Национальная безопасность в период политической модернизации

Информационные факторы

Ираклий Нанадзе

В обеспечении национальной безопасности как в теоретическом, так и в практичном аспекте в основном была признана приоритетность военных сил.

На сегодняшний день обстановка изменилась, так как реальность формирования информационного общества привела к ограниченности подобного подхода.

Информационная революция является составной частью экономической и социальной глобализации.

В основе современной технологической революции лежат те научные и технологические открытия, которые дают возможность разработки и передачи информации с помощью телекоммуникаций.

Общество, которое политологи называют "информационным", значительно отличается от индустриального общества.

Сегодня в самых развитых странах – в США, Канаде, в большей части Западной Европы, Японии, в ряде государств Юго-Восточной Азии – создана информационная инфраструктура, которая лежит в основе функционирования всех сфер общественной жизни этих стран.

При этом отмечается тенденция довольно быстрого перехода в единую глобальную систему.

В техноструктуре возникшего нового информационного общества, несмотря на то, что в этой сфере занято больше людей, промышленность не исчезает и не теряет своей роли, так как для нового общества, в первую очередь, характерна не промышленность, сельское хозяйство и сфера обслуживания в отдельности, а их информационная взаимосвязь.

Во всех отраслях производства информация стала важнейшей составляющей.

Например, по ежегодным международным докладам ООН, в начале 90-х годов в Америке в сфере обработки информации было занято около 60% работающего населения[1].

Так как информация превратилась в глобальный ресурс человечества, настала эпоха интенсивного освоения информационных ресурсов, и информация все большее влияние оказывает на национальную безопасность любого государства. Поэтому происходящие в мире глобальные социальные изменения требуют объективного анализа и изучения.

Чтобы создать нынешнюю оперативную систему информационной политики, американцам понадобилось больше 10 лет (1963–1973 гг.).

В 1967 г. "Акт о национальных целях, приоритетах и средствах" содержал требования по подготовке группой советников ежегодного доклада для президента и созданию комитета социальной информации при конгрессе США. Особое внимание уделялось данным, характеризующим общественную жизнь и взаимодействие социальных групп.

Примечательно, что за последние десятилетия в США основной целью стратегии национальной безопасности стала защита американского образа жизни.

"Главнейшей задачей и конституционной обязанностью моей администрации стала защита национальной безопасности народа, территории и образа жизни", – так считал президент США Б.Клинтон[2].

Именно благодаря вышеуказанной единой государственной системе ("социальные показатели") американцы смогли определить основные параметры образа жизни, что дает военно-политическому руководству США возможность оперативно реагировать на проблемы, возникающие в "социальном настроении нации", фиксировать негативные внутренние и внешние источники информационно-психологического воздействия на них.

Таким образом, в интересах обеспечения национальной безопасности, США создали систему диагностики внутренней информации, а в конце XX в. начали создавать систему диагностики внешней информации, для чего широко используют международные информационные системы (в первую очередь Интернет и др.), находящиеся под контролем США (особенно в странах Восточной Европы).

В условиях формирования единого мирового информационного пространства США именно в нем установили постоянный мониторинг и контроль социальной информации, надежно обеспечив собственную национальную безопасность.

На Западе вопрос влияния информатизации на политическую власть, политический статус страны занимает центральное место.

Исследователи утверждают, что за счет концентрации информации, более широких возможностей ее использования происходит усиление геополитического потенциала государств, отмечается рост возможностей государственного аппарата власти по сравнению с представительной.

Это подтверждается политическими процессами, происходящими в постсоветских странах. Проведенные президентские и парламентские выборы, подтвердили, что контроль над СМИ и компьютерными сетями резко расширяет возможности манипулирования общественным мнением в борьбе за сохранение власти. Фактически вопрос выбора зачастую решают электронные СМИ.

Выборы президента США в 2000 г. стали первой выборной кампанией эпохи Интернета, хотя еще в 1996 г. были проведены эксперименты для использования Интернета в политических целях.

Статистика свидетельствует, что 144 млн. американцев ежегодно в течение 10 час. знакомятся в Интернете с информацией. В результате Интернет превратился в такое

же средство воздействия на избирателя, как газета, телевидение, радио и журналы, хотя с точки зрения оказания влияния пока отстает от них.

И у Буша, и у Гора были свои сайты, которые содержали информацию о претендентах и его политических платформах. Своими сайтами обладали партийные комитеты и разные общественно-политические организации.

Таким образом, в предвыборной борьбе избиратель еще до голосования был включен в предвыборную борьбу. Например, в период съездов республиканских и демократических партий более 600 тыс. чел. ознакомились с сайтами Буша и Гора.

Во время выборов в 2000 г. стал вопрос о голосовании через Интернет.

Эксперимента проводили в г. Феникс (Аризона), г. Сан-Диего и г. Сакраменто (Калифорния).

Кроме этого, 200 военнослужащих, находящихся за границей, голосовали по Интернету по своему местожительству (в штатах Южная Каролина, Техас, Флорида и Юта).

Во всех сферах экономики, науки, политики повышается геополитическое значение информационной техники и информационных ресурсов, так как геополитический потенциал страны и его политические возможности определяются в глобальном масштабе не только положением и размерами территории, качеством населения, но и экономическими, научно-техническими, военными и коммуникационными возможностями.

Бесспорно, что политика опирается на экономические возможности страны и служит экономическим интересам. Вначале экономическая мощь государства определялась в основном природными богатствами (плодородные земли, наличие полезных ископаемых). В дальнейшем основным фактором экономического потенциала стал уровень развития перерабатывающей промышленности.

В настоящее время информация стала стратегическим национальным ресурсом, одним из основных богатств страны, поэтому его геополитический потенциал определяется уровнем развития информационной инфраструктуры. Производство информационных продуктов и информационной техники в развитых странах уже заняло первое место как по объему, так и по количеству занятых.

В начале 80-х годов страны-лидеры, начали принимать государственные программы информатизации (Япония – программа построения информационного общества, США – стратегическая компьютерная инициатива, в Евросоюзе – "Эврика" и др.).

В 1993 г. в США была объявлена доктрина 11 (*National Information Infrastructure*) – создание национальной информационной инфраструктуры.

В меморандуме Клинтона – Гора он был объявлен главной задачей экономического роста США[3].

Сегодня в мире геополитический вес страны измеряется состоянием научно-технического потенциала, в частности уровнем информационно-технического обеспечения труда ученых и инженеров.

Процесс информатизации затронул и военную сферу. Известно, что война – является продолжением политики, а армия – сильным средством и аргументом в руках политиков. В соревновании по вооружению выход из ядерно-ракетного тупика уже найден. В военном деле наступает новый, постядерный этап, происходит новая военно-техническая революция – переход от оружия массового уничтожения к контрсиловому и информационному оружию, которое не угрожает экологической катастрофой и является эффективным средством достижения политических и экономических целей.

Эффективность современного оружия, поражающее действие которого основывается на традиционном огне, все больше определяется не огневой мощью, а следующими информационными параметрами: мощностью, управляемостью, скоростью действия, происходит его превращение из "не смертельного" в "разимое" (имеющее способность угадывать и выбирать цели и др.).

В развитых странах уже с начала 80-х годов информатизация армии признана приоритетной задачей научно-технической и военно-технической политики.

Непосредственно в содержании военных действий растет значение и вес информационно-технических и информационно-психологических компонент. В настоящее время эффективность средств информационного воздействия настолько высока, а их спектр и назначение настолько широки, что речь идет о новой разновидности оружия – информационном и, соответственно, об информационных войнах.

Термин "*информационная война*" американские военные специалисты применили после завершения военных действий в Персидском заливе, где информационное оружие высокой точности проявило себя довольно убедительно.

21 декабря 1992 г. Пентагон принял директиву TS 3600,1 под названием "Информационная война", в которой речь шла не только "о всестороннем учете информационных ресурсов" в будущей войне, но и была выражена глубокая тревога по поводу безопасности использования новейших информационных технологий против США[4].

В директиве № 30, изданной в 1993 г. председателем Объединенного комитета начальников штабов Дж.Шаликашвили, дается детальное обоснование основных положений информационной войны и концепция борьбы с системами управления[4].

Из-за своей специфики информационная война представляет самостоятельный вид и составной элемент всех других видов войны (вооруженной, идеологической, экономической и др.). Это происходит как в мирное, так и в военное время. Масштабы войны настолько грандиозны, что ее подготовка не должна быть спонтанной, она должна иметь систематический характер и должна опираться на глубокое знание законов и закономерностей информационной войны.

Разработка теории информационной войны имеет большое значение, ее нужно рассматривать как систему знаний о характере, законах, закономерностях, принципах, формах и правилах ее подготовки и ведения.

Цель информационной войны – обеспечение безусловного качества собственной информационной безопасности и снижения максимально уровня информационной безопасности противника.

Это можно достичь путем решения целого ряда задач, среди которых основной является уничтожение объектов информационной среды противника и защита собственной информации. Содержание информационной войны, структуру определяют ее цели и задачи, при этом на сущность информационной войны большое влияние оказывают многие факторы, среди которых надо выделить политический, экономический, психологический, собственно военный и информационный[5].

Политический фактор играет важнейшую роль в формировании сущности информационной войны, а именно он определяет:

– ее задачи и цели;

– причину возникновения и пути ее прекращения;

– затраты на нее и ее продолжительность;

– обеспечение материальных и финансовых ресурсов ее проведения.

Экономический фактор оказывает большое влияние на сущность и развитие информационной войны.

От экономики зависит уровень информатизации государства, а исходя из этого – эффективность информационной войны как в мирное, так и в военное время. Научно-технический прогресс, совершенствуя средства информационной войны, вызывает революционные изменения в ее теории.

Психологические факторы оказывают решающее влияние на реализацию положений теории информационной войны.

Общая и профессиональная подготовка обслуживающего персонала информационных систем, его морально-политическое и психологическое состояние, готовность самоотверженной защиты интересов своей страны играют большую роль в решении задач информационной войны.

В основе развития информационной войны лежит *военный фактор*.

Положения собственной военной доктрины, военные доктрины противников, состояние и перспективы развития средств информационной войны, исторический опыт и накопленные знания в данной отрасли являются основной базой разработки функциональных положений информационной войны, определяют ее направления и развитие.

Информационный фактор безраздельно связан с информационной войной зависит от уровня развития информатизации страны.

Этот фактор определяет рамки войны, правила, ее этапы, производство и выбор направлений удара, структуру сил, возможности их маневрирования при действии на информационную среду противника[6].

В информационной войне для оказания влияния на общественную мысль использован метод "информационно-психологического воздействия", который связан:

– с передачей информации (в информации подразумевается наличие фальшивой информации);

– с применением и воздействием на психологические особенности цивилизации.

На разных этапах развития человечества эти методы встречаются в различных формах.

Например, еще при Чингисхане войска применяли разного рода сплетни для деморализации населения и войска врага (например, о слабости противника, о продажности ее правителей и о мощи войск Чингисхана).

Во время войны Великобритании с бурами в Южной Африке буры установили связь с Германией, Ирландией и другими странами, создавая там образ Великобритании, воюющей с женщинами и детьми. В результате, они не только смогли сформировать мировое общественное мнение, но и уладили вопросы доставки оружия и формирования отрядов добровольцев.

Особый эффект производили партизанские действия определенных групп буров, широкое освещение которых помогло развеять миф о непобедимости английской армии.

Пропаганда как самостоятельная военная дисциплина особенно широко сформировалась во время первой мировой войны.

Например, в США был создан так называемый Комитет крили, который координировал пропагандистскую работу для воздействия (в разных аспектах) на население Германии и США.

Основными компонентами информационной войны являются: оперативная маскировка, дезинформация противника, психологические операции, радиоэлектронная борьба, огневое уничтожение системы управления, разведка, дезорганизация системы управления противника по охране собственной системы управления.

В 1995 г. вышел новый устав армии США об информационной войне, а университет национальной безопасности завершил подготовку специалистов первой группы в этой области.

Начиная с 1994 г. устраиваются научные конференции по проблемам информационных войн.

На протяжении последних 10 лет доля расходов США на информатику и подготовку информационных войн возросла втрое и достигла 20% бюджета.

Еще в 2001 г. немецкая разведка предупреждала все спецслужбы мира о росте опасности информационной войны. Эксперты пришли к заключению, что в ряде государств секретные службы систематически готовятся к ведению войны в информационной сфере (в заявлении экспертов эти страны официально не называются). Для этого их учат уничтожать базы компьютерных данных противника. Вся суть информационной войны в том, чтобы вся система государственного управления была быстро повреждена и уничтожена.

В информационной войне главной мишенью удара сначала станут военные структуры, а затем учреждения, банковские системы, полиция и транспорт.

По данным экспертов Германии, существуют специальные программы под именем "Троянский конь", которые могут находиться в компьютерной сети противника годами, а включаться в работу только в определенный момент для вывода всей системы из строя.

Например, ни один из самолетов "Мираж", купленных у Франции, не взлетел в Ираке, так как в них было вмонтировано скрытое электронное устройство, о котором знали только французы, и без их вмешательства оно не могло включиться. Французы этот момент прекрасно использовали в нужное время.

Такие методы были применены НАТО в воздушной войне в Югославии. Американские военные хакеры смогли уничтожить систему воздушной обороны сербов.

Эксперты немецкой разведки указывают, что это не единственный из тех методов, которые можно применить во время ведения информационной войны. Для уничтожения информационной системы противника происходит проникновение в его компьютерную сеть, в нее вносятся так называемые "компьютерные вирусы". Для этого, как правило, применяются Интернет сети[7].

В настоящее время в странах пока не существует единой компьютерной системы управления государством.

Сегодня происходит рассмотрение проектов, хотя отдельные ведомства создают собственные информационные системы.

Для обеспечения сохранности компьютерных систем необходимо проведение особых организационных мероприятий и приобретение соответствующих технических и программных средств, которые стоят дорого и не всем доступны.

Жизненно важное значение имеет охрана собственной информации от несанкционированных доступа.Секретная информация должна быть изолирована от глобальных компьютерных сетей общего пользования и храниться только в информационном виде, который систематически должна контролировать специально созданная группа.

При развитии информационной техники и технологий "холодные войны" постепенно вытеснят "горячие войны", в чем решающую роль сыграет информационное оружие. Уже и сейчас видно, что "холодные войны" становятся все более масштабными и политически результативными. Государства эти войны все чаще используют для достижения своих политических целей (факт, но без выстрела исчезла огромная страна – СССР).

Возможность обретения страной влияния на международной арене все больше зависит от уровня развития информационной инфраструктуры, и, соответственно, страна получает возможность использовать свой интеллекту-

альный потенциал, распространять и внедрять свои духовные и идейные ценности, свою культуру, язык, препятствовать духовной и культурной экспансии других стран, расшатывать их духовно-нравственные основы.

Внешнеполитические успехи США обусловлены не только их военной и экономической мощью, но и успехами в реализации программ "демократии" и "народной дипломатии", контролем над основными информационными и культурными процессами.

США открыто заявляют свои претензии на глобальное геополитическое лидерство и даже подготовили соответствующую базу. Известно, что глобальные и национальные компьютерные сети являются основой из основ будущей информационной инфраструктуры. В США суперкомпьютерная сеть министерства обороны (*ARPA net*) стала ядром мировой глобальной сети – Интернета – самой популярной, и быстро растущей сети. Интернет, фактически, становится основой информационной структуры планеты и находится под фактическим контролем военных специалистов США.

Резко возросла и роль СМИ, так как вырос интерес к средствам массовой информации как инструмента влияния на общественное мнение и лоббирования своих интересов со стороны различных политических и политико-финансовых групп. Слушатели, зрители и читатели все чаще становятся свидетелями информационных войн при разоблачении многочисленных компроматов, утечки информации, заказных публикаций и т.д.

Это повышает социальную направленность, вызывает недоверие народа к институтам гражданского общества новых независимых государств, институтам предпринимательства, возникает недоверие к любым действиям государственной власти, растет обособление государства и общества, возникает неверие людей в свои возможности изменить ситуацию к лучшему. Все больше утверждается стереотип недоверия к демократическому обществу, в том числе и к самим СМИ.

Таким образом, в геополитическом соперничестве государств, в реализации политических планов идет явное перемещение центра тяжести с открытых силовых (экономических, дипломатических, собственно военных) методов и средств на информационные. При этом трансформация борьбы вовсе не замедляет ее, не снижает ее жесткости и упорства, а наоборот, она под прикрытием риторики перехода на "демократическое" мироустройство все больше накаляется, становится все более бескомпромиссной.

Примечания

[1] www.un.org/russian/documen/ scdocs/committees/iraqrep.htm

[2] *Круглов В.В., Воробьев И.Н.* Основы военной футурологии. М., 1988. С. 175.

[3] *Malhotra Y.* National Information Infrastructure: Myths, Metaphors and Realities. BRINT Institute, L.L.C. 1995. P. 29.

[4] www.didgah.de/Russian/ Neuer%20Ordner2/Ketab%20Liachovski.htm

[5] http://users.iptelecom.net.ua/~zhistory/gp0541a.htm

[6] *Василенко И.А.* Политическая глобалистика:. М.: Логос, 2001. С. 60.

[7] *Коэн Ф.* Компьютерные вирусы: теория и эксперимент. М., 1984.