DOI 10.35775/PSI.2024.107.7.032
УДК 32.327

А.М. ЖБАНОВ
аспирант кафедры международных отношений
и интеграционных процессов факультета политологии
МГУ им. М.В. Ломоносова,
Россия, г. Москва

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ПОЛИТИКИ КИБЕРБЕЗОПАСНОСТИ КРУПНЫХ ДЕРЖАВ

В статье рассматривается современные тенденции политики кибербезопасности ключевых акторов современной системы международных отношений. Проанализированы тенденции в области укрепления военного, разведывательного и стратегического потенциала государств в киберпрострнстве. Рассмотрены текущие проблемы и возможные причины милитаризации киберпространства.

Ключевые слова: *киберпространство, кибербезопасность, международная информационная безопасность, информационное противоборство, информационная война, международное право, искусственный интеллект.*

Тенденции политики кибербезопасности в условиях современных вызовов и угроз в текущей статье рассматриваются в оптике наступательного реализма (offensive realism), структурной теории в рамках реалистической школы международных отношений, предложенной Д. Миршаймером. В рамках наступательного реализма развитие стратегических направлений и вооруженных сил обусловлено анархической природой международной системы и стремлением государств к выживанию, безопасности и увеличению безопасности через укрепление международного положения, которое требует наличия соответствующих силовых ресурсов [17. С. 20-22]. Таким образом, государства должны полагаться на свой собственный военный потенциал для обеспечения своего выживания и защиты своих интересов, не только в оборонительных целях, но и для демонстрации мощи, сдерживания потенциальных противников и обеспечения своего положения в международной системе либо усиления своего положения в ней. Киберпространство, таким образом, будучи пространством проекции силы [21], становится объектом классической дилеммы безопасности и требует от международных акторов, претендующих как на сохранение текущего статуса-кво в отношении собственного положения в международной системе (США), так и стремящихся к ревизии существующей системы и увеличению своего влияния (Российская Федерация, Китай) развивать собственный военный, стратегический и оборонительный потенциал в киберпространстве.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 3; 4; 5; 7; 8; 9; 11; 12; 13; 14].

Однако проблему кибербезопасности в условиях современных вызовов и угроз нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Стоит отметить, что в данной статье под киберпространством понимается многоуровневое информационно-коммуникационное пространство, которое имеет три взаимосвязанных атрибута-области, которые могут выступать в качестве объектов направленного воздействия, что основывается на подходах исследователей киберпространства Э. Уолтца [22. С. 148] и Д. Кёля [18. С. 32]:

1) физическое измерение киберпространства – область физических носителей, сетей, компьютеров и серверов, инфраструктуры связи. Данное измерение обеспечивает создание, хранение, модификацию, обмен и использование информации через взаимозависимые и взаимосвязанные сети, что следует из определения;

2) цифровое измерение киберпространства – область, представленная с данными и информацией, программным обеспечением для работы физического измерения киберпространства и обеспечивающая возможность трансграничного обмена информацией и трансграничного моментального воздействия как на физическое измерение киберпространства с помощью специальных действий, так и на измерение пользователей киберпространства с помощью информационного контента;

3) пользовательское измерение киберпространства – область, представленная сознанием пользователей киберпространства и являющаяся адресатом и источником направленных действий в киберпространстве, которые предполагают влияние на поведение пользователей и принятие решений.

Анализ политики кибербезопасности США и Китая позволяют выделить тенденции общего вектора движения государств в отношении киберпространства, которые имеют схожие характеристики, но также обусловлены спецификой положения государств в международной системе и особенностями политических режимов государств. Общие для большинства самостоятельных акторов международной системы тенденции политики кибербезопасности можно обобщить и упростить до двух направлений:

1) усиление контроля за национальным сегментом киберпространства;

2) увеличение собственного потенциала в киберпространстве, опирающегося на противодействие возможным кибератакам со стороны иностранных государств, сбор разведданных, развитие системы национальных вооруженных сил, действующих в киберпространстве и иных действий, всецело этому способствующих.

Данные направления, в свою очередь, переплетаются с требованием проведения гражданской политики, направленной на создание конкурентной технологической базы и развитие человеческого капитала для обладания ресурсами – человеческим и научно-техническим, который необходим для осуществления эффективной реализации данных направлений. Контроль за киберпространством также осуществляется посредством постепенного формирования соответствующей нормативно-правовой базы и законодательных рамок, позволяющих регулировать любые действия пользователей национального сегмента киберпространства. Особое значение в рамках контроля за киберпространством имеет способность государства эффективно противодействовать и воспрепятствовать попыткам иностранных государств оказывать влияние или проводить деструктивные действия в киберпространстве. В подтверждение данной гипотезы выступает всё более активное ужесточение законодательства и усиление контроля за возможным иностранным вмешательством во внутренние дела государств посредством информационно-коммуникационных технологий, которое сопровождает теперь, пожалуй, все избирательные кампании в США, Российской Федерации и странах Европейского Союза. Предыдущие этапы укрепления власти государств в сети Интернет сопровождались постепенным формированием регулирующей законодательной базы в отношении операторов связи и данных их клиентов, а также постепенным формированием специализированных подразделений правоохранительных органов, направленных на предотвращение правонарушений в сети Интернет. По мере расширения академических исследований в области возможности использования киберпространства в качестве потенциального пространства реализации национальных интересов, а также осознания потенциала воздействия информационно-коммуникационных технологий и инструментов на общественное мнение, государства стали укреплять национальную экспертизу в области информационной работы с населением собственных и зарубежных стран, формировать национальные подразделения специальных служб и вооруженных сил для проведения информационных операций и операций вмешательства в национальные сети государств-соперников. Параллельно шел процесс усиления национального законодательства и создания надзорных и регулирующих органов для предотвращения подобной активности иностранных государств. По мере развития интернет-технологий и сервисов гражданского пользования, всё большее значение приобрел контроль за мировыми потоками данных, который определяется через доминирующее положение ИТ-корпораций на рынках данных. Крупные международные акторы, обладающие самостоятельными решениями в области программного обеспечения, социальных сетей, интернет-технологий и сервисов, представленных ИТ-компаниями, получают влияние и технологическое доминирование посредством их монополий в глобальном масштабе, сформировавшихся в условиях проблем цифрового и технологического неравенства малых и средних государств. Проблема цифрового неравенства стран отмечается в обзоре Всемирного экономического форума Global Cybersecurity Outlook 2024 [23. С. 8], а тема зависимости

государств и политики от интернет-технологий присутствует в обзоре мировых рисков Всемирного экономического форума The Global Risks Report 2022 [24. С. 45-56].

Глобальная конкуренция в сегменте цифровых технологий привела к необходимости разработки и внедрения управленческих механизмов регулирования потоков цифровых данных для защиты национальных интересов в глобальном киберпространстве. Политика США в отношении социальной сети TikTok, официальный запрет Китая на использование западных социальных сетей и ограничения доступа к сервисам компании Meta вследствие ее признания экстремистской организацией, запрещенной в Российской Федерации, свидетельствуют о постепенном закате явления цифрового западного глобализма, который, как предполагается, впоследствии будет угасать и дальше. Как видно из политики государств, стремящихся увеличить контроль за киберпространством, в данных целях используются такие практики как цифровой протекционизм, представленный барьерами для иностранных цифровых сервисов и компаний, включающий в себя требования к локализации, ограничения на трансграничную передачу данных, фильтрации, блокировки, интернет-цензуру, ограничения в отношении электронных платежных систем или методов шифрования, а также принудительную передачу технологий или ключей шифрования в интересах национальной безопасности [19]. По мере дальнейшего роста экономик стран, занимающих вторые и третьи роли в международной системе, предполагается, что они также будут использовать цифровой протекционизм для уменьшения возможности иностранного влияния на свои общественные и политические процессы в киберпространстве. Данные тенденции соответствуют логике процесса деглобализации и постепенному снижению влияния США в международной системе. Предполагается, что тенденции кибербезопасности в данной сфере сформируют глобальные цифровые макрорегионы по аналогии с экономическими макрорегионами, при этом «границы» цифрового пространства вероятно, могут соответствовать цивилизационным связям стран и уровнем экономической интеграции. Определение допуска таких цифровых продуктов, как социальные сети на рынок малых государств станет вопросом прежде всего политическим и вопросом культурной идентичности, на принципе которой вероятно, также могут определяться границы цифровых макрорегионов.

Учитывая тенденции развития интернета и телекоммуникаций, постепенный переход к 4-му поколению интернета, или Web 4.0, который будет опираться на новые принципы скорости передачи данных, искусственный интеллект, и главное – интернет вещей, встает вопрос о требованиях безопасности и полной прозрачности интернета для надзорных органов, правоохранителей и специальных служб. Всё большая интеграция производственных процессов и систем критически-важной инфраструктуры, а также производство человеко-машинных интерфейсов с потенциальным доступом в сеть демонстрируют, что цена потенциального взлома со стороны злоумышленников становится слишком высокой – на кону не только экономика, но и физическая и санитарная безопасность

людей. Таким образом, усиление контроля государств за деятельностью пользователей интернета будет возрастать, возможность оставаться анонимным и сохранять конфиденциальность в интернете постепенно будут ассоциироваться с временами эпохи появления интернета (при сохранении риторического вопроса – «был ли на самом деле интернет анонимным и конфиденциальным для всех участников международной системы?»). При этом перспективы и выгоды от возможного доступа к данным в пределах национального сегмента киберпространства потенциального противника, а также объем потенциального ущерба в случае кибератаки на гражданские и военные сетевые инфраструктуры вместе со стратегическими преимуществами, которые могут быть достигнуты за счет анализа собираемых интернет-сервисами данных, делают неизбежным развитие специальных подразделений и увеличение военного и специального контингента государств, претендующих на значимые позиции в рамках будущей системы международных отношений. По аналогии с процессами, происходившими в военном деле и «коэволюцией» средств наступления и средств обороны, киберпространство и деятельность международных акторов в нем будут сопровождаться гонкой вооружений, которая происходит уже сейчас [16]. Особенностью киберпространства является также и то, что «средствами двойного назначения» в нем могут выступать почти все системы гражданского пользования, социальные сервисы, средства связи, вычислительные машины, поскольку данные во всех атрибутах-областях киберпространства могут использоваться в военных целях для направленного воздействия, а почти любое программное обеспечение или средства связи могут быть проводником для его осуществления. Объектом новой гонки вооружений в том числе становится развитие искусственного интеллекта нового типа, полноценное создание которого, по утверждению многих исследователей, в числе которых и бывший госсекретарь США г. Киссинджер [6. С. 131], предоставит одной из сторон колоссальное преимущество в потенциальном вооруженном конфликте будущего как в киберпространстве, так и на конвенциональных театрах боевых действий. При этом «контроль вооружений» в киберпространстве выглядит скорее недостижимой и бессмысленной мерой, которая вряд ли будет реализована в перспективе ближайших 20 лет, о чем свидетельствует отсутствие результатов в выработке единых подходов международного права спустя более чем 10 лет попыток привлечь внимание к их отсутствию на площадке ООН.

Также стоит отметить, что потенциальный интерес крупных держав и акторов международной системы в построении архитектуры международной безопасности в киберпространстве менее выражен, чем интерес малых и средних держав, которые чаще становятся объектами влияния со стороны более ресурсных участников международной системы в киберпространстве. Более того, разница подходов и существующие на текущий момент разногласия между участниками международной системы демонстрируют, что вопросы информационного вмешательства и оказания влияния, а также процессы, связанные с анализом

данных о пользователях сервисов и кибершпионажем также выглядят труднорегулируемыми на текущий момент.

Также, наблюдаются тенденции на институционализацию взаимодействия частного сектора и государства в вопросах обеспечения кибербезопасности, а также в их сотрудничестве в проведении стратегически-значимых для государств действий, будь то сбор и предоставление информации, преференции в отношении продвигаемого контента и политики превентивной блокировки нежелательного контента, содействие в распространении требуемых нарративов. За более чем 20 лет существования частных телефонных и интернет-сетей в России, сформировалась правовая и законодательная база, обязывающая операторов данных предоставлять информацию о пользователях в целях предотвращения правонарушений и преступлений против национальной безопасности. Предполагается, что тенденции к увеличению государственного контроля, характерные для всего мира по мере роста международной напряженности и увеличения числа актуальных вызовов и угроз будут усиливаться и запрос государства на полностью «прозрачное киберпространство» будет осуществляться как минимум в тех областях, где это технически осуществимо.

С другой стороны, стоит отметить, что ряд технических аспектов пользования глобальной сети, таких как возможность сохранения анонимности с помощью использования систем луковой маршрутизации, использование анонимных сетей и систем шифрования на сегодняшний день вызывает много вопросов относительно осуществления государственного контроля в киберпространстве. Системы сохранения анонимности по типу Tor, основанные на принципе луковой маршрутизации и использующие анонимные сети peer-to-peer прокси-серверов, каждый из которых по цепочке передает зашифрованный пакет данных и видоизменяет шифр по мере передачи сигнала в целях сохранения анонимности, используются международной организованной преступностью, террористическими и экстремистскими организациями и, с высокой долей вероятности также используются военными ведомствами и специальными службами многих государств мира. Долгое время считалось, что подобные системы позволяют сохранять полную анонимность их пользователей, многие нелегальные торговые площадки, осуществляющие торговлю оружием, наркотическими веществами, людьми и органами существовали (и продолжают существовать) в рамках системы peer-to-peer прокси-серверов с луковой маршрутизацией. Так, самая масштабная в истории мировой наркоторговли торговая площадка Silk Road, аналог сети Amazon для покупки запрещенных и нелегальных товаров, существовала в рамках системы луковой маршрутизации в анонимной интернет-сети [15]. При этом, стоит отметить, что сама технология подобной маршрутизации была запатентована Военно-морскими силами США в 1998 году [10], а ряд экспертов заявляли о том, что она не может предоставлять полную анонимность своим пользователям, и содержит значительное количество уязвимостей, которые представляют опасность утечки как передаваемых сообщений, так и возможность раскрытия данных об отправителе сообщения [20]. Учитывая

данные обстоятельства, возникает ряд вопросов относительно полной анонимности пользователей сети перед создателями технологии. Не будет преувеличением заявлять о возможности полного контроля за технологией анонимного использования киберпространства со стороны разведсообщества США, учитывая историю появления как технологии, так и способов передачи данных в сети, что теоретически делает «серую зону» в киберпространстве относительно прозрачной для США. Подобная несимметричность международной безопасности создает угрозы для международных акторов, заинтересованных в пересмотре текущей системы международных отношений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А.** Современные подходы ведения гибридных войн США, Великобритании, Франции, Германии // Вопросы национальных и федеративных отношений. 2024. Т. 14. № 3 (108).
2. **Вахитов Р.Р.** Концепции сдерживания в киберпространстве // Вопросы национальных и федеративных отношений. 2024. Т. 14. № 3 (108).
3. **Вахитов Р.Р.** Чувствительность и уязвимость стран в киберпространстве как фактор взаимоотношений // Вопросы национальных и федеративных отношений. 2024. Т. 14. № 1 (106).
4. **Григорян Д.К., Делов Н.С., Тищенко Е.В.** Кибертерроризм как угроза национальной безопасности. Элитарный подход // Евразийский Союз: вопросы международных отношений. 2023. Т. 12. № 2 (48).
5. **Закиров Б.Б.** Перспективы взаимодействия Шанхайской организации сотрудничества и Организации Объединенных Наций в борьбе с современными вызовами и угрозами безопасности // Евразийский Союз: вопросы международных отношений. 2023. Т. 12. № 5 (51).
6. **Киссинджер г.** Искусственный разум и новая эра человечества / Генри Киссинджер, Эрик Шмидт, Дниэл Хаттенлокер; Пер. с англ. М.: Альпина ПРО.
7. **Куликов Д.А.** Цифровые картели как новый вид киберпреступности в российской антимонопольной практике // Вопросы национальных и федеративных отношений. 2023. Т. 13. № 2 (95).
8. **Ло Дунмэй.** Сравнительный анализ кибербезопасности в Китае и США // Вопросы национальных и федеративных отношений. 2023. Т. 13. № 9 (102).
9. **Ло Дунмэй, Ян Бо.** Российско-китайское сотрудничество в области кибербезопасности в XXI веке: возможности и вызовы // Вопросы политологии. 2023. Т. 13. № 11-2 (99-2).
10. Патент Соединенных Штатов Америки № 6266704 (1998) // https://patents.google.com/patent/US6266704B1/en.
11. **Степовая Д.А.** Безопасность национального киберпространства в условиях информационно-психологического противоборства // Вопросы политологии. 2023. Т. 13. № 5 (93).

12. **Сунь Сяомэн, Медведев Н.П.** Нетрадиционные угрозы безопасности и пути им противодействия в контексте международного сотрудничества // Вопросы политологии. 2024. Т. 14. № 5 (105).
13. **Чжао Лэй.** Кибергеополитика: новое направление в геополитике // Вопросы национальных и федеративных отношений. 2023. Т. 13. № 11 (104).
14. **Шакурова Н.Е.** Внутренние и внешние угрозы национальной безопасности России в современных условиях // Евразийский Союз: вопросы международных отношений. 2023. Т. 12. № 7 (53).
15. **Christin N.** Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace // Proceedings of the 22nd international conference on World Wide Web. 2013 // https://scholar.google.com/scholar_lookup?arxiv_id=1207.7139#d=gs_cit&t=1716630835958&u=%2Fscholar%3Fq%3Dinfo%3AtRfyUZ72zCkJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Dru.
16. **Craig A. & Valeriano B.** Conceptualising cyber arms races. Conference: 2016 8th International Conference on Cyber Conflict (CyCon). 2016 // https://www.researchgate.net/publication/305871947_Conceptualising_cyber_arms_races.
17. **John J.** Mearsheimer. The Tragedy of Great Power Politics. 2001.
18. **Kuehl D.T.** From cyberspace to cyberpower: defining the problem // Cyberpower and national security edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Center for Technology and National Security Policy. Washington, 2009.
19. **Lund S. and Manyika J.** Defending Digital Globalization // Foreign Affairs. 20.04.2017 // https://www.foreignaffairs.com/articles/world/2017-04-20/defending-digital-globalization.
20. **Peled M., Goldstein D. & Yavorovsky A.** Attacking Tor with covert channel based on cell counting. 2011.
21. **Venables A., Shaikh S.A. and Shuttleworth J.** The projection and measurement of cyberpower // Security Journal. 2015. Volume 30, no. 3.
22. **Waltz E.** Information Warfare: Principles and Operations. Boston: Artech House, 1998.
23. World economic forum. Global Cybersecurity Outlook 2024 // https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.
24. World economic forum. Global Risk report 2022 // https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

A.M. ZHBANOV
Postgraduate student, Department of International
Relations and Integration Processes, Faculty of Political Science,
Lomonosov Moscow State University,
Moscow, Russia

CONTEMPORARY TRENDS IN CYBERSECURITY POLICY OF MAJOR POWERS

The article examines current trends in cybersecurity policy of key actors in the modern system of international relations. Trends in strengthening the military, intelligence and strategic potential of states in cyberspace are analyzed. Current problems and possible causes of the militarization of cyberspace are considered.

Key words: *cyberspace, cybersecurity, international information security, information confrontation, information warfare, international law, artificial intelligence.*