УДК 327.7
ББК 66.4Ф4

НАТО И КИБЕРБЕЗОПАСНОСТЬ

А.В. Казаковцев

Предпринята попытка рассмотрения политики НАТО в сфере обеспечения информационной безопасности. Выявлены связанные с этой сферой проблемы классификации и терминологии. Рассматривается эволюция механизмов и институтов НАТО по обеспечению информационной обороны. Определены особенности политического измерения информационной безопасности НАТО.

Ключевые слова: *кибербезопасность, киберугрозы, кибервойна, стратегическая концепция, секьюритизация, НАТО.*

Стремительное развитие информационно-коммуникационных технологий в последние два десятилетия оказало серьезное влияние на международные отношения. Как отмечает отечественный специалист в области информационной безопасности П. Шариков, «активное распространение, внедрение и использование информационных технологий быстро привело к тому, что эти технологии стали применяться не только как средство обмена и обработки информации, но и как способ нанесения ущерба» [5, с. 582]. В последние несколько лет термины с приставкой «кибер» получили широкое употребление в международно-политическом дискурсе и нашли свое отражение в стратегических доктринах не только государств, но и международных организаций, включая НАТО.

К. Гирз, представитель США в Центре кибероборонЫ НАТО, отмечает, что термин «кибер» используется применительно к компьютерам, информационным сетям и цифровой информации [7, p. 21].

Рассмотрение вырабатываемых в рамках НАТО подходов по противодействию информационным угрозам и обеспечению кибероборонЫ представляет интерес в свете того, что вопросы в данной области относят к сфере «мягкой» безопасности (soft security), в то время как главная задача НАТО – противодействовать конвенциональным вызовам безопасности (hard security). Более того, после распада биполярного миропорядка НАТО проходит сложный процесс трансформации и до сих пор находится в поисках обретения своего raison d'être. Отсюда возникает необходимость найти ответы на ряд важных для евроатлантического пространства безопасности вопросов. Что понимается в НАТО под кибербезопасностью? Каково содержание и уровень информационных угроз? Кто является их источником?

Принимая во внимание фактическое отсутствие международной нормативно-правовой базы, регулирующей взаимоотношения акторов различного уровня в глобальном ин-

© Казаковцев А.В., 2012

формационном пространстве, а также традиционно высокие политические ставки в сфере евроатлантической безопасности и связанный с ними сложный процесс диалога между Россией и странами НАТО, представляется необходимым изучение политического измерения кибербезопасности внутри Альянса (дебаты о применении к данной сфере принципа коллективной обороны), а также степени секьюритизации данной проблематики в системе отношений Россия – НАТО.

НАТО и «проблемное поле» кибербезопасности

Ядром «проблемного поля» информационной безопасности является определение того, каковы природа и деструктивный потенциал информационных угроз. П. Корниш из лондонского Королевского института иностранных дел (Chatam House) приводит следующую классификацию информационных угроз: 1) деятельность хакеров-одиночек; 2) организованная преступность, действующая в глобальных интернет-сетях; 3) идеологический и политический экстремизм; 4) проводимая государством информационная агрессия [6, p. 7–16].

На сегодняшний день только первые две разновидности угроз из данной классификации обрели *практическое воплощение* в мировой политике. Что касается кибертерроризма и кибервойны между государствами, то они являются скорее *воображаемыми* угрозами, которые могут быть реализованы в будущем. Таким образом, в НАТО под кибербезопасностью понимается поддержание состояния готовности к отражению потенциальных угроз, обладающих «высокой интенсивностью», и принятию наступательных контрмер.

Эксперты из Центра киберзащиты НАТО рассматривают милитаризацию Интернета в качестве одного из главных и наиболее опасных трендов развития мирового киберпространства: «Современные военные структуры готовы использовать информационное пространство как “параллельное поле битвы” в конфликтах будущего». При этом выражается уверенность в том, что проведение кибератаки «в чистом виде» маловероятно [15]. Российские эксперты в области информационной безопасности также убеждены в том, что «отдельных кибервойн вне традиционных быть не может» [4]. Более вероятным является следующий сценарий: агрессивные акции в киберпространстве будут использоваться для усиления эффекта традиционных операций с применением обычных наступательных вооружений. Именно такая формула – обычные вооружения плюс кибероружие – будет лежать в основе стандартных оперативных и стратегических действий в будущих конфликтах.

При этом К. Гирз отмечает, что политические лидеры, ответственные за принятие решений, могут основывать свои действия лишь на теоретических предположениях. Причин тому несколько: на сегодняшний день слишком мало показательных примеров; подавляющий массив информации засекречен и находится вне пространства публичной политики; не было ни одной войны в эпоху Интернета между двумя первоклассными армиями; большинство организаций не осознают истинное состояние своей собственной информационной безопасности. Поэтому для политических элит зачастую сложно ответить на вопрос, действительно ли информационные атаки несут серьезную угрозу национальной безопасности [7, p. 12].

Восприятие кибер-угроз было отражено в новой версии Стратегической концепции НАТО, принятой на саммите в Лиссабоне в ноябре 2010 года. В данной концепции информационные атаки фигурируют в ряду наиболее опасных вызовов и угроз безопасности и процветанию государств-членов Альянса [17]. В иерархии вызовов, представленной в данной концепции, проблема исходящих из информационного пространства угроз располагается сразу после распространения оружия массового уничтожения и терроризма. Такое внимание, в свою очередь, обусловлено феноменом секьюритизации, под которым понимается артикуляция проблемы в контексте и сквозь призму проблем безопасности [3], и благодаря которому кибербезопасность с поразительной скоростью «эволюционировала из технической дисциплины в стратегический концепт» [7, p. 9].

В целом вопросы обеспечения кибербезопасности включают в себя объемный комплекс проблем, среди которых фигурируют угрозы, различающиеся по своим источникам

и мотивам. Важным макроструктурным фактором является отсутствие международно-правового консенсуса в отношении того, что понимать под терминами «кибервойна», «кибератака», «кибертерроризм» или «критически важная информационная инфраструктура».

Единственным на данный момент многосторонним международным документом по информационной безопасности является Конвенция по киберпреступлениям, принятая Советом Европы в 2001 году. Данная Конвенция содержит классификацию компьютерных преступлений, а также рекомендации органам законодательной и исполнительной власти по борьбе с этими преступлениями.

Таким образом, на наш взгляд, вышеперечисленные элементы «проблемного поля» – отсутствие единого понятийного пространства и международно-правовых конвенций, значимая роль новых акторов международных отношений, непрозрачные механизмы воздействия в интернет-среде – позволяют рассматривать глобальное информационное пространство как «серую зону» мировой политики. Как отмечают Д. Балуев и А. Новоселов, «серая зона» выглядит как «черный ящик», на входе в который мы имеем риски низкого уровня, порождаемые новыми акторами. На выходе же появляются серьезные угрозы существованию традиционных акторов – государств» [1, с. 10].

Институциональное измерение кибероборонны НАТО

Впервые вопрос об обеспечении кибербезопасности организации появился в насущной политической повестке дня НАТО на саммите в Праге в ноябре 2002 г., когда лидеры стран Альянса выразили готовность усиливать возможности по оказанию противодействия информационным атакам. С данного момента началось создание специальных органов НАТО, например таких, как Агентство НАТО по обслуживанию коммуникационных и информационных систем, характеризуемое как первая линия защиты Альянса против кибертерроризма.

После того как Эстония подверглась серии кибератак в апреле и мае 2007 г., в НАТО возник консенсус относительно восприятия исходящих из интернет-пространства угроз как стратегически важных. Официальная политика НАТО в сфере кибероборонны (NATO Cyber Defence Policy) была одобрена в январе 2008 г. министрами обороны стран-членов НАТО и представлена участникам организации в апреле 2008 г. на саммите в Бухаресте. Согласно итоговой декларации саммита, данный документ был призван «обеспечить возможности для оказания поддержки стране-союзнице, по ее требованию, в противодействии кибератаке» [14]. 8 июня 2011 г. на встрече министров обороны стран НАТО была принята новая политика кибероборонны. Содержание обоих документов недоступно для широкой общественности.

Тем не менее можно проследить предпринятые НАТО практические шаги в реализации политики кибербезопасности. Так, в 2008 г. было создано Управление по осуществлению кибероборонны. Функционально Управление было призвано инициировать и координировать ответные действия в случае кибератаки, направленной против кого-либо из государств-членов НАТО, или же самой НАТО [12].

Центр передового опыта в области кибероборонны в Таллине, получивший в октябре 2008 г. аккредитацию при НАТО и статус международной военной организации, не наделен оперативными функциями и служит в качестве исследовательского и обучающего центра, где разрабатываются доктринальные и концептуальные основы кибербезопасности и проводятся обучающие семинары. Данная структура позиционирует себя как «главный источник экспертизы в сфере совместной кибероборонны», который «аккумулирует, создает и распространяет знание по ключевым вопросам кибербезопасности внутри НАТО, между государствами Альянса и его партнерами» [16].

Британский эксперт Рекс Хьюз рассматривает эти два специализированных органа в качестве элементов единой организационной системы. Управление по осуществлению кибероборонны, предположительно наделенное «продвинутыми возможностями по осуществлению электронного мониторинга в «реальном времени», действует на оперативно-тактическом уровне. Центр передового опыта в области кибероборонны, разрабатывая долгосроч-

ную доктрину НАТО в данной сфере и представляя собой своеобразную «интеллектуальную платформу», является элементом стратегического уровня [9]. На данный момент трудно судить о том, насколько эффективны указанные институты. После эстонского инцидента и до последнего времени ни против структур НАТО, ни против кого-либо из членов Альянса крупномасштабных кибератак не предпринималось, поэтому, учитывая то, что Управление по осуществлению кибероборонысужит исключительно «для внутреннего пользования», оценить эффективность деятельности данного органа достаточно сложно. Располагающийся в Эстонии Центр за неполных 3 года (с октября 2008 г., когда данному институту был присвоен статус международной военной организации, до сентября 2011 г.) организовал 4 международных конференции: «конференцию по кибервойне» и три «конференции по киберконфликтам», а также несколько обучающих семинаров. Представляя собой своеобразную «коалицию желающих» (coalition of the willing), то есть относительно узкую группу стран, объединенных на основе «общего интереса», эта институциональная единица все же обладает потенциалом для проведения консультаций по вопросам кибербезопасности между странами-членами НАТО.

Таким образом, за короткий срок в НАТО была создана система специализированных механизмов и институтов оперативного и стратегического назначения. Можно ожидать, что степень релевантности данной системы проявится в тот момент, когда НАТО подвергнется (и если подвергнется) атакам «высокой интенсивности» – массированной террористической акции через глобальные информационные сети и (или) инспирированной государством кибератрессии.

Политическое измерение кибербезопасности

Проблема обеспечения безопасности информационных технологий и систем НАТО и ее членов обладает, помимо вопросов технического обеспечения и стратегического планирования, политическим измерением. В первую очередь это относится к возможности применения статьи 5 Вашингтонского договора в отношении информационных атак. Наиболее активными протагонистами расширения действия принципа коллективной ответственности в сфере обеспечения информационной безопасности выступают Эстония и, частично, США.

Эстония позиционирует себя в НАТО в качестве одного из главных экспертов в области киберзащиты и активно продвигает инициативы в международных организациях и на уровне двустороннего сотрудничества. Позиция Эстонии сводится к тому, что по своему воздействию кибервойна сопоставима со значением портовой блокады два века назад [13]. Американское видение проблемы выразила госсекретарь США Х. Клинтон, отметив в своей речи о будущем НАТО, что информационные атаки и сбой в поставках энергоресурсов должны рассматриваться как угрозы, требующие ответных коллективных действий [10]. Экспертно-аналитическое сообщество США в целом солидарно с позицией политической и военной элиты страны. Дж. Голдгейер, профессор университета имени Дж. Вашингтона, отмечает, что по своему определению кибератаки не являются «вооруженным нападением», то есть не подпадают под действие статьи 5 Вашингтонского договора. Однако затем он делает вывод о том, что «если Альянс хоть что-то собой значит, то он должен объединиться в противодействии атакам, угрожающим безопасности кого-либо из членов НАТО» [8, p. 4].

Проблемным фактором, проявляющемся на трансатлантическом уровне, является пресловутое «разделение труда» между членами НАТО, когда одни предпочитают специализироваться на «мягких» темах, а другие проводят жесткие военные миссии. Прямым следствием является принципиальная разница в подходах к сдерживанию кибератак: США, Франция, Великобритания и Германия сопоставляют информационную безопасность с военной стратегией, в то время как не обладающая военным потенциалом Эстония делает акцент на роли гражданского общества и частного сектора [11]. Кроме того, большинство государств-членов Альянса склонны рассматривать информационную безопасность с позиции национального

суверенитета и как исключительную прерогативу внутренней политики.

Другим чрезвычайно важным аспектом киберполитики НАТО является восприятие России как одного из главных киберагрессоров a priori. Как политический истеблишмент, так и экспертные сообщества стран Альянса склонны обвинять Россию в организации ряда массированных информационных атак на информационную инфраструктуру трех постсоветских государств. В 2007 г. были проведены крупномасштабные DDoS-атаки («отказ в обслуживании») на сайты парламента и правительства Эстонии, а также нескольких эстонских банков и новостных агентств. Аналогичные атаки в 2008 г. против Литвы и Грузии также рассматриваются западными политическими элитами и аналитиками как акты российской информационной агрессии [18].

Таким образом, сфера информационной безопасности конституируется в качестве новой линии разделения, отчуждения и даже конфронтации между Россией и НАТО.

В заключение отметим, что будущее как национальной, так и глобальной информационной безопасности будет зависеть от того, в какой степени государства проявят волю к конструктивному сотрудничеству в решении насущных проблем информационной безопасности. Ведь, как отметил министр внутренних дел ФРГ Томас де Мезьер, «поскольку интернет не признает государственных границ, то и усилия по обеспечению его безопасности должны быть международными» [2].

СПИСОК ЛИТЕРАТУРЫ

1. Балуев, Д. Г. «Серые зоны» мировой политики. Очерки текущей политики / Д. Г. Балуев, А. А. Новоселов ; отв. ред. М. А. Троицкий. – М. : Науч.-образоват. форум по междунар. отношениям, 2010. – Вып. 3. – 40 с.

2. Жолквер, Н. Германия выстраивает систему кибербезопасности / Н. Жолквер. – Электрон. текстовые дан. – Режим доступа: http://www.dw-world.de/dw/article/0,,14872477,00.html. – Загл. с экрана.

3. Макарычев, А. С. Безопасность как феномен публичной политики: общие закономерности и проекции на Балтийский регион / А. С. Макарычев. – Электрон. текстовые дан. – Режим доступа: http://megaregion.narod.ru/articles_text_2.htm. – Загл. с экрана.

4. Черненко, Е. Мы пока не так уязвимы, как американцы, но быстро их догоняем : интервью с первым замдиректора Института проблем информационной безопасности МГУ В. Ященко / Е. Черненко // Коммерсантъ. – 2011. – № 72/П (4613). – С. 4.

5. Шариков, П. А. Информационный комплекс / П. А. Шариков // Безопасность Европы / Ин-т Европы РАН. – М. : Весь мир, 2011. – С. 581–591.

6. Cornish, P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks / P. Cornish ; Directorate-General for External Policies of the Union, Policy Department. – Brussels : European Parliament, 2009. – 34 p.

7. Geers, K. Strategic Cyber Security / K. Geers. – NATO Cooperative Cyber Defence Centre of Excellence, 2011. – 169 p.

8. Goldgeier, J. The Future of NATO / J. Goldgeier // NATO Science for Peace and Security Series, E: Human and Societal Dynamics. – Amsterdam : IOS Press, 2011. – Vol. 76. – P. 1–12.

9. Hughes, R. B. NATO and Cyber Security: Mission accomplished? / R. B. Hughes. – Electronic text data. – Mode of access: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf. – Title from screen.

10. Joyner, J. Clinton: Cyber Security and Energy Security as NATO Priorities / J. Joyner. – Electronic text data. – Mode of access: http://www.acus.org/new_atlanticist/clinton-cyber-security-and-energy-security-nato-priorities. – Title from screen.

11. Kempf, A. Considerations for NATO Strategy on Collective Cyber Defense / A. Kempf. – Electronic text data. – Mode of access: http://csis.org/blog/considerations-nato-strategy-collective-cyber-defense. – Title from screen.

12. McGee, J. NATO and Cyber Defense: A Brief Overview and Recent Events / J. McGee. – Electronic text data. – Mode of access: http://csis.org/blog/nato-and-cyber-defense-brief-overview-and-recent-events. – Title from screen.

13. Myrli, S. NATO and Cyber Defence / S. Myrli. – Electronic text data. – Mode of access: http://www.nato-pa.int/Default.asp?CAT2=1765&CAT1=16&CAT0=2&COM=1782&MOD= 0&SMD=0&SSMD=0&STA=&ID=0&PAR=0&PRINT=1. – Title from screen.

14. NATO Bucharest Summit Declaration, Art. 47, 3 April 2008 / NATO. – Electronic text data. – Mode of access: http://www.nato.int/docu/pr/2008/p08-049e.html. – Title from screen.

15. NATO CCD CoE General Trends / NATO Cooperative Cyber Defence Centre of Excellence. –

Electronic text data. – Mode of access: http: //www.ccdcoe.org/8.html. – Title from screen.

16. NATO CCD CoE Mission and Vision / NATO Cooperative Cyber Defence Centre of Excellence. – Electronic text data. – Mode of access: http: //www.ccdcoe.org/11.html – Title from screen.

17. Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation. Active Engagement, Modern Defence / NATO. – Electronic text data. – Mode of access: http: //www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf. – Title from screen.

18. Tikk, E. Global Cyber Security – Thinking About the Niche for NATO / E. Tikk. – Electronic text data. – Mode of access: http://www.ccdcoe.org/articles/2010 /Tikk_GlobalCyber Security.pdf. – Title from screen.

NATO AND CYBER SECURITY

A.V. Kazakovtsev

This article investigates the NATO policy in cyber security domain. Then, urgent problems related to definitions and classifications of "cyber" are examined. Also, this article reveals the evolution of NATO's operational and strategic cyber defence institutions. Finally, it attempts to disclose political dimension of NATO's cyber defence policy.

Key words: *cyber security, cyber threats, cyber warfare, strategic concept, securitization, NATO.*