XX века. Необходимость формирования кибервойск для ведения кибер-войн обосновал бывший министр обороны США Уильям С. Коэн: «История дала нам выбор; наука дала нам шанс; любовь к родине обязывает нас протянуть руку в будущее и нам осуществлять его» [4]. Так появился генеральный план по созданию «Научно-технической Армии» (ASTMP) – стратегическое звено, расположенное между департаментом технологического планирования министерства обороны (МО) США и планом главного командования армии и подчиненных ей командных подразделений. В основе генплана лежит общая оперативная концепция развития будущих ресурсов армии – «ArmyVision-2010» («Видение армии будущего–2010»). Согласно плану, отрабатываются модели по использованию армией технологических возможностей для достижения новых уровней эффективности: (1) защита вооруженных сил, (2) информационное доминирование, (3) решительные действия, (4) формирование темпа сражения, (5) проектирование вооруженных сил, и (6) поддержка вооруженных сил [5].

Создаваемые специальные киберподразделения призваны вывести из строя электронные системы управления. Поэтому в информационно-психологической войне широко используется потенциал хакеров. С их помощью находят слабые места в системе безопасности компьютерных сетей. К примеру, в литературе приводится эффект «арабской весны», которая началась в 2011 г., но была подготовлена намного раньше, и до сих пор не завершилась. Возможно, объектом сетевого вмешательства сегодня является Украина.

Вместе с тем, прослеживаются небезынтересные закономерности сетевой войны или противоборства:

– начинаются они не в момент напряженного противостояния сторон, а намного раньше, в периоды стабильности и мира или в предкризисные годы;

– по длительности сетевые операции занимают больше времени, но в итоге достигается поставленная цель: абсолютный контроль над всеми участниками международного процесса в данный исторический период и в данном пункте;

– чем страна более развита, тем более она уязвима для сетевых операций. Информационные системы развитых стран менее защищены от хакерских атак.

– эффект разрушения информационных систем сравним с военными разрушениями.

Кибернетические подразделения имеются на службе у сравнительно небольшого числа стран, они имеют как общие черты, так особенные различия. Наряду с США и Израилем, они созданы и в России, а вначале о своей деятельности официально было заявлено в Германии и в КНР. Остановимся на этих двух странах и некоторых тенденциях развития кибер-войск.

Мотивация, заставляющая Германию и Китай проводить углубленную модернизацию автоматизированных систем управления вооруженных сил (ВС), вполне объяснима. Обе страны стремятся не отставать от основных тенденций развития информационных технологий

и от своих конкурентов. За последние десять лет отмечается перевод практически всей системы коммуникаций вооруженных сил КНР и ФРГ на современные оптико-волоконные технологии, как наименее подверженные вторжению и наиболее помехозащищенные линии связи. Однако взломы компьютерных сетей ряда важнейших лабораторий, корпораций и военных структур фиксируются регулярно. Происходит своеобразная апробация помеховых «атак» войск противника, то есть информационного подавления других систем: внедрение в управляющие системы какого-либо вредоносного программного обеспечения и вирус, к примеру, атакует средства управления электро- или водоснабжения определенного района. В итоге «противник» вынужден тратить силы на ликвидацию последствий такой диверсии, а не на продолжение войны.

Германские войска «нового поколения» («Computer Network Operations»)

В конце 2011 г. было заявлено о полной боевой готовности немецкого Бундесвера к ведению кибернетической войны. В 2012 г. министр обороны ФРГ доложил парламенту о создании специального подразделении армии для ведения «наступательных» операций в кибер-пространстве [6]. Еще раньше, в 2006 г. на закрытой военной базе под Райнбахом (недалеко от Бонна) было сформировано первое подразделение «Computer Network Operations» (CNO), которое должно было специализироваться на кибер-войнах. CNO стало первым официально признанным подразделением в Европе (по некоторым данным – в мире, прим. М.Г.). Отряд «хакеров» (кибер-солдат) CNO вначале насчитывал более 100 человек, которые в изоляции от внешнего мира проходили подготовку в испытательных центрах по специальной программе, в том числе по «симуляции кибер-атак в лабораторных условиях».

В течение 2006 и 2007 гг. было модернизировано около 1000 автоматизированных рабочих мест (АРМ) в Главном штабе (ГШ), включая объединенное оперативное командование бундесвера и командование сил оперативного задействования, также оперативные командования видов ВС и отдельных объектов ОСО, в частности разведывательного центра Бундесвера и управления геоинформационной службы.

В настоящее время «достигнута способность действовать во враждебных сетях», то есть CNO непосредственно готовы к выполнению военных операций. Только теперь войска «нового поколения CNO» развёрнуты под единым военным командованием Бундесвера, являются специальным подразделением армии Германии, ориентированы на защиту от кибер-атак сетевых инфраструктур значимых объектов, а также операций в глобальной сети Интернет наступательного характера.

Немецкое представление об информационной войне объединяет наступательную и оборонительную составляющие в единое целое для достижения национальных интересов. Все средства управления и связи, опознавания и оповещения, обработки и анализа данных разведки должны быть сведены в единую центральную рабочую сеть управления операциями (VernetzteOperationsFührung). Управление средствами массовой информации является особенностью немецкого представления об информационной войне. Кроме того, специалисты Федеративной Республики Германии отдельно вводят понятие экономической информационной войны. При определении угроз и возможных ответных действий, иностранные государства рассматриваются отдельно от негосударственных объединений (политические партии, международные организации и средства массовой информации), преступных сообществ (организованные преступные группы, хакеры и т.д.), и индивидуумов (включая религиозных фанатиков и др.) [1].

В новых международных условиях задачи Бундесвера меняются. С учетом внедрения современных достижений в области управления, связи и информатизации разрешено использовать контингенты германских войск за пределами национальной территории, а также требований руководства Североатлантического союза. Основным органом, который определяет политику в сфере разработки, внедрения, эксплуатации и организации управления средствами, в вооруженных силах (ВС) Германии является федеральное ведомство управления и информационной техники Бундесвера. Оно входит в состав военной администрации минобороны ФРГ, и напрямую подчинено директору по информационным технологиям в аппарате министра обороны. Оперативное обеспечение и управление информацией всех звеньев, начиная с руководства

страной до штабов лежит на органах военной разведки «Жасмин» (JASMIN), центре бундесвера по контролю за соблюдением договоров в военной области «Верис» (VERIS) и др. [6].

С 2006 г. применяется технология «Сина» (SINA – Sichere Inter-Netzwerk Architektur), которая позволяет организовать параллельно работу с информацией различных категорий секретности по стандартам, принятым как в бундесвере, так и в ОВС НАТО. Ее успешно апробировали в ноябре 2006 г. в ходе учений по проверке готовности германо-голландско-финской БТГ к выполнению задач по планам военного руководства Евросоюза. Известно о двух отдельных сетевых домена с разграничением доступа к информации с грифом «Секретно» и «Секретно ЕС». Первый из них предназначен для обмена информацией между командованием сил оперативного задействования бундесвера и командующими германскими контингентами, а второй – для органов управления сил реагирования Евросоюза.

В 2007-2017 гг. в Германии осуществляется коренная модернизация и обновление информационной и коммуникационной системы национальных ВС в соответствии с концепцией НАТО «Единое информационное пространство» (NATO Network Enabled Capability/NNEC). Конечная цель реализации концепции «Единое информационное пространство НАТО» состоит в создании необходимых и достаточных условий для достижения подавляющего военного превосходства НАТО над любым вероятным противником.

Немецкие специалисты завершили оргтехнические мероприятия по подключению к международной компьютерной сети Интернет германского правительства. Здесь участвуют немецкий Telecom, концерны Bertelsmann и Axel Springer, которые одновременно являются соучредителями совместного предприятия America Online-Europe. Тем самым они оказывают существенное влияние на действия американцев в информационном пространстве Европы. По оценкам германских специалистов, полная интеграция систем управления и связи, включая АСУ видов ВС, займет еще около десяти лет. Тем не менее, предпринимаемые Германией в последнее время энергичные и последовательные меры по осваиванию нового информационного пространства, позволяют утверждать, что ФРГ уже составляет определенную конкуренцию США рамках европейского континента. Так, в феврале 2013 г. федеральное агентство оборонных технологий Германии заказало партию из 60 комплектов «Гладиус», рассчитанных на 600 солдат. Контракт обошелся в стоимость 84 млн евро. Тестовую партию из 30 комплектов предполагалось апробировать в Афганистане в 2013 г. [7].

Китай: апробация виртуальных атак и войн в современных условиях

Китай приступил к созданию собственных кибер–войск («сетевая синяя армия) вслед за западными странами. Заявлено, что защита безопасности сетевых ресурсов «отвечает закону и правовым нормам», апробируется их опыт и вырабатывается модель тренировок по борьбе с кибер–атаками. По мнению военных экспертов КНР, «сетевой синей армией» называют войска во время тренировок, которые выступают в качестве мер предосторожности в борьбе с кибер–атаками (генерал-майор Ло Юань, заместитель секретаря Академии военных наук КНР; Ли Ли, военный эксперт Национального университета обороны). Выбор синего цвета для китайской сетевой армии объясняется так: «Западные страны привыкли называть атакующие подразделения красными. «Сетевая синяя армия» не имеет никакого специализированного назначения» (Ген Яньшэн, представитель министерства обороны КНР). «Синий цвет» китайских кибервойск не носит какой-то специальный смысл, это всего лишь обозначение для распознавания различных войск, «не нужно преувеличивать значение цвета» (Тэн Цзяньцюнь, научный сотрудник Института по изучению международных вопросов) [8].

Руководство НОАК считает, что одним из основных факторов, оказывающих существенное влияние на разрешение конфликтных ситуаций, является превосходство над своими противниками в кибернетической сфере. Центральный военный совет еще в 2002 г. принял решение об активизации усилий на развитие возможностей страны по ведению борьбы в киберпространстве, что было закреплено в Национальной военной стратегии Китая (Military Strategic Guidelines) [9].

В «Белой книге» КНР по национальной обороне говорится о том, что правительство уделя-

ет большое внимание использованию технологий военной промышленности в мирных целях. Оно поощряет и поддерживает оборонную науку, технику и промышленность в выявлении их преимущества в технологиях и кадрах, развивает военно-гражданскую технику и промышленность на основе высокой науки и новейших технологий, что действенно содействует строительству народного хозяйства. Система военной связи переводится на современные цифровые технологии и телекоммуникационное оборудование, которое в перспективе сможет оперативно управлять повседневной деятельностью объединений и соединений, а также позволит отслеживать ход оперативной и боевой подготовки.

Командование НОАК, определяя подготовку к ведению информационной войны в качестве главной тенденции в реформировании китайских вооруженных сил, выделило на перевооружение армии 17 млрд. долларов США. При этом принято решение за счет переоснащения ВС современными видами вооружений, включая новейшие средства радиоэлектронной борьбы и информационного противодействия, в течение трех лет сократить численность ВС на 500 тысяч человек. На предполагаемых театрах военных действий будут оборудованы информационные сети с соответствующим набором баз данных.

Военные специалисты Китая под термином «информационная война» подразумевают «переход от механизированной войны индустриального возраста к войне решений и стиля управления, войне за знания и войне интеллекта». В основу концепции информационной войны положены уникальные китайские представления о войне в целом, прежде всего труды философа Сун Цзы («Искусство войны»), также представления о ведении войны на стратегическом, оперативном и тактическом уровне. В современной концепции кибер-войны важная задача отводится совершенствованию функции, миссии и правил армии в сетевой войне, улучшению объектов сетевых военных операций.

В 2002 г. военно-политическое руководство КНР возложило функции организации оборонительных и наступательных действий в киберпространстве на Третье и Четвертое управления Генерального штаба НОАК (ГШ). Третье управление ГШ отвечает за организацию и проведение радио- и радиотехнической разведки («прослушивание» радиоканалов и иные виды получения информации при помощи технических средств), а также разведки в киберпространстве. Это управление несет ответственность за обеспечение кибер-безопасности НОАК. В ведение Четвертого управления ГШ НОАК находится организация и проведение наступательных операций в киберпространстве. На оба управления работает не менее трех научно-исследовательских институтов и двенадцать оперативных бюро. В 2010 г. в состав «кибернетических войск» Китая вошло Управление информатизации, его целью является осуществление общей координации в IT-сфере [9].

Китай, обладая высоким научным потенциалом, опытным квалифицированным персоналом и современной материальной базой, необходимыми для успешного проведения исследований в IT-сфере, широко сотрудничает с ведущими научными институтами и организациями, проводящими исследования в сфере «критических технологий». В результате такого взаимодействия КНР становятся доступными передовые исследования и технологии, а также телекоммуникационные системы военного и двойного назначения.Успешно развиваются военные отношения между Китаем и Европейского союза. НОАК поддерживает консультации и проводит совещания по вопросам безопасности с органами обороны и соответственными военными органами Австралии, Франции, ФРГ, Индии, Японии, Казахстана, Кыргызстана, Пакистана, России, Таиланда, Великобритании и США.

Кибер-шпионаж Китая

Общеизвестно, что хакеров Китая считают одними из сильнейших компьютерных специалистов в мире. При этом вопросы по кибертехнологиям держатся под контролем высшего политического руководства страны. Быстро растущая экономическая мощь Китая заставляет по-своему реагировать на данный факт мировые державы.

В западных СМИ высказывается подозрение относительно китайских кибер-подразделений и их деятельности в качестве «хакеров». Высокопоставленные чиновники ряда государств периодически выступают с обвинениями в адрес КНР о проводимом кибершпионаже, об оказа-

нии воздействий на объекты критически важной инфраструктуры, о том, что Китай обладает высоким потенциалом для проведения подобных операций в киберпространстве [10]. В подтверждение, в 2013 г. был распространен детальный доклад компании «Мандиан» (Mandiant), которая в течение семи лет расследовала большое количество инцидентов, связанных с несанкционированными проникновениями во внутренние сети различных организаций и их компьютеры по всему миру.

Большинство нарушений компьютерной безопасности классифицируются как «самые современные стойкие угрозы» (Advanced Persistent Threat, APT). Вина возложена на некую китайскую организацию, специализирующуюся по промышленному шпионажу. При этом в 2010 г. отмечалось, что «китайское правительство могло санкционировать шпионскую деятельность, но не существует способа, который бы позволил выяснить степень его причастности к этому делу». А в докладе «Мандиан» 2013 г. утверждается, что группа китайского происхождения осуществляет операции кибер-шпионажа в отношении компаний обширного диапазона деятельности: это систематическая кража сотен терабайт данных у 141-й организации, которые охватывают 20 основных отраслей промышленности [11]. Группа APT1 контролирует тысячи систем, ведет несанкционированные вторжения, похищает широкий спектр информации интеллектуальной собственности, включая технологические проекты, данные закрытых процессов производства, результаты испытаний, бизнес-планы, электронные письма и т. д.

Итак, было публично заявлено о причастности Китая к промышленному кибер-шпионажу на государственном уровне. Более того, утверждается о существовании необходимых доказательств относительно принадлежности киберпреступной APT1-организации к подразделению НОАК.

Действительно, тесная взаимосвязь НОАК с крупными телекоммуникационными компаниями национального сектора, занимающимися производством программного обеспечения и радиоэлектронных средств, теоретически может способствовать проникновению вредоносного кода в их продукцию, ее дальнейшему внедрению на объекты важной инфраструктуры государств-потребителей. Однако требуется критическое рассмотрение самого расследования «Мандиан» и его обвинений в отношении Китая.

Выводы: международно-правовой контекст кибер-войн

Международная информационная безопасность сегодня определяется как “состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве” [12]. В мире «информационной войны» человечество остаётся заложником кибернетического пространства, которое ни предсказать, ни контролировать практически невозможно.

Большинство стран, не обладающих мощными информационными ресурсами, склоняются к созданию международной договорно-правовой базы обеспечения безопасности в глобальном масштабе и налаживанию взаимодействия в указанной сфере. Кроме того, требуется совершенствовать международное законодательство. Европейцы уже приступили к изучению вопроса о принятии нормативных документов по информационной безопасности в рамках ЮНЕСКО, таких, которые позволят придать контролю за глобальными сетями многополюсный характер. Поскольку каждое государство имеет свое понятие кибернетической и сетевой безопасности и свободы, одним из решений проблемы кибернетического противостояния может стать заключение международного соглашения, регулирующего использование этого оружия. По убеждению основателя «Лаборатории Касперского» Евгения Касперского, международное соглашение, которое запретит оборонным структурам вести разработки вирусов, либо поможет уменьшить предполагаемую опасность в мировом масштабе, крайне необходимо [13].

Учитывая угрозу использования информационного оружия с целью взятия под контроль информационной инфраструктуры государства, предстоит разработать кодекс поведения в международном информационном пространстве. Также стоит немало задач по разработке такого международного договора, которое сможет дать определение таким понятиям, как «кибернетическое оружие» или «сетевая атака», дать ответ на вопрос, является ли кибернетическая атака актом военной агрессии или нет.

Литература

1 Исследовательский центр Агентура.ru [Электронный ресурс] – досье: <http://www.agentura.ru/dossier/>

2 Аверченков В. И., Рытов М. Ю. и др. Системы защиты информации в ведущих зарубежных странах. Учебное пособие для вузов. – М.: Флинта, 2011. – С. 46

3 См: доклад директора национальной разведки Дж. Клэппера, сделанныйвходеежегодныхслушанийпооценкеугрозв-КомитетеСенатаповооруженнымсилам(DIA Director Army Lt. Gen. Michael Flynn joins Director of National Intelligence James Clapper for the Annual Threat Assessment Hearing before the Senate Armed Services Committee) // Defense Intelligence Agency (DIA): <http://www.dia.mil/News/Articles/tabid/3092/Article/8028/dia-director-army-lt-gen-michael-flynn-joins-director-of-national-intelligence.aspx>

4 Army Science and Technology Master Plan: <http://www.fas.org/man/dod-101/army/docs/ astmp98/sec1a.htm>

5 “Multispectral Thermal Imager”, 21 October 2000. Available from: <http://www.fas.org/spp/military/program/masint/mti.html.>, Accessed 23 Nov. 2001; John W. Ives. Army Vision 2010: Integrating Measurement and Signature Intelligence. Strategy Research Project: <http://cracking8hacking.com/cracking-hacking/Ebooks/files/003/ ENIGMA/Ives_J_W_02.pdf>, 09 April 2002. – 48 P.

6 Германия сформировала боевое киберподразделение. [Электронный ресурс]: <http://www.xakep.ru/post/58820/>, 08.06.2012

7 Зарубежное военное обозрение (полковник С. Корчагин) // Портал "Современнаяармия": <http://www.modernarmy.ru/article/334/asu-bundesvera>

8 Почему Китай создал «сетевую синюю армию»? // Жэньминь жибао он-лайн: <http://russian.people.com.cn/31521/7421675.html>, 27/06/2011

9 Белая книга Китая (2010 – 2013). Национальная оборона Китая в 2002 г. (Прилож.№2) // МИД КНР: <http://www.fmprc.gov.cn/rus/ziliao/zt/zfbps/t25314.shtml>, 2002/12/31

10 Юрченко Г. Киберборьба по взглядам руководства Китая: <http://www.belvpo.com>, 21.07.2012; <http://www.infowar.delovoy.com/cgi-bin/iwar/start.cgi?prn1=info2&grp=0657>

11 Mandiant. APT1. Разоблачение одного китайского кибера. Шпионские союзы: <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf>; Результаты контрразведывательной операции Mandiant против китайских военных хакеров // <http://www.xakep.ru/post/60141/>, 19.02.2013; APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем // Информационная безопасность. Блогкомпании ESET NOD32: <http://habrahabr.ru/company/eset/blog/170285/>, 23.02.2013

12 Окинавская Хартия глобального информационного общества. Резолюция ГА ООН по информационной безопасности A/RES/58/32, декабрь 2003 г.Док. Генеральной Ассамблеи ООН A/55/40. [Электронный ресурс] – <http://www.ifap.ru/ofdocs/okinhar.htm>

13 Касперский Е. Интервью: <http://zavtra.ru/content/view/neopoznannaya-vojna/>

References

1 Issledovatel'skiy tsentr Agentura.ru [Elektronnyy resurs] – dos'ye: <http://www.agentura.ru/dossier/>

2 Averchenkov V. I., Rytov M. YU. i dr. Sistemy zashchity informatsii v vedushchikh zarubezhnykh stranakh. Uchebnoye posobiye dlya vuzov. – M.: Flinta, 2011. – S. 46

3 Sm: doklad direktora natsional'noy razvedki Dzh. Kleppera, sdelannyy v khode yezhegodnykh slushaniy po otsenke ugroz v Komitete Senata po vooruzhennym silam (DIA Director Army Lt. Gen. Michael Flynn joins Director of National Intelligence James Clapper for the Annual Threat Assessment Hearing before the Senate Armed Services Committee) // Defense Intelligence Agency (DIA): http://www.dia.mil/News/Articles/tabid/3092/Article/8028/dia-director-army-lt-gen-michael-flynn-joins-director-of-national-intelligence.aspx

4 Army Science and Technology Master Plan: <http://www.fas.org/man/dod-101/army/docs/ astmp98/sec1a.htm>

5 “Multispectral Thermal Imager”, 21 October 2000. Available from: <http://www.fas.org/spp/military/program/masint/mti.html.>, Accessed 23 Nov. 2001; John W. Ives. Army Vision 2010: Integrating Measurement and Signature Intelligence. Strategy Research Project: <http://cracking8hacking.com/cracking-hacking/Ebooks/files/003/ ENIGMA/Ives_J_ W_02.pdf>, 09 April 2002. – P. 48

6 Germaniyasformirovalaboyevoyekiberpodrazdeleniye. [Elektronnyyresurs]: <http://www.xakep.ru/post/58820/>, 08.06.2012

7 Zarubezhnoyevoyennoyeobozreniye (polkovnikS. Korchagin) // Portal "Sovremennayaarmiya": http://www.modernarmy.ru/article/334/asu-bundesvera

8 PochemuKitaysozdal «setevuyusinyuyuarmiyu»? // Zhen'min' zhibaoon-layn: <http://russian.people.com.cn/31521/7421675.html>, 27/06/2011

9 Belaya kniga Kitaya (2010 – 2013). Natsional'naya oborona Kitaya v 2002 g. (Prilozh.№2) // MID KNR: <http://www.fmprc.gov.cn/rus/ziliao/zt/zfbps/t25314.shtml>, 2002/12/31

10 YurchenkoG. Kiberbor'bapovzglyadamrukovodstvaKitaya: <http://www.belvpo.com>, 21.07.2012; <http://www.infowar.delovoy.com/cgi-bin/iwar/start.cgi?prn1=info2&grp=0657>

11 Mandiant. APT1. Razoblacheniye odnogo kitayskogo kibera. Shpionskiye soyuzy: <http:// intelreport.mandiant.com/Mandiant_APT1_Report.pdf>; Rezul'taty kontrrazvedyvatel'noy operatsii Mandiant protiv kitayskikh voyennykh khakerov // <http://www.xakep.ru/post/60141/>, 19.02.2013; APT1: razoblacheniye kitayskoy organizatsii, zanimavsheysya promyshlennym kibershpionazhem // Informatsionnaya bezopasnost'. Blog kompanii ESET NOD32: <http://habrahabr.ru/company/eset/blog/170285/>, 23.02.2013

12 Okinavskaya Khartiya global'nogo informatsionnogo obshchestva. Rezolyutsiya GA OON po informatsionnoy bezopasnosti A/RES/58/32, dekabr' 2003 g. Dok. General'noy Assamblei OON A/55/40. [Elektronnyy resurs] – <http://www.ifap.ru/ofdocs/okinhar.htm>

13 Kasperskiy Ye. Interv'yu: <http://zavtra.ru/content/view/neopoznannaya-vojna/>