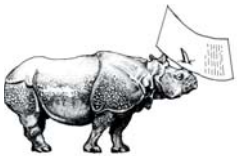

Роуз Готтемюллер[1]

ОТ МАНХЭТТЕНСКОГО ПРОЕКТА К ОБЛАЧНЫМ ТЕХНОЛОГИЯМ: КОНТРОЛЬ НАД ВООРУЖЕНИЯМИ В ИНФОРМАЦИОННЫЙ ВЕК

В настоящее время, проверяя выполнение странами взятых на себя обязательств в рамках договоров по контролю над вооружениями, мы используем сочетание обмена информацией, уведомлений о статусе вооружений (в каком районе страны находится та или иная межконинтентальная баллистическая ракета), инспекций на местах, а также национальных средств, в том числе так называемых национальных технических средств. Национальные технические средства — это крупные объекты: спутники наблюдения, радары с фазированной антенной решеткой, которыми отдельные страны могут управлять и которые они могут контролировать. В отношении договоров по контролю над вооружениями уже давно стало правилом не вмешиваться в национальные технические средства друг друга: мы даем друг другу возможность пользоваться этими глазами и ушами для проверки выполнения договоров. Все элементы, которые я перечислила, в сумме обеспечивают эффективный режим проверки.

ДУХ ИСТОРИИ

Должна объяснить, что мы подразумеваем под эффективной проверкой. Посол Пол Нитце определил ее следующим образом: «Если другая сторона решит выйти за пределы договора любым существенным в военном отношении образом, мы должны быть в состоянии вовремя обнаружить такие нарушения, чтобы эффективно отреагировать и тем самым не позволить другой стороне получить выгоду от нарушения договора». Таково определение эффективного контроля, и оно является критерием проверки соблюдения договора. Теперь давайте подумаем: чтобы соответствовать этому критерию, не можем ли мы встроить общедоступные информационные технологии и социальные сети в режимы верификации и мониторинга в области контроля над вооружениями?

Я осознаю, что новые концепции не изобретаются в одночасье и мы не в силах объять весь спектр возможностей, открывающихся в информационную эпоху. Первые электронно-вычислительные машины были разработаны в то же время, что и атомная бомба. Более того, генерал Лесли Гроувс, который руководил Манхэттенским проектом, также принимал участие в разработке *UNIVAC* — одного из первых компьютеров, созданных для использования в военных целях. Хотите — верьте, хотите — нет,

но кабинет, который я сейчас занимаю в Государственном департаменте, находится рядом с прежним кабинетом Гроувса в тогдашнем Военном министерстве США. Там я часто чувствую дух истории.

И поскольку уж мы заговорили об истории, я хотела бы напомнить, что в конце Второй мировой войны Ванневар Буш, директор Управления по научным исследованиям и разработкам при президенте США, призвал создателей атомной бомбы начать поиск новых способов управления информацией: «[Человек] построил настолько сложную цивилизацию, — заявил Буш, — что ему необходимо более полно механизировать процесс учета информации, если он хочет довести эксперимент до логического завершения, а не застрять на полпути от перенапряжения своей ограниченной памяти», — или, скажем по-другому, своих ограниченных возможностей наблюдения и понимания.

Благодаря интернету мы достигли видения Ванневара Буша с технической точки зрения, но не осознали в полной мере его последствий для политики национальной безопасности. Сегодня любое событие в любой точке планеты может быть транслировано на весь мир в считанные секунды. Интересно то, как это отражается на контроле над вооружениями и верификации. В наше время стало труднее что-либо скрыть. Когда скрывать становится труднее, легче поймать того, кто пытается это сделать. Бдительное око соседа является мощным инструментом.

ОБЩЕДОСТУПНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СОЦИАЛЬНЫЕ СЕТИ

Но как именно могут общедоступные информационные технологии повысить качество проверок в области контроля над вооружениями? Это требование можно выполнять как минимум двумя способами: либо в форме активной задачи, включающей выработку новой информации и ее анализ, либо в форме глубокого анализа уже существующей информации.

Примером первого подхода является конкурс «Красные шары», организованный Управлением перспективного планирования оборонных научно-исследовательских работ (*DARPA*). В 2009 г. в честь 40-летия интернета *DARPA* провела конкурс, в рамках которого в разных регионах континентальной части Соединенных Штатов были подняты 10 красных воздушных шаров в точках, где они были хорошо видны. Первая команда, определившая местоположение всех 10 шаров, награждалась значительной денежной премией — 40 000 долларов. В конкурсе приняли участие более 4300 команд, объединивших примерно 2 млн человек из 25 стран. Победу одержала команда из Массачусетского технологического института (MIT) определившая местоположение всех шаров за удивительно короткий срок — 8 часов 52 минуты. Конечно, чтобы победить в такой малый промежуток времени, или вообще выполнить требование конкурса, члены команда MIT не сами *искали* эти воздушные шары. Они вошли в социальные сети с уникальной структурой стимулов, которая побуждала людей не только искать шары, но и привлекать к этому других. Их победа показала огромный потенциал социальных сетей, а также продемонстрировала, как стимулы могут мотивировать большие группы населения для работы в направлении общей цели.

А не может ли нечто подобное работать в контексте контроля над вооружениями? Представим себе, что некая страна, желая продемонстрировать свои добрые намерения в обстановке глубоких ядерных сокращений, согласится добровольно подвергнуться проверке. Она захочет доказать, например, что не прячет неучтенных ракет в лесу или реактор для производства расщепляющихся материалов в пустыне. Конечно, скорее всего, потребуются некоторые формы международного контроля, чтобы обеспечить легитимность проверки и применяемых процедур. И надо будет подумать, сможет ли такая проверка быть эффективной, если эти

вооружения легко можно скрыть, например, в пещерах или глубоких подземных сооружениях.

Я думаю, что подобный метод — назовем его *задачей общественного контроля* — может оказаться особенно ценным по мере продвижения к все более низкому количеству ядерного оружия. Правительства будут заинтересованы в предъявлении доказательств того, что они выполняют свои обязательства по сокращению, а возможно, захотят задействовать свое население для помощи в сборе доказательств.

Другим примером общественной акции по сбору новой информации был мониторинг окружающей среды после катастрофы с разливом нефти в результате аварии на платформе *Deepwater Horizon* в Мексиканском заливе в 2010 г. Общественная лаборатория открытой технологии и науки (*PLOTS*) в сотрудничестве с другими институтами организовала гражданский проект по контролю разлива нефти с помощью воздушных шаров. Группа предложила представителям общин прикреплять цифровые камеры к воздушным шарам или воздушным змеям для проведения аэрофотосъемки. Полученные снимки были затем сведены воедино с использованием открытого программного обеспечения, чтобы на базе многочисленных отдельных цифровых изображений создать единую карту.

ЛИСТАЯ СТАРЫЕ СТРАНИЦЫ

ЮЛИЯ КИСЛЯК, АЛЕКСЕЙ СОКОЛОВ: Итак, встает серьезнейшая проблема использования доступа к огромным аудиториям пользователей интернета и влияния ведущих интернет-компаний на общественное мнение. Сегодня особое значение имеет наличие торговой марки, что позволяет обладателям данной марки привлекать огромные аудитории на свои сайты. [...] Хотя сама Паутина не создавалась в целях пропаганды отдельных идеологий и взглядов — скорее она преследовала прямо противоположные цели — но именно ее раздробленность на огромное количество источников позволяет самым мощным из них становиться средствами массовой информации нового поколения, объединяющими текстовую, графическую, видео- и аудиоинформацию одновременно. Таким образом, несмотря на демократичность принципов построения Паутины, нельзя исключать возможность использования ее информационных ресурсов и потенциала, например, для продвижения внешне- и внутриполитических целей государства. Влияние на общественное мнение через интернет становится одним из ключевых факторов при формировании стратегических приоритетов общества и затрагивает интересы всех без исключения государств.

Влияние процессов развития интернет-технологий на геополитические интересы государства.
Ядерный Контроль. № 6, ноябрь–декабрь 2000. С. 34.

Итак, гражданские проекты проверки и мониторинга могут применяться для контроля над вооружениями и нераспространением. Если страна *X* заявляет, что некий ядерный объект был закрыт, усилиями граждан можно дополнить стандартные международные гарантии или проверки этого заявления. Опять же, мы должны иметь в виду, что здесь могут возникать существенные ограничения, связанные со свободами, которыми обладают граждане страны *X*: это один из вопросов, который следует обдумать в рамках рассмотрения этой проблемы.

Кроме разработки новой информации, весьма полезным может быть сбор и анализ существующей информации.

После *арабской весны* возросло уважение к таким механизмам социальных сетей, как *Twitter*. Новости о ходе восстаний освещались в режиме реального времени

не только традиционными новостными агентствами, но и рядовыми гражданами на местах. Репортажи о революции вели те, кто ее творил.

Лейла Шерин Сакр из Университета Южной Калифорнии внимательно следила за событиями *арабской весны*, создавая массивные базы данных твитов на арабском языке. Вместо того чтобы самостоятельно выбрать поисковые слова и вести поиск в базе данных, Сакр применила компьютерную программу для агрегации данных и выявления закономерностей. При агрегировании твитов из Ливии программа выявила всплески в использовании некоторых хэштегов или отдельных ключевых слов. Эти всплески стали своего рода импульсом, ранним предупреждением о падении города Завия. Через некоторое время снова стали появляться подобные всплески, что позволило Сакр предсказать предстоящее падение Триполи. Ей удалось сделать это с точностью до нескольких часов.

Способность выявлять закономерности и тенденции в социальных сетях может оказаться подспорьем в процессе проверки в области контроля над вооружениями. Прежде всего социальные СМИ могут привлекать внимание как к обычным, так и к аномальным событиям. Мы, вероятно, сможем выяснять, откуда исходят необычные потоки, выявлять признаки производственной деятельности и нацеливать на этот район датчики и спутники. Подобное нацеливание могло бы помочь нам более эффективно использовать наши ограниченные и дорогостоящие национальные технические средства, а в некоторых случаях — существенно дополнять их. Это важное соображение в эпоху жесткой бюджетной экономии, когда цены на крупные объекты, такие как спутники, продолжают расти. Мы нуждаемся в этом *большом железе*, но мы должны использовать его эффективно.

В этом же духе следует подумать о том, какую пользу мы можем извлечь из использования общедоступных геопространственных баз данных, таких как *Google Earth*. Конечно, общедоступными спутниковыми изображениями уже в течение некоторого времени пользуются для своих исследований НПО, студенты и частные граждане.

Недавно я узнала об интересной работе, проводимой Тамарой Паттон в Монтерейском институте международных исследований. Основное внимание в своем исследовании Паттон уделяет производственной мощности комплекса по производству плутония Хушаб в Пакистане. Она использует свободно доступные геопространственные инструменты для сбора и анализа информации об уровне мощности комплекса. Самое интересное начинается тогда, когда она превращает общедоступные спутниковые снимки комплекса в трехмерные модели с использованием находящейся в свободном доступе программы *Google Sketch-up*. Эта программа строит модели на основе размеров, которые Паттон устанавливает с помощью инструментов в *Google Earth* и элементарной тригонометрии. Модель затем помещается на карту, и на нее наносится рельеф — наблюдаемые признаки. Такое моделирование может быть использовано и в качестве инструмента анализа, и как средство четкой визуализации и обобщения результатов.

Продумывая новые способы использования этих средств, мы должны знать, что впереди нас могут ожидать трудности. Мы не можем полагаться на то, что информация всегда будет столь же легко доступна. Поскольку государства и частные организации продолжают обсуждать границу между неприкосновенностью частной жизни и безопасностью, мы можем предположить, что живем сейчас в золотой век информации из открытых источников, которой со временем станет пользоваться труднее. В недавней статье в газете *Financial Times* Рон Драйберт из Университета Торонто указал: «Возможно, мы будем вспоминать 1990–2000-е гг. как краткий период, когда мы могли свободно общаться и находить информацию в любых источниках». Еще одним предметом беспокойства в отношении общедоступных технологий является надежность. Информацией, получаемой с помощью общедо-

ступных технологий, можно легко манипулировать, ее можно неправильно использовать и неверно истолковывать.

Свои недостатки есть и у социальных сетей, не говоря уже о горах ненужных данных, которые могут маскировать полезную информацию. Иногда социальные сети имеют непредвиденные последствия. Хотя это не помешало миссии и не сделало ее невозможной, далеко не идеальным было то обстоятельство, что штурм дома, где жил Усама бин Ладен, непреднамеренно освещался в реальном времени в сети *Twitter*.

В конечном итоге цель использования технологии открытых источников информации и социальных сетей — расширять наши существующие возможности проверки в области контроля над вооружениями. Например, соблюдение Договора о всеобъемлющем запрещении ядерных испытаний будет контролироваться через Международную систему мониторинга (МСМ). Для обнаружения ядерных взрывов МСМ опирается на четыре устоявшихся метода мониторинга. Можно ли будет интегрировать эту уже надежно действующую систему с социальными сетями, обеспечивая независимое подтверждение официальных выводов? Это тема для обдумывания.

КОНТРОЛЬ НАД КИБЕРВООРУЖЕНИЯМИ?

А теперь, слегка изменив направление, я хочу ясно дать понять, что хотя я и заинтересована в размышлении над тем, как мы можем улучшить политику в области контроля над вооружениями с помощью инструментов информационного века, я думаю, что такие термины, как «контроль над кибервооружениями», могут вносить путаницу и вводить в заблуждение. Слишком часто на не до конца понятые концепции безопасности вешается ярлык, который им совершенно не подходит. Это не удивительно. Новым концепциям требуется время для созревания. Теории о ядерном сдерживании не возникли в одночасье; нам потребовались годы, чтобы понять последствия того, что мы создали.

Контроль над ядерными вооружениями акцентирует внимание на ограничении больших объектов — ракет, подводных лодок, бомбардировщиков, — которые имеют несомненно военное назначение. Технологии же, используемые для производства кибероружия, по своей природе имеют двойное назначение, они легко доступны в Интернете, и по большей части мы видим только их последствия. Способность идентифицировать злоумышленника в реальном времени или с высокой степенью достоверности часто бывает недостижима. Здесь нет громоздких реакторов или больших МБР, которые можно увидеть с неба. Кроме того, физические ограничения и потолки, которые мы применяем к ракетам и запасам химического оружия, неприменимы, когда мы говорим о находящихся на большом расстоянии друг от друга субъектах, порой действующих по заданию правительств, а также об информации и программном обеспечении, а не *железе*. Эта неспособность *видеть* угрозу сгущает туман войны.

Поскольку возможности традиционных инструментов политики в области контроля над вооружениями лишь ограниченно применимы в отношении кибероружия и войны в киберпространстве, мы возлагаем надежды на новые инструменты и стратегии, способные учитывать киберугрозы. Уже накоплен, однако, некоторый опыт, который мы можем использовать.

Хорошей отправной точкой являются меры укрепления доверия. Мы думаем о том, как наши знания в области мер укрепления доверия при контроле над вооружениями могут быть применены к международному сотрудничеству в области кибербезопасности. Например, национальные Центры по уменьшению ядерной опасности (НЦУЯО), традиционно использовавшиеся для обмена информацией, обуслов-

ленной существующими договорными режимами, могут в дальнейшем использоваться для уведомления об угрозах, инцидентах или учениях в киберпространстве. Международные учения могут дать хорошую возможность для выявления новых проблем в области связи в кризисных ситуациях или для технического сотрудничества и обмена, которые могут быть полезны для противостояния общим угрозам и реагирования на них. Даже простые обмены в области государственной политики или законодательства в сфере кибербезопасности могут помочь повысить уверенность государств во внутреннем потенциале решения возникающих проблем, а также содействовать обсуждению общего понимания и передового опыта.

Я понимаю, конечно, что нам придется разработать новые способы применения таких мер по укреплению доверия, но если их внедрить должным образом, они могут создать основу для дальнейшего диалога и способствовать установлению норм и стандартов поведения. Трудность заключается в том, как применять международные нормы и стандарты, чтобы гарантировать, что киберпространство будет расти и развиваться на благо человечества и не станет благоприятной средой для злоумышленников из числа государств или преступников — что является реальной и непосредственной опасностью.

Я часто думаю, сидя в своем кабинете, где витает дух истории, что если людям, осуществившим Манхэттенский проект, хватило ума, чтобы изобрести атомную бомбу, то, конечно, нам хватит ума, чтобы избавиться от нее. 

Примечания

[1] Публикуется в сокращении на основе лекции Роуз Готтемюллер по программе Сидни Дрелла в Стэнфордском университете (27 октября 2011 г.) с любезного разрешения автора.