**Роль новых информационных технологий в современных международных отношениях**

Введение

Все шире применяющиеся информационные технологии кардинальным образом меняют повседневную жизнь миллионов людей. Они привносят изменения не только во внутреннюю политику самых разных по уровню развития стран мира, но и в отношения между этими странами, в роль, которую играют в мировой системе международные организации, общественные движения, финансовые группы, преступные организации и отдельные лица. Меняется сам предмет теории международных отношений. Теоретическое осмысление современных международных отношений без учета роли новых информационных технологий становится просто невозможным. Подобные качественные изменения находят отражение в процессе выработки внешнеполитических решений. Сейчас аналитик, работающий с конкретными внешнеполитическими проблемами, сталкивается с последствиями информационной революции не только при изучении того или иного явления международной жизни.

Информационные технологии меняют сам труд исследователя-международника. Осознание природы этих изменений - необходимая предпосылка для решения практически любой прикладной задачи.

Информационные технологии в современных международных отношениях

Для достижения такой цели необходимо выполнить две основные задачи. Во-первых, следует рассмотреть влияние новых информационных технологий на современные международные отношения (включая изменение роли государства в международных отношениях и изменение в формах международного конфликта).

Во-вторых, требуется ясно осознать, какие изменения новые информационные технологии вносят в процесс исследования международных отношений.

В наше время информация в основной своей массе является продуктом данных, собранных электронными сенсорами. Электронные средства связи расширили зону, в которой можно своевременно обмениваться информацией. Программное обеспечение для обработки данных и аппаратная часть также развивались быстрыми темпами.

Интернет создал беспрецедентную потребность в постоянном и быстром обмене информацией в военном, правительственном и частном секторах. Информационные сети, соединенные в Интернет постоянно обрабатывают частную, деловую и военную информацию. Подобные качественные изменения в процессах сбора данных, их переработки в информацию и распространении этой информации и составляют основу так называемой информационной революции.

Информация сейчас является стратегическим ресурсом, который должен управляться эффективно для того, чтобы достичь превосходства. В силу того, что информация играет такую ключевую роль, любое действие, предпринятое в информационной сфере, может иметь последствия для физической области (материалы, персонал, финансы) и для области абстракций (система убеждений).

Технологии информационной эпохи делают окружение, в котором ведутся боевые действия, более динамичным и непредсказуемым. Это делает национальные экономики более чувствительными к глобальному развитию, повышает культурное и политическое сознание части мирового населения и подпитывает радикальные движения, которые подталкивают мировую фрагментацию и дестабилизацию. Технологии информационной эры могут представить результаты военных действий (малых или больших) глобальной аудитории почти немедленно. Образы войны и мира - реальные или созданные - могут влиять на национальную волю и общественное мнение еще до того как аудитория проверит их аутентичность. Парадоксально, что поток информации в реальном времени налагает на сбор разведывательной информации еще большую потребность.

Уже начала возникать новая экономика, основывающаяся на информационных службах. Эта новая экономика разрушает иерархию промышленного мира. Поздняя промышленная эпоха - олигархическая смесь корпоративно-бюрократических обществ. Власть нынешней элиты основывается на системе плебисцитарной демократии, которая строго ограничивает общественное участие, выборы и знание. Крупные корпорации - как частные, так и государственные - которые и составляют правящую сеть нашего времени, должны контролировать информацию, чтобы держать систему в стабильности. Скоро все это изменится.

Информационная революция существенно снизила, если не полностью устранила способность правительств контролировать информацию, получаемую населением. Наличие информационной технологии является столь важным фактором, что тот, кто использует эту технологию, должен также смириться с огромными социальными изменениями. Тот же, кто отвергает эту технологию, сталкивается с риском физического уничтожения.

Интернет стал очень популярным источником информации и каналом связи. Он показал, как трудно осуществлять контроль над информацией. Содержание печатных средств СМИ и телевидения гораздо легче контролировать - количество продуктов ограничено, а аудитория пассивна - в Интернете же каждый является и потребителем, и производителем.

Информационная революция меняет облик институтов. Она устраняет иерархии, распыляет и перераспределяет власть (часто в сторону меньших элементов), пересекает и перекраивает границы, расширяет горизонты времени и пространства. Информационная революция усиливает важность сетей (например, социальной или коммуникационной). Она дает возможность различным и удаленным действующим лицам связываться, консультироваться, координировать друг с другом действия на больших расстояниях и с лучшей информацией, чем до того. Информационная революция будет являться причиной сдвигов в путях конфликта между обществами и методах военных действий - конфликты на уровне общества и боевые действия в области управления и контроля на военном уровне. Оба типа связаны с информацией, они также лишь формы войны за знания общества или военных о себе и противниках.

Информационная технология является "великим уравнителем" для государств, как в мирное время, так и во время войны. Эта технология не знает государственных границ и распространяется по всему миру. Многие компоненты и системы доступны на международном рынке. Информационная революция создала окружение, в котором государственный суверенитет подвергается пересмотру. Поэтому конфликт между государствами и негосударственными объединениями столь же вероятен, как и конфликт между двумя государствами.

Новые формы международного конфликта

При рассмотрении возможных форм конфликтов следует помнить, что военная мысль состоит из совокупности теорий, подходов, взглядов и парадигм, которые принадлежат к конкретной эпохе, обществу или лицу. Военная теория связана с историческим наблюдением и систематическим изучением организации, стратегий, тактик, техник и процедур от античности до наших дней. Она является средством образования как для военных, так и для политиков. Она также дает основу для выработки доктрины, которая в свою очередь создает общую философию и практику для разрешения проблем в реальном мире (либо посредством боевых действий, либо другими способами). Короче говоря, доктрина - общепринятый канон.

История войн может быть разделена на три больших периода (или волны), соответствующих истории развития человеческих цивилизаций: аграрный, промышленный и информационный. Будущие войны для цивилизаций третьей волны должны принимать форму информационных войн. Часто думают, что информационная война - это война, основывающаяся на совершенных системах связи, доступу к космосу, и процессу принятия решений в реальном времени. На самом деле, простое применение подобных технологических новшеств - это новый путь ведения старых боевых действий. Это война информационной эпохи, а не информационная война.

Борьба за информацию отличается от борьбы за территорию или природные ресурсы. Финансово-промышленные группы и даже государства, которые борются за информацию, будут значительно отличаться от тех, которые воевали за материальные ресурсы. Сама природа информации должна влиять на политику правительства, устанавливать ограничения на государственный суверенитет. Постоянное совершенствование и защита информационных средств являются предпосылкой для выживания обществ "третьей волны".

С древнейших времен враги вели войны в пяти измерениях - политическом, социальном, технологическом, операционном и в области снабжения - которые связаны с четырьмя элементами национальной мощи - политическим, социально-психологическим, военным и экономическим. Игнорирование даже одного из них может привести к катастрофическому поражению. Политическое измерение состоит из политических целей и политики как процесса. Политические цели всегда направляли войны, хотя и не всегда до конца последовательно. Социальное измерение - воззрения и обязательства людей - также остается важным. Технология воздействует на каждое измерение и на все уровни войны. Она взаимодействует с культурой и событиями во времени и пространстве и оказывает воздействие на продолжительность, природу и результаты конфликта. Операционное измерение связано с ведением войны. Оно состоит в основном из попыток доминировать на поле боя и разрушить вражескую волю сражаться.

Последней доминирующей операционной концепцией прединформационной эпохи была концепция последовательных операций, когда в бой постепенно (эшелонами) вводились все новые и новые резервы, и победа зависела от наличия этих резервов и правильного выбора момента для их использования. Однако уже к середине 1980-х годов способность наносить удары одновременно на всем протяжении поля боя сделала последовательные операции устаревшими. Боевые действия в будущем включат в себя множество задач и множество одновременных действий, проводимых на огромных территориях. Появляющиеся информационные технологии предлагают мощные возможности для помощи лицу, принимающему решения, но они же имеют множество ограничений и уязвимы. С точки зрения инженерии каждое новое поколение систем для управления и контроля более сложно, чем предшествующее. Хотя пользователи и признают и принимают эту сложность, они требуют устройств, которыми просто пользоваться.

Мы видим, что революция в военном деле сделала необходимым рассматривать еще и информационное измерение. Однако мы не должны рассматривать информацию как физическое измерение (как территорию, воздух или море). Информационное превосходство не работает так же как превосходство в воздухе. Ведение боевых действий в новых условиях требует и совершенной новой парадигмы. Ее основные положения могут быть сведены к следующему:

каждый компонент системы играет роль в определении результата; предсказуемые и непредсказуемые явления сосуществуют и взаимодействуют, приводя к созданию комплексных сетей с огромным количеством переменных величин, делающим невозможным предсказание результата;

незначительное изменение в системе входа может привести к непропорционально большим изменениям в результатах;

системы - отдельные лица, армии, бюрократия - имеют тенденцию эволюционировать в сторону своего усложнения;

комплексные системы в случае встречи с вызовами могут реорганизовывать себя.

Соперничество (или боевые действия) в рамках подобной парадигмы вероятнее всего способны принять форму информационной войны, которая означает конфликт, связанный с информацией на стратегическом уровне между государствами или обществами. Она может быть направлена на общественное или элитное внимание. Она может включать дипломатию, пропаганду и психологические кампании, политическую и культурную подрывную работу, введение ложных данных в местные СМИ, проникновение в информационные сети и базы данных, продвижение оппозиционных или диссидентских движений посредством компьютерных сетей. Главными целями являются те общественные и экономические области, доступ к которым достаточно легок. Информационная война может вестись правительством против незаконных групп или организаций, вовлеченных в терроризм, распространение оружия массового поражения или транспортировку наркотиков. Или наоборот, она может вестись против политики конкретного правительства приверженцами групп и движений, связанных, например, с вопросами охраны окружающей среды, гражданских прав, или религиозными вопросами. Некоторые движения все в большей степени используют организацию трансграничных сетей и коалиций и используют современные технологии информации и связи для укрепления своих позиций. Это вполне может оказаться сценой нового идеологического конфликта, где информационная война будет его главной характеристикой.

Один из факторов информационной войны - необходимость знать архитектуру и параметры вражеской системы. Сторона, которая лучше понимает мотивацию, структуру и цели врага, лучше подготовлена к конфликту. Понимание вражеской культуры и использования информационных систем в его обществе остается важным.

Глобальная информационная война отличается от компьютерных преступлений тем, что она предполагает враждебные действия со стороны противника - будь то частное лицо, конкурирующая организация или враждебное государство - в борьбе за гегемонию на рынке или политической арене. Однако информационная война шире, чем просто военное измерение. Она гораздо шире, чем боевые действия в области управления и контроля. В основном набор целей для информационной войны не будет набором военных целей. "Информационная война - электронный конфликт, в котором информация является стратегическим активом, достойным завоевания или уничтожения. Компьютеры и другие коммуникационные и информационные системы будут являться целями для первого удара и одновременно оружием в новой войне".

В широкой перспективе информационная война ведется во многих измерениях. Она является государственной стратегией, которая задействует все рычаги национальной мощи для создания преимуществ на стратегическом уровне. Она является больше чем просто применением информационных технологий для увеличения эффективности современных инструментов войны. Она представляет собой действия, необходимые для того, чтобы парализовать не только системы военного управления и контроля противника, но и его политическую и финансовую системы.

Информационные войны

В последние десятилетия достижения науки и технологий как никогда прежде начали определять динамику экономического роста, уровень благосостояния населения, конкурентоспособность государств в мировом сообществе, степень обеспечения их национальной безопасности и равноправной интеграции в мировую экономику.

Стремительное развитие и широкое использование информационно-коммуникационных технологий (ИКТ) ознаменовали собой переход человечества на абсолютно новую ступень развития, явившись результатом революции в сфере информатизации. ИКТ трансформировали не только принципы и формы сбора, обработки и передачи информации, они начали оказывать мощнейшее воздействие на культурный, экономический, политический и военно-стратегический аспекты жизни общества, становясь одним из основных факторов обеспечения и поддержания устойчивого развития.

В настоящее время все мы являемся свидетелями перехода от индустриального общества к обществу информационному, в основе которого лежат новейшие технологии и средства коммуникации. Последние достижения в области ИКТ открыли широчайшие позитивные возможности для расширения взаимодействия на общее благо всех государств, увеличения созидательного потенциала человечества и дополнительных сдвигов к лучшему в распространении информации в глобальном сообществе.

Количество, технический уровень и доступность информационных ресурсов уже сейчас определяют уровень развития страны и ее статус в мировом сообществе и бесспорно станут решающим показателем этого статуса в самое ближайшее время.

Вместе с тем, развитие процесса информатизации мирового сообщества порождает целый комплекс негативных геополитических последствий.

ИКТ быстро становятся важным стимулом развития военного потенциала стан за счет повышения их информационной обеспеченности. Появляется возможность использования информационного потенциала развитыми в научно-технологическом отношении странами для подавления и подчинения себе государств менее развитых и, следовательно, более слабых. Это неизбежно ведет к ускорению поляризации мира, становящейся источником нестабильности, основой для возникновения и развития реальных и потенциальных конфликтов, в том числе тех, которые могут приобрести общемировой характер. Изменение глобального и региональных балансов сил, усиление напряженности между традиционными и нарождающимися центрами силы, появление новых рубежей глобального противостояния порождает возможность возникновения военных конфликтов.

В Беларуси такому аспекту укрепления стратегической стабильности, как обеспечение информационной безопасности, уделяется особое внимание. Действительно, высокая сложность и одновременно уязвимость всех систем, на которых базируются национальное, региональные и мировое информационные пространства, а также фундаментальная зависимость от их стабильного функционирования инфраструктур государств приводят к возникновению принципиально новых угроз. Эти угрозы связаны, прежде всего, с потенциальной возможностью использования ИКТ в целях, несовместимых с задачами поддержания международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека.

Особая озабоченность в этом плане возникает в связи с разработкой, применением и распространением информационного оружия, в результате чего становятся возможны информационные войны и информационный терроризм, способные вызвать мировые катастрофы, разрушительные последствия которых сопоставимы с последствиями применения оружия массового уничтожения.

Компьютерные средства в корне меняют сами принципы ведения военных действий, поскольку могут позволить проводить более оперативные и менее кровопролитные военные операции. Вместо того, чтобы рисковать потерей дорогостоящей и требующей продолжительного времени для своего воспроизводства военной техникой и многочисленными войсками, командование с помощью компьютерных терминалов имеет возможность, осуществляя проникновение в компьютерные сети иностранных государств, выводить из строя радары, электронную аппаратуру, нарушать телефонную связь, то есть воздействовать на объекты критической инфраструктуры, целенаправленно влиять на сознание граждан.

Применение информационного оружия - реальность, с которой нельзя не считаться. Еще в середине 80-х годов стало известно о том, что во время американо-иранского кризиса, вызванного захватом американских заложников в Тегеране, США удалось с помощью специальной компьютерной программы практически мгновенно заблокировать все зарубежные счета этой страны. Отдельные виды информационного оружия применялись в вооруженных конфликтах в Панаме 1989 году, на Гаити в 1994 году, во время карательной операции "Буря в пустыне", а также в Югославии. Применение информационного оружия прогнозируется и при проведении военной операции против Багдада в марте 2003 года.

Информационное оружие стало важной частью вооружения сил общего назначения США и их союзников. Расходы США за последние 15 лет на разработку и приобретение средств информационной борьбы выросли в 4 раза и занимают в настоящее время первое место среди расходов на все военные программы. Новые информационные технологии взяты на вооружение спецслужб.

По данным главного контрольно-финансового управления Конгресса США в настоящее время примерно 120 стран мира ведут работы или уже завершили отдельные разработки по развитию возможностей информационно-компьютерного воздействия на информационный ресурс потенциального противника. Для сравнения: разработки в области ядерного оружия ведутся не более чем в 20 странах.

Активизируется киберпреступность, основной целью которой являются не СМИ и Интернет, как это зачастую представляется в печати, а системы управления государством, экономикой, манипулирование личным и общественным сознанием. Число успешных взломов компьютерных систем различного назначения за последние пять лет выросло в тысячи раз, составив в 2002 году более 30 тысяч проникновений.

Крупнейшие кибератаки последних лет привели к опасным сбоям в работе телекоммуникационных сетей, зачастую угрожающим критическим объектам физической инфраструктуры государств, нанесли значительный материальный ущерб. Так, распространенный в сети Интернет в 2001 году вирус Коуд Ред заразил 314 тысяч серверов и через них осуществил попытку атаковать компьютерную сеть Белого Дома. В 1999 и 2000 годах неидентифицированные хакеры проникли в компьютеры Министерства обороны США и лабораторий в Лос-Аламосе и Ливерморе и похитили внутренние документы, содержавшие весьма чувствительную информацию.

Одной из крупнейших информационных атак на Интернет за всю его историю стала начавшаяся 26 января 2003 года и продолжавшаяся два дня атака сетевого "червя" Хелкерн. Воздействие Хелкерн на мировые информационные ресурсы уже признано экспертами по компьютерной безопасности беспрецедентной по скорости распространения и размерам уже нанесенного и потенциального ущерба --- по оценкам, более 10 млрд. долларов.

В результате атаки было заражено 80 тысяч веб-серверов, а Интернет замедлил свою работу во всем мире в среднем на 25%. Аналитики полагают, что Хелкерн стал "важнейшим шагом в создании информационного оружия", поскольку до сих пор ни одному вирусу не удавалось столь эффективно препятствовать обмену интернет-трафиком.

Уязвимость киберпространства делает его весьма привлекательным средством совершения террористическими организациями, криминальными группами и отдельными злоумышленниками преступного воздействия, направленного против общественных интересов, безопасности государств, организаций и граждан.

Включение новейших информационно-телекоммуникационных технологий и средств в арсеналы террористических организаций чрезвычайно опасно, поскольку оно радикально трансформирует сами методы террористической деятельности. Возможность широкого использования ИКТ экстремистскими элементами позволяет им формировать высокоэффективные и гибкие сетевые организационные структуры, объединяющие разрозненные группы в транснациональные террористические сообщества, существование которых весьма сложно обнаружить вплоть до момента совершения террористического акта. ИКТ позволяют террористическим организациям переходить от "точечных" воздействий к систематическому и зачастую замаскированному воздействию на информационные инфраструктуры. Они дают возможность даже любителям использовать "хакерские" методы в преступных и террористических целях, примером чему может быть и упомянутая атака вируса Хелкерн.

В случае же проведения информационных операций государствами, преступная деятельность может маскироваться под акты террористических групп. В этой связи наряду с проблемами поиска стратегии защиты от террористического воздействия всю большую остроту приобретают задачи идентификации противника в информационном пространстве и адекватного реагирования на возникающие вызовы.

Анализ ставших известными кибератак показывает, что ИКТ уже освоены и международными террористическими и экстремистскими организациями (Хамаз, Аль-Кайда) и национальными сепаратистскими движениями (Тигры освобождения Тамил Илама и др.).

В последнее время в мировых СМИ появились публикации, в которых ставится вопрос о связи крушения шаттла Колумбия с потенциально имевшей место информационной атакой. Так, одной из возможных причин трагедии называется попадание в компьютерную систему челнока вируса во время одного из сеансов связи, осуществлявшегося Центром управления полетами (ЦУП) с помощью впервые установленных на борту Колумбии средств доступа в Интернет. Военные эксперты, входящие в состав одной из комиссий, отвергают такую версию, поскольку вся информация с шаттла на Землю и обратно на корабль проходила через мощную систему контроля в ЦУП, что уже гарантирует ее проверку, однако, даже если это и так, возможность "запуска" вируса потенциально существовала.

Невзирая на уже проведенные кибератаки, осуществленные через Интернет, критические объекты инфраструктуры продолжают подключаться к этой сети. Недавно в США были продемонстрированы образцы новейшей продукции корпорации Боинг, в частности, одного из подразделений корпорации --- Боинг конненшн, которая в настоящее время занимается разработкой и внедрением систем связи с самолетами и предоставления находящимся в воздухе пассажирам возможности пользоваться Интернетом. По этим системам информация с борта самолета о его состоянии будет передаваться на землю. Разрабатываемая система уже сейчас установлена на пяти дальнемагистральных самолетах "Боинг-747" и ведется ее отработка с тем, чтобы к концу этого года приступить к ее внедрению к коммерческую эксплуатацию.

Озабоченность в этой связи вызывает тот факт, что при необходимости с земли можно будет вмешиваться в процесс управления в случае, например, захвата борта террористами. Это означает, что террористы получат потенциальную возможность осуществлять захват прямо с земли, произвольно менять курс самолетов. Это может привести к еще более масштабным и страшным последствиям, чем те, которые произошли в США 11 сентября 2001 года.

Хотя по заявлениям американских официальных лиц причинить смерть или вызвать продолжительные нарушения функционирования объектов жизнедеятельности общества при проведении кибератак весьма сложно, в связи с использованием дублирования систем и жестких проверок услуг или продукции на выходе, такая потенциальная возможность сохраняется. Кроме того, владельцами более 80% критической инфраструктуры в США являются частные компании, которые зачастую не обеспечивают необходимый уровень защиты своих систем.

Несмотря на заявления американских официальных лиц о преувеличенности угрозы кибератак, американцы понимают, что угроза реально существует. 14 февраля 2003 года в США была подписана разработанная по распоряжению президента Буша Национальная стратегия по обеспечению безопасности киберпространства. В основе стратегии лежит осознание того, что с распространением информационных технологий критические инфраструктуры начинают все больше зависеть от работы связывающих их компьютерных сетей, умышленные злонамеренные нарушения в работе которых могут иметь самые разрушительные последствия для государственной безопасности.

В Стратегии, в основном, рассматриваются вопросы технического обеспечения американцами безопасности "своих" участков сетей, в частности, при помощи установления компьютерных антивирусных программ, систем защиты файр-уолл, повышение качества обучения и осведомленности о проблеме, однако игнорируется военно-политический аспект проблемы. Стратегия не прописывает меры по обеспечению безопасности, которые должны предприниматься промышленностью, не прописаны и нормы, регулирующие взаимодействие участников в этой области (правительство, промышленность, неправительственные и другие организации и частные пользователи). Отсутствие таких норм, по мнению многих, приведет к тому, что на деле Стратегия может оказаться неэффективной даже в рамках одних лишь США.

Более того, необходимо понимать, что в сегодняшнем глобальном мире даже такое сильное государство как США не может в одиночку обеспечить свою безопасность. Нельзя рассчитывать на то, что, оставляя возможности для применения и распространения информационного оружия, можно обеспечить безопасность национальных компьютерных сетей и зависящей от них инфраструктуры.

Осознавая сохраняющиеся в ситуации отсутствия всеобъемлющего международного подхода к проблеме обеспечения МИБ опасности в сфере информационного противостояния, американцы готовят почву для нанесения ответного удара в случае, когда это будет необходимо. В соответствии со Стратегией США резервируют за собой право "адекватным образом" отвечать на кибератаки, причем понятно, что такой ответ не будет ограничен одними лишь судебными разбирательствами.

В январе 2003 года официальные лица США заявили о том, что Министерство обороны может вести информационную войну в случае, если на страну будет совершено информационное нападение, а в начале февраля официальные лица в Администрации Президента США сообщили, что Дж. Буш подписал секретную директиву, в соответствии с которой Правительство впервые должно будет разработать национальное руководство, определяющее условия, при которых Соединенные Штаты будут проводить кибератаки на компьютерные сети свих противников, а также правила проникновения в иностранные компьютерные системы и нарушения их нормальной работы.

Интересно отметить, что в части, касающейся международного сотрудничества, которой, кстати, в 76-страничном документе отводится полторы страницы, говорится о том, что США будут работать в рамках международных организаций с тем, чтобы продвигать т. н. "культуру безопасности", содействовать расследованию киберпреступлений и привлечению к ответственности ответственных за их совершение, будут содействовать созданию международной сети по наблюдению и оповещению об угрозах совершения кибератак или же о факте их совершения. О выработке юридически обязывающего международного документа в этой сфере, даже в перспективе, речи не идет.

Проблема общемирового противодействия угрозам информационной безопасности усугубляется тем, что до сих пор не выработано общепринятого определения "информационного оружия". Известно, что этот термин впервые стал употребляться в американских военных кругах в 1991 году, после окончания войны в Персидском заливе. Осложняет вопрос дефиниций то обстоятельство, что информационные технологии большей своей частью выступают как технологии невоенного или двойного назначения. Информационные агрессии могут осуществляться с помощью обычных персональных компьютеров с использованием широких технологических возможностей Интернет и примеры тому многочисленны.

В самом общем виде информационное оружие можно определить как технические и другие средства, технологии, методы и информация, предназначенные для оказания "силового" воздействия на информационное пространство противника, оборонные, управленческие, политические, социальные, экономические и другие критически важные системы государства с целью нанесения им ущерба и достижения превосходства в информационном противоборстве.

Особенность процесса информационной милитаризации заключается в том, что ИКТ, при помощи которые могут осуществляться военные операции, первоначально появляются и, главным образом, задействованы в гражданском секторе, и лишь потом и, зачастую, лишь временно, переходят в военный.

К характерным чертам информационного оружия можно отнести его универсальность, радикальность воздействия, доступность. Для его приведения в действие не требуется больших затрат финансовых средств, что делает информационную войну экономичным и потому весьма опасным средством вооруженной борьбы. Его применение носит обезличенный характер и легко маскируется под мирную деятельность. Одновременно, трудно определить его национальную принадлежность и государство, осуществившее информационную атаку. Дело осложняется еще и тем, что агрессии зачастую осуществляются с территории третьих стран. Информационное оружие не знает географических расстояний, подрывает традиционное понятие государственных границ, делая их технологически проницаемыми. Использование этого оружия может происходить скрыто, без объявления войны, и не нуждается в большой и видимой подготовке. Подчас жертва может даже не осознавать, что находится под информационным воздействием. К тому же, в связи с отсутствием систем и методик, оценивающих угрозу и заранее предупреждающих о готовящемся нападении, осложняется возможность противодействовать такой агрессии. Выработка критериев определения факта атаки на информационные инфраструктуры и создание "системы раннего оповещения", подобной созданной в годы "холодной войны" системы предупреждения о военном нападении представляется затруднительной в связи с постоянной и быстрой эволюцией характера угроз в инфосфере.

Все это делает разработку, постановку на вооружение, применение и распространение информационного оружия и особенно его попадание в руки агрессивных режимов чрезвычайно опасным.

Информационное оружие включает в себя средства высокоточного распознавания и местоопределения оборудования, излучающего в радиомагнитном спектре, наведения на него и его огневого поражения; средства вывода из строя компонентов радиоэлектронных систем и программного обеспечения; средства дезорганизации функционирования подсистем обмена информацией путем воздействия на среду и алгоритм распространения сигналов; средства управления восприятием, пропаганды, дезинформации и, наконец, психотронное оружие.

Наиболее опасно применение информационного оружия против военных и гражданских объектов и структур, которые должны находиться в состоянии непрерывной работоспособности и функционировать в реальном масштабе времени. Результаты враждебного воздействия на их работу могут иметь катастрофический характер.

Хотелось бы отметить псевдогуманную сторону информационной войны. Ее ведение может непосредственно не приводить к кровопролитию, жертвам, видимым разрушениям, сопутствующим обычным военным действиям. Это способно породить в мире опасную беспечность и терпимость в отношении применения информационного оружия, большую снисходительность к их использованию при проведении односторонних санкций, если последние формально будут основываться на электронике, а не на убийстве. Гражданское общество, не осознавая того факта, что развитие военно-информационных возможностей, хотя и не будучи связано с наращиванием вооруженных сил и даже, наоборот, приводя к их сокращению, приводит к наращиванию военного потенциала стран.

Более того, по оценкам экспертов, применение информационного оружия должно постоянно сопровождаться ограниченным применением обычного оружия, особенно высокоточного, или угрозой его применения.

Нельзя не упомянуть и о возможных угрозах правам и свободам граждан в связи с применением информационного оружия. Технологическими методами можно свести на нет величайшие завоевания демократии: право на свободу распространения информации и доступа к ней, конфиденциальность информации о частной жизни и приватного информационного обмена между частными лицами.

Проблема обеспечения международной информационной безопасности осложняется в первую очередь тем, что она до сих пор не стала объектом регулирования международного права. В эпоху глобализации, которая затронула и научно-техническую, и информационно-телекоммуникационную сферы, а, во многом, и была вызвана появлением в этих областях прорывных разработок, связи между странами становятся все более зависимыми от основанных на информационных технологиях инфраструктур, пересекающих государственные границы. Международный характер угроз информационной агрессии и преступности определяет необходимость взаимодействия как на региональном, так и на глобальном уровне, с тем, чтобы принять согласованные меры для снижения существующих угроз. Ни одному государству не под силу добиться этого в одиночку.

Осознание того факта, что появление и распространение информационного оружия, милитаризация информационных технологий явятся мощным дестабилизирующим фактором международных отношений и подвергнут серьезному испытанию всю систему международных договоренностей по поддержанию стратегической стабильности, в т. ч. и на региональных уровнях; стремление выйти из губительного цикла гонки новых технологических вооружений и перевести процессы гражданской и военной информатизации в плоскость международно-правового регулирования побудили Россию и Беларусь взять на себя инициативу в рамках мирового сообщества об официальной постановке вопроса обеспечения международной информационной безопасности.

Принципиальная позиция Беларуси состоит в необходимости жесткого соблюдения принципов неприменения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека и недопущения использования информации и телекоммуникаций в противоречащих Уставу ООН целях.

Учитывая масштабы глобального информационного вызова, ставящихся им проблем, невозможность их решения усилиями одной или даже нескольких стран, на блоковой основе, российская и белорусские стороны приняли политическое решение о том, чтобы продвигать инициативу по МИБ прежде всего в рамках ООН - глобальной организации, способной обеспечить решение любой политической проблемы комплексно, при самом широком представительстве и максимальном учете интересов всего мирового сообщества.

В соответствии с ее рекомендациями Институтом ООН по проблемам разоружения (ЮНИДИР) и Департаментом по вопросам разоружения Секретариата ООН в августе 1999 года в Женеве был организован международный семинар по вопросам международной информационной безопасности. В семинаре приняли участие представители более 50 стран, включая экспертов из наиболее развитых в информационно-технологическом плане государств.

Задача семинара заключалась в выявлении подходов различных стран в связи с предстоящим продолжением дискуссии по этой теме на 54-й сессии ГА ООН. Основным итогом семинара стало подтверждение актуальности проблемы информационной безопасности и своевременности постановки этого вопроса в международном плане.

В то же время, в рамках обсуждения обозначились по крайней мере два различных подхода к существу проблемы.

Эксперты ряда развитых стран, включая США, исходили из приоритета рассмотрения и разработки мер информационной безопасности применительно к угрозам террористического и криминального характера. При этом угроза создания информационного оружия и возникновения информационной войны сторонниками такого подхода рассматривалась скорее как теоретическая. Соответственно отпадал и собственно разоруженческий аспект общей проблемы международной информационной безопасности.

С другой стороны, приверженцы иного курса (в основном это представители развивающихся стран, СНГ, Китая) поддерживали концепцию рассмотрения проблемы международной информационной безопасности в комплексе, с выделением в качестве приоритетной задачи ограничение потенциальной угрозы развязывания информационной войны. При этом подчеркивалась необходимость безотлагательно приступить к обсуждению и практической разработке международно-правовой основы универсального режима международной информационной безопасности. Выдвигалось, в частности, предложение о создании специального международного суда по преступлениям в информационной сфере.

Эта первая такого рода представительная встреча экспертов, несомненно, во многом способствовала рассмотрению на 54-й сессии ГА ООН проекта резолюции "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности". Проект впервые указал на угрозы международной информационной безопасности применительно не только к гражданской, но и к военной сферам. 1 декабря 1999 года резолюция (документ A/RES/54/49) консенсусом была принята Генассамблеей.

Принципы представляют собой своего рода рабочий вариант кодекса поведения государств в информационном пространстве, создавая для них по крайней мере моральные обязательства, и закладывают основу для широких международных переговоров под эгидой ООН и других международных организаций по этой проблематике. Кроме того, Принципы дают необходимые основные понятия по предмету МИБ.

Этой деятельности российской и белорусской сторон по продвижению инициативы МИБ противостояла оппозиция, состоящая, в основном, из США и ряда стран НАТО. В стремлении создать международно-правовой режим МИБ они усматривали угрозу свободе обмена информацией и конкуренции на рынке информационных технологий. Возможность создания информационного оружия и угроза возникновения информационных войн ими принижается. Отрицается, соответственно, и разоруженческий аспект проблемы.

Наблюдается тенденция к сдерживанию ими содержательной части дискуссии вокруг МИБ, сохраняя тем самым свободу для дальнейших разработок в сфере военного применения информационных технологий.

Большинство развивающихся стран мира, с одной стороны, усматривают в подходах Запада угрозу их изоляции от активного участия в решении проблемы и, кроме того, попытку консервации их уязвимости от информационной агрессии и поэтому солидаризируются с предложенной концепцией изучения проблемы в комплексе, с выделением приоритетности потенциальной угрозы информационной войны.

В то же время наблюдаются расхождения в позициях стран НАТО, традиционно поддерживающих США в военно-политических вопросах в связи со значительной зависимостью своего оборонно-промышленного комплекса от этого государства. Европейцы осознали, что даже союзнический статус не гарантирует их от электронного проникновения со стороны США в свои компьютерные системы. В целом ряде стран Западной Европы ведутся официальные расследования по поводу деятельности против них принадлежащей американскому правительству системы электронной разведки, прослушивания, промышленного шпионажа и сбора стратегической информации "Эшелон".

Ряд развивающихся стран, "подхватывая" предложенную концепцию, выступают с крайне радикальных, порой взаимоисключающих позиций - от полного запрещения информационного оружия уже сейчас до призывов обратить это "изобретение Запада" против него самого. Очевидно, что такие подходы могут привести к конфронтации в ООН, блокированию обсуждения этой темы вообще.

Тем не менее, можно констатировать, что, несмотря на противодействие США, международное сообщество осознало существо и актуальность проблемы МИБ и, в целом, склоняется к необходимости ее дальнейшего рассмотрения и согласованного решения.

В итоге 55-й сессии Генассамблеей 20 ноября 2000 года консенсусом был одобрен новый проект резолюции (А/RES/55/28), в котором отмечается, что целям ограничения угроз в сфере информбезопасности отвечало бы "изучение соответствующих международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем".

Данное положение было чрезвычайно важно с дипломатической и политической точек зрения, поскольку оно подготовило почву для следующего очень важного этапа в плане продвижения темы МИБ в ООН.

Принципиальным отличительным моментом резолюции, принятой консенсусом на 56-й сессии Генассамблеи ООН 29 ноября 2001 года (документ A/RES/56/19), является создание в 2004 году специальной группы правительственных экспертов государств-членов ООН для изучения проблемы МИБ, а именно рассмотрения существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению, а также исследования международных концепций, которые были бы направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем. Доклад о результатах исследования должен быть представлен группой экспертов Генеральной Ассамблее на ее 60-й сессии.

Невзирая на противодействие ряда стран, пытавшихся блокировать какие-либо попытки обсуждения военной составляющей вопроса, наличие которой для большинства стран-членов ООН представляется очевидным, российской и белорусской дипломатии удалось добиться перевода обсуждения в практическую плоскость.

Консенсусно принятая 22 ноября 2002 года ГА ООН резолюция по МИБ (документ A/RES/57/53) указывает на недопустимость использования информационно-телекоммуникационных технологий и средств в целях оказания негативного воздействия на инфраструктуру государств. Резолюция подтверждает просьбу к Генеральному секретарю, содержащуюся в пункте 4 резолюции 56/19, относительно создания группы правительственных экспертов.

Необходимо отметить, что в последнее время в позициях ключевых игроков в сфере МИБ наметились некоторые изменения. Так, хотя США продолжают стремиться обеспечить свое доминирование в информационной сфере, относящейся к области вооружений, и продолжают на первый план выдвигать вопросы информационного терроризма, информационной преступности и обеспечения безопасности компьютерных сетей, в Вашингтоне начало расширяться понимание того, что проблемы противодействия современным формам терроризма непосредственно связаны с вопросами распространения информационного оружия.

После терактов, произошедших в сентябре 2001 года в США, европейцы также пришли к выводу о том, что информационная инфраструктура государств-членов ЕС не гарантирована от вероятных информационных атак. Особые озабоченности в этом плане вызвали представленные в мае 2001 года выводы доклада Европарламента о функционировании американской системы электронного шпионажа "Эшелон".

Учитывая признание мировым сообществом необходимости активизации международного сотрудничества в сфере МИБ и собственное весьма активное участие в программах борьбы с компьютерными преступлениями, в частности, европейскими, США поддержали создание группы экспертов по МИБ. Они стали более открыты для проведения двусторонних консультаций, на которые ранее идти отказывались.

Осознание американцами важности проблемы военного применения ИКТ связано также и с обострением ситуации на Ближнем Востоке, вызвавшее резкое возрастание вероятности совершения информационных атак уже не только отдельными лицами, организациями и террористическими группами, но также и государствами, при сохраняющейся неспособности западных государств предупреждать и эффективно отражать такие атаки.

Тем не менее, выстраивание какого-либо будущего международно-правового механизма американцы, можно предполагать, планируют так, чтобы обеспечить себе свободу рук для разработки и применения информационного оружия.

В этом плане показательна подготовка к военной операции в Багдаде. По информации зарубежных СМИ, в США были специально разработаны планы вторжения во внутренние сети банков и целью закрытия счетов Саддама Хусейна и его семьи, вывода из строя серверов иракской службы ПВО и задействованных в военных и гражданских инфраструктурах компьютеров с использованием направленного микроволнового излучения.

Главной своей задачей в плане ведения информационной войны в Ираке американцы считают обнаружение электронных коммуникаций на месте и обеспечение доступа к ним (например, с помощью установки ультрасовременных "жучков"). Такая схема действий была отработана еще во время проведения операции "Буря в пустыне" в 1991 году.

По информации, опубликованной в марте 2003 года на сайте германской телерадиовещательной компании Немецкая волна (http://www.dw-world.de/russian), к поставленным в Ираке в то время "жучкам" в последнее время добавились и специальные идентификаторы, называемые "линками" (от англ. links), установленные местными агентами американских спецслужб. Они уже сейчас позволяют американцам подключаться к линиям оптико-волоконной связи, перехватывать переговоры по мобильным станциям частей иракской армии.

Массированное воздействие на сознание отдельных индивидов, группы общества, военные формирования были проведены США в Ираке в преддверии военной операции против него с тем, чтобы подорвать дух нации, деморализовать, сломить решимость защищать суверенитет страны. США удалось перехватить частоту, на которой осуществлялось вещание иракского государственного телеканала, и начать передачу пропагандистской информации. Усилиями американцев Багдад был отрезан от внешнего мира, оказался в информационной блокаде. Мировое телевещание компании CNN также самым активным образом поддерживает антииракскую компанию, призывая к свержению действующего режима.

В принятой на встрече лидеров стран "восьмерки", состоявшейся в июле 2000 года в Окинаве (Япония), хартии Глобального информационного общества (так называемая Окинавская хартия), страны "восьмерки" признали ИКТ в качестве основного фактора, формирующего общество 21 века, и подтвердили свою готовность содействовать переходу к информационному обществу, а также полной реализации его преимуществ.

Страны выработали и включили в итоговый документ Саммита ключевые направления работы для достижения поставленной цели, в частности, в области укрепления политики и нормативно-правовой базы по борьбе со злоупотреблениями, подрывающими целостность информационных сетей. Стороны согласились с тем, что усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности пространства, осуществлению эффективных мер по борьбе с компьютерной преступностью. Документ предполагает также расширение сотрудничества стран "восьмерки" в рамках Лионской группы по транснациональной организованной преступности. Была поставлена проблема борьбы с попытками несанкционированного доступа и компьютерными вирусами.

Для защиты критических и информационных инфраструктур было решено привлекать представителей промышленности и других негосударственных организаций посредников. Действительно, правительства в одиночку не способны обеспечить безопасность киберпространства, в связи с чем особую важность приобретают усилия каждого пользователя киберпространства по содействию обеспечению безопасности в том участке пространства, которым он владеет или пользуется, и это не только промышленные предприятия, но и организации всех секторов экономики, университеты, местные органы власти, а также граждане --- пользователи Интернет.

Таким образом, страны "Группы восьми" пошли на закрепление в итоговом документе лишь вопросов целостности информационных сетей и пресечения преступлений в компьютерной сфере, игнорируя тем самым военно-политическую составляющую проблемы МИБ. Фактически проблема военного применения ИКТ на уровне государств не была отражена в документе, а ведь именно военный аспект использования информационных средств и технологий является первостепенным по своей значимости и наиболее опасным с точки зрения потенциальных последствий применения информационного оружия.

В настоящее время активно ведется подготовка к проведению Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) (первый этап --- Женева, 10--12 декабря 2003 года, второй --- Тунис, 2005 год). Большую роль в объединении мирового сообщества вокруг темы МИБ сыграла прошедшая в г. Марракеш, Марокко, с 23 сентября по 18 октября 2002 года 16-я Полномочная конференция Международного союза электросвязи (МСЭ) --- специализированного учреждения ООН, являющегося международной межправительственной организации и занимающегося вопросами развития электросвязи. В соответствии с резолюцией ГА ООН A/RES/56/183, принятой консенсусом 21 декабря 2001 года, МСЭ играет ведущую управленческую роль в рамках исполнительного секретариата ВВУИО и процесса подготовки к Саммиту.

В Полномочной конференции (ПК) 2002 года приняли участие около полутора тысяч делегатов, представляющих 143 страны. Решением ПК был принят "Вклад МСЭ в Декларацию принципов и план действий ВВУИО" (документ PLEN/1).

Одним из основных блоков в структуре вклада МСЭ в Декларацию принципов и План действий ВВУИО составляют вопросы доверия и безопасности при использовании ИКТ. Действительно, преимущества, которые может предоставить использование ИКТ, в полной мере могут быть реализованы лишь в случае надежности и безопасности соответствующих технологий и сетей и отказа от их использования в целях, несовместимых с задачами обеспечения международной стабильности и безопасности.

В этой связи в рамках этого блока страны-члены МСЭ вновь выразили опасение относительно того, что ИКТ могут оказывать негативное воздействие на безопасность государств как в гражданской, так и в военной областях и признали необходимость предотвращения использования информационных ресурсов или технологий для преступных или террористических целей.

В качестве одной из мер, которые можно было бы предложить для рассмотрения в ходе подготовке к ВВУИО, страны назвали рассмотрение существующих и потенциальных угроз для безопасности информационных и коммуникационных сетей.

Страны также согласились внести вклад в реализацию усилий ООН, направленных на оценку состояния информационной безопасности, а также рассмотрение вопроса о разработке, в долгосрочной перспективе, международной конвенции по безопасности в среде информационных сетей и сетей связи.

Нашедшие отражение во Вкладе МСЭ формулировки по МИБ в дальнейшем легли в основу соответствующих положений итоговых документов региональных конференций по подготовке к ВВУИО --- Общеевропейской конференции (Бухарест, 7--9 ноября 2002 года) и Азиатской конференции (Токио, 13--15 января 2003 года.

Одним из принципов информационного общества, зафиксированных в Бухарестской декларации, стал принцип укрепления доверия и безопасности при использовании ИКТ. Он подразумевает разработку "глобальной культуры кибербезопасности", которая должна обеспечиваться путем принятия превентивных мер и поддерживаться всем обществом при сохранении свободы передачи информации. Таким образом, это положение фактически повторяет соответствующее положение Окинавской хартии.

Государства, принявшие участие в конференции в Будапеште, пришили к пониманию относительно того, что "ИКТ могут использоваться в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, а также негативно воздействовать на целостность инфраструктуры внутри отдельных государств, нарушая их безопасность как в гражданской, так и в военной сфере". Страны также согласились с тем, что необходимо "предотвращать использование информационных ресурсов или технологий в преступных или террористических целях". В основу этих положений легла консенсусная резолюция ГА ООН по МИБ N 56/19.

В декларации зафиксировано, что в целях содействия доверию и безопасности в использовании ИКТ органы государственного управления должны способствовать осознанию обществом угроз, связанных с кибербезопасностью, и стремиться укреплять международное сотрудничество в этой сфере.

В Токийской декларации, которую приняли представители 47 стран, 22 международной и 116 неправительственной организаций, а также представители 54 частных компаний, выделены "приоритетные области действий" в области ИКТ. Важное место в их числе занимает вопрос обеспечения безопасности информационных технологий и средств. Признавая принцип справедливого, равного и адекватного доступа к ИКТ для всех стран, особое внимание стороны полагают необходимым уделить угрозе потенциального военного использования ИКТ. Стороны также согласились с необходимостью укреплять региональное и международное сотрудничество в целях укрепления безопасности инфосферы. Впервые было высказано мнение о том, что эффективное обеспечение информационной безопасности может быть достигнуто не только технологически, для этого потребуются усилия по правовому регулированию вопроса и выработке соответствующих национальных политик.

Включение важных для нас формулировок по МИБ в декларации подготовительных встреч к ВВУИО имеет принципиальное значение. Оно закладывает хорошую основу для последующего закрепление проблематики МИБ в итоговых документах Саммита. Это, в свою очередь, станет важным шагом в направлении правового регулирования проблематики МИБ.

На пути к выработке международно-правового режима в области МИБ следует обратиться к уже имеющимся прецедентам - принятым международным договорам и конвенциям в высокотехнологичных областях (Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела 1967 года, Конвенция по морскому праву 1982 года и др.), а также военных областях, в частности, целый ряд нераспространенческих договоров: Договор о нераспространении ядерного оружия от 1 июля 1968 года, Договор об ограничении систем ПРО от 26 мая 1972 года, Конвенция о запрещении химического оружия (вступила в силу 29 апреля 1997 года), Конвенция о запрещении биологического оружия (вступила в силу 26 марта 1975 года), Конвенция о запрещении применения, накопления запасов, производства и передачи противопехотных мин и об их уничтожении (Оттавская конвенция) от 18 сентября 1997 года.

Важно отметить, что разработка правовой базы в упомянутых областях велась медленно и непросто, поскольку мировое сообщество столкнулось с задачей кодификации деятельности в новой, технологически сложной и крайне чувствительной для их национальной безопасности сфере. Работа над этими договоренностями шла поэтапно, каждый последующий документ опирался на предыдущий, параллельно принимались общие принципы деятельности государств в соответствующих сферах.

В случаях, когда по тем или иным причинам невозможно было достигнуть согласия относительно строго обязательных договоров, были найдены иные приемлемые формы: международный кодекс поведения (например, по предотвращению распространения баллистических ракет), руководящие принципы (как в случае группы ядерных поставщиков), меморандумы о намерениях (например, в области ракетного нераспространения), ориентированные в некоторых случаях на достижение в последствии юридически обязывающих договоренностей.

Беларуси предстоит не ослаблять своих усилий на мировой арене, видя конечную цель своей дипломатической работы в создании глобального режима международной информационной безопасности.

Новые информационные технологии и исследование международных отношений

Говоря о влиянии новых информационных технологий на процесс исследования международных отношений, следует обратить внимание на две стороны вопроса: фундаментальные теоретические исследования и исследования прикладные.

В фундаментальных исследованиях по теории международных отношений появление этих технологий ведет с одной стороны к изменению самого предмета исследования, то есть самих международных отношений. Меняется роль государства, подвергаются пересмотру старые модели суверенитета, разрабатываются новые концепции безопасности. Разумеется, все это не облегчает жизнь теоретикам международных отношений, требуя от них своевременного теоретического осмысления фундаментальных изменений, происходящих в мировой системе. С другой стороны информационные технологии предоставляют теоретикам множество новых и достаточно мощных исследовательских инструментов. Прежде всего, это связано со все более широким применением количественных методов исследования. Однако их применением дело не ограничивается. Существующие сейчас системы позволяют отдельным исследователям осуществлять моделирование процессов, для которого еще десять-двадцать лет назад требовались усилия целых институтов. Подобное моделирование при правильной организации исследовательского процесса способно на порядок сократить время, необходимое для каждой стадии исследования, от генерирования гипотезы до ее проверки. Таким образом, несмотря на то, что новые технологии оказывают определенное влияние на труд исследователей занятых в теории международных отношений, говорить о революционных изменениях в этой области пока еще рано.

Гораздо заметнее изменения, которые новые информационные технологии внесли в труд аналитиков, занимающихся прикладными проблемами. Прежде всего, объем информации, доступной им, возрос в десятки, а то и в сотни раз. Причем речь идет лишь об информации, действительно относящейся к предмету исследования, игнорирование которой может сделать результаты анализа некорректными. Хотя сам доступ ко всей этой информации большей частью возможен, он далеко не всегда бесплатен (многие данные предоставляются только на коммерческой основе) и требует затрат на коммуникационное оборудование. Сам анализ подобного объема информации (время на который при большинстве прикладных исследований ограничено) также требует специального оборудования, программного обеспечения и труда многих достаточно квалифицированных специалистов самых разных специальностей (не всегда напрямую связанных с международными отношениями). В случае если исследование не являлось заказным, необходимо достаточно широкое распространение его результатов. В этой области потенциальные возможности, предоставляемые новыми информационными технологиями также велики. Однако и здесь зачастую требуются довольно значительные ресурсы.

Таким образом, можно говорить о том, что время аналитиков-одиночек в области прикладных международных исследований уходит в прошлое. Сейчас проводить подобные исследования способны лишь коллективы, обладающие соответствующей материальной базой. Прикладные международные исследования будут становиться уделом различных правительственных агентств и в еще большей степени - аналитических подразделений различных финансово-промышленных и так называемых финансово-информационных групп.