Мусуралиева М.М.

ПОНЯТИЕ И СУЩНОСТЬ ИНФОРМАЦИОННОЙ ВОЙНЫ

Мусуралиева М.М.

МААЛЫМАТ СОГУШУНУН ТҮШҮНҮГҮ ЖАНА МААНИСИ

M.M. Musuralieva

THE CONCEPT AND ESSENCE OF THE INFORMATION WAR

«…Словом можно убить, словом можно спасти,
Словом можно полки за собой повести…»
Вадим Шефнер

УДК:323.9/89

Большинство конфликтов все чаще происходят в информационном пространстве. Однако в современной науке нет четкого подхода в определении информационной войны. Поэтому изучение понятия и сущности информационной войны является актуальной задачей для политической науки.

Ключевые слова: *информационная война, дефиниция, терминология, национальная безопасность.*

Конфликттердин көбү маалымат мейкиндигинде көп кездешип жатат. Бирок, азыр илимде маалымат согушуна карата так аныктама бериле элек. Ошол үчүн маалымат согушунун маанисин жана түшүнүгүн изилдеп чыгуу саясий илими үчүн актуалдуу маселе болууда.

Негизги сөздөр: *маалымат согушу, дефиниция, терминология, улуттук коопсуздук.*

In the modern world, most of the conflicts occur in the information space. However, in the modern science there is no clear definition of information war. Therefore, the study of the concept and essence of information war is one of the important tasks in political science.

Key words: *information warfare, the definition if information war, terminology, national security.*

Введение

Что такое информационная война? Это воздействие на государство, путем распространения определѐнной информации. [1] С ее помощью можно интенсивно воздействовать на любые сферы жизни общества, практически на всех уровнях государственного устройства. Информационная безопасность – это то состояние государства и общества, при котором действует защита от информационных воздействий [2]. С точки зрения многих стран информационная война считается значимым средством и инструментом реализации внешней политики. Особая опасность ИВ заключается в том, что она со временем приобретает все более скрытный характер. Одной из самых важных проблем, связанных с информационной войной, является неосознанность общества того, какую угрозу могут нести современные коммуникативные процессы [3]. Выходящей проблемой так же является не готовность этого общества оказать противостояние попыткам манипулирования общественного сознания. В современном мире информация является неотъемлемой частью хорошейфункциональности любой системы. Это значит, что для того чтобы нарушить боеспособность противника не обязательно использовать техническое оружие, достаточно нарушить его коммуникативные процессы, препятствуя обмену информации или внедрив другую. Иными словами, основной задачей информационной войны можно считать влияние на информацию противника, с целью нарушения его боеспособности. Говоря об информационной войне и пропаганде, нельзя обойти стороной нацистскую Германию, в которой эти тактики придавались особому значению. Гитлер считал, что прежде чем начинать военные действия, противника необходимо деморализовать, «обезоружить» с помощью психологического нагнетания пропагандой

В настоящее время информационное противоборство негативным информационным воздействиям рассматривается как важнейший элемент обеспечения национальной безопасности многих государств и заложено в доктринах, специальных программах США, Германии, КНР, Великобритании, а также большинства государств СНГ. К сожалению, этот фактор в Кыргызской Республике пока не рассматривается.Бесспорно, информационное воздействие порождает угрозу национальной безопасности кыргызской государственности. На сегодняшний день Кыргызская Республика становится открытой ареной для проведения негативного информационного воздействия на индивидуальное и массовое сознание людей, что наносит ущерб психическому и нравственному здоровью населения, разрушает моральные нормы жизни общества, приводит к дестабилизации социально-экономической и общественно-политической обстановки. Поэтому защита населения от негативного информационного воздействия, результатом которого может быть манипуляция общественным сознанием и разрушение единого информационного пространства, должна быть одной из составляющих по обеспечению информационной безопасности Кыргызской Республики.

Заявление о том, что Кыргызская Республика сегодня на практике становится открытой ареной для проведения целенаправленного негативного информационного воздействия можно аргументировать самыми "свежими" примерами из работы наших собственных СМИ и зарубежных информслужб.

Сегодня самыми "актуальными информационными темами дня" являются события на Украине и вокруг нее, действия боевиков ИГИЛ в Ираке и Сирии, вхождение Кыргызстана в Евразийский Экономический Союз и целый ряд других.

Понятие информационной войны и ее составные части

В наше время информационная война является очень актуальной темой и много обсуждается. Однако однозначно никто не сможет дать ответ, что же такое информационная война. Даже специалисты затрудняются ответить, откуда возникло само понятие, кто начал его использовать, и как оно прижилось [4]. В целом, считается, что термин «информационная война» первым использовал американский специалист, советник по науки министерства обороны и Белого дома Томас Рона в отчѐте для компании Boening, в котором он обратил внимание на то, что информация становится ключевым аспектом американской экономики [5]. После появления этого отчета, американские военные заинтересовались поставленной проблемой. Таким образом, к 1980 году, благодаря Т. Рону, информацию стали воспринимать не только как цель, но и как оружие [6].

Информационная война - комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника [7].

Информационную войну, как правило, принято разделять на два основных вида [8] :

- Информационно – психологическая война (психологическая)
- Информационно-техническая Информационная война, как и любая другая сложная система, имеет составные части.

Среди них выделяют: 1. Психологические воздействия на мотивацию военнослужащих; 2. Дезинформация – распространение искажѐнной или ложной информации противнику; 3. Радиоэлектронная война - «ослепляет» противника, не позволяя получить точную информацию 4. Информационная атака - разрушение или искажение информации, без видимого повреждения носителя. 5. Защита информации 6. Физическое воздействие – разрушение информационных систем противника.

Методы информационной войны

Основными методами информационной войны являются: специальный выброс информации, пропаганда, внедрение в сознание искажѐнных фактов, медиа вирусов, формирование стереотипов и дезинформация. В совокупности все эти методы способны изменить общественное сознание, создать панику или сформировать нужную реакцию [9].

В качестве основных приѐмов влияния на массовое сознание можно выделить: скрытие информации, замещение понятий, информационный мусор, внедрение понятий, не имеющих никакого значения, приоритет информации, несущей негативный характер, ложь, информационное табу, отвлечение внимания и др [9]. Рассмотрим некоторые из них более подробно: 1. Скрытие информации – данный метод заключается в скрытии значимой и важной информации. Чаще всего этот метод используют государственные структуры. Например, в СССР скрывали информацию о техногенных катастрофах. 2. Информационный мусор – данный метод удобен тогда, когда информацию нужно скрыть, но полностью это сделать не получается. Суть его заключается в том, что информацию скрывают за потоком, так называемого «информационного мусора», т.е. за потоком неважной информации, «шума». 3. Замещение понятий – состоит в том, что общепринятый термин, начинают использовать не по назначению, как бы замещая его другим смыслом. Таким образом, его настоящий смысл, со временем начинает стираться. 4. Отвлечение внимания – заключается в акцентировании внимания на неважных и незначительных событиях, в то время как наиболее значимые остаются незамеченными. 5. Информационное табу – информация запрещена к распространению. Но на самом деле, эта информация известна для большинства, но не обсуждается публично.

Методы, рассмотренные выше, безусловно, не объясняют все способы, которые используются на практике. Но, тем не менее, дают некоторые представление о том, как работает информационное воздействие. Любое информационное воздействие осуществляется с помощью информационного оружия. Информационное оружие – специальные средства и методы, с помощью которых осуществляется информационное воздействие, приводящее к значительному ущербуважным интересам страны [10].

Основными свойствами информационного оружия являются [11]:

- Скрытый характер (возможность достижения целей войны без ее объявления);
- Возможность масштабного ущерба;
- Многофункциональность (возможность применения военными и невоенными структурами агрессора).

Различают следующие виды информационного оружия: 1. Уничтожение, искажение или похищение информации 2. Взлом средств защиты информации 3. Ограничение допуска законных пользователей к необходимым информационным ресурсам 4. Дезорганизация работы технических и программных средств противника Так же различают основные средства информационного оружия [11]: 1. Компьютерные вирусы 2. Логические бомбы или программ-

ные закладки 3. Средства подавления информационного обменаили навязывание ложной информации. В США информационное оружие разрабатывается и реализовывается на 3 основных направлениях: 1. Воздействие на электронные устройства и программное обеспечение 2. Воздействие на информационные потоки 3. Воздействие на сознание и психику: a) Усиление существующих в сознании людей нужных установок и закреплении их на уровне мировоззрения b) Фундаментальное изменение жизненных установок на основе потрясающих новых данных c) Связано с конкретным частным изменением взглядов на определѐнные события, факты

Цели информационной войны

В любой сложной самоорганизованной системе генетически заложен механизм саморазрушения. Этот механизм имеет информационную основу, и уязвим для чужеродных информационных воздействий. В определённыемоменты, когда сложная система становится неустойчивой, любая информация, воздействующая на систему, может привести к необратимым последствиям. Эти свойства определяют эволюционные процессы в системах любого уровня, т.е. эти процессы используются для ведения информационных войн. [12] Отмечают следующие цели информационной войны: 1. Контролирование информационного пространства врага, с возможностью его использования, защищая при этом свои военные информационные функции от его действий. 2. Использование контроля информацией для атакующих информационных действий на врага. 3. Повышение общей эффективности вооружённых сил с помощью повсеместного использования военных информационных функций.

Заключение

Чем же страшна информационная война? Наиболее влиятельными последствиямимогу быть: утеря части территории государства, эмиграция населения, нарушение промышленной структуры, политическая и военная зависимость от государства, одержавшего победу. Таким образом, существенной разницы в последствиях войны информационной и обычной, нет. Поражённую страну так же ждут утеря ресурсов, упад экономики, возможно даже потеря жизни населения и др. Исходя из вышесказанного, очень важно понимать опасность современной машины информационного воздействия, перестать недооценивать коммуникативные процессы. Учитывая сложность этих процессов, каждому государству необходим орган, который будет заниматься защитой информации, созданием информационного оружия. Так же, необходимо усилить научные исследования в области информационных войн.

Литература:

1. http://ru.wikipedia.org/wiki/Информационная_война
2. http://www.pandia.ru/text/77/238/43089.php
3. В.В. Гафнер Информационная безопасность
4. Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива
5. http://psyfactor.org/psyops/infowar25.htm
6. http://www.iso27000.ru/chitalnyi-zai/informacionnye-voiny/informacionnaya-voinaistoriya-den-segodnyashnii-i-perspektiva
7. Joint Publication 3-13, Joint Doctrine for Information Operations. 9 October 1998.
8. Гриняев С.Н. После битвы – киберпространство
9. Гражданская защита. Понятийно-терминологический словарь. – М.: Издательство «Флайст», Информационно-издательский центр «Геополитика». Под общей редакцией Ю. Л. Воробьева. 2001.
10. Социология: Энциклопедия. – Минск: Интерпрессервис; Книжный Дом. А.А. Грицанов,В.Л. Абушенко, Г.М. Евелькин, Г.Н. Соколова, О.В. Терещенко. 2003.
11. http://bookap.info/psywar/psywar/gl1.shtm
12. К.К. Колин «Социальная информатика»

Рецензент: к.полит.н. Асаналиев У.А.