§8 ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Маркова А. В.

ВИРТУАЛЬНО-КОММУНИКАЦИОННОЕ ПРОТИВОСТОЯНИЕ США И КНР

Аннотация. *Данная статья посвящена противостоянию США и КНР в современных информационно-коммуникативных сетях. Исследуется современное состояние безопасности КНР с точки зрения теории информационных войн. Анализируются основные механизмы манипуляционных методик психологических операций против Китая, основанных на провоцировании в психике индивида симптоматики пограничной психопатологии. Изучается тенденция широкого внедрения информационных технологий в военных подразделениях, что делает обеспечение их кибербезопасности необходимым условием роста их боеспособности. Автор исследует использование информационных и виртуально-коммуникативных способов воздействия на сознание граждан как неотъемлемую частью современных международных процессов. Методология исследования включает в себя следующие методы и подходы: контент-анализ, когнитивное картирование, системный подход и другие. Исследуются основные структуры КНР, занимающиеся разработкой и новейшими исследованиями в области информационных войн и психологических операций. Автор приходит к выводу, что США и Китай постепенно наращивают свои возможности по ведению кибер и информационно-психологических войн. Данное обстоятельство неизбежно приводит к новому витку соперничества, особенно ярко проявляющемуся в Азиатско-тихоокеанском регионе, где у Китайской Народной Республики практически не осталось сравнимых с ней по военной и экономической мощи соперников.*

Ключевые слова: *Манипуляции, НОАК, АНБ, Кибербезопасность, США, Интернет, КНР, Информационные войны, Информационные технологии, Кибервойна.*

Работа частично поддержана грантом (соглашение от 27 августа 2013 г. № 02.B.49.21.0003 между МОН РФ и ННГУ)

DOI: 10.7256/2073–8560.2014.6.13664

ВВЕДЕНИЕ

Современное состояние системы международных отношений является крайне нестабильным, чрезвычайно высоки шансы принципиальных изменений. Постепенное увеличение международной военной активности в Азиатско-тихоокеанском регионе (далее — АТР) и быстрое технологическое развитие азиатских стран актуализирует вопрос информационного противостояния главных акторов АТР на сегодня — США и КНР.

На повестке дня стоит информационная безопасность и средства сдерживания кибератак и киберпреступлений. Технологическое развитие создает условия для роста информационной уязвимости в большинстве стран мира.

Народно-освободительная Армия Китая в техническом оснащении уступает США, но темпы ее роста и модернизации увеличиваются, несмотря на существующие внутриэкономическое отставание и социальные проблемы КНР. Поддерживаемые правительством проекты кибератак и отработка возможных сценариев взлома систем инфраструктуры, энергообеспечения, головных офисов крупных компаний, корпораций, научно-исследовательских центров Китайской Республики Тайвань являются важным элементом в рамках китайской информационной и кибервойны (впоследствии методы, отработанные таким образом методы на тайваньских компаниях, применяются при взломе американских учреждений и организаций).

ХАКЕРЫ — СОЛДАТЫ НОВЫХ ВОЙН

По данным Бюро Национальной безопасности Тайваня Китай постоянно увеличивает численность своей киберармии. В настоящее время она насчитывает около 100000 человек. По некоторым данным на нужды хакеров и проведение различного рода кибероперация Пекин выделяет около $2,7 миллиона (€2 миллиона) в год[1] и данные расходы постоянно растут.

Тайвань и Вашингтон серьезно обеспокоены растущей киберугрозой со стороны КНР:

«В 2012 году большое количество компьютерных систем по всему миру, в том числе и принадлежащих американскому правительству, стали целями злоумышленников, некоторые из которых имеют прямое отношение к китайскому правительству и армии», — говорится в докладе Министерства Обороны США (май 2013 г.)[2].

Министерство госбезопасности Тайваня заявляет, что Китай целенаправленно заражает различными вирусами и вредоносными программами сайты правительственных органов, военных ведомств, а также крупных корпораций Тайваня. В министерстве уверяют, что действия подобного рода обычно существенно активизируются в периоды роста напряженности в отношениях между Тайванем и Китаем[3].

Использование киберпространства в качестве дополнительного рычага воздействия является неотъемлемым элементом современных политических процессов. Учитывая внедрение информационных технологий в военные подразделения, обеспечение кибербезопасности становится важной частью безопасности страны в целом. Так военно-воздушные силы Тайваня готовы использовать беспилотную авиацию для сбора разведданных о китайской армии (были поставлены на вооружение 32 беспилотника)[4], которые позволят поставить под контроль действия армия НОАК в тайваньском проливе. Эти разведданные могут быть использованы Соединенными Штатами, учитывая их опыт работы с дронами в афгано-пакистанском пограничье. Применение армией соперника подобных методов стимулирует правительственное финансирование разработок по кибербезопасности.

---

[1] Belyaev, D. (2013, may 9). United States and Taiwan are seriously concerned about China's actions in cyberspace. Bda-expert.com. Retrieved July 26, 2014, from http://bda-expert.com/2013/05/ssha-i-tajvan-serezno-obespokoeny-dejstviyami-kitaya-v-kiberprostranstve/

[2] Там же

[3] Pushkar, M. (2012, September 4).Taiwan creates a special unit to protect the country's cyberspace. Electronic Journal — «Information Security» Itsec.ru. Retrieved July 26, 2014, from http://www.itsec.ru/newstext.php?news_id=86997#sthash.tL612wKs.dpuf

[4] Tien-pin, Lo. (2014, July 13). Military extends UAV deployment area. Taipeitimes.com. Retrieved July 26, 2014, from http://www.taipeitimes.com/News/front/archives/2014/07/13/2003594974

DOI: 10.7256/2073–8560.2014.6.13664

Разведывательные операции американских дронов засекречены, но известно, что над Китаем с этой целью летают стратегические БЛА Global Hawk, способные подниматься на высоту до 18 километров, что делает их недосягаемыми для большинства средств ПВО.

Китайские военные, в свою очередь, разрабатывают целый ряд альтернативных мер по борьбе с беспилотниками. Среди них: использование средств радиоэлектронной защиты для глушения бортовой электроники и сигналов между БЛА и военными спутниками связи; кибератаки с целью взлома систем управления Global Hawk; обычные дымовые завесы, скрывающие объекты наблюдения от противника[1].

Защита национальных интересов с применением киберпространства не является основным направлением деятельности китайских хакеров. Устремления Пекина — стимуляция научно-технического прогресса[2], что в свою очередь заставляют активно работать научно-техническую разведку, используя для этого широкий спектр возможностей — традиционных и/или нетрадиционных (внедрение, подкуп, провокации) и новых. Так для КНР принципиальное значение имеет приобретение инфраструктуры военного характера, но с применением исключительно в мирных целях, что отображается в сопутствующих документах. Пекин использует разные каналы с целью овладения информацией технического характера, раскрывающий военный потенциал разработок (от легальных — по дипломатической линии до нелегальных).

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ ВОЙНЫ

Другой уровень противостояние в сети Интернет — информационно-психологический. Информация начинает нести в себе как созидательную, так и разрушительную силу, но гораздо в более сильной степени, чем это было ранее. Если ранее целью было корректировка взглядов объекта, создание кратковременных эмоций, то сегодня информационное поле способно внести значительные изменения в картине мироощущений и мировоззрений человека, меняя его когнитивные установки.

И события последних дней, недель, лет лишь утверждают нас в том, что к гонке вооружений технических добавилась и гонка вооружений информационно-психологических. Война идеологий и культур приняла глобальные формы, не стесняясь никаких способов. Совершенствуются методики и схемы, целые институты, например, в США, заняты проработкой новых способов проведения психологических операций (манипуляций) и методам защиты от них. Только одна Национальная криптологическая школа АНБ (Агентство Национальной Безопасности) обучает за год 19 тысяч человек (13,5 тысячи — гражданский персонал АНБ, 2,5 тысячи — военный персонал, 3 тысячи — из других ведомств)[3]. Подготовка специалистов по «информационным войнам» ведется и иными учебными заведениями США.

Основной механизм работы подобных подразделений по информационной войне — организация манипуляционных психологических операций различного масштаба. Классический метод подобных манипуляций — вызывание разных форм невроза у отдельного индивида. В массе же, невроз передаётся как болезнь, переходя от одного индивида к другому. Затем, с «заражённой» таким способом массой, работают, как если бы работали с невротиками.

На провоцировании в психике индивида симптоматики пограничной психопатологии основано значительное действие манипулятивных методик. Посредством, например, информации, передающейся через социальные сети, кодируют психику индивида. Основано такое кодирование на законах психики, согласно которым любая информация сначала

[1] Gertz, B. (2013, December 11). Inside the Ring: China targets Global Hawk drone. Washingtontimes.com. Retrieved July 26, 2014, from http://www.washingtontimes.com/news/2013/dec/11/inside-the-ring-china-targets-global-hawk-drone/?page=all

[2] Петухов А. Ю. Комаров И. Д. Инкорпорация тайвани в Китайскую народную республику. прогнозирование на основе математических моделей // Вестник Нижегородского государственного университета им. Н. И. Лобачевского, Нижний Новгород, вып. 5, с. 69–73

[3] Почепцов Г. Г. Психологические войны. / М.,.Рефл-бук, К., Ваклер, 2008, 528 с.

DOI: 10.7256/2073–8560.2014.6.13664

поступает в подсознание, и уже оттуда оказывает воздействие на сознание. Это является одной из основных действенных методик информационных войн[1].

В Китайской Народной Республике планирование и реализация мероприятий по использованию информационных технологий для нарушения функционирования объектов информационной и телекоммуникационной инфраструктуры зарубежных государств осуществляется по линии министерств и ведомств, отвечающих за обеспечение государственной и военной безопасности страны в целом — министерства обороны (МО) КНР и министерства государственной безопасности (МГБ) КНР.

В Народно-освободительной армии Китая (НОАК) за ведение операций информационной войны и обеспечение информационно-психологической защиты войск отвечает Главное политическое управление НОАК. При этом деятельность по использованию информационных технологий для нарушения функционирования объектов информационной и телекоммуникационной инфраструктуры рассматривается в КНР исключительно как составная часть информационной войны на государственном уровне. Ее основным содержанием является «борьба с системами управления», под которой понимается совокупность мероприятий по комплексному воздействию на системы управления войсками и оружием противника, осуществляемому программными методами, ведением радиоэлектронной борьбы и посредством огневого поражения.

Координацию деятельности по организации информационного противоборства в компьютерных сетях осуществляет Управление радиоэлектронной борьбы Генерального штаба НОАК. Ему подчиняются специализированные центры, занимающиеся изучением возможности доступа к информационным сетям противника и защитой своих сетей управления. Также анализ возможностей ведения информационных войн проводится в частях психологических операций, радиоэлектронной борьбы и связи центрального и окружного подчинения.

Необходимо заметить, что в настоящее время в НОАК разрабатывается организационно-штатная структура подразделений, предназначенных для ведения информационного противоборства. По взглядам китайских специалистов, они должны включать подразделения компьютерной разведки и контрразведки, электронно-вирусных атак, антивирусной защиты и защиты от воздействия на электронно-вычислительную технику других средств поражения[2]. Особенно важную роль подобные подразделения играют в рамках решения вопроса Тайвани[3] и растущего китайского ядерного потенциала[4].

ЗАКЛЮЧЕНИЕ

Таким образом, США и Китай постепенно наращивают свои возможности по ведению кибер- и информационных войн. Соответствующие структуры постоянно растут в численности, оснащении, денежном довольствии, на вооружении появляются всё новые виды техники и приспособлений, десятки научных подразделений работают в интересах подобных организаций.

---

[1] Петухов А. Ю. Моделирование социальных и политических процессов в условиях информационных войн. Социально-энергетический подход // Fractal Simulation, Т. № 1 (3), 2012, 16–32

Петухов А. Ю., Чупракова Н. С. Моделирование социально-политического развития России в 20–21 веке. Социально-энергетический подход. // Вестник Нижегородского государственного университета им. Н. И. Лобачевского, Нижний Новгород, вып.6, 2012, 289–293

Петухов А. Ю. Цепные разветвлённые реакции в сложных социальных системах // Fractal Simulation, 2013, Т. № 1 (5), с. 14–23.

[2] Димлевич Н. Информационные войны в киберпространстве — Китай и Индия // Электронный журнал «Международная жизнь», ссылка (проверено — 27.09.14) — http://interaffairs.ru/read.php?item=614

[3] Petukhov A. Y. and I. D. Komarov, 2013. PROCESS OF INCORPORATION OF TAIWAN. Prediction using mathematical models. World Applied Sciences Journal, Issue 27 (Education, Law, Economics, Language and Communication), 13, p. 469–473 DOI: 10.5829/idosi.wasj.2013.27.elelc.96

[4] Petukhov A. Y. and S. V. Starkin. 2013. Some of the current aspects of the modernization of the Russian strategic nuclear arsenals. World Applied Sciences Journal, Issue 27 (Education, Law, Economics, Language and Communication), 13, p. 375–379 DOI: 10.5829/idosi.wasj.2013.27.elelc.76

DOI: 10.7256/2073–8560.2014.6.13664

Всё это ведёт к неизбежному новому витку соперничества, особенно ярко оно будет проявляться в Азиатско-тихоокеанском регионе, где у Китая практически не осталось сравнимых с ним по военной и экономической мощи соперников. Не зря Япония сейчас кардинально пересматривает собственную военную доктрину. Сложные взаимоотношения у Китая сохраняются и с Вьетнамом.

Плотное экономическое сотрудничество США и Китая, а также их взаимная зависимость не дают серьёзной возможности для военного конфликта и открытого разрыва экономических отношений, введения санкций и т.д. Зато — расширяют возможности для ведения информационных войн и увеличивает значение подобных психологических и кибероперациий.

БИБЛИОГРАФИЯ

1. Belyaev, D. (2013, may 9). United States and Taiwan are seriously concerned about China's actions in cyberspace. Bda-expert.com. Retrieved July 26, 2014, from http://bda-expert.com/2013/05/ssha-i-tajvan-serezno-obespokoeny-dejstviyami-kitaya-v-kiberprostranstve/
2. Там же
3. Pushkar, M. (2012, September 4).Taiwan creates a special unit to protect the country's cyberspace. Electronic Journal-"Information Security» Itsec.ru. Retrieved July 26, 2014, from http://www.itsec.ru/newstext.php?news_id=86997#sthash.tL612wKs.dpuf
4. Tien-pin, Lo. (2014, July 13). Military extends UAV deployment area. Taipeitimes.com. Retrieved July 26, 2014, from http://www.taipeitimes.com/News/front/archives/2014/07/13/2003594974
5. Gertz, B. (2013, December 11). Inside the Ring: China targets Global Hawk drone. Washingtontimes.com. Retrieved July 26, 2014, from http://www.washingtontimes.com/news/2013/dec/11/inside-the-ring-china-targets-global-hawk-drone/?page=all
6. Петухов А. Ю. Комаров И. Д. Инкорпорация тайвани в Китайскую народную республику. прогнозирование на основе математических моделей // Вестник Нижегородского государственного университета им. Н. И. Лобачевского, Нижний Новгород, вып. 5, с. 69–73
7. Почепцов Г. Г. Психологические войны. / М.,.Рефл-бук, К., Ваклер, 2008, 528 с.
8. Петухов А. Ю. Моделирование социальных и политических процессов в условиях информационных войн. Социально-энергетический подход. Fractal Simulation, Т. № 1, 2012, 16–32; Петухов А. Ю., Чупракова Н. С. Моделирование социально-политического развития России в 20–21 веке. Социально-энергетический подход. // Вестник Нижегородского государственного университета им. Н. И. Лобачевского, Нижний Новгород, вып.6, 2012, 289–293; Петухов А. Ю. Цепные разветвлённые реакции в сложных социальных системах // Fractal Simulation, 2013, Т. № 1 (5), с. 14–23.
9. Димлевич Н. Информационные войны в киберпространстве — Китай и Индия // Электронный журнал «Международная жизнь», ссылка (проверено — 27.09.14) -http://interaffairs.ru/read.php?item=614
10. Petukhov A. Y. and I. D. Komarov, 2013. PROCESS OF INCORPORATION OF TAIWAN. Prediction using mathematical models. World Applied Sciences Journal, Issue 27 (Education, Law, Economics, Language and Communication), 13, p. 469–473 DOI: 10.5829/idosi.wasj.2013.27.elelc.96
11. Petukhov A. Y. and S. V. Starkin. 2013. Some of the current aspects of the modernization of the Russian strategic nuclear arsenals. World Applied Sciences Journal, Issue 27 (Education, Law, Economics, Language and Communication), 13, p. 375–379 DOI: 10.5829/idosi.wasj.2013.27.elelc.7

REFERENCES (TRANSLITERATED)

1. Belyaev, D. (2013, may 9). United States and Taiwan are seriously concerned about China's actions in cyberspace. Bda-expert.com. Retrieved July 26, 2014, from http://bda-expert.com/2013/05/ssha-i-tajvan-serezno-obespokoeny-dejstviyami-kitaya-v-kiberprostranstve/
2. Tam zhe

DOI: 10.7256/2073–8560.2014.6.13664

3. Pushkar, M. (2012, September 4).Taiwan creates a special unit to protect the country's cyberspace. Electronic Journal-"Information Security» Itsec.ru. Retrieved July 26, 2014, from http://www.itsec.ru/newstext.php?news_id=86997#sthash.tL612wKs.dpuf
4. Tien-pin, Lo. (2014, July 13). Military extends UAV deployment area. Taipeitimes.com. Retrieved July 26, 2014, from http://www.taipeitimes.com/News/front/archives/2014/07/13/2003594974
5. Gertz, B. (2013, December 11). Inside the Ring: China targets Global Hawk drone. Washingtontimes.com. Retrieved July 26, 2014, from http://www.washingtontimes.com/news/2013/dec/11/inside-the-ring-china-targets-global-hawk-drone/?page=all
6. Petukhov A. Yu. Komarov I. D. Inkorporatsiya taivani v Kitaiskuyu narodnuyu respubliku. prognozirovanie na osnove matematicheskikh modelei // Vestnik Nizhegorodskogo gosudarstvennogo universiteta im. N. I. Lobachevskogo, Nizhnii Novgorod, vyp. 5, s. 69–73
7. Pocheptsov G. G. Psikhologicheskie voiny. / M.,.Refl-buk, K., Vakler, 2008, 528 s.
8. Petukhov A. Yu. Modelirovanie sotsial'nykh i politicheskikh protsessov v usloviyakh informatsionnykh voin. Sotsial'no-energeticheskii podkhod. Fractal Simulation, T. № 1, 2012, 16–32; Petukhov A. Yu., Chuprakova N. S. Modelirovanie sotsial'no-politicheskogo razvitiya Rossii v 20–21 veke. Sotsial'no-energeticheskii podkhod. // Vestnik Nizhegorodskogo gosudarstvennogo universiteta im. N. I. Lobachevskogo, Nizhnii Novgorod, vyp.6, 2012, 289–293; Petukhov A. Yu. Tsepnye razvetvlennye reaktsii v slozhnykh sotsial'nykh sistemakh // Fractal Simulation, 2013, T. № 1 (5), c. 14–23.
9. Dimlevich N. Informatsionnye voiny v kiberprostranstve — Kitai i Indiya // Elektronnyi zhurnal «Mezhdunarodnaya zhizn'», ssylka (provereno — 27.09.14) -http://interaffairs.ru/read.php?item=614
10. Petukhov A. Y. and I. D. Komarov, 2013. PROCESS OF INCORPORATION OF TAIWAN. Prediction using mathematical models. World Applied Sciences Journal, Issue 27 (Education, Law, Economics, Language and Communication), 13, p. 469–473 DOI: 10.5829/idosi.wasj.2013.27.elelc.96
11. Petukhov A. Y. and S. V. Starkin. 2013. Some of the current aspects of the modernization of the Russian strategic nuclear arsenals. World Applied Sciences Journal, Issue 27 (Education, Law, Economics, Language and Communication), 13, p. 375–379 DOI: 10.5829/idosi.wasj.2013.27.elelc.7

DOI: 10.7256/2073–8560.2014.6.13664