ЕКАТЕРИНА СТЕПАНОВА

Терроризм как угроза критической инфраструктуре

Новые масштабные теракты, совершенные 29 марта 2010 года на станциях «Лубянка» и «Парк Культуры» московского метро — критической для мегаполиса транспортной системы, а также арест в том же месяце более 100 человек в Саудовской Аравии в связи с предполагаемыми террористическими атаками на объекты нефтяного комплекса страны вновь ставят проблему террористической угрозы критической инфраструктуре. К ней относятся технологические и экономические системы, жизненно важные для функционирования общества и экономики (транспорт, энергетика, связь и т. д.).

В оценке террористических угроз безопасности критической инфраструктуры существуют определенные различия и даже некоторая разобщенность в подходах между специалистами в области технологий и инфраструктуры, с одной стороны, и экспертами по терроризму, с другой. Технократы и управленцы оценивают риски и уязвимость инфраструктуры, в основном исходя из технологически возможного, а не из того, что в наибольшей степени соответствует целям и задачам террористов. Специалисты же по терроризму сосредоточивают свое внимание не столько на конкретных механизмах и особенностях функционирования той или иной инфраструктуры, сколько на мотивациях, целях и организационных формах террористических организаций, а также на специфике терроризма как формы политического насилия.

Терроризм — пожалуй, наиболее асимметричная форма политического насилия*. Главная его особенность состоит в нацеленности на эффект широкой политической, психологической и общественной дестабилизации, масштабы которой намного превышают прямой ущерб от терактов для населения и инфраструктуры. Для террористов значение этого метода

СТЕПАНОВА Екатерина Андреевна — ведущий научный сотрудник отдела международных политических проблем ИМЭМО РАН, кандидат исторических наук.

* Терроризм — преднамеренное использование или угроза насилия со стороны негосударственных игроков против гражданских лиц и некомбатантов для достижения политических целей в асимметричном противостоянии (*см.* **E. Stepanova**. Terrorism in Asymmetrical Conflict: Ideological and Structural Aspects. Oxford, 2008).

измеряется не просто числом убитых и раненых, метражом разрушенной взрывом части трубопровода или этажностью взорванного жилого дома. Главное для них — это именно возможность *влиять на политическую ситуацию* путем *асимметричного* использования или угрозы насилия против населения или инфраструктуры.

Суть такой асимметрии в следующем: чтобы несравнимо более слабому по общему потенциалу и более низкому по статусу вооруженному негосударственному игроку относительно ограниченными средствами добиться непропорционально и максимально широкого дестабилизационного эффекта, а также резонанса в конфронтации со своим главным противником — государством. Возможность с помощью терактов влиять на общественно-политическую ситуацию не измеряется лишь в количественных параметрах. Она зависит от многих факторов, включая конкретный политический контекст, тип общества, которому угрожают террористы (в том числе степень его «устойчивости» к терактам), выбор ими мишеней для атак и т. д. Тому, насколько эта возможность связана с атаками на критическую инфраструктуру и как ей противостоять, и посвящена эта статья.

Асимметричная природа терроризма диктует и особенности определения «масштабного», или крупного, теракта. В отличие, например, от военных операций, в данном случае термин «масштабный» подразумевает не только и необязательно массовые жертвы, масштабный ущерб физическим объектам, многочисленность самих террористов или, например, технологический уровень используемых ими средств. Мощь теракта определяется в первую очередь масштабом его общего дестабилизационного эффекта в конкретном политическом контексте вне зависимости от того, как именно террористам удалось его достичь (за счет массовых жертв или убийства всего лишь одной, но «знаковой» общественной фигуры, атаки на объект чисто символического значения или удара по жизненно важной инфраструктуре). Конечно, массовые жертвы и масштабные разрушения усиливают дестабилизационный политический эффект теракта, однако они не являются обязательным, а порой и достаточным условием для создания эффекта общественно-политической дестабилизации, на который рассчитывают террористы.

Подчеркнем: абсолютное большинство масштабных терактов в мире совершается с помощью *обычных (конвенциональных) вооружений, материалов и средств*. Преобладающей тактикой масштабного теракта остаются взрывы с использованием стандартных взрывчатых веществ и материалов. Несмотря на то что эти средства могут быть относительно доступными, недорогими и далеко не высокотехнологичными, их асимметричное применение против незащищенных гражданских мишеней может иметь тяжелые, а в отдельных случаях (например, в результате терактов 11 сентября

2001 года в США) и катастрофические последствия. Изредка террористы могут использовать и неконвенциональные — химические, биологические, радиологические и ядерные — материалы, но до сих пор все масштабные разрушения вследствие терактов были результатом использования конвенциональных средств*. Из всех крупных неконвенциональных терактов за последние 25 лет лишь распыление нервно-паралитического газа группировкой «Аум синрикe» в токийском метро в 1996 году было действительно масштабной по своему дестабилизационному эффекту террористической атакой**. Однако даже она привела к меньшим людским потерям, физическому ущербу и перебоям в транспортной системе, чем многие теракты на общественном транспорте с использованием обычных средств.

Масштаб угрозы

Как часто узлы и другие объекты критической инфраструктуры становятся мишенями терактов по сравнению с другими целями? Как показывает статистика, не так уж и часто: критическая инфраструктура становится объектом лишь сравнительно небольшого числа терактов, сильно уступая таким мишеням, как скопления гражданского населения в общественных местах, а также правительственные и другие политические объекты.

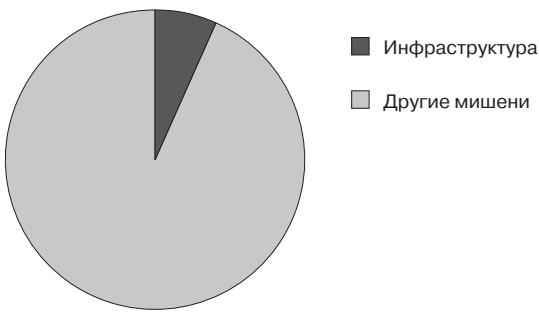

Рис. 1. **Мишени террористических атак**

Источник: Global Terrorism Database (GTD), 1998—2004.

Например, 547 терактов против объектов инфраструктуры, совершенных в мире в 1998—2004 годах, составили менее 7 процентов от всех

* До сих пор все теракты, приведшие к действительно масштабным разрушениям, были совершены с использованием обычных материалов и взрывчатки (например, взрыв федерального здания в Оклахома-Сити правым экстремистом Т. Мак-Бимом в 1995 году или взрывы посольств США в Кении и Танзании в 1998 году) либо путем нестандартного использования стандартных средств и объектов инфраструктуры, например гражданских самолетов в качестве управляемых ракет в ходе терактов 11 сентября 2001 года в США.

** Подробнее об этом *см.*: **J. V. Parachini.** Comparing Motives And Outcomes of Mass Casualty Terrorism Involving Conventional and Unconventional Weapons. — «Studies in Conflict and Terrorism». 2001. Vol. 24. № 5. P. 390. *См.* также: **А. Пикаев, Е. Степанова.** Ядерный терроризм: утопия или угроза? — «Разоружение и безопасность, 2004—2005. Новые подходы к международной безопасности». М., ИМЭМО РАН, 2007.

7954 терактов за тот период (*см. Рис. 1*)*. Из этих 547 терактов 51 процент пришелся на железнодорожный и другой наземный и подземный транспорт, 30 — на объекты энергоснабжения, системы коммунального хозяйства и т. п., 11 — на воздушный транспорт, 4 — на системы (теле)коммуникаций и 2 процента — на водный транспорт (*см. Рис. 2*).

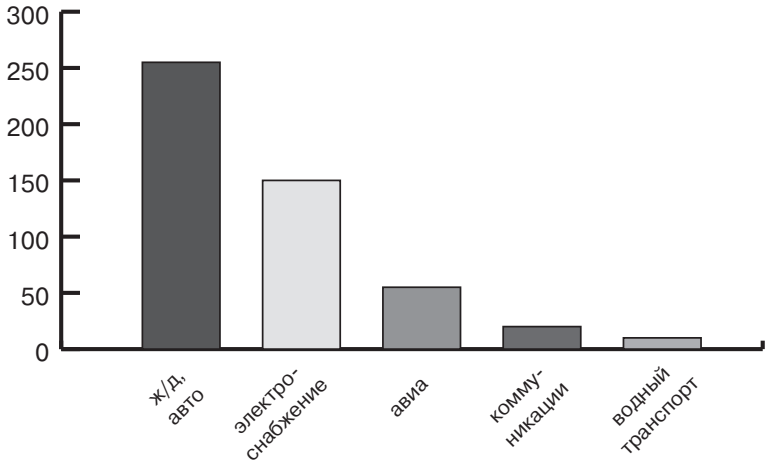

Рис. 2. **Теракты по объектам инфраструктуры**

Источник: Global Terrorism Database (GTD), 1998–2004.

В целом среди всех объектов критической инфраструктуры общественный транспорт — прежде всего наземный, подземный и воздушный — остается приоритетной мишенью террористов.

Очевидная мишень: теракты на общественном транспорте

Если теракты с массовыми жертвами**, а также теракты против критической инфраструктуры и пересекаются, то в основном в форме *терактов на общественном транспорте*. Террористы на всех уровнях — от локального до глобального — предпочитают атаки в общественных местах, с большей вероятностью по определению ведущие к массовым жертвам. Еще задолго до терактов 11 сентября 2001 года (в ходе которых пассажирские самолеты были использованы и как мишень, и как средство терактов) абсолютное большинство террористических ударов одновременно по населению и по объектам критической инфраструктуры, приведших к массовым жертвам,

* Здесь и далее все вычисления проведены на основе материалов Глобальной базы данных по терроризму, которая поддерживается Национальным консорциумом исследования терроризма и антитерроризма при Университете Мэриленда (*см.* http://www.start.umd.edu/data/gtd).

** Теракт с массовыми жертвами — неизбирательная атака, в основном направленная против гражданских лиц и приведшая к гибели не менее 25 человек.

совершалось на общественном транспорте. Они составляют до половины всех терактов с массовыми жертвами. Во второй половине XX века 34 из 76 всех террористических взрывов с массовыми жертвами[1] были атаками по инфраструктуре — почти исключительно по транспортным системам: в основном по авиатранспорту и аэропортам (17 инцидентов), а также объектам железнодорожного транспорта (7), автобусам и автобусным терминалам (6), реже — по объектам водного транспорта.

[1] *См.* **C. Quillen.** Mass-casualty Bombings Chronology. — «Studies in Conflict and Terrorism». 2002. Vol. 25. № 5.

В свою очередь не все атаки по критической инфраструктуре оборачиваются массовыми жертвами: в 1998—2004 годах лишь 15,0 процентов терактов на авиатранспорте, 13,5 — на наземном транспорте и 10,0 процентов на водном транспорте привели к большим потерям среди гражданских лиц. В отличие от терактов на общественном транспорте, массовые жертвы в терактах против других систем критической инфраструктуры — пока скорее исключение, чем правило.

Более того, если теракт нацелен в первую очередь на массовые жертвы, выбор в качестве мишени объектов общественного транспорта (например, взрыв пассажирского автобуса) часто носит чисто инструментальный характер. Объект инфраструктуры важен здесь не столько сам по себе, сколько как способ нанести максимальные жертвы в условиях скопления людей в ограниченном пространстве, с ограниченной возможностью быстро покинуть такие объекты, что позволяет резко увеличить число жертв. В таких случаях разрушение транспортного объекта или нанесенный ему ущерб не обязательно ведет к более широкой дестабилизации инфраструктуры. В других случаях критическая транспортная инфраструктура представляет собой и важную самостоятельную мишень, а не только «плацдарм» для нанесения масштабных людских потерь. Например, даже временное прерывание ее нормального функционирования может значительно дестабилизировать жизнь таких мегаполисов, как Лондон, Мадрид, Москва или Нью-Йорк, нарушить транспортное сообщение между городами, районами или даже странами, тем самым резко расширяя и усиливая общий дестабилизационный эффект терактов.

Если же главной мишенью террористов являются системы энергетики, водоснабжения, информации, связи, финансов и другой нетранспортной инфраструктуры, такие теракты, как правило, редко приводят к массовым жертвам и вообще не всегда предполагают прямые людские потери. Например, лишь 4,5 процента всех терактов против телекоммуникационных систем, 1,8 процента атак по системам водо-, тепло- и энергоснабжения влекут за собой массовые жертвы. Это, впрочем, не означает, что такие теракты не могут произвести эффект общественно-политической дестабилизации.

Тем не менее до сих пор террористы всех мастей явно отдают приоритет именно терактам в общественных местах, как правило сопряженным

с жертвами, в том числе массовыми, над терактами против инфраструктуры как таковой, особенно нетранспортной. Если террористический взрыв в толпе, на вокзале или в метро говорит сам за себя, то теракт против нетраснпортной инфраструктуры не всегда и не сразу можно даже распознать как таковой. Неудивительно, что в ряду мишеней транснациональных террористических сетей, связанных с «Аль-Каидой», теракты в общественных местах, включая общественный транспорт, стоят на первом месте. На втором — атаки против правительственных объектов, на третьем — теракты против иностранных граждан, представительств и туристов. За исключением общественного транспорта, из всех систем критической инфраструктуры на самом высоком — да и то лишь пятом — месте в этом списке стоят объекты нефтяного комплекса[2].

[2] *См.* **A. Schmid.** Terrorism and Energy Security. — «Memorial Institute for the Prevention of Terrorism (MIPT) Insight Report». March 2007. P. 1—2.

В целом самой уязвимой точкой перед лицом масштабных террористических атак служит именно пересечение мест массового скопления людей с инфраструктурой общественного пользования, прежде всего транспортной. Одна из наиболее тревожных глобальных тенденций в этой сфере — относительно недавний значительный рост числа терактов с массовыми жертвами на наземном транспорте, особенно на железных дорогах и в метро (при сокращении общего числа терактов на авиатранспорте).

Теракты против критической инфраструктуры в зонах конфликтов

Теракты против объектов инфраструктуры, не связанной с общественным транспортом, достаточно редки и обычно приводят к гораздо меньшим жертвам и ограниченному прямому ущербу инфраструктуре, который, как правило, удается довольно быстро локализовать и ликвидировать. Если такие атаки и носят более регулярный, разрушительный и скоординированный характер, то в основном когда терроризм является одной из тактик вооруженного противостояния в ходе локальных конфликтов, особенно в регионах, богатых углеводородами и располагающих протяженной энергетической инфраструктурой (Нигерия, северные районы Колумбии или Ирак). В Нигерии до 45 процентов всех терактов в 1998—2004 годах пришлось на объекты инфраструктуры. Целью 90 процентов таких терактов были нефтяные объекты (в основном захват в заложники работающего на них персонала), однако лишь один крупный взрыв на нефтепроводе можно квалифицировать как действительно «масштабный» по силе воздействия теракт, хотя он и не привел к массовым жертвам. В тот же период в Колумбии 19 процентов всех терактов также были направлены — исключительно или в сочетании с другими целями — против объектов инфраструктуры (что составило 20 процентов всех террористических атак на объекты инфра-

структуры в мире). Пока именно в Колумбии теракты против критической инфраструктуры отличают наивысшая степень координации, самая высокая доля серий одновременных ударов по нескольким объектам и самый широкий спектр мишеней (54,0 процента терактов против инфраструктуры связаны с энергетическим сектором, 27,0 — с транспортом, 10,5 — с финансовым сектором и 5,7 процента — с системами связи и коммуникаций). Тем не менее лишь в 15 процентах случаев эффект терактов против критической инфраструктуры вышел за рамки локального ущерба, а два теракта этого типа за семь лет привели к массовым жертвам.

Еще одним примером систематических терактов против объектов инфраструктуры как средства подорвать «вражескую» экономику и помешать противнику и местным коллаборационистам эксплуатировать национальные ресурсы служат теракты против объектов нефтяной инфраструктуры со стороны повстанцев в постсаддамовском Ираке. По некоторым оценкам, число таких терактов только против объектов нефтяной инфраструктуры за первых три года после интервенции США достигло не менее 300. Несмотря на то, что обилие таких атак, особенно против объектов энергетики, в конфликтных и постконфликтных зонах частично мешает восстановлению экономики и сказывается на уровне экспорта углеводородов, даже в таких регионах прямой ущерб инфраструктуре обычно достаточно быстро ликвидируется.

Масштаб и эффект терактов против объектов инфраструктуры, не связанных с общественным транспортом или с энергетической инфраструктурой в конфликтных зонах, сравнительно ограниченны. Это частично объясняется таким обстоятельством: большинство ключевых объектов наиболее «критической» инфраструктуры, удары по которым могут иметь действительно масштабные разрушительные последствия, представляют собой отнюдь не «мягкие», незащищенные мишени, в отличие, например, от скоплений людей в общественных местах. В числе таких охраняемых («режимных») объектов — например, предприятия атомной промышленности, нефтеперерабатывающие заводы и терминалы по хранению и перекачке сжиженного газа. Неудивительно, что факты или угрозы действительно серьезного нарушения работы такой инфраструктуры в результате терактов пока остаются скорее исключениями, чем правилом. Примером может служить неудавшаяся атака против крупнейшего в мире нефтеперерабатывающего комплекса в Абкейке в Саудовской Аравии в феврале 2006 года[3].

[3] *См.* **K. R. Al-Rodhan.** The Impact of the Abqaiq Attack on Saudi Energy Security. — «Center for Strategic and International Studies». Wash., 2006.

Напротив, системы, обладающие большой протяженностью (крупные нефтяные месторождения, тысячи километров трубопроводов и кабелей и т. п.), являются гораздо более «мягкими» мишенями, обеспечить полную

физическую защиту которых вряд ли возможно. Однако, за исключением терактов на общественном транспорте, где временная дестабилизация инфраструктуры многократно усилена эффектом от массовой гибели людей, намеренный ущерб любой другой протяженной инфраструктуре носит в основном локальный характер, и систему обычно удается довольно быстро восстановить. Иными словами, чем более «мягкий» характер носят объекты той или иной инфраструктуры, тем они, как правило, менее «критичны» с точки зрения возможного ущерба в случае любой чрезвычайной ситуации — будь то теракт или авария. И наоборот, чем более «критический» характер носят «узловые» объекты инфраструктуры, тем они обычно лучше защищены, что ограничивает вероятность выбора террористами именно этих объектов в качестве мишеней.

Проблемы обеспечения безопасности критической инфраструктуры

Стратегия обеспечения безопасности критической инфраструктуры должна быть нацелена на снижение ее уязвимости по отношению к любому ущербу, в том числе перед лицом чрезвычайной ситуации природного или техногенного характера или несанкционированного вмешательства, включая теракт. Интенсивность угрозы инфраструктуре может варьироваться от стандартного неблагоприятного инцидента до катастрофы. Последние имеют особенно масштабные разрушительные последствия, но в среднем составляют не более 1 процента всех связанных с инфраструктурой «чрезвычайных инцидентов».

В начале XXI века в стратегиях обеспечения безопасности критической инфраструктуры развитых стран доминируют два взаимосвязанных подхода, или принципа. Первый подход связан с определением преобладающего типа (типов) угроз инфраструктуре. Например, в США в последнее десятилетие наблюдался постепенный отход от «стратегии защиты от одной угрозы», преобладавшей в первые годы после событий 11 сентября, в том числе в подходах нового государственного Департамента внутренней безопасности, к проблемам безопасности критической инфраструктуры. Она была зациклена на защите от угроз именно террористического типа в ущерб другим, гораздо более распространенным угрозам (one-hazard strategy). После коллапса чуть ли не всей критической инфраструктуры в прибрежных районах Юго-Востока США в результате неспособности противостоять последствиям ураганов Катрина и Рита в 2005 году правительство США постепенно вернулось к стратегии защиты от двух или нескольких наиболее вероятных угроз, включая природные бедствия и крупные технологические аварии (multiple-hazard strategy). Эта стратегия более адекватна и давно доминирует в странах Европейского Союза.

До недавнего времени второй базовый подход к обеспечению безопасности критической инфраструктуры был почти исключительно сосредоточен именно на *защите* ее конкретных структур, ресурсов и объектов от ограниченного числа опасных, но в целом известных и относительно ожидаемых угроз. Соответствующая этому подходу стратегия противодействия угрозам и предотвращения ущерба инфраструктуре опирается на формальные, централизованные системы командования и контроля, специализированные профессиональные службы и персонал, «закрытые» системы коммуникаций с использованием спецсвязи, межведомственное взаимодействие и взаимодействие с населением по иерархическому принципу «от одного ко многим».

В то же время такая стратегия подвержена чрезмерному влиянию или даже диктуется реакцией на последние крупные катаклизмы (масштабные теракты, разрушительные стихийные бедствия или крупные техногенные катастрофы). Конечно, необходимость обеспечить определенную степень защиты критической инфраструктуры от более привычных и сравнительно хорошо известных угроз не вызывает сомнений. Для одних систем инфраструктуры (например, общественного транспорта или объектов, связанных с химическими, биологическими, радиологическими и ядерными материалами) необходимость в такой защите неизбежно будет выше, чем для других. Однако подход, сосредоточенный на защите основных узлов наиболее «критической» инфраструктуры от нескольких знакомых угроз по аналогии с последними крупными чрезвычайными ситуациями, в принципе не может обеспечить защиту от будущих чрезвычайных ситуаций.

В целом такой «механический» и «статичный» подход остается продуктом индустриального общества, его экономики и культуры. Он не вполне адекватен вызовам постиндустриальной эпохи, глобализации, а также информационного общества и вряд ли может обеспечить защиту от множественных новых, неожиданных и плохо поддающихся прогнозированию угроз[4].

[4] *См.* **L. J. Perelman.** Shifting Security Paradigms: Toward Resilience. — «Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience». Wash., 2007. P. 26.

Насколько критическая?

Стандартное определение критической инфраструктуры подразумевает отрасли экономики и технологические системы, одновременно уязвимые и жизненно важные для безопасности и стабильного функционирования общества. Это прежде всего транспорт, энергетика, водоснабжение (в северных странах — и теплонасбжение), химическое, биологическое и атомное производства, основные системы связи и коммуникаций, а также (в какой-то мере) банковско-финансовый сектор. Дестабилизация, не говоря уж о коллапсе, этих систем оборачивается тяжелыми, а при наихуд-

шем сценарии и катастрофическими последствиями для современного общества, экономики и государства.

Подход, сосредоточенный на выборочной защите конкретной критической инфраструктуры от ограниченного набора относительно прогнозируемых угроз, отдает приоритет той или иной инфраструктуре в зависимости от степени ее «критичности». Однако само понятие «критичность» — точнее, то, как оно интерпретируется в рамках традиционных подходов, — вызывает минимум два серьезных вопроса.

Во-первых, такие подходы не делают никаких различий между инфраструктурой, имеющей критическое значение с точки зрения безопасного и стабильного функционирования общества и экономики, и инфраструктурой, представляющей собой особый интерес в качестве мишени для террористов. Конечно, некоторые виды инфраструктуры, например общественный транспорт, рассматриваются как «критические» и государством, обществом и бизнесом, с одной стороны, и террористами, с другой. Однако далеко не вся «критическая» для общества и экономики инфраструктура представляет интерес для террористов в качестве мишени, удар по которой может обеспечить им максимальный эффект общественно-политической дестабилизации. Например, для террористов объекты культурно-политического или религиозного значения (национальные памятники, известные небоскребы, мемориальные правительственные здания) могут быть не менее, если не более, «критическими», желанными и доступными мишенями, чем многие объекты критической инфраструктуры.

Во-вторых, в условиях глобализирующейся экономики и современного динамичного информационного общества понятие «критичность инфраструктуры» становится более *относительным*. За исключением общественного транспорта, ряда особо опасных производств, системы снабжения питьевой водой и некоторых других отраслей, действительно все труднее определить, какие именно ресурсы имеют наиболее «критическое» значение и для чего. В условиях роста глобальной взаимозависимости и оптимизации производства практически *любая* инфраструктура, включая, например, рутинное производство достаточно стандартных товаров или материалов, может в определенных условиях оказаться «критической» — до такой степени, что локальная авария или временный коллапс может внезапно обернуться глобальной дестабилизацией целой отрасли*.

* Ставший уже классическим пример такой локальной аварии с глобальными последствиями — взрыв на заводе химической компании «Сумитомо» в Японии в 1993 году, который обернулся значительной дестабилизацией глобальной компьютерной индустрии в результате недостатка компьютерных чипов, так как эта компания одна производила 60 процентов всей эпоксидной смолы в мире, которой заливались чипы для защиты микросхемы (а почти всю остальную смолу необходимого качества производила еще одна японская фирма). Крайняя уязвимость такой системы выяснилась только после того, как произошла эта авария (*см.* **J. Robertson**. Sumitomo Epoxy Resin Plan Gutter. — «Reed Business Info Electronic News». 12.07.1993).

Нередко реальная степень «критичности» того или иного элемента инфраструктуры выясняется уже после того, как произошел такого рода коллапс.

Из этого следует, что, во-первых, угрозы инфраструктуре становятся более множественными, разнородными и менее предсказуемыми. Во-вторых, реальность такова, что в этих условиях у государства, бизнеса и общества отсутствуют возможности и ресурсы для одновременного обеспечения одинаково высокой степени защиты всей инфраструктуры от всех возможных угроз. В-третьих, терроризм — особо опасная, но лишь одна из многих таких угроз. Если даже специалисты-инсайдеры не всегда в состоянии предсказать, дестабилизация каких элементов инфраструктуры может иметь наиболее «критическое» значение, можно ли того же ожидать от политических (идеологических, религиозных) террористов?

Основные дилеммы

Вызовы безопасности критической инфраструктуры не исчерпываются проблемами определения сравнительной «критичности» той или иной инфраструктуры. Из ряда важных дилемм в этой области отметим следующие две.

Национальная или международная ответственность? Ответственность за обеспечение безопасности критической инфраструктуры лежит прежде всего на национальном уровне, а например, Контртеррористический комитет ООН относит эту задачу к «внутригосударственным мерам безопасности». Однако угрозы инфраструктуре по определению включают трансграничные и более широкие — транснациональные катаклизмы и атаки, в том числе международные теракты (из недавних примеров — серия терактов в Мумбаи в ноябре 2008 года с множественными целями, включая крупный железнодорожный узел). В глобализирующемся мире новые системы информации и коммуникации, энергетики и транспорта являются частью более широких международных сетей. Это усиливает заинтересованность государств и бизнес-сообщества в международном сотрудничестве в защиту транснациональной критической инфраструктуры от общих угроз, несмотря на ряд препятствий и ограничений для такого сотрудничества. Среди них — например объективные различия в технологическом потенциале и ресурсах заинтересованных сторон, в принципах функционирования различных национальных систем безопасности критической инфраструктуры.

Одно из таких различий состоит в разном *соотношении контроля над критической инфраструктурой со стороны государства и частного бизнеса* в разных странах. Например, в развитых постиндустриальных странах

Запада специфика задачи заключается в необходимости обеспечить безопасность в значительной мере децентрализованных систем, находящихся под управлением и в собственности частного сектора. Так, в США до 85 процентов всех систем критической инфраструктуры находится в частных руках, а государственный Департамент внутренней безопасности отвечает лишь за 5 из ее 13 секторов. В других странах, например в Китае или России, большая часть критической инфраструктуры находится под прямым контролем государства, играющего главную роль в обеспечении ее безопасности. Интересно также, что, например, меньшая зависимость ряда развивающихся стран от высокотехнологичных систем управления инфраструктурой и сосредоточение ее значительной части под контролем государства парадоксальным образом в чем-то даже делает их менее уязвимыми перед угрозами нового типа. Это, впрочем, слабо компенсирует такие хронические проблемы критической инфраструктуры в этих государствах, как ее громоздкий и слабоадаптивный характер, изношенность, недостаток в финансировании и рыночных решениях.

Особенности террористических угроз критической инфраструктуре

Итак, хотя теракты и другие намеренные (диверсионные, криминальные) атаки входят в число серьезных угроз критической инфраструктуре, они не являются наиболее распространенными — такими, как технологические аварии или природные катаклизмы. Если для отдельных отраслей инфраструктуры — прежде всего систем общественного транспорта — террористическая угроза довольно высока, то для многих других отраслей инфраструктуры она достаточно низка. Тем не менее значение террористических угроз критической инфраструктуре вряд ли можно считать преувеличенным по следующим причинам.

Во-первых, террористы могут оказать дополнительное дестабилизирующее воздействие на инфраструктуру и даже попытаться использовать ее в своих интересах. Наряду с *прямым воздействием* на нее (прерыванием ее функционирования путем прямого удара по критическому узлу или системе) большинство масштабных чрезвычайных ситуаций всех типов имеют и *вторичный, косвенный эффект*. Он может выражаться, например, в так называемом каскадном эффекте, когда ущерб одной инфраструктуре тянет за собой каскад нарушений в работе других, в финансовом ущербе государству и бизнесу, а также в определенной доле дестабилизации уже в ходе реакции на теракт. Хотя по силе прямого воздействия на инфраструктуру теракты могут сильно уступать, например, природным бедствиям или крупным техногенным катастрофам, в отличие от терактов, ни технологические, ни природные катаклизма не являются заранее спланированными попытками

добиться максимального воздействия на общество, специально рассчитанного на его дестабилизацию. Для террористов же этот вторичный эффект более широкой дестабилизации даже важнее, чем прямой ущерб инфраструктуре. Кроме того, помимо прямого ущерба и вторичного воздействия террористы могут пытаться получить контроль над ключевыми узлами или другими объектами инфраструктуры с целью использовать их для атаки по другим целям.

Во-вторых, после событий 11 сентября 2001 года терроризм стал рассматриваться как одна из основных и относительно ожидаемых угроз критической инфраструктуре. Но насколько хорошо она прогнозируема? Если сравнительную степень террористических рисков для тех или иных стран еще можно пытаться оценить*, то растущее многообразие уязвимых, «мягких», невоенных мишеней и целей в современном обществе, а также форм и проявлений самого терроризма крайне осложняет задачу «прогнозирования» конкретных масштабных терактов. За исключением общественного транспорта (излюбленной мишени террористов всех мастей) и транспортно-энергетических систем, проходящих через зоны локальных конфликтов, «угадать», элементы какой именно инфраструктуры могут стать следующей мишенью террористов, крайне трудно.

В-третьих, по мере того как укрепляется безопасность относительно более предсказуемых мишеней, связанных с критической инфраструктурой, например авиатранспорта и аэропортов, террористы оперативно переключаются на удары по элементам менее защищенных инфраструктур. Проще говоря, если террористам нужно найти «критическую» мишень, в том числе связанную с инфраструктурой, они ее найдут. Само по себе усиление мер антитеррористической защиты на одной инфраструктуре (например, на одном виде транспорта), не способствующее повышению общего уровня безопасности других уязвимых инфраструктур, конечно, обеспечит повышенную защиту этому конкретному виду инфраструктуры, но одновременно усилит вероятность переключения террористов на другой вид целей. Например, повышение антитеррористической безопасности на авиатранспорте сопровождалось ростом числа атак на других видах транспорта.

Все это говорит об одном: готовность террористов искать новые пути достижения максимального резонанса и дестабилизирующего эффекта своих атак может выразиться в экспериментировании не только и не столько с неконвенциональными средствами и материалами, сколько с *выбором новых целей и мишеней* для своих ударов, в том числе связанных с объектами и системами критической инфраструктуры.

* Такую попытку предпринял, например, Economist Intelligence Unit в рамках проекта «Global Peace Index».

Повышение общей устойчивости инфраструктуры как ответ на вызовы постиндустриального общества

Рост внимания к терактам как угрозам безопасности критической инфраструктуры может помочь прояснить само понятие «критичность» в современном мире и выявить наиболее «критические» инфраструктуры, требующие приоритетного внимания и инвестиций в их безопасность. Так, угроза терроризма диктует необходимость в первую очередь сосредоточиться на повышении безопасности следующих узлов и систем:

— которые не только подвержены прямому ущербу теракта и вторичному дестабилизационному воздействию, но и в случае захвата террористами могут быть сами использованы для ударов по другим целям;

— где увеличение уровня безопасности повысит общий эффект безопасности и для других связанных с ними элементов, а также секторов критической инфраструктуры.

Из более общих стратегических направлений повышения безопасности критической инфраструктуры, не связанных лишь с террористической угрозой, отметим необходимость перехода от «стратегии нескольких угроз» к стратегии защиты и реагирования на *множественные угрозы*. Простая замена «стратегии одной угрозы» «стратегией нескольких угроз» автоматически предполагает заведомо недостаточное внимание к иным, в том числе новым и неожидаемым, угрозам инфраструктуре. Более того, необходимо вообще выйти за рамки подхода, зацикленного лишь на статичной «защите» отдельных, наиболее «критических» объектов и инфраструктур от ограниченного спектра известных угроз, в основном определяемых по аналогии с предыдущими кризисами. Меры этого типа будут адекватными только в контексте общего повышения *устойчивости* (*resilience*) системы инфраструктуры к внешним и внутренним угрозам и рискам, в том числе новым, неожиданным и плохо поддающимся прогнозированию.

Конечно, предусмотреть все потенциальные угрозы и риски попросту невозможно. Однако в условиях растущей сложности и взаимозависимости систем инфраструктуры и жизнеобеспечения, диверсификации управления и контроля над ними, множественности и неявности рисков, угроз и уязвимостей в постиндустриальную эпоху залог стабильности критической инфраструктуры — в достижении высокого уровня ее устойчивости к любым системным шокам. Это предполагает создание таких систем и механизмов, которые обладают пониженной уязвимостью и «встроенной» способностью адаптироваться к резким изменениям, включая чрезвычайные ситуации разных типов — будь то физическая угроза или, например, внезапное блокирование поступления или доступа к тому или иному ресурсу. В данном случае «устойчивость» подразумевает способность системы не только выдерживать масштабный удар, но и быстро

восстанавливаться, в том числе в видоизмененном виде, адаптированном к новым условиям.

Повысить адаптивность и снизить общую уязвимость системы можно путем сочетания разных методов и стратегий, например поиска и достижения оптимального баланса между:

— удешевлением стоимости, снижением громоздкости и повышением гибкости инфраструктуры за счет оптимизации управления, адаптивного менеджмента, модернизации систем связи и информации, более активного внедрения сетевых элементов, опоры на социально-технические инновации;

— обеспечением страховочных и резервных мощностей, систем связи и управления.

Сетевые, децентрализованные системы связи и коммуникаций, построенные по принципу «от многих к многим» (от системы «Skype» до блогосферы), также нередко демонстрируют бóльшую устойчивость в информационную эпоху, чем традиционные коммуникационные системы по приниципу «от одного к многим».

Существуют разные примеры критических инфраструктур, сохраняющих довольно высокий уровень общей устойчивости и способность к быстрому восстановлению, несмотря на невозможность обеспечить их полную защиту даже от основных угроз. В их ряду — и децентрализованная сетевая коммуникационная система «Skype», и саудовская нефтяная инфраструктура, сочетающая жесткую физическую защиту с хорошей обеспеченностью резервными системами. В их числе — и московский метрополитен, не в первый раз демонстрирующий способность восстанавливать нормальный режим работы в тот же день после достаточно крупных терактов (например, в лондонском метро после масштабных терактов июля 2005 года это удалось сделать только на следующий день).

В целом для повышения уровня безопасности критической инфраструктуры необходимы и определенная степень защиты от наиболее вероятных, ожидаемых и типичных угроз, и меры по повышению общей устойчивости и приспособляемости системы, позволяющие снизить ее уязвимость перед лицом новых и неожиданных угроз. Соотношение мер этих двух типов может варьироваться от одной инфраструктуры к другой. Например, на системах общественного транспорта, где легче определить если не конкретное время и место, то характер наиболее вероятных, в том числе террористических, угроз, основной упор по определению должен быть сделан на комплексе защитных мер. В то же время, например, в сфере информационных технологий, (теле)коммуникаций, энергетики, финансовой инфра-

структуры особое внимание следует уделять обеспечению общей устойчивости системы, ее диверсификации, резервным мощностям и ресурсам.

Такая сбалансированная и комбинированная стратегия не только лучше соответствует современным потребностям безопасности критической инфраструктуры, но и позволит более эффективно предотвращать и реагировать на масштабные террористические угрозы. При этом следует иметь в виду, что современные террористические сети, особенно транснационального типа, часто способны обеспечить не менее, а более высокий уровень устойчивости своей «системы», чем государственные структуры. Такие террористические сети все чаще стараются избегать формирования собственных «критических» узлов, на которых государство могло бы сосредоточить свои упреждающие или ответные удары, строят гибкие и фрагментированные, но в целом устойчивые организационные системы, используя инновационные, порой не имеющие аналогов модели координации действий и нередко обладают достаточно продвинутыми навыками в области современных технологий информации и связи. Угрозы, исходящие от организаций такого типа, в том числе для инфраструктуры, требуют систематической деятельности государства по подрыву и нейтрализации прежде всего их идеологии и структуры.