Мусуралиева М.М.

МААЛЫМАТ СОГУШУ: МАКСАТТАРЫ, ТҮРЛӨРҮ, МЕТОДДОРУ

Мусуралиева М.М.

ИНФОРМАЦИОННАЯ ВОЙНА: ЦЕЛИ, ВИДЫ, МЕТОДЫ

M.M. Musuralieva

INFORMATION WAR: OBJECTS, FORMS, METHODS

УДК: 32(575.2)(04)

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.*

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.*

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.*

Ключевая цель информационной войны – достижение ин формационного доминирования. Информационное доминирование имеет своей задачей не дать противоположной стороне воспользоваться информационным пространством в полной мере. Наиболее известным примером информационной войны считается холодная война 1946-1991 годов (точнее, её идеологический аспект). Часть исследователей считает, что распад СССР был обусловлен применением информационных методов.

Информационные войны могут вестись: - между государствами; - между финансово-промышленными группами; - между властью и финансово-промышленными группами, - между властью и оппозицией, которую в свою очередь поддерживают определенные финансово-промышленные группы (иностранные государства); - между разными сегментами власти, поддерживающие различные финансово-промышленные группы (иностранные государства) [3].

В современное 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.

Первоначально некто Томас Рона использовал термин "информационная война" в отчете, подготовленным им в 1976 году для компании Boeing, и названный "Системы оружия и информационная война". Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина "информационная война" [4]. Согласно интернет ресурсам, информационная война (англ. *Information war*) – это термин, имеющий два значения: 1. Процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и (или) вооружённые силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов, и, противодействия таким воздействиям на собственную сторону. Термин «информационно-психологическая война» был заимствован в русский язык из словаря военных кругов США. Перевод этого термина («information and psychological warfare») с английского языка может звучать и как «информационное противоборство», и как «информационная, психологическая война», в зависимости от контекста конкретного официального документа или научной публикации.

В этом смысле также используется термин психологическая война – психологическое воздействие на гражданское население и (или) военнослужащих другого государства с целью достижения политических или чисто военных целей. 2. Целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем [1]. С ее помощью можно интенсивно воздействовать на любые сферы жизни общества, практически на всех уровнях государственного устройства. Согласно проекту Концепции информационной безопасности Кыргызской Республики, информационная безопасность – это состояние защищенности от внешних и внутренних угроз ее информационной сферы, формируемой, развиваемой и используемой с учетом согласованных и сбалансированных жиз-

ненно важных интересов личности, общества и государства [2]. С точки зрения многих стран информационная война считается значимым средством и инструментом реализации внешней политики. Особая опасность информационной войны 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. Выходящей проблемой так же является не готовность этого общества оказать противостояние попыткам манипулирования общественного сознания. В современном мире информация является неотъемлемой частью хорошей функциональности 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 информационных служб. 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.

Основными методами информационной войны являются: специальный выброс информации, пропаганда, внедрение в сознание искаженных фактов, медиа вирусов, формирование стереотипов и дезинформация. В совокупности все эти методы способны изменить общественное сознание, создать панику или сформировать нужную реакцию [1].

В качестве основных приемов 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. 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 ущербу важным интересам страны [3].

Основными свойствами информационного оружия являются:

- 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 [5]:

1. Компьютерные вирусы

2. Логические бомбы или программные закладки

3. Средства подавления информационного обмена или навязывание ложной информации. Например, 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 определенные события, факты.

В любой сложной самоорганизованной системе генетически заложен механизм саморазрушения. Этот механизм имеет информационную основу, и уязвим для чужеродных информационных воздействий. В определённые моменты, 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.

Заключение

Чем же страшна информационная война? Наиболее влиятельными последствиями могуть быть: утеря целостности территории государства, эмиграция населения, нарушение промышленной структуры, политическая и военная зависимость от государства, которое одержало победу. Так, получается что, существенной разницы в последствиях информационной и обычной войны нет. Поражённое государство 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. Должна быть принята Концепция информационной безопасности государства.

Литература:

1. http://ru.wikipedia.org/wiki/Информационная_война
2. Постановление Правительства КР “О проекте Концепции информационной безопасности КР” от 11 июля 2008 г. № 372 // ИПС “Токтом”. - Бишкек, 2009.
3. Гафнер В.В. Информационная безопасность. - М., 2010
4. Гриняев С. Н. Информационная война: история, день сегодняшний и перспектива. /http://www.infwar.ru
5. Шеховцов Н.П., Кулешов Ю.Е., Информационное оружие: теория и практика применения в информационном противоборстве. - Вестник АВН 2012, №1 (38). - С. 35-40.
6. Мусуралиева М.М. Тенденции развития информационного пространства. // Республиканский научно-теоретический журнал «Известия вузов Кыргызстана», №6, 2016 год. - С. 158-161.

Рецензент: к.полит.н., доцент Нурматова Г.А.