# Connections

Ежеквартальный Журнал

Консорциум «Партнерство ради мира» военных академий и институтов по изучению вопросов безопасности

## Сети социального взаимодействия

## Кибер(без)опасность на море

## Как Талибан и мир видят друг друга

Лето-Осень 2021

*Консорциум военных академий*
*и институтов изучения проблем безопасности*
*программы «Партнерство ради мира»*



Издание выходит про поддержке правительства США. Серия публикаций Консорциума доступна бесплатно по адресу http://www.connections-qj.org. Если вы хотите заказать для своей библиотеки печатные экземпляры или у вас есть вопросы касательно публикаций Консорциума, просим обращаться в Консорциум «Партнерства ради мира», PfPCpublications2@marshallcenter.org.

Летне-осенний выпуск 2021 года журнала *Connections: The Quarterly Journal* был опубликован с задержкой. Содержание может отражать информацию и события, которые произошли позже указанной на обложке даты.

Д-р Рафаэль Перл
Исполнительный директор

Шон Костиган
Главный редактор Редколлегии

ISSN 1812-1101, e-ISSN 1812-2973

# CONNECTIONS

## THE QUARTERLY JOURNAL

**том 20, № 3-4, лето-осень 2021**

Консорциум оборонных академий и институтов по изучению безопасности в рамках программы «ПрМ»

*Connections: The Quarterly Journal*
**ISSN 1812-1101, e-ISSN 1812-2973**

https://doi.org/10.11610/Connections.rus.20.3-4

**Содержание**

# Том 20, № 3-4, лето-осень 2021 г.

## Рецензированные статьи

*Connections: The Quarterly Journal*
**ISSN 1812-1101, e-ISSN 1812-2973**

Хилтон Рут, *Connections QJ* 20, № 3-4 (2021): 5-31
https://doi.org/10.11610/Connections.rus.20.3-4.01

**Рецензированная статья**

# Как сети социального взаимодействия масштабируются в цивилизации

## *Хилтон Рут*

*Университет Джорджа Мэйсона, Школа политики и управления им. Дуайта Шара, https://schar.gmu.edu*

**Аннотация**: Статья анализирует структуру и функции сетевого устройства минувших режимов Китая и Западной Европы в обоснование теории развития обществ и государств на основе внутренних механизмов социальных изменений. В ней показано, как их сетевые структуры развивались независимо, но имея общую черту: обе они – «маленькие миры», а это значит, что из любого узла сети можно достичь любого другого узла за несколько шагов. Автор объясняет различия в формальных институтах, доверии между людьми, культурных нормах и моральных протоколах, исследуя различия в сетевых топологиях и их роль в распространении и масштабировании. Сетевая структура как независимая переменная выводит дискуссию о расхождении Востока и Запада за рамки традиционных дебатов о централизованном Китае в противопоставлении децентрализованной Европе. Она позволяет нам выявить упущенный из виду фактор структурных изменений в государственном устройстве, помогая понять, что отличает развитие мировых цивилизаций.

**Ключевые слова**: политическая экономия, сети, сравнительное развитие, Европа, Китай, структурная трансформация.

## Вступление

Социально-экономические модели, изучавшие сотрудничество, десятки лет предрекали, что оно будет существовать только в группах, выработавших

социальные нормы обязательств, доверия и взаимности.[1] Но, как заметил Мэтью Джексон (и это справедливо до сих пор), эти прогнозы всегда основаны на моделях, касающихся небольших групп агентов и игнорирующих вопросы о том, как сообщества встраивают сети в исторические режимы, способные создавать связи, выходящие за рамки родства и происхождения.[2] Как, например, формировались и пережили тысячелетия культурные и исторические комплексы Европы и Китая? Как они могли координировать сложные многоуровневые функции преемственности руководства, передачи собственности, использования доходов и оружия, а также разработки кодексов поведения и морального убеждения? Массовое появление агентного моделирования позволяет расширить диапазон анализа на большие сети, из которых можно получать глобальную информацию о структурах, например, о существовании глубинного маленького мира или о безмасштабных характеристиках.

Ученые, занимающиеся вопросами устойчивых культурных различий Китая и Запада, предлагают противоречивые объяснения, основанные на экономических, географических, демографических, организационных или политических интерпретациях, но одно остаётся неизменным: Китай был централизован, а Европа децентрализована.[3] В этой статье я рассматриваю эко-

---

[1] Общий обзор этой литературы см. в Mark S. Granovetter, "The Impact of Social Structure on Economic Outcomes," *Journal of Economic Perspectives* 19, no. 1 (2005): 33-50, https://doi.org/10.1257/0895330053147958.

[2] Matthew O. Jackson, *Social and Economic Networks* (Princeton: Princeton University Press, 2008).

[3] Традиционную точку зрения, поясняющую динамизм Европы её децентрализованной межгосударственной конкуренцией, отстаивают Marc Bloch, *Feudal Society* (Chicago: The University of Chicago Press, 2014), 431; Avner Greif and Guido Tabellini, "The Clan and the Corporation: Sustaining Cooperation in China and Europe," *Journal of Comparative Economics* 45, no. 1 (February 2017): 1-35, https://doi.org/10.1016/j.jce.2016.12.003; David S. Landes, "Why Europe and the West? Why Not China?" *The Journal of Economic Perspectives* 20, no. 2 (Spring 2006): 3-22, https://doi.org/10.1257/jep.20.2.3; Nathan Rosenberg and L.E. Birdzell Jr., *How the West Grew Rich. The Economic Transformation of the Industrial World* (New York: Basic Books, 1986); Joel Mokyr, *The Lever of Riches: Technological Creativity and Economic Progress* (Oxford: Oxford University Press, 1990), https://doi.org/10.1093/acprof:oso/9780195074772.001.0001, 231; Chiu Yu Ko, Mark Koyama, and Tuan-Hwee Sng (2018). Другие видные ученые придерживаются парадигмы конкурентной государственной системы в противопоставлении единой империи: Montesquieu (trans. 1900), Karl Marx, *Division of Labour and Mechanical Workshop: Tool and Machinery*, Economic Manuscripts of 1861-63 (New York: International Publishers, 1991); Max Weber, *General Economic History* (London: Allen & Unwin, 1927); Jared M. Diamond, *Guns, Germs, and Steel: The Fates of Human Societies* (New York: W.W. Norton, 2005); Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West 1500-1800* (Cambridge: Cambridge University Press, 1996); Geoffrey Parker, *The Cambridge Illustrated History of Warfare: The Triumph of the West* (Cambridge:

номические траектории Китая и Европы, изучая их сетевые структуры и механизмы обмена информацией. Открытия в исследованиях сетей сместили фокус анализа социальных сетей с центральности одного узла и представления связей небольшой схемы на рассмотрение масштабных свойств всей схемы (сетевой структуры). Теперь исследователи могут видеть, как сетевые механизмы обеспечивают связь на уровне системы и распространяют инновации для масштабного сотрудничества, а также как сами системы развиваются вместе с сообществами, которые они поддерживают. Ведя поиск сетевых механизмов, позволяющих отдельным людям и сообществам участвовать в масштабном сотрудничестве, я также хочу обнаружить в сетевых структурах источники, которые помогут объяснить распространение инноваций. Таким образом я могу исследовать не только общие свойства Китая и Европы, но и различия в социальной организации, которые сформировали их «инновационные культуры» и позволили им создать масштабные сети для решения задач социального сотрудничества.[4]

Важным элементом сотрудничества и распространения инноваций в любой сети является связь одного сообщества с другими. Легко увидеть, как современные информационные технологии связаны с динамикой взаимозависимости внутри стран и между ними. Обмен информацией происходит повсюду вокруг нас. Но во многих плохо управляемых государствах прошлого верования и институты, представляющие единство общества, тоже могли быть сплетены воедино. Механизмы диффузии также позволили режимам в Европе и Китае, существовавшим в течение длительного времени, перейти от первоначальных племенных и сельских сетей к более широким сообществам, королевствам, государствам, нациям и, в конечном счёте, цивилизациям.[5]

Автор предлагает относить долгоживущие цивилизации, государства и общества к универсальному классу систем, сетевая структура которых включает множество различных моделей пересечений, но которые имеют общее свойство: способность соединять части — хутора, сёла, поселки — и координировать их деятельность, независимо от того, насколько они удалены или слабо управляемы, через сеть обмена информацией, обеспечивающую

---

Cambridge University Press, 2008); и Immanuel Wallerstein, “The Rise of State-System: Sovereign Nation-States, Colonies and the Interstate System,” in *World-Systems Analysis*, ed. Immanuel Wallerstein (Duke University Press, 2004), 42-59.

[4] Сложные сети анализируют Fernando Vega-Redondo, *Complex Social Networks*, Econometric Society Monographs, Series Number 44 (New York: Cambridge University Press, 2007); Mark E.J. Newman, “The Structure and Function of Complex Networks,” *SIAM Review* 45, no. 2 (2003): 167-256, https://doi.org/10.1137/ S003614450342480; и Mark Newman, Albert-László Barabási, and Duncan J. Watts, *The Structure and Dynamics of Networks*, Princeton Studies in Complexity (Princeton: Princeton University Press, 2006).

[5] Ранняя Европа и Китай имели сложный государственно-социальный потенциал, намного превосходивший жизнеспособность империй монголов, османов или великих моголов, располагавшихся в центре Евразии.

коллективную память и чувство общей цели. Это гигантские сети связи, в которых на неком фундаментальном уровне каждый узел обрабатывает информацию от других узлов, образующих систему. Я использую сетевую науку, чтобы узнать, как происходил такой обмен информацией без современных коммуникационных технологий.[6]

Сетевые структуры, или топологии, Западной Европы и Китая развивались независимо, но, как в сетях маленьких миров, каждый узел там может достичь любого другого узла сети за несколько шагов. Их связь в маленьком мире сама по себе имеет ещё одно свойство: в обоих случаях связь исторически была воплощена в системе правления наследственной королевской власти. Изучая различия между двумя сетевыми структурами, мы увидим, как распространение информации внутри них давало каждой из них свои преимущества.

В 1 разделе автор рассмотрит устойчивость сетей маленького мира, их эволюционную конвергенцию и их преимущества для расширения сотрудничества за рамки родства и происхождения. В этом разделе описано, как социальные структуры сплетаются в сеть, с описанием и определением малого и большого миров, а завершается он обсуждением роли связей малого мира в формировании устойчивых исторических режимов. Во 2 разделе рассмотрены структуры системного уровня на Западе и в Китае, а также роль мостовых узлов. В двух следующих разделах приведены исторические аналогии для рассмотрения конкретных социальных институтов, поддерживающих взаимосвязи: в 3 разделе рассмотрен общий институт Китая и Запада — наследственная преемственность, а в 4 разделе — институциональные различия, такие, как религия, а также социальная мобильность, формирование элит и местное самоуправление. В 5 разделе рассмотрено, как эти сетевые структуры могут объяснить разные инновационные системы со ссылками на различия экономических структур двух режимов. В 6 разделе рассмотрены сетевые источники межличностного социального доверия и укоренённость культурных норм. В заключении мы подумаем о том, как устойчивые различия в их сетевых топологиях могут влиять на дальнейшую эволюцию этих двух обществ, принимая во внимание тот факт, что в Китае нет каких-либо исторических параллелей с сетями и институтами доверия, имевшими важное значение для развития Западной Европы.

## Связанность: Как топология системы позволяет сообществам «сплетаться» в сеть

Первобытные человеческие сообщества представляли собой небольшие сети, основанные на родоплеменной принадлежности. Эта гомофилия —

[6] О связи информационных технологий с более широкими национальными интересами и международным положением см. Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, eds., *The Uses and Abuses of Weaponized Interdependence* (Washington DC: Brookings Institution Press, 2021).

склонность общаться только с подобными — позволила им выжить.[7] Согласно большинству этнографических описаний ранних человеческих поселений, при господстве гомофилии возникали определённые традиции, например, божества, законы и культурные нормы. В одних обществах статус зависел от происхождения, в других – от достижений. Без общих убеждений, моральных норм и правил сообщества воздерживались от широкого сотрудничества. Многие примитивные общества также имели почти непроницаемые внутренние барьеры, усиливавшие расслоение их членов, что приводило к ещё большей разобщенности.[8]

А ещё гомофилия превратила бóльшую систему, в которой они жили, в «большой мир» — теоретический термин, отражающий реальность, при которой связь и взаимодействие в основном локальны и изолированы. На схеме сеть большого мира демонстрирует высокий коэффициент кластеризации, но низкую сетевую связанность.[9,10] Таким образом, сеть большого мира может состоять из узлов, сведённых в немаленькие группы, но каждый узел будет связан только с несколькими соседними узлами, а сообщества (узлы) не связаны друг с другом. В этой высоко децентрализованной структуре нет длинных путей для сокращения дистанции между разными узлами.

Там, где нет длинных путей, есть *большая средняя длина пути* — ещё одно системное свойство больших миров. Длина пути характеризует не длину как таковую, а эффективность. Она показывает, как быстро и по каким каналам информация распространяется по общей сети. В большом мире информация проходит короткими путями: от одного узла к другому, затем к следующему. Передача по всей системе может потребовать тысяч взаимодействий между отдельными узлами — следовательно, большой длины пути от любой начальной точки A до конечной точки B — что удорожает распространение, отнимает много времени и ведёт к сбоям и искажениям. По

---

[7] Miller McPherson, Lynn Smith-Lovin, and James M. Cook, “Birds of a Feather: Homophily in Social Networks,” *Annual Review of Sociology* 27 (2001): 415-444, https://doi.org/10.1146/annurev.soc.27.1.415.

[8] Kent Flannery and Joyce Marcus, *The Creation of Inequality: How Our Prehistoric Ancestors Set the Stage for Monarchy, Slavery, and Empire* (Cambridge: Harvard University Press, 2012); Hilton L. Root, *Network Origins of the Global Economy: East vs. West in a Complex Systems Perspective* (Cambridge University Press, 2020), 115-119.

[9] Связи малых сетей обычно распределяются довольно равномерно по отношению друг к другу и объединяются в некое подобие сети улиц или станций метро в городе, дорог в сельской местности или пикселей цифрового изображения. Сеть авиарейсов, напротив, представляет собой маленький мир, поскольку в ней имеется множество взаимосвязанных узлов, которые сокращают пути и улучшают общесистемную координацию.

[10] Thomas Michelitsch et al., *Fractional Dynamics on Networks and Lattices* (Wiley, 2019), https://doi.org/10.1002/9781119608165.

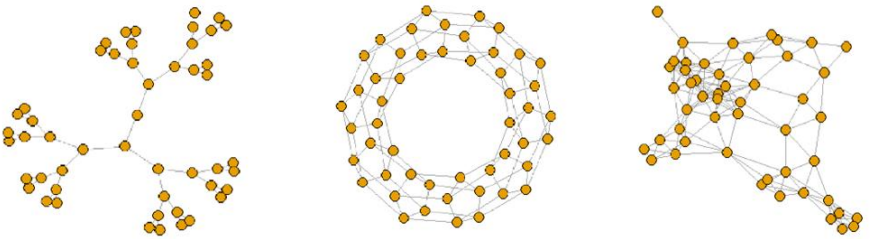

**Рис. 1: Три схемы сетей «большого мира».**

Это высоко децентрализованные системы с плотной локальной связанностью; для передачи информации в системе требуется много шагов, что ведёт к увеличению средней длины пути.

этой причине большой мир может поддерживать лишь ограниченное общение, бóльшая часть которого остается локальной, а изменения ограничиваются пределами сообщества, где они возникают; системных изменений мало, и происходящее незначительно. Ранние сообщества представляли собой компактные группы с небольшим количеством пересекающихся взаимодействий или связей и ограниченным техническим или общественным прогрессом. Очевидно, что децентрализация – недостаточное предварительное условие для решения фундаментальных задач социальной координации.

Грановеттер [11] показал важность «слабых» связей благодаря их встроенности в социальные сети, а Уоттс и Штрогац [12] решили головоломку преодоления ограничений локальной кластеризации для распространения информации по более широкой сети. Их концептуальный прорыв — создание кольцевой модели — показывает, что сеть большого мира может отображать как многочисленные локальные кластеры, что они называют *высоким коэффициентом кластеризации*, так и короткие средние длины пути между кластерами — и, таким образом, трансформироваться в сеть маленького мира. Они сделали это, добавив несколько случайных длинных связей, чтобы замкнуть круг.[13] Нужно всего нескольких таких мостов между боль-

[11] Mark S. Granovetter, “The Strength of Weak Ties,” *American Journal of Sociology* 78, no. 6 (1973): 1360-80, www.jstor.org/stable/2776392.

[12] Duncan J. Watts and Steven H. Strogatz, “Collective Dynamics of ‘Small-World’ Networks,” *Nature* 393 (6684) (1998): 440-42, https://doi.org/10.1038/30918.

[13] Идея «шести степеней разделения», увековеченная на Бродвее в 1990-х гг. — это явление маленького мира, обычное для социальных сетей. Задолго до того, как эта идея стала популярна, Траверс и Милгрэм показали, что современную инфраструктуру связей можно смоделировать как «маленький мир» (Jeffrey Travers and Stanley Milgram, “An Experimental Study of the Small World Problem,” *Sociometry* 32, no. 4 (December 1969): 425-43). Это модель технологии первого мира. Система связи волнует нас больше, чем электричество или пароходы.

шими кластерами, чтобы упростить поток информации и передать её из любой части сети в другие части.[14,15] Введение длинных путей в отдельные кластеры или сообщества может резко снизить «степень разделения» населения и тем самым увеличить скорость распространения информации в более широкой сети.[16]

Когда даже несколько центров могут выступать в качестве мостовых узлов, длинные связи, которые они обеспечивают, сокращают среднюю длину пути, так что информация может «срезать» дистанцию и быстро распространяться. Большой мир становится маленьким, когда любой узел может связаться с другими узлами через связи и промежуточные узлы. Мосты, сокращающие среднюю длину пути, позволяют формироваться маленьким

---

[14] Albert-László Barabási, *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life* (New York: Penguin Group, 2003); Duncan J. Watts, "The 'New' Science of Networks," *Annual Review of Sociology* 30 (2004): 243-70, https://doi.org/10.1146/annurev.soc.30.020404.104342.

[15] Сентола и Мэйси моделируют генеративные механизмы распространения сложных инфекций в сложных социальных топологиях (Damon Centola and Michael Macy, "Complex Contagions and the Weakness of Long Ties," *American Journal of Sociology* 113, no. 3 (November 2007): 702-34, https://doi.org/10.1086/521848). Связанные работы в области информатики (Jon M. Kleinberg, "Navigation in a Small World," *Nature* 406, no. 6798 (2000): 845, https://doi.org/10.1038/35022643), эпидемиологии (M. J. Keeling, "The Effects of Local Spatial Structure on Epidemiological Invasions," *Proceedings of the Royal Society B Biological Sciences* 266, no. 1421 (1999): 859-867, https://doi.org/10.1098/rspb.1999.0716); физики (Mark E.J. Newman, S.H. Strogatz, and Duncan J. Watts, "Random Graphs with Arbitrary Degree Distributions and Their Applications," *Physical Review E* 64 (2001): 026118, https://doi.org/10.1103/PhysRevE.64.026118) показывают, как случайно расположенные дальние связи могут влиять на процессы распространения в обществе. Свойства структуры влияют на коммуникацию, как показали Альберт, Чонг и Барабаши (Réka Albert, Hawoong Jeong, and Albert-László Barabási, "Internet: Diameter of the World-Wide Web," *Nature* 401, no. 6749 (1999): 130-31) и Доддс, Мухамад и Уоттс (Peter Sheridan Dodds, Roby Muhamad, and Duncan J. Watts, "An Experimental Study of Search in Global Social Networks," *Science* 301 (5634) (September 2003): 827-29, https://doi.org/10.1126/science.1081058). Динамику влияния виртуальных сетей раскрыли Бэкстром с коллегами (Lars Backstrom et al., "Group Formation in Large Social Networks: Membership, Growth, and Evolution," in *KDD'06: Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, August 20-23, 2006, Philadelphia, Pennsylvania, USA, https://www.cs.cornell.edu/~lars/kdd06-comm.pdf, 44-54) и Сентола (Damon Centola, "The Spread of Behavior in an Online Social Network Experiment," *Science* 329 (5996) (2010): 1194-97, https://doi.org/10.1126/science.1185231; Damon Centola, "An Experimental Study of Homophily in the Adoption of Health Behavior," *Science* 334 (6060) (2011): 1269-72, https://doi.org/10.1126/science.1207055). Расстояние между узлами сравнивают с размером сети Митлтон-Келли, Параскевас и Дэй (Eve Mitleton-Kelly, Alexandros Paraskevas, and Christopher Day, eds., *Handbook of Research Methods in Complexity Science* (London: Edward Elgar, 2018), https://www.e-elgar.com/shop/usd/handbook-of-research-methods-in-complexity-science-9781785364419.html, 413).

[16] Centola and Macy, "Complex Contagions and the Weakness of Long Ties."

мирам. Важность такой связанности маленьких миров в социальную организацию и возникновение системы объясняется её способностью передавать информацию при минимуме необходимых для этого связей. Чем больше *длинных* связей, тем больше инноваций можно передать по общей сети. В этом смысле государства, нации и цивилизации — это разные воплощения сети с топологией «маленького мира».

Исторические модели связанности часто образуют макроскопические модели непреднамеренного порядка, логика которых лежит за пределами намерений и предвидения отдельных агентов. Хотя действия человека целенаправленны, и люди не создают социальные связи случайно, действия масс людей могут создавать целостные структуры, позволяющие достичь важных целей, не будучи предназначенными для этого.

## Системная структура социальных отношений в Европе и Китае

Уоттс и Штрогац [17] показывают, что кольцевая сеть превращается из сети большого мира в сеть маленького мира при добавлении нескольких случайных связей к обычной сети. Ключом к использованию их анализа для понимания развития режима является определение ключевых мостовых узлов, или перемычек, а также их сути, конкретных форм, которые они могут принимать, и механизмов, объясняющих их развитие.[18] При прошлых режимах Китая и Европы королевские дома, защищенные общепринятыми обычаями и правилами, были главными «мостами» системы. Я рисую сетевую структуру европейской иерархии и, проводя исторические аналогии, сравниваю её с китайской.

На Рис. 2.1 схематично показаны европейские династические браки в XIV-XX вв. Сеть имеет смешанные черты маленького мира и безмасштабной сети. У неё выражено асимметричное распределение степеней с несколькими крупными центрами, преобладающее в безмасштабных моделях, хотя это и не идеальное распределение степеней (рис. 2.2). Она также демонстрирует характеристики маленького мира, поскольку средняя длина кратчайшего пути сравнима со случайной сетью, но с гораздо более высоким коэффициентом кластеризации. В сети каналы связи с более крупными узлами или центрами сильно перекошены: несколько центров с сильными связями связывают меньшие узлы друг с другом. Выявление этих важных свойств сети показывает, почему описание Европы исключительно с точки зрения децентрализации не учитывает модели коммуникации между центрами, которые обеспечивают

[17] Watts and Strogatz, “Collective Dynamics of ‘Small-World’ Networks.”

[18] Peter Hedström and Richard Swedberg, eds., *Social Mechanisms: An Analytical Approach to Social Theory* (Cambridge University Press, 1998), https://doi.org/10.1017/CBO9780511663901; Peter Hedström, *Dissecting the Social: On the Principles of Analytical Sociology* (Cambridge University Press, 2005), https://doi.org/10.1017/CBO9780511488801.

горизонтальную передачу данных в сети. Мы постарались визуализировать, как связанность периферийных узлов с центральными узлами соответствует дискретным моделям, которые обеспечивают единство всей сети.

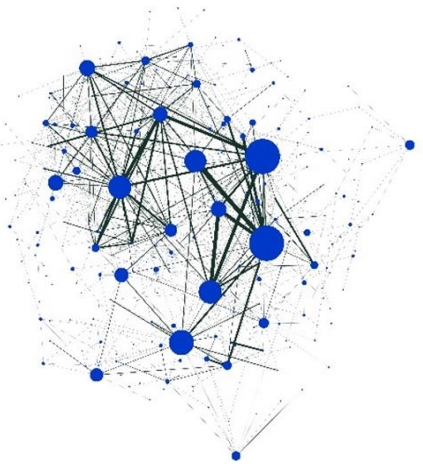

**Рис. 2.1: Схема династических браков королевских домов Европы XIV-XX вв.**

Линия возникает при заключении брака между двумя королевскими домами. Толщина линий соответствует количеству браков между двумя королевскими домами (от 1 до 92). Размер узла представляет его важность – количество домов, с которыми он имеет брачные отношения (от 0 до 41). Сеть включает 239 узлов и 622 линий, исключая самозацикливание (браки между членами одного дома). Узлы также включают дворянство, пап, епископов и курфюрстов. Епископы и папы должны были соблюдать целибат, но у некоторых были дети специально для создания союзов, и они учтены здесь. Брачная сеть напоминает сеть маленького мира. При помощи Python были сгенерированы 100 случайных сетей с одинаковым количеством узлов и линий, а также рассчитан коэффициент кластеризации и средний кратчайший путь для каждой моделируемой сети. Европейская сеть имеет среднюю длину кратчайшего пути 3,3857, что сравнимо с длиной в случайной сети – 3,4844, но с гораздо более высоким коэффициентом кластеризации – 0,2010, по сравнению с 0,0218 в случайной сети.

### *Мотивы, влияющие на формирование связей в сетях династических браков*

Разбросанные по всей Западной Европе многочисленные королевские дома континента выстраивали макросвязи в полицентричном институциональном контексте, опираясь на силу убеждения и создание альянсов для решения задачи коллективных действий.[19] Такого рода *распределённая сеть* приобретает стабильность за счёт добавления новых узлов. Некоторые узлы останутся случайными, так сказать, «одинокими форпостами». Некоторые из них сами станут центрами, привлекающими многочисленные связи

[19] Elinor Ostrom, *Understanding Institutional Diversity* (Princeton University Press, 2005).

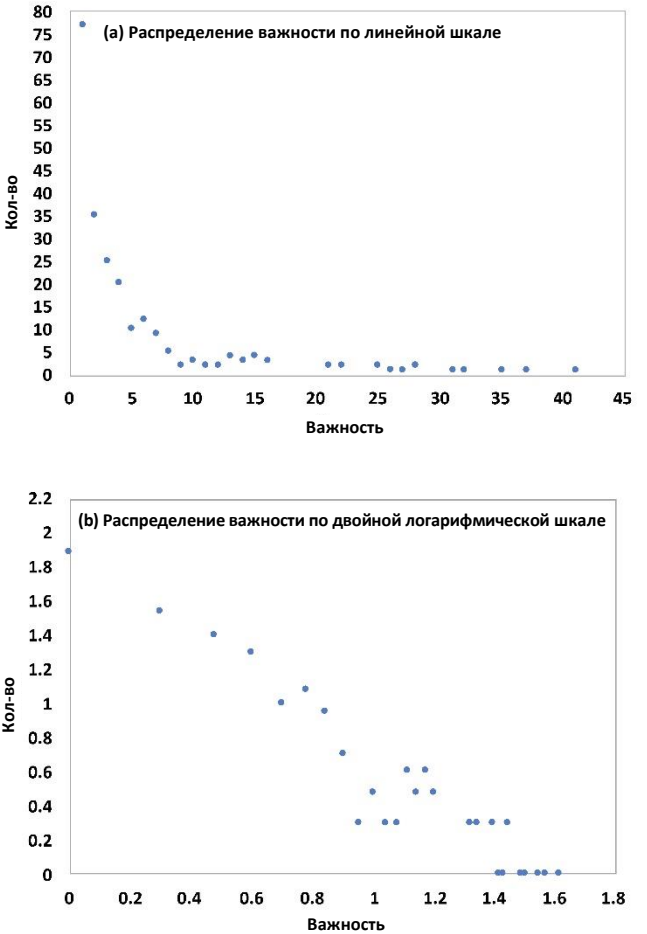


**Рис. 2.2: Распределение важности на схеме династических браков королевских домов Европы (a) по линейной шкале, и (b) по двойной логарифмической шкале**

Схема династических браков в определённой степени напоминает безмасшабную сеть. Строго говоря, ожидается, что безмасштабная сеть будет иметь явно асимметричное распределение степеней с длинным хвостом, согласно распределению по степенной зависимости, которое должно быть линейным, по двойной логарифмической шкале.

в системе и играющими решающую роль в её устойчивости. Центры постоянно меняют свою относительную значимость в системе, и по мере того, как каждый ищет преимущества за счёт привлечения новых узлов, динамизм на системном уровне усиливается. Для процветания королевский род должен научиться использовать местную кластеризацию в своих интересах. Короли

должны уметь собрать лоскутки из нескольких юрисдикций, с обязательством защищать от покушений их административные, финансовые, юридические и языковые свободы. Этот способ привлечения потенциальных союзников обеспечивал дополнительную связанность и разнообразие местных экономических условий. На протяжении всей истории Средневековья и начала Нового времени в Европе этот процесс работал, формируя политические границы и культурную идентичность. Побочным результатом было то, что когда один связанный кластер боролся за доминирование над другим, инновации процветали; без связанности не было бы такого динамизма внутри системы.

Когда центры и возникшие в них узлы, т.е. сообщества со схожими интересами или функциями, образуют подсистемы без размывания базовой структуры, это может привести к совместным эволюционным изменениям. В Европе сети, объединяющие политически и культурно разрозненные регионы, развивались, давая возможность для распространения научных, культурных и технологических инноваций по всему континенту. Периодические эпизодические изменения фундаментально не меняли ключевых свойств сети межнациональных королевских домов, а долговечность сети обеспечила возможность экономических и правовых изменений в общеевропейском контексте.

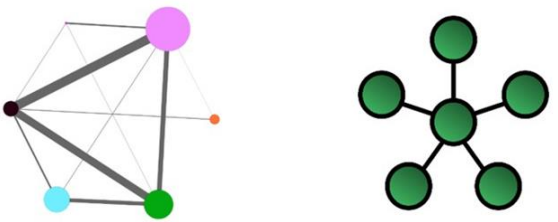


**Рис. 2.3: Разная структура связанности ядра и периферии в европейских и китайских монархических сетях.**
Западная Европа (a) развилась в распределённую сеть, в которой некоторые узлы стали центрами, привлекая больше связей и упрощая отношения между кластерами власти. Размер узла означает центральность по посредничеству, то есть то, как часто данный узел оказывается на кратчайшем пути между двумя любыми другими узлами. Толщина линии пропорциональна количеству браков между двумя домами. Сетевая структура Китая (b) подобна звезде, в центре которой император и двор решают, делиться или нет информацией, поступающей от других центров. Структура «ядро-периферия» более подробно рассмотрена в тексте через исторические аналогии, сравнивая приведенную выше идеальную модель с наблюдениями за поведением сети на основе исторических источников.

В Китае император был главным центром *радиальной сети*, и он один был связан со всеми прочими узлами. Его власть была результатом завоеваний, а не союзов, что давало ему большую свободу управления дальней-

шими процессами развития сети благодаря такой лучевой связанности с периферией.[20] Трон опирался на государственную систему конфуцианского чиновничества – мандаринов, которых набирали на государственную службу на основе системы экзаменов, и производил важные официальные назначения, управлял общесистемной обратной связью и передавал информацию из одной точки в другую по обширной империи. Такая сетевая структура снижает избыточность и бережёт ресурсы. Таким образом, центральный узел может направлять рост сети в соответствии с принципами, усиливающими его контроль над узлами. Такое эффективное распределение сверху вниз позволяет быстро распространять нужные инновации. Стабильность системы зависит от способности императорского двора решать общенациональные задачи государственного управления, защищать своё верховенствующее положение по отношению к местному руководству, сдерживать формирование конкурирующих элит, способных бросить вызов центру, и устанавливать границы режима.

Династия за династией, китайские монархи полагались на одну и ту же систему набора, идеологической обработки и экзаменов как средство контроля над распространением идей и сохранения власти.[21] Когда династия рушилась из-за войны или внутренней коррупции, новая династия восстанавливала экзаменационную систему, чтобы тоже иметь источники информации, охватывающие всю империю. Сетевой подход помогает понять, как эта система государственной службы укрепляла стабильность имперского правления. Знание топологии маленького мира, а также взаимного влияния и совместной эволюции индивидуальных действий и сетевой структуры поможет нам понять, как исторические институты сплетаются в структуру, и найти ключ к разгадке их эволюции.[22]

---

[20] В определённые периоды политическое единство Китая переживало проблемы, аналогичные европейским. Как королевской власти в Европе приходилось бороться с устремлениями региональных элит, так и китайская элита исповедовала взгляды на централизацию, противоречившие взглядам имперских управленцев. Как отмечает экономический историк Эрик Джонс, это особенно касается IX-XIII вв., когда инновации в Китае процветали благодаря социально-политическому сходству с Европой. Джонс объясняет этот расцвет конкуренцией множества источников институциональной легитимности, которые в конечном итоге были устранены в процессе объединения империи (Eric L. Jones, *The European Miracle: Environments, Economies and Geopolitics in the History of Europe and Asia* (Cambridge, UK: Cambridge University Press, 1981).

[21] Frederic Wakeman Jr., *The Great Enterprise: The Manchu Reconstruction of Imperial Order in Seventeenth-Century China*, Vol. 1 (Berkeley, CA: University of California Press, 1986).

[22] Индивидуальные действия и сетевая структура развивались совместно в динамическом процессе взаимного влияния – см. Stefano Tasselli, Martin Kilduff, and Jochen I. Menges, “The Microfoundations of Organizational Social Networks: A Review and an Agenda for Future Research,” *Journal of Management* 41, no. 5 (2015): 1361-87, https://doi.org/10.1177/0149206315573996.

## Общие институты в Китае и на Западе: наследственная преемственность и первородство

Стоит отметить, что в радиальной китайской и в более распределенной европейской сетевой структуре возникла институциональная общность: наследственное управление. В обоих регионах монархи получили право передавать свой статус и привилегии своим детям, обычно через первородство. Это отличает обе системы от других известных исторических метарежимов, таких, как империи Рима, Османов или Великих Моголов, которые не смогли установить правила династической преемственности.[23] Там, где не был решён вопрос престолонаследия, споры между дальними родственниками с большей вероятностью заканчивались конфликтом: либо гражданской войной, либо вмешательством соперничающей державы. Так, в Риме наследники мужского пола в целом имели право на наследование, но императоры обычно выбирали преемника, чаще – члена семьи, иногда приёмного наследника, причём было важно символическое согласие Сената и генералов. Ни император, ни его наследник не получали неотъемлемого «права» на управление, что оставляло возможности для оспаривания.[24]

В Европе многочисленные *не королевские* общественные сети тоже основывались на наследственных привилегиях. В Китае правящую элиту отбирали по системе набора, основанной на индивидуальных достижениях, и как следствие, она больше способствовала социальной мобильности. Такое продвижение бюрократии, основанной на достижениях, может показаться странным, если учесть, что Европа пришла к демократии раньше. Но ирония рассеивается, если мы примем во внимание исследования Дэвидом Биеном старого режима Франции,[25] в которых он обнаружил, что демократия сначала развивалась внутри привилегированных слоев общества, а затем охватывала более широкие слои.[26] Согласно рассуждениям Биена, анализ показывает, что демократический плюрализм зародился в европейской

---

[23] Хотя имперское правление в Китае насчитывает 4000 лет, внутренняя узурпация успешно закончилась после династии Сун (960-1279). С этого момента соблюдались чёткие правила династической преемственности, и династии обычно сменялись в результате внешних завоеваний.

[24] Keith Hopkins, “The Political Economy of the Roman Empire,” in *The Dynamics of Ancient Empires: State Power from Assyria to Byzantium*, ed. Ian Morris and Walter Scheidel Morris (Oxford: Oxford University Press, 2009), 178-204.

[25] Rafe Blaufarb, Michael S. Christofferson, and Darrin M. McMahon, eds., *Interpreting the Ancien Régime: David Bien* (Oxford: Voltaire Foundation, 2014).

[26] Привилегии нобилитета и модернизация государства часто шли рука об руку (David Bien, “Offices, Corps, and a System of State Credit: The Uses of Privilege under the Ancient Regime,” in *The French Revolution and the Creation of Modern Political Culture: The Political Culture of the Old Regime*, Vol. 1, ed. Keith Michael Baker et al. (Oxford: Pergamon Press, 1987), 89-115). Биен утверждает, что борьба за демократию и участие в управлении происходит внутри государственных институтов, а не только между государством и обществом. См. также Blaufarb, Christofferson, and McMahon, eds., *Interpreting the Ancien Régime*.

аристократии и затем распространился на другие системы внутри более крупного децентрализованного целого. Он возник в результате взаимодействия многих конкурирующих монархий и их связей с подсистемой относительно автономных вассальных аристократов, каждый из которых стремился к той или иной форме коллективного представительства в решениях, затрагивающих всех.

И в Китае, и в Западной Европе преемственность власти обычно осуществлялась через первородство по мужской, или отцовской линии. В Европе первородство стабилизировало феодальную систему и способствовало её распространению в XI веке из государств бывшей империи Каролингов, а затем на восток, в XII и XIII вв.[27] Ограждая поместья феодалов от раздробления, система первородства укрепляла их способность выполнить военный долг перед королём. Но эта геополитическая безопасность достигалась ценой увековечения богатства, власти и социального положения благородных родов.[28] Оно также поставило развитие и мощь государства в зависимость от сотрудничества благородных семей, что позволило зафиксировать их права в конституционных соглашениях, ограничивших рамки королевской власти. Демократия возникла из этих договоров между элитами и правителями. В Китае такие семьи чаще рассматривались как потенциальная угроза конкретной императорской линии. Не существовало формальных консультативных процедур, несмотря на трактаты по морали и этике, такие, как «Наследственные предписания» (1375 г.) при династии Мин, но это были не конституции.[29]

---

[27] В средневековье первородство приняли бывшие регионы Каролингской империи, включая Арагон, Австрию, Баварию, Миланское Герцогство, Флоренцию, Францию, Наварру и Пруссию.

[28] Западная церковь также признавала не королевское первородство, тем самым укрепляя элитные родословные. Адам Смит поясняет политэкономическую логику первородства в «Исследовании о природе и причинах богатства народов»: «Когда землю стали считать не только источником существования, но и источником власти и влияния, было признано лучшим передавать её неразделённой одному из детей. В те смутные времена каждый крупный землевладелец был своего рода небольшим государем. Держатели его земли были вместе с тем его подданными. Он был их судьей и в некоторых отношениях был для них законодателем в мирное время и вождем во время войны. Он вел войну, когда считал это нужным, часто против своих соседей, а иногда и против своего государя. Поэтому безопасность поместья, защита, которую его владелец мог оказывать тем, кто жил в нем, зависели от размеров владения. Дробить его значило вести к его разорению и подвергать все части его опасности угнетения и поглощения при набегах соседей». (Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, ed. Edwin Cannan (London: Methuen & Co., 1904), 306).

[29] Определение чётких линий династической преемственности стало важным элементом формирования прочных режимов и, следовательно, усложнения общества. Согласно Кокконену и Санделлу, первородство стабильнее альтернативных механизмов преемственности в некоторых современных авторитарных режимах (Andrej Kokkonen and Anders Sundell, “Delivering Stability – Primogeniture and Autocratic Survival in European Monarchies 1000-1800,” *American Political Science Review*

Тем не менее наследственное правление не устранило все споры о преемственности феодальных правителей Европы. Церковь имела собственные правила и не терпела разводов, сожительства и признания внебрачных потомков. Это делало королевские роды уязвимыми при отсутствии наследника мужского пола, создавая новую категорию разногласий (наследники по женской линии с конкурирующими претензиями), что часто вызывало споры о наследовании и войны.[30]

Тем не менее, по причинам, которые мы намерены рассмотреть, европейские конфликты за престолонаследие в целом локализовывались без угрозы стабильности системы смешанных королевских родословных, пронизывавшей весь континент.[31] Во многих случаях споры заканчивались союзами между родами, соперничавшими на незанятый трон. Даже когда неспособность произвести наследника приводила к исчезновению всей линии, связи между оставшимися королевскими домами просто менялись, обеспечивая непрерывность системы на макроуровне.

В Китае императорская династия обычно рушилась не из-за отсутствия наследника по мужской линии. Императоры могли иметь огромный гарем для производства преемников мужского пола. Внебрачное сожительство укрепляло промежуточную стойкость режима, снижая угрозу кризиса престолонаследия.[32] Так называемый «династический цикл» чаще всего возобновлялся, когда военная победа сметала одну династическую линию и

---

108, no. 2 (April 2014): 438-53, http://dx.doi.org/10.1017/s000305541400015x). Введение наследственной преемственности при автократии ограничивает попытки переворота со стороны претендентов. См. Peter Kurrild-Klitgaard, "Autocratic Succession," in *The Encyclopedia of Public Choice* (Boston, MA: Springer, 2004), 358-62, https://doi.org/10.1007/978-0-306-47828-4_39.

[30] Плавная смена власти уменьшает конфликты, ставящие под угрозу существующий институциональный и социальный баланс и угрожающие экономическому развитию. См. Avidit Acharya and Alexander Lee, "Path Dependence in European Development: Medieval Politics, Conflict, and State Building," *Comparative Political Studies* 52, no. 13-14 (2019): 2171-2206, https://doi.org/10.1177/0010414019830716. Нормандское королевство в Италии пришло в упадок из-за неспособности производить наследников мужского пола. Столетнюю войну (1337–1453) Англии и Франции спровоцировал спор о женском наследовании. Большинство конфликтов о престолонаследии, как правило, были кратковременными, вплоть до Религиозных войн (1562–1598 гг.), которые раскололи Церковь и подняли ставки в борьбе за престол, добавив ещё один фактор стремления к власти, поскольку они дали королевской семье больше контроля над назначением епископов в своей юрисдикции, а также больше влияния на конфессиональные вопросы.

[31] Королевские семьи, связанные живыми узами, были менее склонны вести войны. См. Seth G. Benzell and Kevin Cooke, "A Network of Thrones: Kinship and Conflict in Europe, 1495-1918," *American Economic Journal: Applied Economics* 13, no. 3 (July 2021): 102-33, https://doi.org/10.1257/app.20180521.

[32] Китайские правители были более живучими, чем европейские, обеспечивая стабильность и процветание на большой территории. См. Yuhua Wang, "Sons and Lovers: Political Stability in China and Europe before the Great Divergence," *SSRN Electronic Journal* (October 2018), http://dx.doi.org/10.2139/ssrn.3058065.

начинала другую после восстания или завоевания. А поскольку периферические узлы соединялись главным образом через центр, они тоже рушились, что делало последствия гораздо более разрушительными и масштабными.[33] Тут важны два момента: Кризисы династической преемственности в Китае были менее частыми, что обеспечивало стабильность и процветание на большой территории более длительное время. С другой стороны, конфликты за престолонаследие в Европе случались чаще, но были локальней и оказывали менее драматичное влияние на стабильность режима и на демографические и экономические тенденции на континенте. Я вернусь к долгосрочному динамическому эффекту этого свойства сети в разделе 5.

## Западная церковь, конфуцианская этика и сетевая динамика социальных изменений

Этот раздел посвящен мостовым узлам, которые ускоряют распространение убеждений и моделей поведения, формирующих представления об общей идентичности и общей судьбе. Хотя религия играла важную роль в сохранении системы и расширении границ как в Китае, так и в Европе, уменьшая разделение между социально, географически и культурно удаленными группами, она также была источником разных представлений о политическом и социальном порядке, которые должны были давать плоды на протяжении столетий. Что касается сетевой структуры в Европе, религия, т.е. Римско-католическая церковь, получила институциональную точку опоры в качестве независимого центра распределённой сети континента. Он развивался одновременно с другими узлами, также демонстрируя весьма асимметричное распределение степеней, подобно взаимосвязанным королевским семьям, и в конечном итоге стал мощной силой, с которой приходилось считаться даже самым могущественным. Широкие права и полномочия Церкви простирались от самых высоких центров власти, где священники были исповедниками королевской семьи, до местных приходов, где деревенские монахи смешивались с крестьянством. С раннего Средневековья легитимация династического господства по божественному праву требовала от королей святого помазания, и Римско-католическая церковь стала играть важную роль в эволюции европейской государственной системы.[34]

[33] Albert-László Barabási, Réka Albert, and Hawoong Jeong, “Scale-Free Characteristics of Random Networks: The Topology of the World-Wide Web,” *Physica A: Statistical Mechanics and Its Applications* 281, no. 1-4 (2000): 69-77, https://doi.org/10.1016/S0378-4371(00)00018-2.

[34] Когда папа Лев III короновал Карла Великого императором Римской империи в 800 г., он создал на Западе прецедент, согласно которому император должен быть помазан папой, а все короли — представителями папы, архиепископами. Несколько столетий спустя коронация Вильгельма во время норманнского завоевания Англии стала примечательным, но редким примером признания Церковью

Хотя симбиоз был выгоден и религиозному, и светскому руководству, каждая сторона постоянно стремилась одержать верх над другой. Со сменой условий их взаимоотношения поддерживались общей заинтересованностью в том, чтобы обеспечить единство всего населения на основе общей веры, и желанием каждой линии избежать сжатия в сеть, в которой доминирует одна линия. Таким образом, и светские, и духовные государственные деятели приняли и извлекли выгоду из симбиоза в долгосрочных отношениях.

Западная церковь как институт пользовалась относительной автономией при назначении чиновников и управлении своими судами и приходами в соответствии с её собственными процедурами. В период Классического средневековья (1000–1250 гг.) «светская власть могла черпать свою власть от Бога, но только в подчинении власти духовенства, воплощенной в её главе, Папе, преемнике Св. Петра».[35] Светские правители были вассалами Бога, осуществлявшими свою власть как слуги Церкви под эгидой Папы, как наместника Бога. А раз целью христианской жизни является спасение, *духовенство* было выше светских правителей.

В религиозной истории Китая мы не найдём эквивалента Римской церкви, с её независимой иерархией и источниками легитимности. Один лишь император был воплощением Небесной воли; его полномочия нисходили прямо с Небес. Для занятия этого поста никогда не требовалось божественного благословения (помазания) независимого религиозного органа. Религиозная практика, как и всё в Китае, была подчинена государственной власти. Даже обряды вступления на престол, освящавшие должность императора, проводились в соответствии с правительственными постановлениями и несли ключевые элементы государственной идеологии.

Один из примеров такого подчинения возник при династии Хань (206–220), когда было создано Министерство церемоний, одно из девяти министерств Империи. Оно отвечало за проведение церемоний, а также за охрану священной горы Тай, считавшейся святым местом на протяжении трёх тысяч лет. Императоры Мин и Цин поклонялись Небу и Земле в Храме Неба недалеко от Запретного города. Министерство церемоний, по сути, связывало императора с природным и божественным мирами. Оно также осуществляло надзор за образованием, что в конечном счёте включало экзамены для государственной службы. Мандарины императорского двора, получившие классическое конфуцианское образование, в одиночку производили все важные назначения чиновников и устанавливали образовательные стандарты для имперского университета, включая назначение учёных, толковавших конфуцианские каноны.

---

новой королевской линии. Трудность получения согласия Церкви отпугивала некоролевских претендентов и особенно усложняла претензии на европейский трон для нехристиан.

[35] Henry Orton Wiley, *Christian Theology*, Vol. 3 (Kansas City, MO: Beacon Hill Press, 1951), 941.

Это подчинение укрепил философский поворот в истории китайской культуры, который произошел очень рано, в IV в. до нашей эры, с подъёмом и упадком моизма – философии, основанной на учении философа Мо Ди (или Мо-цзы, ок. 470 – ок. 391 до н.э.). Моизм возник в то же время и в том же месте, что и его главный соперник – конфуцианство, в раздираемую войнами эпоху Сотни школ мысли. Идея равной и беспристрастной заботы обо всех, вопреки чрезмерной привязанности к семье и клану, могла побудить людей создавать социальные структуры вне своего рода. Догмы Конфуция возобладали, и конфуцианская модель национального сообщества на основе сыновней почтительности воплотилась в верность императору и придала трону легитимность.

Прежде чем конфуцианская мысль распространилась по всей империи, основой социального порядка были поклонение предкам и род, но им не хватало чёткой идеологии. Конфуцианская доктрина дополнила широко распространённые клановые культурные нормы, укоренившиеся в древнем Китае. Поскольку у конфуцианства не было собственных формальных институтов, оно легко подчинялось государству, обеспечивая социальную и моральную основу, делавшую его привлекательным для императора.[36]

## Развитие сети, инновации и долговечность режима

Несмотря на такие свойства маленького мира, как высокая локальная связанность и относительно короткая средняя длина пути, общие для Китая и для Европы, различия в организационной структуре (топологии) сформировали соответствующие культуры инноваций, что привело к расходящимся экономическим траекториям.

Западная сеть маленького мира, включавшая множество центров с крайне неравномерным распределением степеней, давала европейским монархам ограниченные возможности сдержать распространение инноваций, угрожавших их власти, или контролировать системы производства, что дало бы им контроль над экономикой. Но она обеспечивала максимальную живучесть в условиях повторяющихся революций и социальных движений, опирающихся на предыдущие достижения, создавая что-то новое, иное, но сохраняя при этом контекст общей европейской традиции.[37]

Способность иерархических связей, убеждений и институтов содействовать адаптации центров к быстрым изменениям на более низких уровнях, не затрагивая общую топологию, повышала устойчивость системы. Понимание этой устойчивости говорит нам об ускоренной идеологической адаптации и распространении технологий в ходе таких движений на континенте,

---

[36] Zhuo Xinping, “Spiritual Accomplishment in Confucianism and Spiritual Transcendence in Christianity,” In *Confucianism and Spiritual Traditions in Modern China and Beyond*, Vol. 3, ed. Fenggang Yang and Joseph Tamney (Leiden and Boston: Brill, 2011), 280-81.

[37] Harold J. Berman, *Law and Revolution: The Formation of the Western Legal Tradition* (Cambridge, MA: Harvard University Press, 1983), 19.

как Возрождение, Реформация, Просвещение и индустриализация. Каждое из них зарождалось в одной части Европы, устраняя на своем пути некоторые узлы, но уцелевшие центры смогли самоорганизоваться в новые структуры. Как следствие, Европа успешнее, чем Китай, использовала движущие силы инноваций; её взаимосвязанные правящие элиты смогли пережить волны культурных, организационных и технологических изменений, а социальное развитие вышло далеко за пределы начала раннего средневековья, несмотря на разрушения, вызванные новыми общественными силами.

В имперском Китае, где связанность всей системы исходила из центра, потенциальные новые центры не поощрялись. Торговые гильдии, благотворительные общества и другие гражданские структуры местного уровня тоже редко получали институциональную автономию, поскольку новые связи ослабляли центральный контроль. Наряду с ограничениями внутренней мобильности посредством регистрации семей в древней системе «хукоу», это давало центру широкие возможности определять, какие инновации нужно поддержать, а какие отфильтровать. Систему «хукоу», например, использовали для контроля внутренней миграции ещё в доимперский период. Её сложные механизмы использования коллективных уязвимостей способствовали интересам государства и его представителей, но ослабляли творческий потенциал для революционных инноваций. Значительный сдвиг в мировоззрении обычно происходил по требованию имперской власти, часто – в связи со сменой династии, а не в результате самоорганизации или взаимодействия.

Императорский двор полностью контролировал мандаринов благодаря классической учебной программе, по которой кандидатов обучали с раннего возраста, системе экзаменов, которые они сдавали, и регионам, куда их направляли. Распределение сети укрепляло единство в Китае, но связанность всей сети зависела от долговечности центра. Когда рушился центр, рушились и остальные узлы системы, связанные только с ним. После краха каждой династии надо было возрождать бюрократию и восстанавливать общесистемные связи.

Но возрождение мандаринов при каждой династии — это ещё не вся история сохранения китайских культурных норм на протяжении тысячелетий. Местные сети, основанные на родственных и клановых связях, сыграли важную связующую роль в истории Китая. В следующем разделе мы рассмотрим, как эти сети стали возможными.

## Культурная диффузия и устойчивость

Используя науку о сетях как метод определения глобальных правил и механизмов изменений в социальной системе, я выявил глубинную динамику связанности маленького мира на макроуровне, которая воспроизводится в прошлых режимах Европы и Китая. Применение подхода «маленького

мира» провозгласил Грановеттер[38] и формализовали Уоттс и Штрогац,[39] а автор раскрыл основные схемы построения крупномасштабных сетей, но это не даёт исчерпывающего описания эволюции системы с течением времени. Не даёт это и эффективного объяснения культурной устойчивости. В этом разделе я сначала рассмотрю местные модели Европы, а затем покажу, что не учитывает подход «малого мира», при внимательном взгляде на Китай, и проанализирую, как его религиозные и гражданские институты связаны с глубокими структурными отличиями в организации его экономики.

Длина пути в крупномасштабной сети является ключом к пониманию динамики распространения информации и технологических изменений, т.е. с формированием центров и уменьшением длины пути внутри системы распространение усиливается. А как насчёт связанности на более низких уровнях, между локальными узлами? Там успешное распространение инновационного поведения требует поддержки множества источников, в том числе общественных групп, для чего нужны пересекающиеся связи, которые Дэймон Сентола назвал «расширителями мостов».[40] Людям пришлось немало поработать, чтобы создать эти устойчивые пути социальной координации в группах.[41] Их распространению способствовал религиозный идеал.

В Средние века Церковь как институт и система верований сыграла важную роль в укреплении новых, особых групп ради общего блага. Фюстель де Куланж в классической книге середины XIX в. «Древний город» показал, что христианство привнесло идею о том, что «это не домашняя религия какой-то семьи, не национальная религия какого-то города или какой-то расы. Оно не принадлежит ни касте, ни корпорации».[42] Идея всеобщей морали отличала управление средневековыми городами от управления в Древней Греции и Риме, где каждая семья и община поклонялись собственным богам. Это позволило добровольным объединениям развиваться и строить сети организованного сотрудничества, выходящие за рамки родства. Институциональные рамки и обычаи, вдохновлённые ими, поддержали экономические возможности в условиях децентрализации.

Будучи защитником норм, предписывающих справедливость по отношению к чужакам, церковная доктрина братской любви лежала в основе общего идеала городов как моральных сообществ. Она сформировала отношение к мигрантам и помогла городам справиться с миграцией, позволяя

---

38 Granovetter, “The Strength of Weak Ties.”

39 Watts and Strogatz, “Collective Dynamics of ‘Small-World’ Networks.”

40 Социальная диффузия в крупных, сложных обществах может зависеть от групп социальных «посредников», связывающих социально далёкие группы воедино. См. Damon Centola, *How Behavior Spreads: The Science of Complex Contagions* (Princeton: Princeton University Press, 2018), 34-62.

41 Centola, *How Behavior Spreads*, 133.

42 Numa Denis Fustel de Coulanges, *The Ancient City: A Study on the Religion, Laws and Institutions of Greece* (Garden City, N.Y.: Doubleday and Co., 1956), 391.

чужакам получить права.[43] Для развития добровольных объединений нужна общая мораль. Грайф и Табеллини предлагают объяснение роли христианского гуманизма в построении гражданского общества городов раннего средневековья.[44] Сети гильдий, монашеских орденов и других добровольных обществ, вдохновлявшиеся христианским гуманизмом, помогли ускорить распространение новых моделей поведения, особенно после массовой миграции и замещения населения после эпидемии чумы (1346–1348), и сделали города центрами инноваций.

Многочисленные добровольные общества и объединения по интересам, такие, как *Lex mercatoria*, создавшее собственную оргструктуру для устранения многих рисков, стали Сентоловыми «расширителями мостов». Предоставленные ими гарантии снизили риск обмена с чужаками, поэтому группы людей, ранее не поддерживавшие отношений, смогли объединить ресурсы и создать крупные частные фирмы и рынки.

Явно иную модель организации сотрудничества в Китае тоже можно отследить в давних исторических схемах. Их реляционная сеть появилась, а затем возобладала в торговле и решении местных проблем на протяжении всей истории, по сей день. В Китае не было религиозного института, способного побудить людей доверять социальным связям, выходящим за рамки прихода, семьи или деревни. Не было и института, действующего из одного центра, такого, как приход, и влияющего на повседневные потребности населения. Радиальная сетевая структура Китая, опиравшаяся на древнюю конфуцианскую мораль, не позволяла адекватно решать проблемы на местном уровне. Государственная бюрократия была слишком слаба, чтобы проникнуть в местное общество до уровня деревни, что делало государственных чиновников зависимыми от старейшин рода при выполнении указаний, требовавших поддержки на местах. Это приводило к негативным последствиям для функций управления, от сбора налогов до ирригации.[45]

Сотрудничество или помощь между людьми, семьями и группами, разделяющими общие интересы, при посредничестве гражданских организаций, редко поощрялись. При самостоятельных действиях общин по решению местных проблем участие основывалось на родстве, а не на общих интересах. В Китае развилась сеть отношений «гуаньси», прививша китайскому обществу замкнутую культуру малых групп, личного сотрудничества

---

[43] Miri Rubin, *Cities of Strangers: Making Lives in Medieval Europe* (Cambridge: Cambridge University Press, March 2020), https://doi.org/10.1017/9781108666510.

[44] Greif and Tabellini, “The Clan and the Corporation.”

[45] Joseph Esherick and Mary Backus Rankin, *Chinese Local Elites and Patterns of Dominance* (Berkeley: University of California Press, 1990), 3; James Kai-sing Kung, and Chicheng Ma, “Friends with Benefits: How Political Connections Help Sustain Private Enterprise Growth in China,” *Economica* 85, no. 337 (January 2018): 41-74, https://doi.org/10.1111/ecca.12212; Ting Chen, James Kai-Sing Kung, and Chicheng Ma, “Long Live Keju! The Persistent Effects of China’s Imperial Examination System,” *SSRN*, June 2017, http://dx.doi.org/10.2139/ssrn.2793790.

и обменов в небольших сообществах. Высокие моральные обязательства, прививаемые таким узким группам, редко распространяются на внешние отношения, например, с правительством, и вообще с чужаками.

Оценки управления на основе родства во всем мире и в современных условиях показали, что когда старейшины родов играли доминирующую роль в организации сообщества, это приводило к отторжению инноваций в поведении и культурной инерции. Кроме того, близость родства коррелирует с меньшим вниманием к общей морали и неблагосклонностью к тем, кто не входит в группу, зато укрепляет лояльность к членам семьи, даже когда они нарушают договор с обществом.[46] Сильная внутригрупповая лояльность и резкое различие между «своими» и «чужими» способствуют общему недоверию к чужакам, что снижает качество управления.[47]

Современные исследования Китая показывают, что кланы с общим происхождением по мужской линии и сегодня остаются главными социальными группами в китайских деревнях.[48] Сюй и Яо[49] пишут, что когда у власти находится один из двух главных семейных кланов деревни, государственные инвестиции там увеличиваются, но за это придётся заплатить; кланы

---

[46] Jonathan F. Schulz, Duman Bahrami-Rad, Jonathan P. Beauchamp, and Joseph Henrich, "The Church, Intensive Kinship, and Global Psychological Variation," *Science* 366, no. 6466 (2019): 5141, https://doi.org/10.1126/science.aau5141; Joseph Henrich, *The WEIRDest People in the World: How the West Became Psychologically Peculiar and Particularly Prosperous* (New York: Farrar, Straus and Giroux, 2020), 196.

[47] Jonathan F. Schulz, "Kin Networks and Institutional Development," *SSRN*, September 1, 2016, http://dx.doi.org/10.2139/ssrn.2877828; Mahsa Akbari, Duman Bahrami-Rad, and Erik Kimbrough, "Kinship, Fractionalization and Corruption," *Journal of Economic Behavior & Organization 166* (C) (2019): 493-528, https://doi.org/10.1016/j.jebo.2019.07.015.

[48] Hsiao-Tung Fei, "Peasantry and Gentry: An Interpretation of Chinese Social Structure and Its Changes," *American Journal of Sociology* 52, no. 1 (July 1946): 1-17, https://www.jstor.org/stable/i328827; Francis L. K. Hsu, *Under the Ancestors' Shadow: Chinese Culture and Personality* (New York: Columbia University Press, 1948); Maurice Freedman, *Lineage Organization in Southeastern China* (London: University of London and Athlone Press, 1958); Maurice Freedman, "Ancestor Worship: Two Aspects of the Chinese Case," in *Social Organization: Essays Presented to Raymond Firth*, ed. Maurice Freedman (Chicago, IL: Aldine, 1967); James J. Watson, "Chinese Kinship Reconsidered: Anthropological Perspectives on Historical Research," *The China Quarterly* 92 (December 1982): 589-622, https://doi.org/10.1017/S030574100 0000965; Prasenjit Duara, *Culture, Power, and the State: Rural North China, 1900-1942* (Stanford: Stanford University Press, 1988); Myron L. Cohen, "Lineage Organization in North China," *The Journal of Asian Studies* 49, no. 3 (1990): 509-34, https://doi.org/10.2307/2057769; Lily L. Tsai, "Solidary Groups, Informal Accountability, and Local Public Goods Provision in Rural China," *American Political Science Review* 101, no. 2 (May 2007): 355-72, https://doi.org/10.1017/S0003055407070153.

[49] Yiqing Xu and Yang Yao, "Informal Institutions, Collective Action, and Public Investment in Rural China," *American Political Science Review* 109, no. 2 (2015): 371-91, https://doi.org/10.1017/S0003055415000155.

набивают себе карманы, вступая в сговор с местной властью. Грайф и Табеллини [50] видят влияние клана не только в разрешении гражданских и коммерческих споров, но и в обеспечении благосостояния, охране прав собственности, защите местных жителей от злоупотреблений со стороны властей и даже в инвестициях в общественные проекты.[51] Сегодня частные фирмы – это в основном клановые предприятия, отмечает Чжан,[52] утверждающий, что «клановая культура» слабее в регионах с лучшими рыночными условиями. Пэн[53] отмечает сильную и важную корреляцию родства на уровне деревни с количеством частных предприятий, и Чжан, как и Пэн, предполагает, что эта связь помогла успеху рыночных реформ после 1979 г., дополняя слабые правовые институты. Фольц, Гуо и Яо[54] показывают, что родственные связи помогают увеличить миграцию и создание общественных благ в быстрорастущих новых районах. Хе, Пань и Саранги[55] пишут, что однородные по происхождению деревни более склонны взаимодействовать с членами своего рода и участвовать в производстве общественных благ, распределяемых в пределах рода, чем люди, живущие в деревнях, неоднородных по происхождению. Родовые группы в масштабах всей деревни в значительной степени коррелируют с обеспечением общественных благ и привлечением к ответственности государственных чиновников у Цай.[56] Организации, основанные на родстве, пережили реформы коммунистической революции. С 1949 по 1979 гг. кланы были официально распущены, их имущество конфисковано, правила признаны недействительными, а генеалогии сожжены. Но как только запреты сняли, их культурное

---

[50] Greif and Tabellini, “The Clan and the Corporation.”

[51] На основе China Social Survey, 2005 (Greif and Tabellini, “The Clan and the Corporation”) подсчитано, что «почти 70 % населения проживает в уезде с положительной выборочной вероятностью наличия в селе [клановой] организации, а в 41 % уездов вероятность наличия в селе клановой организации составляет не менее 50 %. Доля кланов, владевших общей собственностью, составляла от 21 % до 28 %». Их оценка роли кланов в истории Китая совпадает с этой: кланы формируют эволюцию китайской социальной организации и делают её культуру совершенно отличной от культуры западных стран.

[52] Chuanchuan Zhang, “Clans, Entrepreneurship, and Development of the Private Sector in China,” *Journal of Comparative Economics* 48, no. 1 (March 2020): 100-123, https://doi.org/10.1016/j.jce.2019.08.008.

[53] Yusheng Peng, “Kinship Networks and Entrepreneurs in China’s Transitional Economy,” *American Journal of Sociology* 109, no. 5 (March 2004): 1045-74, https://www.journals.uchicago.edu/doi/10.1086/382347.

[54] Jeremy Foltz, Yunnan Guo, and Yang Yao, “Lineage Networks, Urban Migration and Income Inequality: Evidence from Rural China,” *Journal of Comparative Economics* 48, no. 2 (June 2020): 465-82, https://doi.org/10.1016/j.jce.2020.03.003.

[55] Quqiong He, Ying Pan, and Sudipta Sarangi, “Lineage-Based Heterogeneity and Cooperative Behavior in Rural China,” *Journal of Comparative Economics* 46, no. 1 (March 2018): 248-69, https://doi.org/10.1016/j.jce.2017.10.006.

[56] Tsai, “Solidary Groups, Informal Accountability, and Local Public Goods Provision in Rural China.”

влияние на социальные нормы населения вновь проявилось. В целом, недавние исследования показывают, что опора на неформальные институты родовых групп решает проблемы коллективных действий, способствуя мобилизации местных ресурсов и обеспечению общественных благ на местах – но с риском сговора и слабым влиянием на подотчётность местных властей. Это повторяет модели старых времен.

Всемирный индекс благотворительности (CAF) Фонда благотворительной помощи [57] оценил Китай ниже всех из 128 стран по готовности помогать чужакам, жертвовать деньги и уделять время. В отчёте CAF отмечается, что принятие официальных решений происходит без заметного участия местных сообществ. Организации гражданского общества строго контролируют, им не хватает детальной регламентации, они редко высказываются независимо по общественным вопросам, доверие к ним низко. При этом институты обезличенного доверия и регламентация договорных отношений в Китае отстают от аналогичных европейских институтов почти на тысячелетие. Подход Сентолы предлагает ответ на эти примеры культурной устойчивости. Информация может идти длинными путями, охватывающим всю систему, но изменение поведения требует расширения мостов, которые обеспечивают сильную поддержку общества, когда одобрение требует значительного личного участия.[58]

Хотя сила родства роднит Китай со многими другими неэффективными режимами, слабость гражданских связей в сообществах не мешала императорам править огромной империей. В этом отношении имперский Китай мало чем отличался от Римской и Османской империй и многих других режимов прошлого, действовавших со сложной макрокоординацией и зависевших от родовой организации на микроуровне. Тем не менее, его меритократическая и относительно инклюзивная система государственной службы имеет мало параллелей в мировой истории или среди развивающихся стран сегодня.

### *Государство, нация, или цивилизация: культурные источники китайской живучести*

Как могли две, казалось бы, противоположные силы – меритократическая система государственной службы и поклонение роду и предкам – ужиться в одной системе? Эти две противоречивые черты развития Китая уже давно заставляют ученых задуматься. Очевидно, что необычайную живучесть Китая нельзя объяснить одними лишь длительными связями политического

[57] Charities Aid Foundation (CAF), “CAF World Giving Index: Ten Years of Giving Trends,” Report, 10th Edition (London, UK: Charities Aid Foundation, October 2019), https://www.cafonline.org/about-us/publications/2019-publications/caf-world-giving-index-10th-edition.

[58] Damon Centola, *Change: How to Make Big Things Happen* (Little, Brown Spark, January 2021), 95-109.

режима, поскольку династии гибли много раз. Я предполагаю, что стабильность системы в периоды упадка государства и краха империи проистекает из её гиперлокальной сети и родовой упорядоченности низового общества. Они становились временной системой «жизнеобеспечения», поддерживавшей долговременную преемственность китайской культуры. Когда преимущества инфраструктуры, сокращающей путь, иссякли, сообщества зависели от самых базовых ячеек общества до тех пор, пока не удалось восстановить системный порядок – бюрократическую инфраструктуру. Хотя гиперлокальная связанность не обеспечивала долговременную *общесистемную* связанность, она не позволила падению империи привести к гибели китайской культуры. Представление о Китае как о цивилизации сохранялось, даже когда исчезало государство.

Различная роль добровольных гражданских объединений имела ещё один долгосрочный эффект в обоих регионах: национальная идентичность населения Западной Европы сегодня выражается в терминах Просвещения – в построении индивидуализма и закона. В Китае национализм до сих пор проявляется в эвристике родства и поклонения предкам. Призывы к национальному единству основаны на этнических связях, а не на политическом выборе или общественном договоре, с противопоставлением своей «человеческой сущности» европейской.[59] Принимая во внимание эти тенденции, характеризующие китайское этическое мышление, трудно найти китайскую философскую традицию, которая поощряла бы веру в постоянный культурный прогресс в направлении общего соблюдения прав человека, основанную на принципах человеческой природы и человеческом разуме.

## Заключение

В «Анализе социальных сетей» Боргатти, Эверетт и Джонсон пишут: «Исследования сетей малого мира и безмасштабных сетей обычно ограничиваются описанием этих свойств, то есть принятием решения о том, является сеть безмасштабной или малым миром. Последствия таких структур недостаточно изучены, и трудно делать выводы об отдельных участниках или даже небольших группах участников таких сетей. Основная цель — получить некоторое представление об общей сетевой структуре».[60] Это исследование – первая попытка применить модели общей сетевой структуры к обстоятельствам и социальной организации реальных исторических режимов.

---

[59] Коммунистическая партия Китая в своих притязаниях на Тайвань подчеркивает «кровную» связь между ними и ведёт информационную кампанию, направленную на отрицание кровных уз в тайваньской национальной идентичности (*guojia rentong*). См. Gang Lin and Weixu Wu, “Chinese National Identity under Reconstruction,” in *Taiwan and China: Fitful Embrace*, ed. Lowell Dittmer (Oakland: University of California Press, 2017), 75-92.

[60] Stephen P. Borgatti, Martin G. Everett, and Jeffrey C. Johnson, *Analyzing Social Networks*, 2nd ed. (London, UK: Sage Publications, 2017), 303.

Оно выявило закономерности, интересные для исследователей сетей, политэкономистов и учёных, изучающих фундаментальные характеристики мировых цивилизаций; позволило по-новому взглянуть на повторяющиеся, узнаваемые и знакомые модели, наблюдаемые в исторической политэкономии, в частности, на устойчивую тенденцию китайских режимов к авторитарной централизации. Почему при переходе к безличной сложности современной экономики Китай по-прежнему меньше полагается на частные рынки и организации и больше на государство?[61] Какие структурные особенности поддерживают устойчиво низкий уровень доверия в обществе и высокий уровень «гуаньси», или обмена на основе отношений?

У Китая и Западной Европы есть социальные сети для решения таких проблем, как информационная асимметрия в экономике. Они могут быть источниками неформальных ограничений, которые либо препятствуют сотрудничеству, либо стимулируют его, и могут ослаблять или укреплять связи и сообщества, выходящие за рамки родства. Различия в распространении и внедрении неформальных норм в формальные структуры можно распознать с помощью сетевой науки. Мы видели, что во время урбанизации средневековой Европы распространение добровольных гражданских объединений увеличивало количество узлов в одном сообществе, имевших связи с узлами в другом сообществе, что ослабляло родственные сообщества и гомофилию. Христианская доктрина и институты способствовали этому процессу. С исчезновением разделения сообществ связанность всей системы возросла, создав дух «метрополии». В Китае конфуцианская этика усиливала разделение между однородными сообществами с сильными родственными связями, но слабыми моральными обязательствами по отношению к другим сообществам. Такая провинциальность ограничивала распространение поведенческих инноваций между сообществами, формируя вместо этого дух «деревни», где решения, основанные на отношениях, преобладают над анонимными рыночными обменами.[62] Акцента на централизации или децентрализации не достаточно, чтобы пояснить эти модели. Я объясняю эти давние различия с Западом тем, что у Китая были свои собственные короткие пути — система бюрократов-мандаринов, набранных со всей империи — что позволило ему расти, как государству, и обеспечило общесистемную связанность, но ограничило возможности проникновения в местные сети, что укрепляло местные нормы.

Мое утверждение о том, что модель взаимосвязанности центров высокого уровня фундаментально влияет на устойчивость системы, и что ради-

[61] John Ray Bowen II and David C. Rose, “On the Absence of Privately Owned, Publicly Traded Corporations in China: The Kirby Puzzle,” *The Journal of Asian Studies* 57, no. 2 (1998): 442-52, https://doi.org/10.2307/2658832.

[62] Samuel Bowles and Herbert Gintis, “Persistent Parochialism: Trust and Exclusion in Ethnic Networks,” *Journal of Economic Behavior & Organization* 55, no. 1 (September 2004): 1-23, https://doi.org/10.1016/j.jebo.2003.06.005.

альная топология Китая более уязвима к масштабной и немедленной фрагментации в случае разрушения центра, не означает, что руководство Китая не способно преодолеть глубоко укоренившийся консерватизм и неприятие культурных и технических изменений. Напротив, пекинский режим уверен, что он сможет обеспечить общественный порядок, не ограничивая своё владение революционными технологиями будущего, и не отступит из-за этических последствий развития технологий, эксплуатирующих личность ради коллектива. Фактически руководство заявляет, что режим преследует «высшее этическое благо». На Западе высшее этическое благо определяется наследием норм права. Различия в сетевой топологии дают двум обществам разные возможности для мониторинга и регулирования, а также выживания и способности интегрировать новые узлы и самоорганизовываться. Благодаря этим знаниям, полученным из сетевой науки о связях, компонентах и процессах изменений, исследователи получили новый подход к масштабированию взаимодействия при прошлых режимах и к формированию культурных различий среди населения. Теперь они могут включать сетевую структуру, как независимую научную переменную, в число внутренних факторов, задающих разные траектории развития мировых цивилизаций.

## Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

Конфликт интересов, о котором необходимо заявлять, отсутствует. Финансовая поддержка для проведения исследования, подготовки и/или написания этой статьи не предоставлялась. Исследования на людях и/или животных не проводились.

## Наличие данных

Данные, на которых основаны выводы данного исследования, можно получить от автора по запросу.

## Об авторе

**Хилтон Рут** – американский учёный, профессор политологии в Школе политики и управления им. Дуайта Шара Университета Джорджа Мэйсона в штате Виргиния. Специализируется в международной политэкономии и международном развитии.

Электронная почта: hroot2@gmu.edu

*Connections: The Quarterly Journal*
**ISSN 1812-1101, e-ISSN 1812-2973**

Ч. Бриггс, Ю. Данык, Т. Малярчук
*Connections QJ* 20, no. 3-4 (2021): 33-61
https://doi.org/10.11610/Connections.rus.20.3-4.03

**Рецензированная статья**

# Аспекты безопасности гибридной войны, пандемия COVID-19 и кибер-социальные уязвимости

*Чэд Бриггс,[1] Юрий Данык,[2] Тамара Малярчук [3]*

[1] *Университет Аляски в Анкоридже, https://www.uaa.alaska.edu*

[2] *Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского», https://kpi.ua/en/*

[3] *Рабочая группа Программы совершенствования военного образования (DEEP) НАТО, https://deepportal.hq.nato.int/eacademy/*

**Аннотация**: В то время как развитие кибертехнологий способствовало распространению и росту масштабов гибридных войн, пандемия COVID-19 обострила многие уязвимости и критические зависимости. В этой статье рассмотрены основные цели и стратегии гибридной войны с точки зрения психологической основы и технологического охвата, а также связи с возникающими проблемами дезинформации, киберпреступности, фейковых новостей, информационной травмы и влияния новых форм образования на национальную безопасность и устойчивость государства.

**Ключевые слова**: гибридная война, кибератака, кибербезопасность, информационная травма, электронное обучение, эмоциональная война, когнитивное хакерство, кибер-социальные уязвимости, кибертехнологии, COVID-19.

## Вступление

Концепция гибридной войны привлекает всё больше внимания при обсуждении вопросов безопасности и военной стратегии, часто – на примере действий России по захвату украинского Крымского полуострова в 2014 г. При

комплексном подходе к пониманию наступательных операций, от кампаний в соцсетях до обычной (кинетической) войны, термин «гибридная война» можно применить к широкому спектру действий. Чаще всего акцент делают на нерегулярном характере операций, когда традиционное западное понимание конфликта прикрыто силами и тактикой, которые трудно увязать с враждебным государством. В наших предыдущих статьях мы подробно описали использование кибертехнологий для широкого спектра атак на Украину с 2013 г., включая удары по энергетической инфраструктуре.[1] Для понимания уязвимости стран к утрате контроля за энергоснабжением важна способность противника подорвать доверие общества к институтам: когда основные потребности не удовлетворены, социальные расколы в стране или регионе усугубляются, и управление усложняется.

Ведение гибридных войн во всём мире в настоящее время неоспоримо. Страны от России до Китая на протяжении десятилетий включают идеи войны четвертого поколения в военные доктрины, где «красная линия» между миром и войной размывается, а по отношению к противнику действуют в рамках общей стратегии асимметричного, теневого (скрытого) конфликта.[2] Это не во́йны в традиционном смысле Гаагской или Женевской конвенций с чётким началом и концом, физической оккупацией территории, видимыми участниками и ясными намерениями. Гибридные войны пересекают границы и могут вестись постоянно, иногда – с нападением на целые страны, а иногда в отношении конкретных групп или людей. Но действия гибридной войны всегда имеют цель и мобилизуют ресурсы для её достижения. Все остальное — лишь инструмент достижения этой цели в интересах конкретных игроков (субъектов). Важным элементом тут является комплексная стратегия игрока, направленная на то, чтобы вывести другого игрока из равновесия, дестабилизировать его настолько, чтобы вскрыть стратегическое пространство для политических, экономических и военных действий.[3]

Гибридные войны – это вид постоянной войны разной интенсивности во многих сферах, с каскадными негативными последствиями и синергетическими эффектами, в которые в какой-то мере, сознательно или неосознанно, вовлечено всё население страны и международное сообщество. Их последствия ощущаются во всех сферах жизни, во всех слоях общества и по всему государству. Использование инновационных технологий позволило сместить конфликт с преимущественно открытых и силовых (кинетических)

---

1 Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs, “Hybrid War: High-tech, Information and Cyber Conflicts,” *Connections: The Quarterly Journal* 16, no. 2 (2017): 5-24, https://doi.org/10.11610/Connections.16.2.01.

2 Robert Wilkie, “Hybrid Warfare: Something Old, Not Something New,” *Air & Space Power Journal* 23, no. 4 (Winter 2009): 13-18.

3 Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory* (FT Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, 2009), https://apps.dtic.mil/sti/pdfs/ADA513663.pdf.

средств на менее очевидные стратегии, нацеленные на структурные уязвимости противников, в том числе за счёт достижения когнитивного преимущества и контроля над ними.

Такая гибридная тактика позволяет взять под контроль или дестабилизировать основные институты страны и достичь стратегических интересов нетрадиционным кибер- и когнитивным воздействием (с побочными эффектами). Основным театром асимметричных действий стало киберпространство, в силу того, что киберпространство имеет экстерриториальный, универсальный и глобальный характер. Оно также мало соотносится с географическими границами стран, может служить средой общения для людей почти всех возрастов и постоянно расширяется в масштабах и влиянии. Информационные потоки могут быть реализованы посредством диалога с массовой аудиторией и с использованием соцсетей для достижения или имитации индивидуального общения. На данный момент кибертехнологии стали важнейшим инструментом формирования коллективного и индивидуального сознания и ценностей общества.

Таким образом, кибертехнологии позволяют применять гибридные стратегии для достижения целей широкомасштабного воздействия на общество на расстоянии без возможности однозначно идентифицировать агрессора. Наиболее эффективные пользователи кибер-гибридных подходов выбирают конечные цели, которых нужно достичь, и выстраивают соответствующий набор синергетических действий с перекрывающимся, каскадным и усиливающим воздействием. Эти действия направлены на выведение из строя противника, продвижение заранее подготовленных нарративов и контроль когнитивной сферы на эмоциональном, моральном, культурном и ментальном уровнях. Успешные действия могут создать систему устойчивых стереотипов и восприятия действительности или же просто способствовать нестабильности и отрицанию объективных стандартов и истины.

Пандемия COVID-19, бушевавшая на планете с декабря 2019 г., добавила новые черты к спектру гибридных противостояний и методов. Их необходимо учитывать при анализе и прогнозировании для снижения рисков и предотвращения и/или смягчения последствий. Данная статья посвящена социальной природе гибридной войны и технологическим возможностям использования социальной и политической уязвимости и поляризации в подвергшихся нападению государствах. Эти вопросы рассмотрены в контексте гибридной войны, пандемии COVID-19 и возникающих кибер-социальных уязвимостей.

При всей важности внимания к военной и физической инфраструктуре гибридных атак, такие наступательные операции используют хрупкие социальные и политические структуры, являющиеся неотъемлемым элементом планирования наступательных стратегий и, соответственно, защиты от гибридных атак. Исторический опыт показал, что действия гибридной войны в этой сфере выгодны атакующему – хотя такие страны, как США, и ранее

использовали гибридные методы для усиления политической поддержки в зонах конфликтов, чаще успешно (например, Филиппины в 1950-х гг.), чем провально (Ирак после 2003 г. или Афганистан).[4] Там, где агрессор хорошо знает своего противника, общественные разногласия легко использовать, и они гораздо более уязвимы при умелом использовании киберинструментов, таких как социальные сети. На примере Украины и США в этой статье подробно описаны методы применения технологий асимметричного подхода для влияния и подрыва управления противника.

Идея атаковать социальную структуру противника не нова. Ещё Сунь-Цзы говорил о подрыве морального духа противника и предупреждал, что затяжной конфликт снизит поддержку войны обществом.[5] Клаузевиц тоже отмечал политическую природу войны, понимая, что победы в сражении может быть недостаточно, чтобы выиграть войну в целом.[6] Эксперты по борьбе с повстанцами и нерегулярной войне в XX веке ещё больше отмечали важность морального духа общества вне традиционного поля боя и указывали, что прямая военная сила может оказаться контрпродуктивной для завоевания политической поддержки в конфликте. Показательным примером стали дебаты по поводу стратегических бомбардировок ВВС США, особенно по гражданским целям во время Второй мировой войны в Европе. Официально имея промышленные и военные цели, американские бомбардировки с больших высот в Европе часто приводили к большим жертвам среди гражданского населения, при этом выдвигался аргумент (особенно в Королевских ВВС) о том, что разрушение городов подорвёт моральный дух общества и поддержку немецкой агрессии против Запада.[7] Немецкие «Люфтваффе» приводили аналогичные аргументы в пользу бомбардировок Великобритании в 1940-41 гг., со столь же разочаровывающими результатами.[8] Вместо того, чтобы подорвать моральный дух немцев или британцев, видящих, как разрушают их города, а соседи гибнут в результате бомбардировок, общество обычно сплачивалось в поддержку государства в ответ на такую открытую агрессию.

Аналогичным образом, десятилетия спустя, военные действия США против вьетнамских деревень, подозреваемых в укрытии партизан Вьетконга,

---

4 Ivan Arreguin-Toft, “How to Lose a War on Terror: A Comparative Analysis of a Counterinsurgency Success and Failure,” in *Understanding Victory and Defeat in Contemporary War*, ed. Jan Angstrom and Isabelle Duyvesteyn (Routledge, 2006), 160-185.

5 Sun Tzu, “The Art of War,” in *Strategic Studies: A Reader*, ed. Thomas G. Mahnken and Joseph A. Maiolo (Routledge, 2014), 86-110.

6 Carl von Clausewitz, *On War* (Penguin UK, 1982).

7 Kenneth P. Werrell, “The Strategic Bombing of Germany in World War II: Costs and Accomplishments,” *The Journal of American History* 73, no. 3 (December 1986): 702-713, https://doi.org/10.2307/1902984.

8 Edgar Jones, Robin Woolven, Bill Durodié, and Simon Wessely, “Civilian Morale During the Second World War: Responses to Air Raids Re-examined,” *Social History of Medicine* 17, no. 3 (2004): 463-479, https://doi.org/10.1093/shm/17.3.463.

казалось, лишь усилили поддержку Вьетконга или по крайней мере настроили общественное мнение против американцев.[9] Карр утверждал, что открытое насилие против гражданского населения (в отличие от военных), будь то со стороны американских военных во Вьетнаме или Ирландской республиканской армии в Великобритании/ Ирландии, вело к пониманию незаконности этих действий и утрате народной поддержки.[10] Но ключевым элементом таких оценок была очевидность таких действий и их ясные намерения. В тех же случаях, когда в агрессивных действиях можно было обвинить других (нападения под чужим флагом) или когда характер нападения не включал физического насилия, установить виновных и обвинить кого-либо очень сложно.

## Разделённый дом

Российские военные давно признали важность асимметричных подходов к военному конфликту, то есть использования уязвимых мест противника, непропорциональное имеющимся силам. Обычный подход России – проведение операций влияния, действий, не достигающих порога военного реагирования в западных странах, которые можно скрыть, не признавая своих агрессивных действий или намерений. Операции влияния предполагают использование в основном непрямых и некинетических средств для раздора и раскола у противника, используя уже имеющиеся внутренние/ внешние силы для поляризации политики, делегитимизации правительства и его институтов, а также подрыва стойкости населения и общества при реагировании на внешние угрозы.[11] Хотя история операций влияния не нова, кибертехнологии позволили эффективно проникать из любой точки мира прямо в компьютеры и телефоны людей, маскируя при этом истинный источник информации или дезинформации.

В некоторых военных стратегиях, включая стратегии Российской Федерации и Китая, немало внимания уделено информационным операциям как элементу более крупных стратегий и операций, а не отдельным операциям, как это часто бывает в США и Западной Европе. Независимо от того, называют ли их частью «революции в военном деле» или других доктрин, на практике эти стратегии относятся к асимметричным и информационно-ориентированным активным мерам против противника. Как отмечал Госдепар-

---

[9] Richard Shultz, “Breaking the Will of the Enemy During the Vietnam War: The Operationalization of the Cost-Benefit Model of Counterinsurgency Warfare,” *Journal of Peace Research* 15, no. 2 (June 1978): 109-129, https://doi.org/10.1177/002234337801500202.

[10] Caleb Carr, *The Lessons of Terror: A History of Warfare Against Civilians* (New York: Random House, 2003).

[11] Maria Snegovaya, “Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare,” *Russia Report* 1 (Washington, D.C.: Institute for the Study of War, September 2015).

тамент США в 1989 г. в отношении действий СССР, «активные меры» означают сочетание дезинформации и фейков, подставных групп, оппозиционных партий и операций политического влияния. Всё это использовалось для маскировки войны под видом безобидных действий.[12]

Бэгги описывал концепцию рефлексивного контроля в российской стратегии так: «Рефлексивный контроль служит для разрушения самой системы принятия решений, чтобы заставить её работать в интересах агрессора и, таким образом, установить власть без привлечения серьёзных военных или политических ресурсов, не превышая признанного порога вмешательства в международные дела суверенной страны».[13] Рефлексивный контроль является развитием советской военной доктрины, где особое внимание уделялось нарушению процессов принятия решений противником и дезинформации с тем, чтобы противник реагировал так, как выгодно для Советов (русских). Если командир противника чувствует, что его выбор ограничен определёнными вариантами, успешный рефлексивный контроль возникает, когда эти варианты способствуют стратегии России, и решение легче предвидеть.

В совокупности гибридная война, в понимании российского правительства и военных, предполагает целостную стратегию подрыва и дестабилизации противника, применяя широкий спектр средств, но (по возможности) используя слабости врага в интересах российской стратегии. В конечном счёте концепция рефлексивного контроля заключалась в том, чтобы влиять на информацию, доступную военным, ведя их по заранее определённому (русскими) пути, который можно было спланировать и который позволил бы России использовать свои сильные стороны в боевых действиях. Хотя это трудно в полной мере реализовать в традиционной войне (британские военные и разведслужбы исторически были успешнее других в стратегической дезориентации противника), кибертехнологии повышают возможности дезинформации. Успех позволит не только расколоть общество, подвергшееся нападению, но и заставит сами «мишени» распространять дезинформацию и негативные нарративы.

## Когнитивное хакерство

Применяя новые развивающиеся технологии, злоумышленники всё чаще используют психологические приемы и манипуляции в когнитивном пространстве. Эти тактики часто повторяют хакерские (фишинг, спуфинг и т.д.) и представляют собой особый тип социальной инженерии. Их применение увеличивает возможность несанкционированного доступа к информационным ресурсам в киберпространстве, важным для когнитивной сферы общества, с возможностью деструктивного воздействия на неё. Это явление

[12] Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (Washington, DC: Defense Press, February 2019).

[13] Bagge, *Unmasking Maskirovka*.

называют «когнитивным хакерством».[14] В его основе лежит манипулирование общественным сознанием в киберпространстве – не только с целью кражи денег или данных, но и чтобы повлиять на поведение пользователей, навязать им свою волю и контролировать их. Практически любой пользователь киберпространства может заниматься когнитивным хакерством в виде дезинформации, манипулирования репутацией и/или распространения на интернет-платформах контента, меняющего восприятие реальности у других пользователей. Оно может принимать форму кибератак, кибердействий и операций, направленных на манипулирование человеческим восприятием реальности с использованием уязвимостей обработки информации людьми и соцсетями. Такие атаки направлены на изменение поведения, восприятия или отношения людей к значимым событиям или темам, таким, как пандемия COVID-19, и преследуют конкретную цель.[15]

В 2019 г. количество фишинговых атак (создание фейковых сайтов или ссылок, имитирующих сайты известных компаний) выросло на 400 %. При этом более 24 % адресов вредоносных страниц (URL) располагались на легитимных доменах, используя доверие к ним пользователей, а фишинг стал более персонализированным, включая отслеживание присутствия и активности конкретного пользователя в киберпространстве.[16] Помимо фишинга, киберпреступники используют спуфинг (маскировку вредоносной программы под легальную) для политических атак. Так, в марте 2016 г. высокопоставленный чиновник предвыборного штаба Хиллари Клинтон, Джон Подеста, ввёл свои учетные данные на странице, не распознав фейковое уведомление, якобы полученное от Google. Так произошёл взлом, и злоумышленники получили доступ к его данным, которыми затем воспользовались иностранные и местные политики.[17]

## Эмоциональная война

В более сумрачном, некинетическом спектре гибридной войны контроль над информацией нацелен не только на когнитивные процессы, но и на

---

[14] Darren L. Linvill et al. "'The Russians Are Hacking My Brain!' Investigating Russia's Internet Research Agency Twitter Tactics During the 2016 United States Presidential Campaign," *Computers in Human Behavior* 99 (October 2019): 292-300, https://doi.org/10.1016/j.chb.2019.05.027.

[15] Ian Baxter, "The Cognitive Psychological Tricks Hackers Use to Dupe Users," *ITProPortal*, March 12, 2020, www.itproportal.com/features/the-cognitive-psychological-tricks-hackers-use-to-dupe-users.

[16] Muhammad Adil, Rahim Khan, and M. Ahmad Nawaz Ul Ghani, "Preventive Techniques of Phishing Attacks in Networks," in *Proceedings of the 3rd International Conference on Advancements in Computational Sciences*, ICACS 2020, Lahore, Pakistan, February 17-19, 2020 (IEEE, 2020), 1-8, ISBN 978-1-7281-4235-7.

[17] Travis Farral, "Nation-state Attacks: Practical Defences against Advanced Adversaries," *Network Security* 2017, no. 9 (September 2017): 5-7, https://doi.org/10.1016/S1353-4858(17)30111-3.

лимбические, эмоциональные центры мозга.[18] Людям присуще делить мир на различные категории идентичности, чтобы понять смысл сложного мира и объяснить причины происходящего. Политические психологи уже давно показали, что эти категории не обязательно должны иметь какую-то внутреннюю ценность. Они могут быть совершенно произвольны, основываться на мифах, или быть усвоены от авторитетов, например, путём разделения школьников на случайные группы по цвету глаз, или национальные категории, основанные на исторических событиях, имевших место столетия назад. Посторонним такое разделение может показаться случайным, как в сатире Джонатана Свифта на различия между католиками и протестантами в 1723 г. Тем не менее в соцсетях это разделение может выглядеть реальным и подкрепляться политической, экономической и медийной практикой.

Психологи определили траектории, по которым разделение на «своих» и «чужих» может перерасти из социально приемлемых различий в потенциально жестокие и трудноразрешимые антагонизмы. Во-первых, различия делают существенными или характерными, то есть на группу налагают широкие стереотипы, объясняющие, что социальные (расовые, языковые, религиозные и т.д.) различия являются важными чертами этой группы. Если человек рождается или воспитывается в такой группе, эти различия считаются устоявшимися, и их нелегко изменить. Затем «чужих» обесценивают в соответствии с этими чертами, а образы и истории в СМИ часто толкуют так, чтобы усилить эти негативные стереотипы.[19] Первые два процесса часто способствуют повышению оценки своей группы, подчеркивая отличия в том, что делает человека «хорошим». Американский патриотизм на протяжении всей холодной войны часто основывался на различии между «трудолюбивыми американцами» и «неэффективными, безбожными коммунистами», в то время как другие националисты будут стараться подчеркнуть превосходство своей культуры над другими.[20]

Более опасные процессы происходят, когда потребности общества не удовлетворены или не могут быть удовлетворены, от базовых потребностей, таких, как дорогая еда, до более экзистенциальных угроз утраты культуры или престижа. Когда в обществе открыто или скрыто присутствуют та-

---

[18] Linton Wells II, “Cognitive-Emotional Conflict: Adversary Will and Social Resilience,” *Prism* 7, no. 2 (December 2017): 4-17, https://cco.ndu.edu/PRISM-7-2/Article/1401814/cognitive-emotional-conflict-adversary-will-and-social-resilience. Мы также благодарны Александре Несич за её работу об эмоциональной войне.

[19] Marilynn B. Brewer, “The Psychology of Prejudice: Ingroup Love and Outgroup Hate?” *Journal of Social Issues* 55, no. 3 (Fall 1999): 429-444, https://doi.org/10.1111/0022-4537.00126.

[20] Robert T. Schatz, Ervin Staub, and Howard Lavine, “On the Varieties of National Attachment: Blind Versus Constructive Patriotism,” *Political Psychology* 20, no. 1 (March 1999): 151-174, https://doi.org/10.1111/0162-895X.00140. Следует отметить, что некоторые виды национализма по своей природе негативны, концентрируясь на исторических поражениях и ощущении жертвы.

кие страхи, возникает возможность приписать эти угрозы сторонним группам. Исторически антисемитизм часто основывался на том, что евреев обвиняли в финансовых проблемах большинства населения, исходя из стереотипа об их исторической социальной роли банкиров, юристов и ученых. Дегуманизация и/или деполитизация групп в сочетании с виной за неспособность общества достичь основных целей или потребностей опирается на предполагаемые существенные характеристики группы, чтобы поляризовать мнения и согласиться с насильственными средствами защиты от угроз извне.[21]

Пропагандистские кампании во время войны часто использовали такие стратегии, будь то стереотипы Первой мировой о немецких «гуннах», убивающих невинных женщин и детей, или агитация в США против якобы фанатизма и бесчеловечности японцев.[22] Но самые крайние проявления возникали, когда дегуманизация группы принимала такие масштабы, что геноцид принимался и поощрялся, как, например, в отношении евреев во время Второй мировой войны, мусульман в Боснии и Герцеговине или «нежелательных элементов» в Камбодже при Красных кхмерах.[23] Но открытая война и оправдание геноцида не всегда сопровождают раскол в обществе, как критический элемент конфликта. Модель гибридной войны не предполагает массового насилия против населения, предпочитая использовать раскол у противника против него самого.

## США: Познай себя

Разведка США предупреждала о вмешательстве России в американскую политику как минимум с 2016 г. В недавнем докладе Мюллера указано, что серьёзные попытки России повлиять на выборы начались не позднее 2014 г. Это было совсем не то, что некоторые критики пренебрежительно называют «несколькими рекламными объявлениями в Facebook»: усилия России (как кибер-, так и человеческие) вылились в скоординированную кампанию по подрыву доверия к институтам США, усилению политической неуверенности и поляризации.[24] Отсутствие окончательного вердикта об эффекте таких

---

[21] Ervin Staub, “The Roots of Evil: Social Conditions, Culture, Personality, and Basic Human Needs,” *Personality and Social Psychology Review* 3, no. 3 (1999): 179-192, https://doi.org/10.1207/s15327957pspr0303_2.

[22] Harold D. Lasswell, *Propaganda Technique in the World War* (Ravenio Books, November 2015).

[23] Michał Bilewicz and Johanna Ray Vollhardt, “Evil Transformations: Social-Psychological Processes Underlying Genocide and Mass Killing,” *Social Psychology of Social Problems: The Intergroup Context*, ed. Agnieszka Golec de Zavala and Aleksandra Cichocka (New York, NY: Palgrave Macmillan, 2012): 280, https://doi.org/10.1007/978-1-137-27222-5_11.

[24] Robert S. Mueller, “Report on the Investigation into Russian Interference in the 2016 Presidential Election,” The Final Report of the Special Counsel into Donald Trump, Russia, and Collusion (Washington, D.C.: US Department of Justice, March 2019), https://www.justice.gov/archives/sco/file/1373816/download.

действий на выборах 2016 г. не имеет значения: если цель заключалась в усилении неуверенности и подрыве доверия, то сама постановка таких вопросов уже говорит о достижении главной цели.

США во многих отношениях были и остаются уязвимыми для кибероперациий гибридной войны ещё до событий 6 января 2021 г. Это страна с глубокими политическими, экономическими, региональными, расовыми и гендерными различиями. Большинство американских политиков не подчёркивают различий, кроме партийных, предпочитая вместо этого говорить об общих политических устремлениях американцев. Тем не менее существовала возможность использовать скрытые разногласия и недовольство, а такие киберинструменты, как социальные сети, обеспечили беспрепятственный доступ к миллионам американцев. Проводимая российским ГРУ и «Лахтой» (Агентством интернет-исследований) целенаправленная кампания была направлена на поляризацию американцев по таким разделяющим общество вопросам, как иммиграция, гендерные права и религия. В рассекреченном отчёте разведки США от января 2017 г. резюмируется: «Мы считаем, что президент России Владимир Путин приказал в 2016 г. провести кампанию влияния на президентские выборы в США. Целью России было подорвать веру общества в демократический процесс в США, очернить госсекретаря Клинтон и помешать её избранию и возможному президентству. Мы также считаем, что Путин и российское правительство явно отдают предпочтение избранному президенту Трампу. Мы вполне уверены в этих оценках».[25]

Считают, что поскольку Клинтон была фаворитом на выборах, действия России могли помешать её президентству, посеяв сомнения в его легитимности. Предпринятые кибердействия включали взлом электронной почты партий (как демократов, так и республиканцев), киберагрессию – публикацию избранных сообщений в изменённом виде в таких источниках, как Wikileaks, создание псевдообщественных политических групп в соцсетях, подставных аккаунтов в сетях Facebook и Твиттер, выдающих себя за избирателей США, организацию надуманных протестов и контрпротестов, создание и распространение фейковых и лживых новостных сообщений, нацеленных в основном на избранные группы населения в ключевых штатах. Использование метаданных социальных сетей очень упростило процесс: пользователи, использовавшие ключевые слова, например, с беспокойством по поводу иммиграции мусульман, могли получать рекламу и политические сообщения, усиливающие такие опасения по отношению к определённым кандидатам.[26]

Хотя тактика России часто имела успех, её можно применить только в

[25] Bill Priestap, “Assessing Russian Activities and Intentions in Recent US Elections,” Unclassified Intelligence Community Assessment (Office of the Director of National Intelligence, January 2017), p. ii.

[26] Philip N. Howard et al., “The IRA, Social Media and Political Polarization in the United States, 2012-2018” (University of Oxford, 2018).

политическом ландшафте, где уже существуют значительные разногласия, фейковые новости и теории заговора могут найти отклик у значительной части населения, а технологии достаточно распространены – по меньшей мере 30 миллионов американцев могли получать российские сообщения.[27] Вместо того, чтобы ощутить себя американцами, совместно противостоящими действиям России, люди в США нападали друг на друга, разделившись на «своих» и «чужих», используя выражения наподобие «настоящие американцы» и говоря о патриотизме. «Лахтоботы» не ограничилась выборами, а активно участвовали в антинаучных кампаниях, особенно по вопросам изменения климата и против вакцинации. Их содействие распространению таких дремлющих болезней, как корь (к весне 2019 г. некоторые штаты США объявили чрезвычайное положение из-за её вспышек), нельзя объяснить одними лишь действиями России, но они имели целью вывести на поверхность подводные течения, уже имевшиеся в американском обществе,[28] «прыгая» по существующим темам, «критичным» для общества или отдельных целевых групп.

Пандемия COVID-19 высветила многие из этих различий: разногласия использовали или провоцировали в ответ на меры здравоохранения. В протестах против вакцин от COVID в 2021 г. участвовали и левые, и правые, при этом использование масок от коронавируса было связано с линией партии.[29] Многие хотели раздуть пожар, не соглашаясь с происхождением и смертоносной природой вируса; подобные стереотипы окутывали различные споры, чаще политические, чем медицинские. Общая стратегия России и Китая заключалась в том, чтобы зародить сомнения в эффективности реакции демократических институтов на пандемию.[30]

Политическая психология разделения на «своих» и «чужих» помогает понять, что когда эти разногласия усилены средствами массовой информации и политическими нарративами, разделение становится гораздо более резким как для сторонних наблюдателей, так и для тех, кто относит себя к тому или иному лагерю. Это не только крайне усложнило традиционное двухпартийное законотворчество и управление на федеральном уровне, но и усилило разногласия. Когда появляется новая дезинформация (или пред-

---

[27] Howard et al., “The IRA, Social Media and Political Polarization.”

[28] David A. Broniatowski et al., “Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate,” *American Journal of Public Health* 108, no. 10 (October 2018): 1378-1384, https://doi.org/10.2105/AJPH.2018.304567; Shanta Barley, “Climategate: Russian Secret Service Blamed for Hack,” *New Scientist* 7 (2009).

[29] Rose Bernard, Gemma Bowsher, Richard Sullivan, and Fawzia Gibson-Fall, “Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare,” *Health Security* 19, no. 1 (2021): 3-12, https://doi.org/10.1089/hs.2020.0038.

[30] Sergey Sukhankin, “COVID-19 as a Tool of Information Confrontation: Russia’s Approach,” *The School of Public Policy Publications* 13, no. 3 (April 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3566689.

взятый целевой контент запускает заранее определённые (спланированные) процессы или идеи), независимо от первоисточника, американцы могут делиться такой информацией в соцсетях, а алгоритмы отбора (например, через Facebook) ещё больше укрепляют мысль о том, что этой информации можно доверять, потому что ею поделился заслуживающий доверия американец. В то время как советской пропаганде в 1970-х – 1980-х гг. приходилось целенаправленно работать над отмыванием источников по нескольким фронтам, с помощью киберинструментов сообщение или нарратив можно вбросить и распространить без особых усилий, если они отражают то, что люди хотят или ожидают увидеть.

Технологии социальных сетей – не исключение. Эффективная гибридная война использует различные инструменты для достижения цели разрушения или контроля. Атаки на энергетическую инфраструктуру были отмечены и в США, при чём правительство США признало, что атаки типа «отказ в обслуживании» нарушили работу электросетей на западе США в марте 2019 г. После того, как стало известно о возможности таких атак, и что попытки взлома уже предпринимались ранее, стало понятно, что США могут реально пострадать от сбоев в работе критических служб, как это ранее было в Украине (которая, в некотором смысле, стала испытательным полигоном для технологий будущих войн, включая кибернетические, информационные и когнитивные действия). Стратегическая цель таких угроз или действий – создать ощущение неуверенности и незащищённости, отвлечь граждан и руководителей, заставив их думать о том, как интерпретировать события и информацию.

Полагают, что события в США находятся на гораздо более низкой ступени эскалации, чем в других странах (например, в Грузии, Эстонии, Украине, Сирии). Тем не менее важно ещё раз подчеркнуть, что не существует «красной линии», которая отличала бы стратегии гибридной войны в одной стране от другой. Цели различаются по степени желаемой дестабилизации с учетом того, что может вызвать активный ответ государству-агрессору. Опыт США показал, что постепенные и скрытые действия могут со временем снизить порог реагирования, допуская большее вмешательство и дестабилизацию при отсутствии сильной скоординированной защиты.[31]

## Пожар на Востоке

Нынешний конфликт в Украине часто приводят в качестве одного из главных примеров гибридной войны последних лет, хотя многие аналитики прежде всего вспомнят об оккупации Крыма в 2014 г. Открытый конфликт в Донецкой и Луганской областях с середины 2014 г. привлекает меньше внимания,

[31] Rubén Arcos, Manuel Gertrudix, Cristina Arribas, and Monica Cardarilli, “Responses to Digital Disinformation as Part of Hybrid Threats: A Systematic Review on the Effects of Disinformation and the Effectiveness of Fact-checking/Debunking,” *Open Research Europe* 2, no. 8 (2022), https://doi.org/10.12688/openreseurope.14088.1.

а в западных СМИ его часто ошибочно называют «гражданской войной». Даже когда анализ насильственного конфликта на востоке включает сбитие рейса МН-17 Малайзийских авиалиний в июле 2014 г., эти насильственные действия представляют собой лишь наиболее видимые аспекты гибридной войны.[32] Этот конфликт имеет ряд характерных черт, наиболее примечательной из которых является появление свидетельств того, что некинетическая (т.е. информационная) война оказывает существенное травмирующее воздействие на общество вдали от линии фронта на востоке Украины.

Деструктивные действия концентрируются на критических узлах социальных и связанных с ними систем, уязвимостях, которые можно использовать, а затем переходят в самоподдерживающийся нисходящий цикл повторяющихся шагов и воздействий (в научных терминах – петли положительной обратной связи). Но поскольку целевые узлы разнесены по географическим и функциональным зонам, стороннему наблюдателю может быть трудно увидеть характер предполагаемых воздействий и общую стратегию агрессора. Для стратегий национальной безопасности важно уметь выявлять такие рассредоточенные и тайные действия и противостоять им, а также понимать сложные каскадные последствия агрессивных действий, которые не приводят в действие традиционную концепцию «актов войны».

Как и для других сложных систем безопасности, таких, как энергетика или окружающая среда, часто критичней всего не первоначальное воздействие, а эффекты второго и третьего порядка, возникающие в результате первоначального нарушения. Поначалу может быть трудно увидеть причинно-следственную связь событий, а неправильные ответные меры могут усугубить цепочки последствий.[33] Так, реакция советского руководства на катастрофу на Чернобыльской АЭС в 1986 г. стала, пожалуй, одним из худших примеров реагирования. Тогда политические соображения привели к облучению десятков тысяч граждан в Украине и за её пределами. Подобная неадекватная реакция на изменившиеся условия легко может усугубить другие бедствия или конфликты.[34] Следуя принципам рефлексивного контроля, эффективная кампания гибридной войны может завести правительство в петлю положительной обратной связи с ухудшающимися последствиями второго и третьего порядка.

Гибридная война в Украине показала стратегическую важность плановых скоординированных действий и необходимые компоненты в киберсфере:

- Конечные цели, которые должны быть достигнуты;

---

[32] Irina Khaldarova and Mervi Pantti, “Fake News: The Narrative Battle over the Ukrainian Conflict,” *Journalism Practice* 10, no. 7 (2016): 891-901, https://doi.org/10.1080/17512786.2016.1163237.

[33] Aura Reggiani, “Network Resilience for Transport Security: Some Methodological Considerations,” *Transport Policy* 28, no. C (2013): 63-68, https://doi.org/10.1016/j.tranpol.2012.09.007.

[34] Andrew Leatherbarrow, *Chernobyl 01:23:40: The Incredible True Story of the World’s Worst Nuclear Disaster* (Lancaster, UK: Andrew Leatherbarrow, 2016).

- Стратегия ведения кампании;
- Организация кампании;
- Используемая тактика и инструменты;
- Оценка первичного, вторичного и третичного воздействия;
- Оценка и усугубление последствий.

Кибердействия могут вестись последовательно, одновременно, параллельно, рассредоточено или целенаправленно. Рассредоточенные кибердействия направлены на наиболее уязвимые элементы (объекты) инфраструктуры. Совокупность одновременных и/или последовательных кибервоздействий обеспечивает синергетический эффект на непредсказуемые места (элементы, системы, сферы), которые могут быть административно или политически отделены от главной цели, но функционально влияют на критические системы. Вот пример из мира, не связанного с кибербезопасностью: в 2001 г. произошла серия атак сибирской язвы на политиков через почтовую систему США, и в результате пришлось закрыть все почтовые отделения в Вашингтоне. Неожиданным (для специалистов по стихийным бедствиям) результатом стало то, что не были получены чеки об оплате местной коммунальной компании PEPCO, и энергокомпании пришлось обратиться в Белый дом с просьбой о финансировании, чтобы не отключать энергоснабжение столицы США.[35] Кибердействия могут иметь больше прямых последствий в тесно взаимосвязанном мире, где компании надеются на электронные платежи и своевременные поставки товаров и комплектующих. Так, кибератаки Petya в Украине в июне 2017 г. имели побочные эффекты в европейской и мировой финансовой системах, хотя основной целью было украинское государство и компании этой страны в канун национального праздника.[36]

Хотя атаки Petya в 2017 г. встретили эффективный отпор украинских кибервойск, предполагаемые цели в виде финансовых учреждений быстро перекинулись на больницы и страховые компании по всему миру. Эти методы применяют, планируя кибервоздействие с широкими цепными последствиями. Они создают разрушительную волну на взаимосвязанных объектах и системах, одновременно воздействуя на множество пересекающихся сфер. Кибератаки могут проводиться синхронно или асинхронно, параллельно по нескольким линиям атаки или последовательно несколько раз на одном и том же целевом кластере. Ущерб целевым объектам наибо-

[35] Reshma Pradhan Lensing, “Historical Events and Supply Chain Disruption: Chemical, Biological, Radiological and Cyber Events,” PhD Dissertation (Massachusetts Institute of Technology, 2003).

[36] Jagmeet S. Aidan, Harsh K. Verma, and Lalit K. Awasthi, “Comprehensive Survey on Petya Ransomware Attack,” In *Proceedings of the 2017 International Conference on Next Generation Computing and Information Systems* (ICNGCIS), IEEE, pp. 122-125.

лее разрушителен и эффективен по критериям «эффективность-время-затраты», хотя некоторые цели могут служить для демонстрации возможностей концепции другим странам, которые могут быть атакованы. Исследования и анализ боевых действий показывают, что действия, связанные с кибербезопасностью, и информационная война становятся всё более масштабными и важными для военных.[37] В этой связи, гибридная война и применение киберсредств в ней относятся к наиболее важным факторам для понимания дуги будущих конфликтов.

Кибератака России на электростанции «Прикарпатьеобленерго» в декабре 2015 г. потребовала месяцев тщательной подготовки и внедрения, а подача электроэнергии была нарушена менее чем на сутки. Но настоящей целью атаки могла быть не только Украина. Атака могла стать проверкой новых методов гибридной войны и предупреждением для других стран, чьи энергосистемы могут быть уязвимы для подобной тактики. Новые кибератаки 2021 и начала 2022 гг. подтверждают, что в Украине идёт настоящая информационная и кибернетическая война, включающая весь спектр деструктивного воздействия как на техническую инфраструктуру, так и на общество. Использование соцсетей для кибератак ещё более выгодно, поскольку они используют собственные алгоритмы систем для распространения дезинформации или нужных нарративов. Миллионы людей можно охватить относительно небольшими усилиями, а в сочетании с кибердарами по другим местам (учреждениям, инфраструктуре) социальные последствия могут резко усилиться.[38]

## Гибридная форма коллективной травмы

Хаотичный фон непонимания будущих рисков безопасности в стране, восприятия информации, незнание, кому доверять и можно ли надеяться на основные услуги и институты, усугублённые гибридной войной, могут привести к распространению когнитивного резонанса, диссонанса или дисбаланса. Помимо смятения, описываемого когнитивной психологией, люди могут получить травмы в виде биологических и неврологических патологий, индивидуальную и коллективную психику выталкивают за рамки нормального восприятия, а понимание и доверие искажается, в той или иной степени.[39] Исследования в Украине позволили оценить последствия травм в

[37] Iskren Ivanov and Velizar Shalamanov, “NATO and Partner Countries Cooperation in Countering Asymmetric and Hybrid Threats in South Eastern Europe’s Cyberspace,” in *Toward Effective Cyber Defense in Accordance with the Rules of Law* 149, ed. Alan Brill, Kristina Misheva, and Metodi Hadji-Janev (2020): 59-70, https://doi.org/10.3233/NHSDP200041.

[38] Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” *Wired*, March 3, 2016, www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[39] Jack Saul, *Collective Trauma, Collective Healing: Promoting Community Resilience in the Aftermath of Disaster* 48 (Routledge, 2013).

районах открытого конфликта на востоке. Последние исследования показывают, что «синдром гибридной войны» сильнее, когда вся территория является зоной активного деструктивного воздействия на индивидуальную и общественную психику.

Последствия гибридной войны не ограничиваются числом погибших, искалеченных и пропавших без вести. Они также включают воздействие на когнитивную сферу граждан, сообществ и всего общества. Гибридная война прямо и косвенно влияет на сознание и подсознание, на психофизиологическое, психическое состояние и общественное здоровье участников и очевидцев конфликта. Но в кибермире гибридного конфликта свидетели живут не только в «горячих зонах» кинетической войны. Всё население является свидетелем конфликта и объектом кампаний по подрыву традиционных концепций идентичности, доверия и объективной реальности. В предыдущих конфликтах травму получали те, кто находился в географически определённой зоне боевых действий или там, где средства массовой информации могли транслировать тревожные образы войны в домах людей. Киберинструменты позволяют расширить охват, стирая старые геопространственные границы и односторонний поток информации. Таким образом, и комбатанты, и гражданское население оказываются в зоне гибридного конфликта, что проявляется в ряде психологических и поведенческих характеристик, которые можно в совокупности обозначить как «синдром гибридной войны» и его производные, «военный синдром гибридной войны», «специфическое посттравматическое стрессовое расстройство гибридной войны» и т.д.[40]

В странах, переживающих затяжной конфликт, у определённого слоя населения развился «военный синдром гибридной войны». Этот синдром объясняется боевыми (военными) действиями низкой интенсивности при гибридном конфликте и широким спектром нетрадиционных параллельных воздействий. У тех, кто особенно подвержен насилию в зоне конфликта, часто развиваются серьёзные изменения в индивидуальной психологии и реакции на окружающих, особенно когда они возвращаются из зоны конфликта и испытывают сильный когнитивный диссонанс и отчуждение.[41] Такие люди могут обладать боевыми навыками, неприменимыми в гражданской жизни, и испытывать чрезмерное восприятие угрозы (включая потен-

[40] Yuriy Danyk and Oleksandra Zborovska, “Development and Implementation of a New Concept of Crisis Situations Syndrome: ‘Syndrome of a Hybrid War’,” *EUREKA: Health Sciences* 6 (2018): 15-29, https://doi.org/10.21303/2504-5679.2018.00797; Piotr Pacek and Olaf Truszczyński, “Hybrid War and Its Psychological Consequences,” *Toruń International Studies* 1, no. 13 (2020): 23-30, https://doi.org/10.12775/TIS.2020.002.

[41] Yuriy Danyk et al., “The Technology of Objective Diagnosis, Treatment and Prevention of PTSD in Members of the Armed Forces under Conditions of Hybrid War,” *International Journal of Research and Innovation in Applied Science* 4, no. 1 (January 2019): 7-11, www.rsisinternational.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

циальную агрессию против воображаемых угроз), вторжение травматических воспоминаний во все аспекты жизни и неверие в возможность избежать травматического опыта. Эту форму отличает от традиционной боевой травмы то, что вернувшиеся солдаты или участники боевых действий не возвращаются в состояние мира и стабильности, но по-прежнему живут в нестабильной среде, в которой угрозы и раздражители пронизывают повседневную жизнь.[42]

Стратегии гибридной войны не только многими путями создают непосредственные травматические ситуации, но и воспроизводят диссоциативные состояния так долго, что психобиологические реакции становятся неразличимыми. Описывая боевую травму, Кардинер писал: «…весь аппарат согласованной, скоординированной и целенаправленной деятельности разбит. Восприятие становится неточным и наполнено страхом, координационные функции суждения и различения не работают … органы чувств могут даже перестать функционировать».[43] В условиях гибридной войны человек, пытающийся преодолеть постоянный стресс и чувство угрозы, безнадёжности и потери контроля, не может вполне полагаться на более крупные социальные резервы устойчивости. Когда ощущается социальная травма и группы начинают распадаться, другие члены общества усиливают неуверенность и ощущение риска, и этот феномен существенно возрастает при доступе и использовании соцсетей.

Те, кто не участвовал в боевых действиях и не испытал насилия на фронте, тоже могут ощущать многие факторы стресса, связанные с посттравматическим стрессовым расстройством, и медицинские исследования показали, что длительное воздействие этих факторов сказывается на качестве биофизиологических маркеров.[44] Это, может быть, и не удивительно, учитывая методы гибридной войны, но любопытно, что киберинструменты позволяют острому стрессу проникнуть в районы географически удалённые от традиционных конфликтов. Эти синдромы возникают как следствие длительной коллективной и индивидуальной травмы от угроз жизни и здоровью, постоянного изменения форм и интенсивности боевого напряжения, продолжительности боевых действий и специфического небоевого стресса разной силы. Всё это часто превышает возможности психологической устойчивости человека. Традиционными факторами посттравматического стрес-

---

[42] Judith L. Herman, *Trauma and Recovery: The Aftermath of Violence – From Domestic Abuse to Political Terror* (New York: Basic Books, July 2015).

[43] Цитата из Herman, *Trauma and Recovery*, 35.

[44] Iryna Boichuk et al., "Characteristics of Eye Movements in the Anti-terrorist Operation Area's Residents with Potential Posttraumatic Stress Disorder," *Journal of Opthamology* 1 (Ukraine) (2019): 52-55; Yuriy Danyk et al., "The Objectivization of the Complex PTSD Diagnostic by Identifying Opthalmological Biomarkers," *International Journal of Research and Innovation in Applied Science* 4, no. 2 (January 2019): 7-11, www.rsisinternational.org/journals/ijrias/DigitalLibrary/Vol.4&Issue1/07-11.pdf.

сового расстройства являются потеря товарищей и участие в насилии в отношении врага. В гибридных кампаниях, наподобие украинской, эффект усиливается на фоне сложной этнонациональной идентичности. В то же время масштаб и географический охват внешних факторов стресса преднамеренно разрывает социальные ткани, лишая людей чёткого представления о том, где они находятся и во что им верить с точки зрения текущих событий и будущих целей. Под сомнение ставятся идеи мирной жизни, стандартные ценности общества, оценки участников боевых действий мирными гражданами.

В Украине гражданам приходится противостоять конкурирующим версиям о том, что конфликт в Донецкой и Луганской областях является результатом российского вторжения, гражданской войной между украинцами, следствием этнического разделения русских и украинцев, борьбой за свободу и независимость от коррумпированного украинского правительства или частью более масштабного экспансионистского проекта «Новороссии». Доминирующий нарратив отсутствует намеренно. Чем меньше согласия относительно природы конфликта, его причин и оценки его участников, тем больше напряжения и разногласий может возникнуть в мирных районах Украины и соседних странах. В отличие от усиления коллективной идентичности перед лицом явного агрессора (американский идеал Второй мировой войны), в гибридной войне никто не знает, кто на самом деле агрессор и почему. Мир может наступить в любое время или не наступить никогда, история становится туманной, а ощущение стабильности – эфемерным.[45]

Способность населения протестовать против конфликта или поддерживать его тоже можно использовать как средство эксплуатации гибридной войны в целевой стране. Разочарование и негодование, порождённые масштабным конфликтом, в сочетании с мыслями о коррупции или злоупотреблениях политической, военной и деловой верхушки могут легко усиливать различные киберкампании и целевое воздействие. Ухудшение социально-экономических условий и невозможность изменить жизнь к лучшему можно рефлекторно контролировать, чтобы изменить результаты выборов или вызвать миграцию из одного региона в другой. В этом случае мигранты могут стать мишенью, как участники этнического или культурного «вторжения» для изменения политических настроений в третьей стране. Это явление наблюдалось как в Украине по отношению к внутренне перемещенным лицам из Крыма/Донецка/Луганска, так и в недовольстве украинцами, переехавшими в такие страны, как Польша. Кампании дезинформации в российских СМИ сработали против сирийских беженцев в Германии и латиноамериканских мигрантов в Соединённых Штатах Америки при помощи лжи-

[45] Joanna Szostek, “Nothing Is True? The Credibility of News and Conflicting Narratives during ‘Information War’ in Ukraine,” *The International Journal of Press/Politics* 23, no. 1 (January 2018): 116-35, https://doi.org/10.1177/1940161217743258.

вых историй, которые вбрасывались и распространялись внутренними источниками в Германии и США.[46]

## Угрозы кибербезопасности из-за пандемии COVID-19 в условиях гибридной войны и кибер-социальные уязвимости

Пандемия COVID-19 стала серьёзным испытанием эффективности систем здравоохранения во всем мире и способности государств, местных и национальных органов власти противостоять соответствующим вызовам и угрозам безопасности. Хотя понятное внимание к пандемии коронавируса попрежнему сосредоточено главным образом на прямом воздействии на здоровье населения и реагировании на экономические последствия, вспышка резко изменила взаимодействие в обществе с применением информационных технологий. Киберсистемы и информационные технологии могут предоставить некоторые полезные возможности, но необходимо также выявить и устранить системные риски и уязвимости безопасности в условиях гибридной войны.

Непосредственным последствием пандемии COVID-19 в Китае стала не только изоляция городов друг от друга и полная блокада города Ухань, но и введение обязательных приложений для отслеживания на личных телефонах. Южная Корея отправляла подробные описания перемещений людей, подозреваемых в заражении, что вызывает серьёзные опасения по поводу конфиденциальности и точности данных.[47] Такая политика отслеживания отражает технологические возможности контроля перемещений, помогая прогнозировать распространение таких инфекционных заболеваний, как коронавирус. Тем не менее они применялись, на фоне опасений по поводу внутренней безопасности, частной жизни и возможного использования правительственными и неправительственными организациями, особенно с учетом региональных и геополитических трансформаций, вызванных пандемией COVID-19.

Европейская комиссия в 2020 г. объявила о намерении отслеживать перемещение граждан с помощью мобильных технологий. Европейский комиссар по внутреннему рынку и услугам Тьери Бретон заверил, что план ЕС не ставит целью контролировать людей, данные останутся анонимными и будут удалены после пандемии. Европейский инспектор по защите данных заявил, что это решение не нарушает правил конфиденциальности. Vodafone, Deutsche Telekom, Orange, Telefonica, Telecom Italia, Telenor, Telia и A1 Telekom Austria согласились предоставить данные. В Германии такое

[46] Stefan Meister, “The ‘Lisa Case’: Germany as a Target of Russian Disinformation,” *NATO Review*, July 25, 2016, https://www.nato.int/docu/review/2016/Also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm; Howard et al., “The IRA, Social Media and Political Polarization.”

[47] Олег Мавеичев, «Что получил Китай за три последних месяца», *LiveJournal*, 20 марта 2020, https://matveychev-oleg.livejournal.com/9896483.html.

наблюдение запрещено законом. Тем не менее пандемия COVID-19 вызвала дискуссию о необходимости затронуть фундаментальные права граждан, особенно со стороны государства, которое уже вводит существенные ограничения на свободу передвижения. Министр здравоохранения Германии Йенс Шпан был первым, кто предложил собирать данные с мобильных телефонов инфицированных людей.[48]

Deutsche Telekom уже предоставил Институту Роберта Коха (RKI) информацию о миллионах своих клиентов. RKI специализируется на изучении инфекционных заболеваний и принимал активное участие в обсуждении информационной политики при пандемии COVID-19. Вирусологи RKI хотели составить карты перемещения жителей Германии и понять, как долго люди в городских условиях подвергались воздействию вируса во время карантина, вызванного пандемией. Эта информация позволила более точно предсказать распространение инфекционных заболеваний, а также разработать систему быстрого расчёта всех социальных связей данного человека: с кем он контактировал, с кем путешествовал, где был и с кем общался.[49] Например, подобные системы массового наблюдения внедрены в таких странах, как Китай и Россия. В России премьер-министр Михаил Мишустин предложил отслеживать всех подозреваемых в заражении COVID-19 по геолокации их мобильных телефонов. Многие страны также предлагали новые программы эпиднадзора для лучшего планирования потребностей больниц и имеющихся ресурсов, но это требует существенного смягчения конфиденциальности медицинских данных и создаёт дилемму между конфиденциальностью, общественным благом и доверием к учреждениям, хранящим такую информацию.[50]

## Доверие, фейки и дезинформация

Вопрос доверия выходит за сферу деятельности отдельных правительств. В катастрофических ситуациях достоверная информация – всегда ценный ресурс, а в условиях длительного стресса люди более уязвимы к инсинуациям, слухам и намеренной дезинформации. Лёгкость распространения такой дезинформации по миру существенно повышают современные информационные сети, от мессенджеров до соцсетей. Пандемия COVID-19 создала благоприятную почву для появления и распространения теорий заговора. Когда информации недостаточно, а неопределённость высока, вакуум

[48] Foo Yun Chee, “Vodafone, Deutsche Telekom, 6 Other Telcos to Help EU Track Virus,” *Reuters*, Technology News, March 25, 2020, по состоянию на 1 апреля 2020, https://uk.reuters.com/article/us-health-coronavirus-telecoms-eu/vodafone-deutsche-telekom-6-other-telcos-to-help-eu-track-virus-idUKKBN21C36G.

[49] “Geolocation Surveillance: What Is Allowed in Germany for the Fight Against Coronavirus,” *DW Made for Minds Journal*, April 2020.

[50] Radu Mîrza, “COVID-19 and Digital Rights in Romania, Moldova and Ukraine,” *Central and Eastern European EDem and EGov Days* 341 (March 2022): 195-211, https://doi.org/10.24989/ocg.v341.14.

легко заполняет дезинформация и истории, которые невозможно проверить.[51] Коронавирус несёт особые проблемы, связанные с дезинформацией: долгий инкубационный период, возможность передачи бессимптомными носителями, зарубежное происхождение вируса в сочетании с дилеммой политики общественного здравоохранения, которая может оказаться отрицательной. Примерные прогнозы потенциальных смертей могут быть изменены из-за значительного социального дистанцирования, а первоначальные оценки – завышены. Экономические издержки более очевидны и непосредственны, в то время как выгоды для общественного здравоохранения в значительной степени эфемерны, пока они не исчезают.[52]

Одна из главных баек о коронавирусе заключалась в том, что он создан искусственно в лаборатории некой страны. Спор 2019 г. о китайском учёном из Национальной микробиологической лаборатории в Виннипеге послужил основой для измышлений о том, что правительство Канады создало вирус, который затем украл и распространил китайский учёный.[53] Спор Канады с китайской телекоммуникационной компанией Huawei тоже стал частью теории заговора, согласно которой вирус распространяют сети 5G. Заговор 5G, проявившийся в Великобритании, вылился в многочисленные нападения на вышки сотовой связи.[54] Во многих странах в 2020-2022 гг. циркулировала разнообразная информация о пандемии со значительными неточностями и ложными сведениями/ дезинформацией.[55] Эта часто противоречивая информация звучала на многих официальных брифингах и в новостях почти обо всех аспектах COVID-19.[56]

Противоречивые сообщения о реакции государства, информация и комментарии СМИ практически во всех странах создали серьёзную путаницу в отношении масштаба рисков пандемии, с резкими расхождениями по поводу опасности вируса. Звучали утверждения о том, что некоторые деятели используют средства массовой информации для сговора, чтобы подорвать

---

[51] Sally McManus, Joanna D'Ardenne, and Simon Wessely, "Covid Conspiracies: Misleading Evidence Can Be More Damaging Than no Evidence at All," *Psychological Medicine*, no. 1-2 (2020), https://doi.org/10.1017/S0033291720002184.

[52] Edward Lucas, "Mutations of Misinformation," *Tyzhden.ua*, March 1, 2020, по состоянию на 5 апреля 2020, https://tyzhden.ua/Columns/50/240946.

[53] Dax Gerts et al., "'Thought I'd Share First' and Other Conspiracy Theory Tweets from the COVID-19 Infodemic: Exploratory Study," *JMIR Public Health and Surveillance* 7, no. 4 (April 2021): e26527, https://doi.org/10.2196/26527.

[54] Takele T. Desta and Tewodros Mulugeta, "Living with COVID-19-Triggered Pseudoscience and Conspiracies," *International Journal of Public Health* 65, no. 6 (2020): 713-714, https://doi.org/10.1007/s00038-020-01412-4.

[55] Sahil Loomba et al., "Measuring the Impact of COVID-19 Vaccine Misinformation on Vaccination Intent in the UK and USA," *Nature Human Behaviour* 5, no. 3 (2021): 337-348, https://doi.org/10.1038/s41562-021-01056-1.

[56] Emily Chen et al., "COVID-19 Misinformation and the 2020 U.S. Presidential Election," *Harvard Kennedy School (HKS) Misinformation Review*, March 3, 2021, https://doi.org/10.37016/mr-2020-57.

авторитет определённых политиков или медицинских специалистов, и что утверждения о возможном заражении и смерти от COVID-19 сильно преувеличены. Такие схемы дезинформации в Украине не просто сеяли стресс и неуверенность. Можно вспомнить хотя бы яростные протесты в Украине, разразившиеся в феврале 2020 г. из-за ложной информации о рисках распространения вируса гражданами, возвращающимися из Китая. Дезинформация о пандемии распространялась в соцсетях в Украине в 2020-2021 гг. и серьёзно подрывала действия правительства.

Поэтому дезинформацию планируют так, чтобы множить неопределённость и сеять сомнения. Тексты и сообщения часто подаются в доверительной форме, с обращением к близкому другу. Обычно они содержат всю информацию о том, что может заинтересовать получателя, включая призыв к действию. Людям говорят, что делать, чтобы защитить себя; их также просят распространить эту «секретную» бесценную информацию, чтобы помочь как можно большему числу людей. Такие сообщения часто мотивируют тем, что власти якобы скрывают пути решения проблемы пандемии или её происхождение. Источник информации обычно не указывают, ссылаясь на эксперта или знакомого. Информация может исходить как от иностранцев, планирующих спровоцировать беспорядки, так и от сограждан, финансово заинтересованных в распространении дезинформации. В 2020 г. усилия КНР по дезинформации заметно сместились в сторону индивидуальных пользователей телефонных мессенджеров в США, в частности, для распространения дезинформации о COVID.[57]

Кампании дезинформации не только влекут долгосрочные последствия для отдельных лиц, которые могут творить зло, но и наносят ущерб социальной и политической структуре, когда невозможно отличить достоверную информацию от ложной. Информационные технологии децентрализации источников новостей делают быстрое распространение ложной информации практически неконтролируемым и труднопреодолимым. После чернобыльской катастрофы 1986 г. в Украине часто говорили, что сотни людей погибли от радиации, а тысячи – от информации. Во время пандемии трудно подсчитать число жертв неточной информации, лжи или дезинформации, но по самым скромным оценкам, тысячи жизней можно было бы спасти при более своевременном вмешательстве правительства и действиях системы здравоохранения.[58]

Столь сильное киберинформационное воздействие у многих вызывает

---

[57] Edward Wong, Matthew Rosenberg, and Julian E. Barnes, “Chinese Operatives Helped Sow Panic in U.S., Officials Say,” *The New York Times*, April 23, 2020, A10.

[58] Nicholas Charron, Victor Lapuente, and Andrés Rodriguez-Pose, “Uncooperative Society, Uncooperative Politics or Both? How Trust, Polarization and Populism Explain Excess Mortality for COVID-19 across European Regions,” The QoG Institute Working Paper 12 (Göteborg, Sweden: The Quality of Government Institute, Department of Political Science, University of Gothenburg, December 2020), http://hdl.handle.net/2077/67189.

стрессовое состояние, сохраняющееся длительное время с разной интенсивностью. Данное состояние можно охарактеризовать как «пандемический информационный стресс», который в дальнейшем может претерпеть различные психосоматические изменения: посттравматическое стрессовое расстройство (ПТСР), развитие тревожно-депрессивных состояний, приступы паники, формирование фобий и последствия обсессивно-компульсивных расстройств. На их появление и развитие существенно влияют состояние экономики, угроза снижения уровня жизни, безработица и неуверенность в будущем.[59] Глобальной тенденцией стало тиражирование ложной информации в социальных сетях, распространение фото и видео без понятного контекста, но с чёткой эмоциональной направленностью, достоверность которых сложно оценить при просмотре. Во время пандемии подобные информационные воздействия влекут особо тяжкие социальные последствия и становятся мощным инструментом гибридной войны.

## Киберпреступность и шпионаж

Связанная, но отдельная проблема – рост киберпреступности. Некоторые преступления прямо связаны с медицинскими учреждениями и их информационными системами. Например, преступники ищут информацию о лекарствах, испытаниях или вакцинах от короновируса для продажи на чёрном рынке. Ещё одной тенденцией является оборот поддельных так называемых лекарств от коронавируса на открытом рынке, учитывая всеобщую осведомленность о вирусе и сильное желание избежать заражения. Кроме того, деструктивные кибердействия направлены на взлом лечебных учреждений и кражу конфиденциальных данных. Также были попытки шифровать большие объёмы важных медицинских данных для получения выкупа за их восстановление. Пандемия сделала больницы, научные центры и университеты беззащитными перед организованными киберпреступниками. Атакам подверглись университетская больница в Брно (Чехия) – крупный центр тестирования на COVID-19, британская компания Hammersmith Medicines Research, разрабатывающая вакцины от COVID-19, парижская больница AP-HP и ряд испанских больниц. Кроме того, Всемирная организация здравоохранения (ВОЗ) предупредила о подозрительных электронных письмах, полученных от злоумышленников, пытавшихся воспользоваться чрезвычайной ситуацией для кражи денег и конфиденциальной информации, а также о попытках взлома компьютерных систем ВОЗ и её базы данных по коронавирусу.[60] Президент Еврокомиссии Урсула фон дер Ляйен

[59] Ali Farooq, Samuli Laato, and AKM Najmul Islam, “Impact of Online Information on Self-Isolation Intention during the COVID-19 Pandemic: Cross-Sectional Study,” *Journal of Medical Internet Research* 22, no. 5 (2020): e19128, https://doi.org/10.2196/19128.

[60] World Health Organization, “Beware of Criminals Pretending to be WHO,” April 2020, по состоянию на 5 апреля 2020, https://www.who.int/about/cyber-security.

предупредила, что в ЕС выросла киберпреступность из-за вспышки коронавируса. «Они следят за нами в Интернете и используют наш страх коронавируса. Наш страх – это их бизнес-возможность», – пишет EU Observer.[61]

Внезапный переход к удаленной работе и банковскому обслуживанию также подвергает многих людей опасности воровства через финансовые системы или коммерческие и промышленные сети, никогда не предназначавшиеся для широкого распространения. Эксперты по кибербезопасности опасаются, что предприятия будут использовать упрощенные методы обеспечения сетевой безопасности, чтобы сохранить прибыль во время серьёзного экономического спада. Коммерческая и промышленная информация будет передаваться через частные сети и на персональные компьютеры, а служба информационной безопасности не сможет контролировать использование этих открытых сетей. В странах, которые до пандемии уже подвергались риску промышленного шпионажа, киберпреступники и посторонние лица обязательно увидят открывшиеся им возможности.[62]

## Образование и переход к электронному обучению

Образование – ещё один важный вопрос, прямо связанный с пандемией и кибер-социальными уязвимостями в условиях гибридной войны. Из-за связанного с COVID карантина произошли глубокие изменения в установившемся ритме жизни, работы и обучения всех групп населения почти во всех странах. Человечество впервые столкнулось с пандемией такого уровня в условиях высокотехнологического информационного общества, глобализации и доступности поездок по всему миру. В одночасье были нарушены бизнес, туризм, миграция и мобильность населения. Вынужденный, реальный, быстрый и массовый переход к электронному обучению во всех сферах и на всех уровнях образования стал стрессом для всех участников образовательного процесса, которым пришлось в спешном порядке осваивать новые инструменты и методы.

Образование в условиях пандемии стало стратегической проблемой с далеко идущими последствиями для всего мира. Генеральный секретарь ООН Антониу Гутерреш отметил, что около миллиарда студентов и школьников в 160 странах мира не могли получить полноценное образование из-за закрытия учебных заведений, вызванного эпидемией коронавируса. Это грозит миру «катастрофой поколений». Согласно опросам, проведенным в Украине в июле 2020 г., и оценкам Госслужбы качества образования Украины, электронное обучение в школах не поддерживают 48 % родителей и

---

[61] "The EU Recorded a Sharp Increase of Cybercrime: What Is Happening," *Informacionnoe Soprotivlenie*, March 25, 2020, по состоянию на 1 апреля 2020, https://sprotyv.info/analitica/v-es-zafiksirovali-rezkij-rost-kiberprestupnosti-chto-proishodit.

[62] Eduard Babulak, James C. Hyatt, Kim Kyu Seok, and Jang Sun Ju, "COVID-19 & Cyber Security Challenges US, Canada & Korea," *Transactions on Machine Learning and Data Mining* 13, no. 1 (2020): 43-59, http://www.ibai-publishing.org/journal/issue_mldm/2020_October/13_2_43_59_mldm.pdf.

45 % учащихся, а «полностью поддерживают» электронное обучение лишь 9,9 % опрошенных.[63]

Проблемы заключаются не только в сути электронного обучения, но и в связанных с ним социотехнических противоречиях и киберсоциальных уязвимостях. Электронное обучение многогранно и междисциплинарно. Проблема включает технические, социальные, демографические, психологические, содержательно-информационные, методологические, дидактические, организационные, кибернетические и иные аспекты, а также способность правительств готовить кадры для планирования и проведения электронного обучения. Студенты должны уметь правильно и эффективно использовать технологии и беречь психическое и физическое здоровье в условиях неопределённости и стресса.

Проблемы образования, возникшие в условиях гибридного противостояния и пандемии, напрямую затрагивают все сферы функционирования государства и национальной безопасности. В целом это вопрос судьбы государства и государственности, их дальнейшего существования и развития. В отсутствие государственного контроля и регулирования электронное обучение потенциально может привести не только к усилению неравенства в образовании и потере человеческого потенциала, но и к опасным изменениям в обработке информации, критическом мышлении и зависимости от соцсетей. Это может сделать их уязвимыми для когнитивных и эмоциональных методов кибервойны.

Пандемия породила спрос на официальные стандарты электронного обучения специалистов и разработку курсов электронного обучения, которые помогут оценить эффективность электронного обучения и продвигать системный подход в новом режиме образования в разных странах, от США до Украины. Это означает, что электронное обучение требует стандартизации, систематизации и стратегических подходов для обеспечения эффективного дистанционного образования, одновременно предоставляя ресурсы для достижения целей на тактическом институциональном уровне. Пандемия рано или поздно закончится, но образование (гражданское, государственное и военное) вряд ли вернется к прежнему состоянию, и необходимо учитывать последствия этого для национальной безопасности. COVID-19 вызвал глубокие резкие изменения в обществе, и наша зависимость от технологий требует от государства разумных политических решений, касающихся не только реагирования на сам вирус, но и признания уязвимостей, создаваемых технологиями.

---

[63] Yuriy Danyk and Tamara Maliarchuk,“Strategic Aspects and Problems of E-learning in the Context of Pandemic and National Security,” *S-Direct 24* 3, no. 14 (July 2020), International scientific journal published under the auspices of NATO Defence Education Enhancement Program.

## Заключение

Цель этой статьи – показать главные проблемы, созданные гибридной войной и COVID-19, и возможные пути их решения в киберпространстве, общественной жизни и национальной безопасности, охватывающие все сферы деятельности государства. Использование кибер-социальных уязвимостей играет важную и всё возрастающую роль в гибридных конфликтах. Создание эффективной национальной системы кибербезопасности и киберзащиты государства, включая характеристики кибер-социальных уязвимостей – один из главных приоритетов национальной безопасности и обороны. Эффективное заблаговременное предупреждение о кибер-социальных уязвимостях требует анализа структуры и параметров киберсистем и их пользователей и понимания того, как распространяются, принимаются и воспроизводятся сообщения в киберсистемах. Стратегии повышения устойчивости информационных систем опираются не только на модели «крепости» от злоумышленников, но и на готовность населения к уловкам, взломам и кампаниям дезинформации изнутри и извне.

Главной стратегической целью гибридной войны представляется дестабилизация – т.е. не физическая оккупация территории, а недоверие к институтам и самой информации. Такие атаки разрушают не только критическую инфраструктуру, но и общество. Установлено, что основные разрушительные кибердействия были выборочными и нацеленными на уязвимые киберсоциальные элементы. Разрушительные целенаправленные кибератаки проводились в рамках крупномасштабных комплексных кибероперациий.

Главные проблемы, возникшие или проявившиеся в связи с пандемией COVID-19 в контексте гибридной войны, таковы:

- Недостаточная готовность кибер-общественных систем здравоохранения большинства стран;
- Глубокая перестройка национальных экономик из-за реагирования на COVID-19 и формирования новых моделей жизни общества;
- Быстрое и полное погружение населения в киберпространство и переход к дистанционным (удалённым) формам работы и учёбы;
- Рост активности в соцсетях, увеличение объёмов онлайн-торговли, развлечений и услуг (дистанционная медицина, электронное обучение, электронное банковское обслуживание);
- Рост числа разнообразных киберпреступлений, распространение фейковых новостей, связанных с пандемией, дезинформация и информационное перенасыщение общества;
- Недостаточная киберинформационная грамотность, неумение или нежелание использовать интернет-системы и информационные технологии в повседневной жизни, а также неспособность обеспечить кибернетическую и информационную безопасность, особенно в условиях глобальной гибридной войны.

Хотя ранее мы уже говорили о развёртывании кибер-гибридных войн, пандемия COVID-19 усилила действия и уязвимости, связанные с конфиденциальностью, изоляцией, затруднением идентификации и распространением дезинформации.[64] Пандемия привела к усилению присутствия дестабилизирующих факторов в жизни людей, повышению зависимости от виртуальной информации, из-за разрыва традиционных социальных связей, а также росту зависимости от кибертехнологий во всех областях жизнедеятельности.

Особого внимания заслуживает введение контроля за соблюдением требований карантина с применением высоких технологий. Непринятие своевременных мер предосторожности для защиты прав граждан может привести к посягательству на конфиденциальность личной информации. Есть основания ожидать, что такой контроль и надзор за гражданами и их деятельностью во многих странах, особенно с авторитарными режимами, может не только сохраниться, но и усилиться после того, как утихнет пандемия. Такое развитие событий представляет угрозу для собственной страны и даёт возможность внешним игрокам использовать такие системы «социального кредита» в своих интересах. Чем больше мы зависим от таких технологий, тем больше уязвимостей позволяют использовать такие связи, сейчас в основном независимые от традиционной социальной устойчивости. Каковы последствия для безопасности, если посторонние меняют медицинские записи, вносят людей в списки не допущенных к полётам или подделывают их личность не только для подачи заявки на получение кредита, но и в мировых средствах массовой информации?

Пандемия COVID-19 потрясла мировую систему не только с точки зрения экономической активности и поездок за рубеж, но и в том, как мы относимся к технологиям, измеряем и ценим социальную и политическую стабильность, а также наши способности реагировать на спектр атак гибридной войны с использованием кибертехнологий и уязвимостей. Наши общества становятся всё более уязвимыми для когнитивной и эмоциональной войны, которая подавляет обработку нами информации, обходит рациональное мышление и поражает нас на базовом уровне «выживания», часто – в рамках стратегии, направленной на дальнейшее разделение наших обществ и недоверие к институтам. Хотя мы давно ожидали роста значимости кибергибридной войны, сейчас нужно устранить недостатки в дезинформации, конфиденциальности, киберпреступности и электронном обучении, которые могут повлиять на более важные вопросы безопасности и стабильности.

Таким образом, данное исследование помогает дать определение кибервойны или киберконфликта в киберпространстве. Противостояние в ки-

[64] Tamara Maliarchuk, Yuriy Danyk, and Chad Briggs, “Hybrid Warfare and Cyber Effects in Energy Infrastructure,” *Connections: The Quarterly Journal* 18, no. 1-2 (2019): 93-110, https://doi.org/10.11610/Connections.18.1-2.06.

берпространстве и (или) при помощи киберпространства – это сложное социально-политическое явление с использованием киберразведки, киберзащиты и кибероружия для нанесения противнику различных потерь в разных областях и минимизации собственных потерь в экономической, военной, политической, социальной, кибернетической, информационной, идеологической и других сферах. В отличие от других деструктивных действий, конфликтов и (или) войн, кибервойну (киберконфликт, деструктивные кибердействия) не объявляют. И если она началась, она не закончится, но будет продолжаться непрерывно до тех пор, пока одна из сторон конфликта не будет полностью разгромлена либо не сможет продолжать разрушительные действия. Она может завершиться только с уничтожением киберпространства.

Хотя военные стратегии по-прежнему действуют, удар всё чаще наносят «под дых» обществу.

## Примечание

Представленные здесь взгляды принадлежат исключительно авторам и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

## Об авторах

Д-р **Чэд Бриггс** – доцент, руководитель кафедры государственной политики и управления Университета Аляски в Анкоридже. Д-р Бриггс имеет опыт информационной и гибридной войны, а также разработки оборонительных стратегий защиты критически важных систем в Восточной Европе и на Балканах. Имеет степень доктора политологии Карлтонского университета в Канаде. Ранее был старшим советником Министерства энергетики США, зав. кафедрой «Минерва» и профессором энергетической и экологической безопасности Авиационного университета ВВС США. Соавтор (совместно с Мириам Матеёвой) труда *Disaster Security: Using Intelligence and Military Planning for Energy and Environmental Risks*.
*Электронная почта*: chad.briggs@alaska.edu

Генерал-майор **Юрий Даныk**, профессор, доктор технических наук, Национальный технический университет Украины «Киевский политехнический институт имени Игоря Сикорского». Д-р Даник является экспертом в области военного искусства, национальной обороны и безопасности, информационной и кибербезопасности, электронных и информационных технологий, разработки и применения робототехнических комплексов, а также развития сил специального назначения. Имеет боевой опыт применения передовых оборонных технологий в условиях современной войны.
*Электронная почта*: zhvinau@ukr.net

Д-р **Тамара Малярчук** была членом рабочей группы НАТО по реализации программы DEEP в Вооружённых силах Украины. Была аналитиком Житомирского военного института им. С. Королева (Украина) и сотрудничала с ВС США по вопросам языковой и кибернетической защиты. Занимается исследованиями в области электронного обучения, инновационных технологий обнаружения и терапии посттравматического стрессового расстройства, а также манипулятивных сетевых технологий.
*Электронная почта*: maliarchuktamara@gmail.com

*Connections: The Quarterly Journal*
**ISSN 1812-1101, e-ISSN 1812-2973**

Я. Тодоров, *Connections QJ* 20, № 3-4 (2021): 63-83
https://doi.org/10.11610/Connections.rus.20.3-4.04

**Рецензированная статья**

# Кибер(без)опасность на море: Растущая угроза странам ЕС

## *Явор Тодоров*

*Докторант Военно-морской академии Болгарии, http://www.naval-acad.bg/*

**Аннотация**: Широкое применение передовых информационно-коммуникационных технологий на судах, в портах, в управлении движением и грузами повышает их эффективность, но одновременно создает уязвимости. Разного рода злоумышленники готовы воспользоваться доступом в киберпространстве для получения выгоды. В этой статье мы рассмотрим киберриски и угрозы в морской киберсфере и проанализируем действующие европейские, американские и международные нормы, стандарты и механизмы, направленные на укрепление кибербезопасности. Автор выделяет шесть направлений усилий в области обмена информацией, повышения осведомленности, сертификации и стойкости.

**Ключевые слова**: безопасность на море, вызовы кибербезопасности, нормы, гармонизация, правовая база, обмен информацией, информированность, обучение, стойкость.

*Мир изменился. Я чувствую это в воде, вижу в земле, ощущаю в воздухе. Многое из того, что было – ушло.*[1]

## Вступление

За последние 10 лет морской сектор существенно вырос. Сейчас это обширная, тесно связанная сеть грузовых судов, нефтетанкеров, химовозов, контейнеровозов, пассажирских судов, страховых компаний, морских и береговых операторов, национальных и международных органов, военных флотов, служб навигации и управления на море, спутниковых систем, систем связи. Сегодня морская сфера прямо влияет на экономическую, политическую и демографическую динамику в мире.

[1] Джон Рональд Руэл Толкин, «Властелин колец: Братство кольца».

Катастрофы на море – не редкость. Ещё в 1912 г. затонул «Титаник», унеся 1 517 жизней. С ростом применения информационно-коммуникационных технологий (ИКТ) в морской сфере вероятность катастроф возрастает в геометрической прогрессии. Эти технологии обеспечивают основные услуги судоходства, такие как навигация, контроль двигателей, контроль доступа, развлечения, связь и управление экипажем. Но компьютеризация увеличивает такие риски, как остановка портов или судов, манипулирование основными услугами, а также массовые разрушения, беспорядки и гибель людей. Эти риски затрагивают всех – частные компании, правительства, отдельных граждан. Как отметила президент и главный исполнительный директор Палаты судоходства США Кэти Меткаф, морская отрасль остается уязвимой к кибератакам, которые могут спровоцировать катастрофические события, например, захват судна и таран моста Верразано-Нэрроуз.[2] Эта опасность подтверждается ростом кибератак в морской сфере на 400 % в 2020 г.[3]

Кибербезопасность на море регулируется многочисленными международными и национальными государственными и частными органами, включая Международную морскую организацию (ММО), Агентство кибербезопасности Европейского Союза (ENISA) и Балтийский и международный морской совет (BIMCO). К сожалению, эти организации не обладают достаточными техническими и кадровыми возможностями для внедрения, сертификации и мониторинга системы кибербезопасности судоходства. Нет у них и адекватной политики и процедур обеспечения соблюдения конкретных требований.

Нынешняя нормативная база не способна минимизировать риски и угрозы, прежде всего из-за разнобоя существующих стандартов кибербезопасности и процедур контроля морского сектора. Международный кодекс управления безопасностью ММО, Указания ММО по управлению морскими киберрисками, соответствующие директивы ЕС и национальные нормы слишком широки, и операторы не могут построить надёжную систему кибербезопасности судоходства.

Ещё одна проблема заключается в отсутствии стандарта протоколов кибербезопасности для судов разных стран. Это связано с количеством судов, работающих в разных условиях под флагами разных стран. Эти суда, как правило, следуют минимальным существующим стандартам, игнорируя требования национальных морских властей.[4]

---

[2] John Grady, "Experts: Maritime Industry Remains Vulnerable to Cyber Attacks," *USNI News*, September 28, 2020, https://news.usni.org/2020/09/28/experts-maritime-industry-remains-vulnerable-to-cyber-attacks.

[3] "Greater Cyber Security Needed for Coronavirus and Economic Crises," *Hellenic Shipping News*, May 6, 2020, https://www.hellenicshippingnews.com/greater-cyber-security-needed-for-coronavirus-and-economic-crises/.

[4] Jeff Spivey, "Security by Design," *United States Cybersecurity Magazine* (Fall 2017), https://www.uscybersecurity.net/csmag/security-by-design/.

Информационная система многих судов построена по принципу «конструктивной кибербезопасности». Согласно этой модели, кибербезопасность корабля планируется с самого начала проектирования и учитывается на каждом этапе строительства. Но этот «конструктивный» подход обеспечивает предупреждение и предотвращение, а не исправление и восстановление после инцидента.[5] Поскольку нынешние векторы атак многомерны, и для проникновения в системы используются самые современные инструменты, эта модель создает значительные риски и проблемы для судоходной отрасли.[6]

Многочисленные поставщики различного оборудования и услуг позволяют каждому подрядчику использовать свои средства защиты, что усложняет гармонизацию. Тот же принцип используется и в общедоступных системах, необходимые для идентификации и определения местонахождения терпящего бедствие судна.[7]

Вероятность срыва судоходства при помощи кибератак высока и чревата катастрофическим ущербом судам и критической инфраструктуре. Важно повышать информированность судовладельцев, экипажей и компетентных органов о морской кибербезопасности. Ниже приведены обоснованные рекомендации по совершенствованию международных правил, политики и принципов международной кибербезопасности на море для решения существующих проблем кибербезопасности.

## Нынешнее положение дел на море

Значение портов для экономики Европейского Союза (ЕС) и всего мира возрастает. Это главные перекрёстки мировой торговли – на них приходится примерно три четверти торговли товарами ЕС с третьими странами и больше трети грузоперевозок внутри ЕС.[8]

С 1970 г. мировая морская торговля стабильно растёт как в объёме, так и по размеру судов. Конференция Организации Объединённых Наций по торговле и развитию (ЮНКТАД) ожидает роста объёмов морской торговли на 2,4 % в год до 2030 г. Примерно две трети мировой торговли товарами приходится на развивающиеся страны, что составляет 60 % мировых грузоперевозок. Больша́я часть этого роста пришлась на Восточную Азию, особенно

---

5 Reciprocity, “What is Security by Design?” *Reciprocity*, March 7, 2020, https://reciprocity.com/resources/what-is-security-by-design/.

6 Rory Hopcraft and Keith M. Martin, “Effective Maritime Cybersecurity Regulation – the Case for a Cyber Code,” *Journal of the Indian Ocean Region* 14, no. 3 (2018): 354-366, http://doi.org/10.1080/19480881.2018.1519056.

7 Hopcraft and Martin, “Effective Maritime Cybersecurity Regulation.”

8 Boyan Mednikarov, Yuliyan Tsonev, and Andon Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry,” *Information & Security: An International Journal* 47, no. 1 (2020): 27-43, https://doi.org/10.11610/isij.4702.

Китай. Так же быстро растут объёмы на Транстихоокеанском торговом пути, связывающем Восточную Азию с Северной Америкой.[9]

### *Анализ кибербезопасности на море*

Прогресс в мореплавании существенно зависит от технических инноваций судовых цифровых систем. Постоянно растёт важность информационных систем, поскольку они обеспечивают связь и принятие решений, повышают видимость, эффективность и надежность, укрепляют безопасность морских перевозок в различных условиях.

| Год | Танкеры | Балкеровозы | Другие сухогрузы | Всего (все грузы) |
|---|---|---|---|---|
| 1970 | 1 440 | 448 | 717 | 2 605 |
| 1980 | 1 871 | 608 | 1 225 | 3 704 |
| 1990 | 1 755 | 988 | 1 265 | 4 008 |
| 2000 | 2 163 | 1 186 | 2 635 | 5 984 |
| 2005 | 2 422 | 1 579 | 3 108 | 7 109 |
| 2006 | 2 698 | 1 676 | 3 328 | 7 702 |
| 2007 | 2 747 | 1 811 | 3 478 | 8 036 |
| 2008 | 2 742 | 1 911 | 3 578 | 8 231 |
| 2009 | 2 641 | 1 998 | 3 218 | 7 857 |
| 2010 | 2 752 | 2 232 | 3 423 | 8 408 |
| 2011 | 2 785 | 2 364 | 3 626 | 8 775 |
| 2012 | 2 840 | 2 564 | 3 791 | 9 195 |
| 2013 | 2 828 | 2 734 | 3 951 | 9 513 |
| 2014 | 2 825 | 2 964 | 4 054 | 9 842 |
| 2015 | 2 932 | 2 930 | 4 161 | 10 023 |
| 2016 | 3 058 | 3 009 | 4 228 | 10 295 |
| 2017 | 3 146 | 3 151 | 4 419 | 10 716 |
| 2018 | 3 201 | 3 215 | 4 603 | 11 019 |
| 2019 | 3 163 | 3 218 | 4 690 | 11 071 |
| 2020 | 2 918 | 3 181 | 4 549 | 10 648 |

**Рис. 1: Международная морская торговля, 1970-2020 гг.**[10]

В 2017 г. крупное событие изменило подход правительств и частного сектора к системам кибербезопасности судоходства и портов. В июне хакеры, работавшие на российскую военную службу безопасности, отправили программу-вымогатель *NotPetya* на объекты критической инфраструктуры. Воспользовавшись уязвимостями крупнейшего в мире судоходного конгломе-

[9] United Nations Conference on Trade and Development (UNCTAD), *Review of Maritime Transport 2021* (United Nations, 2021), https://unctad.org/webflyer/review-maritime-transport-2021.

[10] UNCTAD, *Review of Maritime Transport*.

рата Maersk, хакеры нарушили работу Глобальной системы морского транспорта.[11]

После этой атаки ММО выпустила Указания по управлению морскими киберрисками.[12] В Указаниях содержатся рекомендации касательно основных услуг судоходства, как то: мостовые системы, погрузочно-разгрузочные работы, системы управления, двигательные установки, системы питания, системы контроля доступа, пассажирское обслуживание, системы связи.[13] Для этих услуг используются следующие платформы:

- ECDIS (электронная система отображения графических данных и информации);
- AIS (система автоматической идентификации);
- Radar/ARPA (средства радиопеленгации, определения расстояния, радиолокационный автопрокладчик курса);
- Гирокомпас;
- Рулевое управление (компьютеризованная система автоматического управления курсом);
- VDR (морской маршрутный самописец);
- GMDSS (Глобальная система оповещения о бедствиях и обеспечения безопасности на море);
- ESD (системы аварийного отключения).

Технический анализ выявил следующие уязвимости некоторых из этих систем (Таблица 2).[14]

Кроме того, многие новые программы несовместимы с используемым оборудованием. Наиболее распространенной операционной системой на торговых судах является Windows XP, хотя срок её поддержки Microsoft истёк в 2014 г. В 2015 г. проведенное в США исследование показало, что 37 % серверов не обновлялись и считались потенциально уязвимыми для кибератак.[15] В 2020 г. были получены схожие цифры, поскольку главное судовое оборудование не менялось.

---

[11] Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyber attack-ukraine-russia-code-crashed-the-world/.

[12] International Maritime Organization (IMO), “Maritime Cyber Risk,” www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[13] IMO, “Maritime Cyber Risk.”

[14] Mednikarov, Tsonev, and Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry.”

[15] Ms. Smith, “Maritime Cybersecurity Firm: 37% of Microsoft Servers on Ships Vulnerable to Hacking,” *CSO*, May 4, 2015, https://www.csoonline.com/article/2917856/maritime-cybersecurity-firm-37-of-microsoft-servers-not-patched-vulnerable-to-hacking.html.

**Таблица 2. Анализ угроз платформ судоходства** [16]

| Платформа | Применение | Уязвимость | Воздействие |
|---|---|---|---|
| **ECDIS** | Отображение навигационных карт | Отсутствие механизма идентификации | Изменение маршрута |
| **AIS, GMDSS** | Идентификация и оповещение о бедствии | Не имеет механизмов безопасности и проверки данных | Генерирование ложных команд AIS и изменение маршрута судна |
| **Системы аварийного отключения (ESD)** | Блокировка управления силовой установкой в чрезвычайной ситуации | Доступны с берега | Судовую машину можно остановить дистанционно |

Источник: Mednikarov et al., 2020.

Главные виды кибератак на суда с использованием существующих уязвимостей таковы:

- Фишинг – рассылка электронных сообщений на множество адресов с просьбой предоставить важную или конфиденциальную информацию. Такие атаки могут также спровоцировать пользователя обратиться к некоему ресурсу, открыв тем самым несанкционированный доступ к информационной инфраструктуре.
- Программы-вымогатели – действия, при которых вредоносный код шифрует хранящиеся в системе данные и требует выкуп за их расшифровку. Суда уязвимы к ним, поскольку у них отсутствуют планы проверки используемых файлов, а у большинства из них нет механизма проверки входящей и исходящей электронной почты.[17]
- Сканирование – процесс поиска уязвимостей в системе.
- Отказ в обслуживании – процесс, при котором трафик определенного количества удаленно управляемых компьютеров перегружает пропускную способность связи или прерывает доступ к определенному ресурсу или услуге.
- Атака на цепочку снабжения – процесс зловредного воздействия на системы судна через устройство, в которое внедрён хакерский код.
- Подмена GPS – процесс, при котором хакер вынуждает GPS-приёмник изменить отображение местоположения судна.

[16] Mednikarov, Tsonev, and Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry.”

[17] Mohamed Amine Ben Farah et al., “Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends,” *Information* 13, no. 1 (2022), 22, https://doi.org/10.3390/info13010022.

- Атака через посредника – процесс, при котором хакер может перехватывать обмен судна с берегом и воздействовать на него.

В Указаниях по кибербезопасности на борту [18] Балтийского и международного морского совета (BIMCO) описаны несколько типов источников киберугроз для судов. Первый из них – это активист. Его целью может быть, например, уничтожение или публикация конфиденциальных данных для привлечения внимания средств массовой информации или DoS (отказ в обслуживании) и кража интеллектуальной собственности.[19] Это может быть инсайдерская угроза, которая сорвёт обслуживание и испортит репутацию. Второй – преступники, стремящиеся получить финансовую выгоду посредством коммерческого и промышленного шпионажа. Их конечная цель – продажа и выкуп украденных данных, блокировка системы и организация мошеннических грузоперевозок. Третья группа, вероятно, самая опасная – это государственные субъекты, поддерживаемые государством, преследующим политические или военные цели, мешая работе судна или судоходной компании. Успешная кибератака может подорвать авторитет правительства или изменить политические цели и направленность действий государства.[20] Государственные субъекты, как правило, занимаются кражей конфиденциальных и секретных данных или воздействуют на важные услуги. Они имеют практически неограниченные ресурсы и могут идти к своей цели без ограничений во времени или получения финансовой прибыли. Среди примеров серьёзных нападений на государства – кибератака на избирательную систему в Эстонии в 2007 г.,[21] кибератаки во время русско-грузинской войны [22] и атаки DDoS на американские банки в 2013 г.[23]

Наиболее серьёзные примеры этих видов кибератак приведены в таблице ниже.

## Правовая база кибербезопасности на море

Для оценки факторов, приведших к нынешнему состоянию системы безопасности на море, сначала нужно проанализировать основы кибербезопасности на море. В этом разделе описаны особые проблемы кибербез опасности на море, связанные с отсутствием последовательной и эффектив-

[18] Baltic and International Maritime Council, 2020.

[19] IMO, “Maritime Cyber Risk.”

[20] IMO, “Maritime Cyber Risk.”

[21] Patrick Howell O’Neill, “The Cyberattack That Changed the World,” *Daily Dot*, May 20, 2016, https://www.dailydot.com/debug/web-war-cyberattack-russia-estonia/.

[22] “The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict,” *AFCEA*, May 24, 2012, https://www.afcea.org/committees/cyber/documents/therussogeorgianwar2008.pdf.

[23] Nicole Perlroth and Quentin Hardy, “Banking Hacking was the Work of Iranians, Officials Say,” *The New York Times*, January 8, 2013, https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

**Таблица 2. Основные примеры морских кибератак**

| Тип атаки | Год | Описание |
|---|---|---|
| **Вирус-вымогатель / фишинг** | 2021 | Ведущая судоходная компания Южной Кореи HMM: кибератака ограничила доступ к электронной почте [24] |
| **Вирус-вымогатель** | 2020 | Порт вблизи Ормузского пролива: попытка кибератаки повредила некоторые системы порта [25] |
| **Вредоносная программа** | 2020 | Mediterranean Shipping Company (MSC): из-за проблем с безопасностью были закрыты сервера MSC для защиты данных компании, в результате упал вебсайт компании [26] |
| **Вредоносная программа** | 2019 | Атака на американское судно с хищением важных учётных данных. Береговая охрана и ФБР сообщили, что атака стала возможной из-за отсутствия мер безопасности на судне: весь экипаж пользовался одним и тем же логином и паролем для доступа к судовому компьютеру. Задачу хакера упростило и применение внешних устройств. Ещё одна серьёзная ошибка — отсутствие антивирусных программ [27] |
| **Фишинг** | 2019 | Хакеры получили несанкционированный доступ к британской компании «James Fisher and Sons»[28] |
| **Вирус-вымогатель** | 2018 | Китайские хакеры атаковали подрядчиков ВМС США [29] |
| **Вирус-вымогатель Petya** | 2017 | Зашифрованная вредоносная программа поразила все услуги судоходной компании Maersk. Атака *Not-Petya* повредила компьютерные сервера в Европе и Индии. Атака уничтожила операционную систему компьютеров, инфицировав основной загрузочный |

[24] Naida Hakirevic Prevljak, "HMM Hit by Cyber Attack," *Offshore Energy*, June 15, 2021, https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/.

[25] Tzvi Joffre, "Cyber Attack Targets Iranian Port near Strait of Hormuz," *The Jerusalem Post*, May 11, 2020, https://www.jpost.com/breaking-news/cyber-attack-targets-iranian-port-near-strait-of-hormuz-627616.

[26] Marcus Hand, "MSC Confirms Malware Attack Caused Website Outage," *Seatrade Maritime News*, April 17, 2020, https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage.

[27] Davey Winder, "U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit by Cyberattack," *Forbes*, July 9, 2019, https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/.

[28] "Marine Firm James Fisher Reports Cyber Breach," *Reuters*, November 5, 2019, https://www.reuters.com/article/us-james-fisher-cybercrime-idUSKBN1XF1SQ.

[29] "China Hackers Steal Data from US Navy Contractor," *BBC*, 9 June 2018, https://www.bbc.com/news/world-us-canada-44421785.

| | | |
|---|---|---|
| | | сектор. Пострадали 17 контейнерных терминалов, убытки превысили 200 млн. долларов [30] |
| **Подмена GPS** | 2017 | Об атаке сообщила морская администрация США. GPS судна в порту Новороссийск (Россия) показывала неверное местоположение [31] |
| **Атака на систему навигации** | 2017 | Столкновение корабля ВМС США Fitzgerald с контейнеровозом, приведшее к смерти семи моряков (у побережья Японии) [32] |
| **Подмена GPS** | 2013 | Группе учёных Техасского университета удалось подменить сигнал GPS приёмника яхты [33] |

ной нормативной базы для минимизации рисков и угроз и повышения киберустойчивости. Тут же представлен общий обзор международно-правовой базы, а также нормы и правила ЕС и США.

### *Общий обзор основ международной кибербезопасности на море*

Меры безопасности на море, например, Международный кодекс по охране судов и портовых сооружений (ОСПС),[34] обычно принимались в ответ на крупные глобальные потрясения или катастрофы. В ответ на угрозы судам и портам в 2004 г. в соответствии с главой XI-2 Международной конвенции по охране человеческой жизни на море (Конвенция SOLAS) был принят Кодекс ОСПС, в котором признаётся важность портов для мировой безопасности и изложен набор обязательных инструментов и рекомендаций для судов и портовых сооружений.[35] Кодекс исходит из того, что обеспечение безопасности судов и портов является видом управления рисками. Хотя Кодекс и имеет отношение к кибербезопасности (например, меры контроля доступа и требования аутентификации), он прежде всего нацелен на обеспечение физической безопасности портовых сооружений.

Ещё одной важной международной нормой, тоже разработанной в рамках ММО, является Конвенция об облегчении международного морского

[30] Greenberg, “The Untold Story of NotPetya.”

[31] David Hambling, “Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon,” *NewScientist*, August 10, 2017, https://www.newscientist.com/ article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.

[32] Sam LaGrone, “7 Sailors Missing, CO Injured after Destroyer USS Fitzgerald Collided with Philippine Merchant Ship,” *USNI News*, June 16, 2017, https://news.usni.org/2017/06/16/destroyer-uss-fitzgerald-collides-japanese-merchant-ship.

[33] Brian Dodson, “University of Texas Team Takes Control of a Yacht by Spoofing Its GPS,” *New Atlas*, August 11, 2013, https://newatlas.com/gps-spoofing-yacht-control/28644.

[34] International Maritime Organization (IMO), “SOLAS XI-2 and the ISPS Code,” https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx.

[35] IMO, “SOLAS XI-2 and the ISPS Code.”

судоходства (FAL).[36] Эта конвенция, действующая с 1967 г., направлена на повышение эффективности морских перевозок. Она стандартизует формы обмена информацией в морских портах, особенно при связи портов с судами.[37] Для повышения действенности FAL в 2019 г. её обновили, добавив требование к государственным органам внедрить системы, обеспечивающие электронный обмен информацией между судами и портами.[38] Важным нововведением конвенции стало поощрение концепции «единого окна», при которой все заинтересованные стороны обмениваются данными через единую точку доступа. Её недостаток заключается в том, что если злоумышленник получит доступ к любой из точек входа, он получит доступ ко всей сети.

В 2017 г. ММО приняла резолюцию MSC.428(98) об управлении морскими киберрисками в системах управления безопасностью (СУБ).[39] В резолюции сказано, что утвержденная СУБ должна учитывать управление киберрисками в соответствии с целями и функциональными требованиями Международного кодекса управления безопасностью (ISM Code).[40] Она также призвала национальные органы обеспечить надлежащий учёт киберрисков в системах управления безопасностью в Документе о соответствии компании до 1 января 2021 г. Если они не устранены, судно считается небезопасным и рассматривается как морская угроза для мира.

Главным документом ММО, прямо касающимся кибербезопасности на море, является документ ММО под названием «Руководство по управлению морскими киберрисками» (MSC-FAL.1/ Circ.3), принятый на 41-й сессии Комитета FAL.[41] По сути, документ признаёт, что морская сфера нуждается в лучшем информировании о кибербезопасности и реализации конкретных рекомендаций для повышения киберустойчивости.[42] Руководство признаёт, что все участники морской отрасли индивидуальны. Поэтому каждый должен реализовать наиболее подходящие ему требования, введённые руководством страны регистрации. Руководство[43] также призывает соблю-

[36] International Maritime Organization (IMO), “FAL Convention,” 1967, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

[37] IMO, “FAL Convention,” 1967.

[38] International Maritime Organization (IMO), “FAL Convention,” 2017, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

[39] IMO, “Maritime Cyber Risk Management in Safety Management Systems,” Resolution MSC.428(98), adopted on June 16, 2017, https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf.

[40] IMO, *ISM Code: International Safety Management Code with Guidelines for Its Implementation* (London, UK: IMO Publishing, 2018).

[41] IMO, “Maritime Cyber Risk.”

[42] Akash Rana, “Commercial Maritime and Cyber Risk Management,” *Safety & Defense* 5, no. 1 (2019):46-48, https://doi.org/10.37105/sd.42.

[43] IMO, “Maritime Cyber Risk.”

дать международные стандарты безопасности, в частности, ISO/IEC 27001,[44] где изложены требования к системе информационной безопасности. В Руководстве принят к сведению передовой опыт отрасли и упомянуты пять элементов: идентификация, защита, обнаружение, реагирование и восстановление. Новым в этом правиле стала возможность признания судна непригодным, если рекомендации не будут выполнены.[45] Хотя Руководство ММО по управлению морскими киберрисками содержит рекомендации по защите судов от существующих киберрисков и угроз, там нет конкретных указаний об обеспечении безопасности каналов связи между портом и судном. Ещё одна серьёзная проблема заключается в том, что контроль реализации возложен на страну регистрации и национальные морские власти.[46]

Для повышения совместимости ММО совместно с Международной электротехнической комиссией (МЭК) ввела новый стандарт оборудования и систем морской навигации и радиосвязи IEC 63.154 «Кибербезопасность – Общие требования, методы испытаний и требуемые результаты испытаний».[47] Этот стандарт устанавливает требования, методы тестирования и стандарты для судового оборудования, обеспечивающие базовый уровень защиты от киберинцидентов.

### *Общий обзор нормативной базы кибербезопасности на море Европейского Союза*

На стратегическом уровне главные усилия ЕС сосредоточены на Стратегии безопасности ЕС в 2020-2025 гг.[48] Стратегия утверждает, что кибератаки и киберпреступность продолжают расти, и её основная цель – вовлечь всё общество в решение проблем безопасности. Сюда входят отраслевые инициативы по устранению конкретных рисков, угрожающих критической инфраструктуре, включая транспорт и судоходство.

Общие усилия по обеспечению безопасности морских перевозок ЕС основаны на Директиве (ЕС) 2016/1148, также известной как Директива NIS (сетевая и информационная безопасность).[49] Её разработали, чтобы повы-

---

[44] International Organization for Standardization (ISO), “ISO/IEX 27001: Information Security Management,” 2013, www.iso.org/isoiec-27001-information-security.html.

[45] IMO, “Maritime Cyber Risk.”

[46] Nineta Polemi, *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains* (Amsterdam: Elsevier, 2017).

[47] International Electrotechnical Commission (IEC), “IEC 63154:2021 – Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results,” по состоянию на 13 мая 2021, https://webstore.iec.ch/publication/61003.

[48] European Commission, “About the European Security Union,” https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en.

[49] “NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network

сить безопасность сетей, услуг и информационных систем.[50] Цель Директивы NIS – усилить потенциал кибербезопасности ЕС, снизить угрозы сетям и информационным системам, используемым при предоставлении основных услуг в критических секторах, и обеспечить сохранение таких услуг после инцидентов в сфере кибербезопасности.[51] Директива подчеркивает, что растущая взаимозависимость различных основных услуг может нарушить деятельность организаций и секторов и оказать каскадное негативное воздействие на предоставление услуг на рынках. Поэтому операторы основных услуг стран-участниц должны делать всё возможное для снижения рисков нападения и сообщать властям о покушениях на их кибербезопасность.[52]

Директива NIS требует от каждой страны ЕС определить операторов основных услуг, работающих на их территории для достижения своих целей. Важным фактором недейственности Директивы NIS стали широкие критерии определения этих операторов основных услуг (ООС). Требования таковы:

- Предприятие предоставляет услугу, нужную для поддержания критически важной общественной и экономической деятельности;
- Предоставление этой услуги зависит от сети и информационных систем;
- Инцидент может иметь существенные негативные последствия для этой услуги.[53]

Применение этих критериев зависит от оценки риска национальным органом для конкретной базовой услуги. Другими словами, хотя транспорт назван критической услугой в ЕС, некоторые страны-участницы могут решить, что какая-то их морская инфраструктура не соответствует этим критериям. Поэтому не все порты и суда в ЕС отнесены к критической инфраструктуре.

Ещё одной особенностью морской сферы ЕС является разнообразие национальных морских компетентных органов. Различные организации, перечисленные в таблице ниже, имеют разные цели, нормативную базу, партнеров и бюджеты, что усугубляет несогласованность в данной сфере.

В ответ на растущие угрозы, связанные с компьютеризацией и ростом кибератак, Комиссия ЕС предложила заменить Директиву NIS, ужесточить

and information systems across the Union," Document 32016L1148, *EUR-Lex*, July 19, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

50 "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

51 "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

52 ENISA, https://www.enisa.europa.eu.

53 "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

требования безопасности и ввести более строгие меры надзора и правоприменительные требования, включая общие санкции Евросоюза.[54] После добавления новых секторов в список основных услуг NIS 2 обеспечит безопасность цепочек поставки и унифицирует требования отчётности.

**Таблица 2. Компетентные национальные органы стран ЕС** [55]

| Страна | Компетентный орган |
|---|---|
| **Бельгия** | Федеральный министр по вопросам мобильности (Федеральная служба мобильности) |
| **Болгария** | Министерство транспорта |
| **Венгрия** | Национальный генеральный директорат защиты от бедствий |
| **Германия** | Федеральное управление информационной безопасности (BSI) |
| **Греция** | Национальный орган кибербезопасности (Генеральный секретариат цифровой политики – Министерство цифровой политики, телекоммуникаций и средств массовой информации) |
| **Дания** | Датское управление транспорта, строительства и жилищного хозяйства |
| **Ирландия** | Национальный центр кибербезопасности (NCSC) |
| **Испания** | Государственный секретарь по вопросам безопасности (Министерство внутренних дел) – через Национальный центр защиты инфраструктуры и кибербезопасности (CNPIC) |
| **Латвия** | Министерство транспорта |
| **Литва** | Министерство национальной обороны |
| **Люксембург** | Люксембургский институт регулирования |
| **Мальта** | Отдел защиты критической инфраструктуры Мальты (CIP) |
| **Нидерланды** | Министерство инфраструктуры и водопользования |
| **Польша** | Министерство морской экономики и внутренней навигации |
| **Португалия** | Национальный центр кибербезопасности Португалии |
| **Румыния** | Группа реагирования на компьютерные чрезвычайные ситуации (CERT-RO) |
| **Словакия** | Министерство транспорта и строительства Словацкой Республики |
| **Словения** | Управление информационной безопасности |

[54] European Parliament, “The NIS2 Directive: A High Common Level of Cybersecurity in the EU,” EU Legislation in Progress, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

[55] ENISA, “National Competent Authorities for the Water transport subsector,” www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool.

| | |
|---|---|
| **Финляндия** | Управление транспорта и связи Финляндии (Traficom) |
| **Франция** | Национальное агентство кибербезопасности (ANSSI) |
| **Хорватия** | Министерство моря, транспорта и инфраструктуры |
| **Чехия** | Национальное агентство кибернетической и информационной безопасности (NCISA) |
| **Швеция** | Шведское транспортное агентство |
| **Эстония** | Управление информационных систем (RIA) |

NIS 2 преследует следующие главные цели:

- Повышение уровня киберстойкости служб стран ЕС путём введения правил, которые обязаны соблюдать все государственные и частные органы, ответственные за эти услуги;
- Уменьшение несоответствий в обеспечении безопасности на внутреннем рынке в важных секторах услуг путём дальнейшей гармонизации требований безопасности и отчётности об инцидентах, а также национального надзора и правоприменения;
- Улучшение коллективного понимания ситуации и коллективных способностей подготовки и реагирования, принимая меры по укреплению доверия между компетентными органами. Расширение обмена информацией и установление правил и процедур на случай крупномасштабного инцидента или кризиса;[56]
- Совершенствование списков операторов основных услуг стран-участниц на основе стандартного набора критериев.

Защита и киберстойкость основаны на систематизации масштабных киберинцидентов общеевропейскими группами сотрудничества в рамках NIS,[57] где определены все возможные злонамеренные действия в привязке к соответствующим правилами реагирования на политические кризисы в ЕС. Другие нормы снижения рисков и угроз европейской морской отрасли включают Европейскую программу защиты критической инфраструктуры (EPCIP) [58] и Директиву по определению и обозначению европейской критической инфраструктуры.[59] Недавний проект Директивы по обеспечению

[56] ENISA, https://www.enisa.europa.eu.

[57] Группа сотрудничества NIS включает представителей стран-участниц ЕС, ENISA и Европейской Комиссии. Создана согласно Статье 11 Директивы NIS.

[58] European Programme for Critical Infrastructure Protection.

[59] "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)," Document 32008L0114, *EUR-Lex* December 23, 2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

устойчивости важных объектов предлагает более целенаправленный подход к защите критической инфраструктуры.[60]

Конкретные меры регулирования морской кибербезопасности основаны на Стратегии безопасности на море ЕС (EUMSS).[61] Эта стратегия определяет риски и угрозы морской безопасности – «терроризм и другие преднамеренные незаконные действия на море и в портах против судов, грузов, экипажей и пассажиров, портов и портовых сооружений, а также критической морской и энергетической инфраструктуры, включая кибератаки».[62] EUMSS была принята в 2014 г. и пересмотрена в 2018 г., как общий и всеобъемлющий инструмент выявления, предотвращения и реагирования на любые проблемы, затрагивающие безопасность европейцев, деятельность и активы в морской экосистеме. Пересмотр EUMSS, утверждённый Советом по общим вопросам 26 июня 2018 г., нацелен на более чёткий процесс отчётности для улучшения понимания и лучшего выполнения стратегии.

Для реализации нормативной базы в ЕС создали специализированные органы, такие, как Агентство кибербезопасности Европейского Союза (ENISA),[63] Европейский центр киберпреступности (EC3) [64] в составе Europol и Группа реагирования на компьютерные чрезвычайные ситуации (CERT-EU).[65] Генеральный директорат по мобильности и транспорту (DG MOVE) и Европейское агентство по безопасности на море (EMSA) осуществляют общий надзор на выполнение требований национальными органами. ЕС также выступил с инициативами по повышению кибербезопасности в ряде важных секторов. В частности, Центры обмена и анализа информации (ISAC) [66] должны завоевать доверие в деле обмена информацией и передовым опытом в области физических и кибернетических угроз и их снижения, но пока что ЕС отстает в создании ISAC для морской сферы.

Важную для стран ЕС программу представили странам-участницам в

---

[60] "Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities," Document 52020PC0829, *EUR-Lex*, December 16, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN.

[61] Council of the European Union, "Maritime Security Strategy," June 26, 2018, https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/maritime-security-strategy_en.

[62] Council of the European Union, "Maritime Security Strategy."

[63] ENISA, https://www.enisa.europa.eu.

[64] "European Cybercrime Centre – EC3: Combating Crime in a Digital Age," *Europol*, updated March 1, 2022, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[65] "CERT-EU – The Computer Emergency Response Team for the EU institutions, bodies and agencies," https://cert.europa.eu/.

[66] "Information Sharing and Analysis Centers (ISACs)," https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

марте 2021 г.: это «Цифровой компас 2030»,[67] цель которого – внедрить конкретные процедуры продвижения цифровой трансформации ЕС, усиления его цифрового суверенитета и политики, а также устранить уязвимости и угрозы. Эта программа должна содействовать компьютеризации и обменам на море путём реализации самых современных мер кибербезопасности. «Цифровой компас 2030» опирается на четыре ключевые идеи:

- Цифровые возможности населения;
- Повышение связанности и производительности цифровой инфраструктуры;
- Цифровая трансформация бизнеса;
- Цифровизация общественных услуг.[68]

В целом «Цифровой компас 2030» является наглядной демонстрацией амбиций ЕС по реализации расширенной политики и стратегии кибербезопасности и созданию других инструментов для продвижения цифровизации, улучшения экономических и социальных показателей ЕС.

Важной задачей стран-участниц является соблюдение правил ЕС. В настоящее время большинство стран-участниц не обладают техническими возможностями для мониторинга критической морской информационной инфраструктуры и не внедрили специальные правила защиты своих основных услуг. Недостатком является и отсутствие эффективных платформ для обмена передовым опытом и укрепления сотрудничества между странами-участницами и их зарубежными коллегами, например, государственно-частного партнерства.[69]

Ещё одним серьёзным препятствием для достижения реальной киберстойкости в ЕС является наложение штрафов на организации, не соблюдающие требований. Из-за отсутствия воли у стран-участниц штрафы в большинстве случаев не применяются.[70]

### *Общий обзор базы кибербезопасности на море в США*

База кибербезопасности на море в США принципиально не отличается от подхода ЕС. Кибербезопасность на море регулирует американский Национальный план кибербезопасности на море. Его принципы:

- Свобода мореплавания;
- Поддержка и защита торговли для обеспечения бесперебойных поставок;

---

67 "2030 Digital Compass: The European Way for the Digital Decade," *EU4Digital*, March 9, 2021, https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/.

68 "2030 Digital Compass."

69 Cecilia Gondard and Enrique Guerrero Salom, "The Problem with Public-Private Partnerships and the Role of the EU," *Eurodad*, December 4, 2018, https://www.eurodad.org/PPPs-EU.

70 Этот вопрос решён в NIS2.

- Содействие перемещению нужных товаров и людей через границы при отсеивании опасных людей и материалов.[71]

План охватывает ресурсы, участников и инициативы, снижая текущие угрозы, уязвимости и т.д.[72]

Другими документами США, касающимися кибермер в морской сфере, является Циркуляр по навигации и инспекции судов № 01-20 «Руководство по устранению киберрисков в Законе о безопасности морского транспорта» (MTSA) [73] и Рабочая инструкция по соблюдению требований для коммерческих судов CVC-WI-018(1).[74] Эти документы устанавливают сроки включения мероприятий по киберзащите судов и прибрежных сооружений в оценки и планы безопасности.

Разработка конкретной политики и самостоятельная оценка надёжности инфраструктуры кибербезопасности является одной из важных задач американских морских властей – Береговой охраны США, что связано с недостаточным обменом и отчётностью, а также с отсутствием возможностей и процедур оценки уязвимости.

Серьёзной задачей для межнациональных и региональных механизмов кибербезопасности на море является минимизация угроз для портов и грузов от судов, использующих «удобные флаги». Их регистры не предъявляют особых национальных требований к судоходным компаниям, использующих их флаг.[75] По данным ЮНКТАД, почти 73 % судов зарегистрированы не в той стране, где судовладелец.[76] Проблема состоит в том, что несмотря на ратификацию нескольких международных морских и трудовых конвенций, у стран «удобных флагов» часто нет ресурсов и воли для реального обеспечения соблюдения международных норм безопасности на море и кибербезопасности. Поэтому они создают критическую уязвимость для всей морской транспортной системы.

Таким образом, основные проблемы эффективности действующей нормативной базы связаны со следующими основными факторами:

---

[71] "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security" (The White House, December 2020), https://www.hsdl.org/?view&did=848704.

[72] "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security."

[73] U.S. Coast Guard, "Navigation and Vessel Inspection Circular (NVIC) No. 01-20 – Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities," February 26, 2020, https://www.dco.uscg.mil/Our-Organization/NVIC/Year/2020/.

[74] USCG Office of Commercial Vessel Compliance (CG-CVC), "Commercial Vessel Compliance Work Instruction – CVC-WI-018(1)2020," September 1, 2020, www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-018(1).pdf.

[75] "Flags of Convenience," *NGO Shipbreaking Platform*, https://shipbreakingplatform.org/issues-of-interest/focs.

[76] "Review of Maritime Transport," *UNCTAD*, https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport.

- Несогласованность и отсутствие стандартизации существующих нормативных баз;
- Недостаток воли для обеспечения применения эффективных инструментов кибербезопасности и санкций за их невыполнение;
- Недостаточная киберграмотность.

### *Примеры*

К счастью, несмотря на все сложности и проблемы, примеры показывают, что киберстойкость и киберзнания вполне можно обеспечить. Норвежское морское ведомство предупредило судовладельцев и судоходные компании, что хакеры используют социальные сети, в частности LinkedIn, Facebook Messenger и WhatsApp, для внедрения вредоносных программ, и дало судам конкретные рекомендации, сумев снизить потенциальную эффективность кибератак.[77]

Страховая компания Shipowners Claims Bureau, Inc. разработала новый метод обучения персонала на борту и в портовых терминалах при помощи иллюстрированной брошюры под названием «Cyber Awareness». Рисунки и юмор помогают объяснить, что морякам нужно знать о мерах противодействия кибератакам, будь то вирус-вымогатель или фишинг.[78]

Некоторые страны-члены ЕС включили инициативы в области киберзнаний в свои Национальные стратегии кибербезопасности. В Хорватии эти инициативы охватывают электронную связь, критическую информационную инфраструктуру и киберпреступность.[79] В Национальной стратегии кибербезопасности Чехии этому вопросу посвящена отдельная глава под названием «Устойчивое общество 4.0».[80] Национальная стратегия кибербезопасности Эстонии включает конкретные меры по обучению граждан, предотвращению инцидентов кибербезопасности и информированию людей о возможных угрозах.[81] Главная цель Стратегии кибербезопасности Польши – повысить устойчивость к киберугрозам, что включает специальные программы информирования о кибербезопасности.[82]

---

77 Norwegian Maritime Authority, https://www.sdir.no/en/.

78 Shipowners Claims Bureau, Inc., “Shipboard Safety Cartoon,” https://www.americanclub.com/files/files/Shipboard_Safety.pdf.

79 “The National Cybersecurity Strategy of the Republic of Croatia,” Zagreb, October 7, 2015 (Official Gazette No.108/2015), https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.

80 “Czech Republic Cybersecurity,” *International Trade Administration*, по состоянию на 13 мая 2021, www.trade.gov/market-intelligence/czech-republic-cybersecurity.

81 Ministry of Economic Affairs and Communications, *Cybersecurity Strategy, Republic of Estonia 2019-2022*, https://www.mkm.ee/media/703/download.

82 Waldemar Kitler, “The Cybersecurity Strategy of the Republic of Poland,” in *Cybersecurity in Poland*, ed. Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz, and Tadeusz Zieliński (Cham: Springer, 2022), https://doi.org/10.1007/978-3-030-78551-2_9.

Инструмент по управлению киберрисками для портов ENISA – ещё один пример благотворного эффекта морского сотрудничества. Этот инструмент позволяет операторам портов проводить оценку киберрисков в четыре этапа, следуя общим принципам управления рисками. Кроме того, операторы определяют меры безопасности, исходя из своих приоритетов, и оценивают своё умение в реализации этих мер.[83]

Для обмена морской информацией в США действуют Центры обмена и анализа информации для обмена данными о киберугрозах. В морском секторе США имеются ещё три Центра обмена и анализа информации (MPS-ISAO, Морской ISAC, и ISAC системы морского транспорта).[84]

## Реагирование

С компьютеризацией и внедрением ИКТ в торговом судоходстве суда столкнулись с рисками и угрозами кибербезопасности. В отрасли торгового морского судоходства в настоящее время действует множество участников и регулирующих органов, использующих разные нормы. Из-за недостатка киберзнаний и современных технических возможностей для мониторинга информационной инфраструктуры судов, а также из-за того, что существующие нормы слишком широки и необязательны, морское судоходство уязвимо для кибератак, способных нанести серьёзный ущерб.

Первая и самая важная программа должна быть сосредоточена на улучшении обмена информацией об угрозах на море. Этого можно достичь при использовании Центров обмена и анализа информации (ISAC) и содействии государственно-частному партнерству. Вторая программа должна повышать киберзнания во всей морской сфере. Этого можно достичь, организуя занятия, семинары и конференции для всех участников морской сферы. Кроме того, обучение и сертификация на протяжении года могут быть предусмотрены и организованы государственными органами, которые регулируют и стандартизируют этот процесс. Обе инициативы являются важными элементами Директивы ЕС NIS 2.[85]

Третья программа должна заняться стандартизацией существующей правовой базы. Этого можно достичь, приняв Глобальный кодекс кибербезопасности на море, который будет легче отслеживать и соблюдать. Кроме того, Глобальный кодекс обобщит существующий передовой опыт в области стандартов кибербезопасности. Поскольку эти стандарты уже получили международное признание, их соблюдение должно встречать меньшее со-

---

[83] “Cyber Risk Management for Ports,” *ENISA*, https://www.enisa.europa.eu/cyber-risk-management-for-ports#/.

[84] Jaikumar Vijayan, “What is an ISAC or ISAO? How These Cyber Threat Information Sharing Organizations Improve Security,” *CSO*, July 26, 2021, www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.

[85] European Parliament, “The NIS2 Directive.”

противление судовладельцев и национальных властей. Кодекс кибербезопасности на море должен включать как обязательные, так и добровольные положения. Обязательная часть должна быть нацелена на обеспечение судами основных услуг. В добровольном разделе должны быть описаны методы реализации дополнительных мер безопасности. Отдельная подпрограмма должна охватывать аккредитацию и сертификацию «удобных флагов» путём введения дополнительных обязательных требований к их информационной инфраструктуре. Кроме того, Морской кибер-кодекс должен содержать конкретные указания и процедуры для установления и наказания виновных в кибератаках.

Четвертая программа должна обеспечить возможность заблаговременного обнаружения разрушительных киберсобытий. Заблаговременное обнаружение может осуществляться по-разному, включая мониторинг сетей и потоков данных. На оперативном уровне эта программа также должна предусматривать гарантированные средства для совместного использования сторонами и эффективные средства, гарантирующие непрерывность работы судна. Киберстойкость должна включать четкие планы альтернативных каналов связи, альтернативных баз данных, полностью независимых от обычных систем, и альтернативных инструментов и систем на борту судов, гарантирующих бесперебойную работу основных служб судна в случае взлома систем. Эта программа может быть реализована через специальные программы и фонды ЕС и США.

Пятая программа должна восполнить недостаток навыков обнаружения кибератак. Обучение должно гарантировать способность каждого обнаружить аномальное поведение системы и сообщить о нем в установленном порядке. Кроме того, экипаж должен быть обучен строгим правилам кибергигиены, включая сложные методы аутентификации, ограниченный доступ к ресурсам и проверку съёмных устройств памяти.

Наконец, последняя программа должна быть посвящена восстановлению после киберинцидентов. Она может включать специальные упражнения и обучение восстановлению основных служб судна, восстановлению данных, реагированию и расследованию цифровых инцидентов. Важный аспект этой программы составляет компенсация пострадавшим, путём страхования ответственности или государственных выплат. Адекватная компенсация снижает социальные риски и ущерб и способствует восстановлению экономики, социальной стабильности и доверию к институтам.

## Заключение

В заключение отметим, что морская киберсфера — это «Титаник», плывущий к айсбергу. Без должного предвидения и способности руководителей морского сообщества устранить возникающие уязвимости, катастрофическое воздействие кибератак на море на глобальную морскую транспортную систему будет лишь вопросом времени. Хотя исследования показали, что

различные организации признают угрозы системе кибербезопасности судоходства в своих нормах и стратегиях, анализ свидетельствует, что это мало повлияло на глобальную кибербезопасность. В этой связи международное морское сообщество при поддержке региональных и национальных морских властей должно реализовать комплексную программу информирования о кибербезопасности и гармонизации существующей нормативной базы для противодействия этой угрозе. Успех такой программы зависит от того, насколько активно все субъекты морского сообщества будут снижать свою кибер-уязвимость и противодействовать рискам и угрозам. Только так можно обойти айсберг.

## Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

## Об авторе

**Явор Тодоров** – стипендиат Центра Маршалла, старший эксперт Государственного агентства национальной безопасности /ДАНС/ Болгарии, возглавляет подразделение Департамента кибербезопасности. Г-н Тодоров имеет 20-летний опыт работы в болгарских службах безопасности и в последние восемь лет занимал различные должности, в том числе в сфере борьбы с терроризмом, контрразведки и кибербезопасности. Г-н Тодоров – бывший военно-морской офицер, принимал участие в ряде многонациональных учений, направленных на укрепление безопасности в Черноморском регионе. Член Горизонтальной рабочей группы по киберпроблемам при Совете ЕС, автор проекта Национального закона о кибербезопасности и подзаконных актов. В настоящее время его команда проводит оценку уязвимости критической национальной информационной инфраструктуры. Тесно сотрудничает с правоохранительными органами и службами Болгарии. Владеет английским, итальянским и русским языками. Имеет степень магистра в области телекоммуникаций и управления портами Болгарской военно-морской академии и магистра стратегических исследований Университета национальной обороны в Вашингтоне. В настоящее время заканчивает диссертацию на тему «Кибербезопасность на море».

*Connections: The Quarterly Journal*
**ISSN 1812-1101, e-ISSN 1812-2973**

А. Ризки, Ф. Тимур, *Connections QJ* 20, № 3-4 (2021): 85-96
https://doi.org/10.11610/Connections.rus.20.3-4.05

**Рецензированная статья**

# Угрозы безопасности вследствие радикализма в соцсетях на фоне пандемии Covid-19: Опыт Индонезии

***Атхтхаарик Ризки, Фаузиа Густарина Чемпака Тимур***

*Программа изучения асимметричной войны, Индонезийский университет обороны.*

**Аннотация**: Пандемия Covid-19 породила массу сомнений в обществе. Людям пришлось адаптироваться к «новой нормальности» все стороны жизни. Правительство Индонезии применило новую политику ограничения передвижения людей – систему «работай дома». В результате масштабные социальные ограничения усилили нагрузку на Интернет, что усугубило риски безопасности. Хотя использование социальных сетей для распространения радикализма – не новость, пандемия сделала соцсети удобной платформой для радикалов и экстремистов, ежедневно втягивая все больше людей. Цель данного исследования – используя качественные методы, проанализировать как распространение радикализма через соцсети превратилось в реальную угрозу для Индонезии во время пандемии, вместе с правительственной стратегией реагирования. Исследование показало, что количество пользователей соцсетей в Индонезии с начала пандемии достигло максимума – 51,5 %, представляющий в основном продуктивные возрастные группы. В исследовании содержится вывод о том, что пандемия активизировала вербовку и радикализацию через соцсети за счёт обращения к большему числу людей и распространения различных нарративов и выдумок. Для противодействия этим угрозам правительство Индонезии использует стратегию борьбы с такими нарративами, повышая цифровую грамотность и блокируя контент и учётные записи, чтобы приглушить голос радикализации в соцсетях.

**Ключевые слова**: Covid-19, угроза радикализма, социальные сети, Индонезия

## Вступление

Развитие информационно-коммуникационных технологий быстро прогрессирует. Технологии, по сути, созданы для помощи и облегчения человеческой деятельности, но иногда из них делают орудие преступлений, особенно во время пандемии Covid-19, когда люди широко используют технологии, чтобы устроить свою жизнь, от работы до повседневной деятельности.

Согласно отчёту Международного союза электросвязи (МСЭ), число Интернет-пользователей в мире в 2018 г. достигло 3,9 млрд., что составляет половину населения планеты. Количество Интернет-пользователей в Индонезии тоже существенно выросло. По данным исследования APJII 2020 г., число Интернет-пользователей в Индонезии составило 171,1 млн., что на 27,9 млн. больше, чем годом ранее, когда их было всего 143,2 млн. Последнее исследование в 2019-2020 гг. (Q2) показало, что Интернет-пользователей в Индонезии стало уже 196,71 млн. Таким образом, сейчас Интернетом пользуются 73,1% индонезийцев.

В 2019-2020 гг. использование Интернета в Индонезии ещё больше увеличилось. Этот рост связан с распространением Covid-19, не миновавшим Индонезию. Выступая по *VOI* («Голос Индонезии»),[1] руководитель APJII пояснил, что рост числа Интернет-пользователей в Индонезии произошёл благодаря дистанционному обучению и политике работы дома из-за пандемии Covid-19 с марта 2019 г. При «домашнем» проведении многих мероприятий онлайн, использование Интернета тоже вырастет.

Пандемия Covid-19 вынудила правительство Индонезии применить политику масштабных социальных ограничений. По словам министра-координатора по вопросам человеческого развития и культуры,[2] «масштабные социальные ограничения» – это ограничения на некоторые виды деятельности жителей района, где предполагается заражение вирусом SARS-CoV-2. Цель этой политики – предотвратить распространение Covid-19 путём ограничения общественной деятельности, включая работу. Любая совместная деятельность должна соответствовать протоколам здравоохранения «трёх М» (Маски, Мытьё рук, Максимальная дистанция). По данным APJII,[3] во время пандемии Covid-19 51.5% индонезийцев активно использовали Интернет для доступа к соцсетям.

---

1 Tachta Citra Elfira and Aditya Fajar Indrawan, “APJII: Pandemi COVID-19 Buat Pengguna Internet di Indonesia Meningkat Hampir 200 Juta,” *VOI*, November 10, 2020, https://voi.id/teknologi/19331/apjii-pandemi-Covid-19-buat-pengguna-internet-di-indonesia-meningkat-hampir-200-juta.

2 “Apa itu PSBB,” *Kemenko PMK*, February 18, 2020, https://www.kemenkopmk.go.id/apa-itu-psbb.

3 Asosiasi Penyelenggara Jasa Internet Indonesia, “Laporan Survei Internet APJII 2019-2020 [Q2],” December 23, 2020, https://apjii.or.id/survei.

В связи с широким распространением соцсетей во время пандемии Covid-19 возникли многочисленные угрозы и опасения по поводу использования соцсетей в преступных и других злонамеренных целях. Одна из угроз связана с тем, что ряд партий используют соцсети для пропаганды радикализма. Глава Национального контртеррористического агентства (BNPT) Бой Рафли Амар [4] подтвердил, что радикализм распространяется не только при личном общении. В настоящее время радикалы распространяют радикальные идеи нетерпимости через соцсети. Радикальные партии используют существующие каналы в соцсетях для пропаганды своих крайних взглядов. По его словам, соцсети стали одним из наиболее эффективных средств охвата молодого поколения и разжигания радикализма во время пандемии. Основная целевая группа – подростки в возрасте от 17 до 24 лет. В этом возрасте они молоды, энергичны, а их взгляды еще не устоялись.

Исследования Сунарто [5] показали, что прогресс информационных технологий создаёт угрозы существованию нации и государства. Одной из них является простота доступа к Интернету и соцсетям, откуда легко почерпнуть информацию о радикализме, изготовлении бомб и преступлениях. Низкий уровень грамотности может способствовать радикализации благодаря усвоению ценностей в ходе общения в соцсетях при отсутствии крепкой семьи.[6] Однако вторичная социальная среда, в которой человек общается с соседями и в процессе обучения, может противодействовать радикализации за счет терпимости к другим, отличным от него людям, благодаря чему на него трудно будет повлиять при помощи радикального контента.[7]

Ряд учёных согласен с Сунарто и отмечает распространённость радикализма в Индонезии. Поэтому правительству нужна подходящая коммуникационная стратегия борьбы с радикализацией, способная тоже использовать соцсети.[8] Гхифари тоже заметил, что соцсети способствуют распространению радикализма в обществе, стали средством пропаганды нетерпимых

---

4 Sania Mashabi, "Kepala BNPT: Penyebar Paham Radikalisme Manfaatkan Media Sosial," *Kompas*, July 3, 2020, https://nasional.kompas.com/read/2020/07/03/15343511/kepala-bnpt-penyebar-paham-radikalisme-manfaatkan-media-sosial?page=all.

5 Andang Sunarto, "Dampak Media Sosial Terhadap Paham Radikalisme," *Nuansa: Jurnal Studi Islam dan Kemasyarakatan* 10, no. 2 (December 2017): 126-131, https://doi.org/10.29300/nuansa.v10i2.647.

6 Widodo Agus Setianto, "Literasi Konten Radikal di Media Online," *Jurnal Ilmu Komunikasi* 16, no. 1 (January-April 2018): 75-88, https://doi.org/10.31315/jik.v16i1.2684.

7 Surryanto D. Waluyo, Fauzia Gustarina Cempaka Timur, and Ningsih Susilawati, "Pengajaran Nilai Bela Negara Melalui Pendidikan Kewarganegaraan Sebagai Upaya Cegah Dini Terhadap Radikalisme," *Bhineka Tunggal Ika: Kajian Teori dan Praktik Pendidikan PKN* 8, no. 1 (May 2021): 10-20, https://ejournal.unsri.ac.id/index.php/jbti/article/view/12125/pdf.

8 Ratna Puspita, "Kontra-Radikalisasi Pada Media Sosial Dalam Perspektif Komunikasi," *Jurnal Komunikasi Universitas Garut: Hasil Pemikiran dan Penelitian* 6, no. 2 (October 2020): 509-529, https://journal.uniga.ac.id/index.php/JK/article/view/785.

действий, включая вербовку, подготовку, обучение, расширение сетей для совершения террористических актов и подрывов смертников в Индонезии.[9] Замзами [10] добавляет, что распространение социальных сетей позволяет радикальным группам вести вербовку, пропагандировать и распространять свою идеологию. Если при традиционном методе распространения радикализма нужно встретиться с носителем идеологии, то теперь это возможно онлайн. Радикализация — это процесс поиска, нахождения, восприятия и продвижения верований и крайностей. Существование соцсетей – это инструмент, способный ускорить процесс радикализации. От Аиша с коллегами [11] мы знаем, что для решения этой проблемы правительство усилило киберпатрули, чтобы предотвратить распространение радикального контента. К тому же Министерство связи и информатики строго контролирует контент, распространяемый через приложения соцсетей, что повлияло на схемы вербовки и распространение радикализма.[12]

Кроме того, Хандоко и Сусанто [13] поясняют, что Министерство связи и информатики уже занимается предотвращением радикализма: оно продолжает информировать общественность об опасности радикализма и противодействовать любому радикальному контенту в соцсетях, распространяя позитивные, мирные нарративы. Взаимодействие в соцсетях можно оценить по количеству лайков, репостов и комментариев. Эти показатели взаимодействия иллюстрируют охват других пользователей соцсетей. Упоминание связанного с радикализмом слова в соцсетях связано не только с религией: радикализм также связан с выборами, политикой, правительством, преступностью и другими проблемами общества.[14]

Фанинди и Мупида в своих исследованиях объясняют воздействие соцсетей ещё и тем, что это первый выбор молодого поколения в быстром поиске информации, поэтому они подвержены воздействию радикального

---

[9] Iman Fauzi Ghifari, "Radikalisme di Internet," *Religious: Jurnal Agama dan Lintas Budaya* 1, no. 2 (March 2017): 123-134, https://journal.uinsgd.ac.id/index.php/Religious/article/view/1391.

[10] Ahmad Zamzamy, "Menyoal Radikalisme di Media Digital," *Dakwatuna: Jurnal Dakwah dan Komunikasi Islam* 5, no. 1 (February 2019): 13-29, https://doi.org/10.36835/dakwatuna.v5i1.318.

[11] Bilqis Rihadatul Aisy et al., "Penegakan Kontra Radikalisasi Melalui Media Sosial Oleh Pemerintah Dalam Menangkal Radikalisme," *Jurnal Hukum Magnum Opus* 2, no. 1 (February 2019): 1-8, https://doi.org/10.30996/jhmo.v2i2.2174.

[12] Achmad Sulfikar, "Swa-radikalisasi Melalui Media Sosial di Indonesia," *Jurnal Jurnalisa* 4, no. 1 (May 2018): 76-89, https://doi.org/10.24252/jurnalisa.v4i1.5622.

[13] Jefri Handoko and Eko Harry Susanto, "Humas Kominfo Dalam Mencegah Bahaya Radikalisme Di Media Sosial," *Jurnal Prologia* 3, no. 1 (July 2019): 147-153, https://doi.org/10.24912/pr.v3i1.6232.

[14] Abdul Wahid, Nia Ashton Destitry, and Fariza Yuniar Rakhmawati, "Radikalisme di Media Sosial: Penyebutan dan Konteks Sosial Penggunaannya," *Jurnal InterAct* 9, no. 1 (2020): 60-70, https://doi.org/10.25170/interact.v9i1.1711.

контента.[15] Молодое поколение подвержено радикализму, потому что оно ищет свою идентичность; на них легко влияет то, что они читают. Кроме того, поскольку экстремистским группам известно, как соцсети могут мгновенно предоставлять разнообразную информацию, они используют ту же логику. Сначала они проповедовали радикализм во имя религии, чтобы поддержать идеологию халифата и отвергнуть демократическую систему в сочинениях, книгах и журналах, но их размещение в соцсетях было сочтено более эффективными.

Итак, если посмотреть на предыдущие аргументы, протоколы здравоохранения и политика правительства во время пандемии Covid-19 ограничили физическое передвижение людей, что привело к росту активности в Интернете, особенно в соцсетях. Конечно, это создаёт потенциал для роста угрозы радикализма в соцсетях. Поэтому ниже мы более подробно разберем восприятие угрозы радикализма в соцсетях в Индонезии во время пандемии Covid-19.

## Метод

При написании этой статьи авторы использовали метод качественных исследований с обзором литературы. Согласно Кресвеллу,[16] обзор литературы — это исследовательский подход, основанный на нечисловых данных в письменном или графическом виде, с фильтрацией данных для толкования обзора. Исследование проводилось с использованием литературных источников: журналов, книг, диссертаций, отчётов об исследованиях и научных статей, опирающихся на реальные и надёжные источники.

## Результаты и их обсуждение

### *Использование соцсетей во время пандемии Covid-19 в Индонезии*

Исследование Digital Trends Report, проведённое в Facebook совместно с YouGov, показало, что более 140 млн. индонезийцев вступили в группы в соцсетях, активные во время пандемии Covid-19. Сейчас население Индонезии составляет 267,7 млн. человек. 95 % респондентов сообщили, что предоставляли моральную и бытовую поддержку членам сообществ в соцсетях во время пандемии Covid-19. 54 % респондентов получили моральную поддержку от друзей в группе Facebook, ещё 55 % оказывали моральную поддержку в соцсетях. Больше половины пользователей соцсетей уютно чувствуют себя на цифровых платформах. 67 % респондентов заявили, что сообщество стало более важным для них во время пандемии

[15] M. Nanda Fanindy and Siti Mupida, "Pergeseran Literasi pada Generasi Milenial Akibat Penyebaran Radikalisme di Media Sosial," *Millah: Jurnal Studi Agama* 20, no. 2 (February 2021): 195-222, https://doi.org/10.20885/millah.vol20.iss2.art1.

[16] John W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 2nd ed. (Thousand Oaks, California: Sage Publishing, 2003).

Covid-19. Кроме того, как сообщил *Kompas*[17] на основе последнего отчёта маркетингового агентства «We Are Social» и платформы управления соцсетями Hootsuite, больше половины населения Индонезии «грамотно», т.е. активно использовало соцсети в январе 2021 г. во время пандемии Covid-19. В отчёте под названием «Digital 2021: Новейший взгляд на состояние цифровых технологий» утверждается, что из 274,9 млн. индонезийцев 170 млн. пользовались соцсетями. Таким образом, охват составляет около 61,8 %.

По состоянию на январь 2021 г. число активных пользователей соцсетей в Индонезии выросло на 10 млн., или примерно на 6,3 %, по сравнению с январём 2020 г. За то же время число пользователей Интернета в Индонезии тоже выросло на 27 млн., или на 15,5 %, так что сейчас в Индонезии 202,6 млн. Интернет-пользователей. Исследование Рохма[18] показало, что из 50 случайно выбранных в Instagram людей 80% согласились, что социальные сети можно использовать для общего информирования, а 93% согласились, что соцсети можно использовать для информирования о Covid-19. Кроме того, Рохма[19] сообщил, что 80% респондентов в его исследовании согласились, что в соцсетях можно спрятаться ото всех проблем. Для людей, изолированных во время пандемии Covid-19, социальные сети стали местом, где можно отвлечься и отдохнуть.

Такой рост использования соцсетей связан с их удобством.[20] Пять превосходных характеристик соцсетей делают их предпочтительней традиционных СМИ. Вот их преимущества:

1. *Доступность*: соцсети легко доступны за небольшую плату или бесплатно;
2. *Скорость*: информация и контент в соцсетях немедленно становится доступна каждому в сетях, на формах и в сообществах, как только этот контент или информация публикуется;
3. *Интерактивность*: соцсети могут иметь два или больше каналов коммуникации;
4. *Долговременность*: информация или контент в соцсетях могут быть доступны долгое или даже неограниченное время;

---

17 Conney Stephanie, “Riset Ungkap Lebih dari Separuh Penduduk Indonesia ‘Melek’ Media Sosial,” *Kompas*, February 24, 2021, https://tekno.kompas.com/read/2021/02/24/08050027/riset-ungkap-lebih-dari-separuh-penduduk-indonesia-melek-media-sosial.

18 Nurliya Ni’matul Rohmah, “Media Sosial Sebagai Media Alternatif Manfaat dan Pemuas Kebutuhan Informasi Masa Pandemik Global Covid-19 (Kajian Analisis Teori Uses And Gratification), *Al-I’lam: Jurnal Komunikasi dan Penyiaran Islam* 4, no. 1 (September 2020): 1-16, https://journal.ummat.ac.id/index.php/jail/article/view/2957.

19 Rohmah, “Media Sosial Sebagai Media Alternatif Manfaat dan Pemuas Kebutuhan Informasi Masa Pandemik Global Covid-19.”

20 Varinder Taprial and Priya Kanwar, *Understanding Social Media* (London: Ventus Publishing ApS, 2012).

5. *Охват*: соцсети и Интернет предлагают безграничный выбор контента.

Тем временем, исходя из исследования, проведённого GWI в третьем квартале 2020 г. на базе телеканала Beritasatu,[21] YouTube остаётся самой популярной соцсетью в Индонезии. Количество пользователей YouTube достигло 94% населения в возрасте от 16 до 64 лет. Вторая по популярности соцсеть в Индонезии – WhatsApp, третья – Instagram. Согласно отчёту, Instagram вышел на третье место, опередив Facebook, ставший четвёртым.

### *Угроза терроризма и радикализма в Индонезии во время пандемии Covid-19*

Аиш с коллегами[22] поясняют, что радикализм является предтечей терроризма. Радикализм – это мировоззрение, в целом направленное на быстрые изменения, против существующих ценностей, и сопряжённое с применением насилия и крайностями. Во время пандемии Covid-19 в Индонезии часто отмечался радикализм и террористические проявления. Даже в начале 2021 г. террористическая активность радикальных группировок возрастает. Теракт со взрывом бомбы произошел в Макассаре – террорист-смертник атаковал Кафедральный собор Макассара в Южном Сулавеси. Полиция заявила, что террористы принадлежали к радикальной группировке Jamaah Ansharut Daulah (JAD). Глава национальной полиции генерал Листьё сообщил, что эти четыре человека были партнерами L и YSF, обучавшимися на вилле Мутиара. В этом жилом комплексе в Макассаре были арестованы участники террористической сети JAD.[23] Подозреваемый ZA совершил теракт с применением страйкбольного пистолета в штаб-квартире Национальной полиции. В своем заявлении начальник Национальной полиции сообщил, что ZA сумел пробраться в штаб полиции через заднюю дверь, а затем подошел к полицейскому посту у главного входа и совершил теракт. Согласно отчету полиции, ZA покинул пост, но затем вернулся и произвел шесть выстрелов.[24]

В интервью для Indonesia Intelligent Agency (2020) в Национальной полиции пояснили, что в марте-декабре 2020 г. они подозревали 143 человек в причастности к терроризму и радикализму. Полиция сообщила, что из 143

---

[21] Yudo Dahono, “Data: Ini Media Sosial Paling Populer di Indonesia 2020-2021,” *Beritasatu.com*, February 15, 2021, https://www.beritasatu.com/digital/733355/data-ini-media-sosial-paling-populer-di-indonesia-20202021.

[22] Aisy et al., “Penegakan Kontra Radikalisasi Melalui Media Sosial Oleh Pemerintah Dalam Menangkal Radikalisme.”

[23] Tommy Kurnia, “4 Kasus Terorisme yang Terjadi di Dunia Selama Pandemi COVID-19,” *Liputan 6*, March 29, 2021, https://www.liputan6.com/global/read/4518650/4-kasus-terorisme-yang-terjadi-di-dunia-selama-pandemi-Covid-19.

[24] Berita Utama, “Penembakan Mabes Polri: ‘Terduga teroris berideologi ISIS’, polisi ungkap identitas perempuan 25 tahun pelaku serangan,” *BBC News*, March 31, 2021, https://www.bbc.com/indonesia/indonesia-56579674.

подозреваемых 97 принадлежали к группировке Jamaah Ansharut Daulah (JAD), 20 — к Jamaah Islamiyah (JI), 12 — к Моджахедам Восточной Индонезии (MIT), и 14 были из соцсетей.

Подъём террора и радикализма со стороны радикальных группировок неотделим от факторов, способствующих распространению радикализма и терроризма в Индонезии. Это подтверждает мнение Фатхкури,[25] согласно которому распространение радикализма и терроризма в Индонезии провоцируют два фактора, а именно экономическое обнищание и политическая несправедливость. Экономическое обнищание представляет собой серьёзную проблему. В репортаже Виджаи по BBC Indonesia [26] Центральное Статистическое Агентство (BPS) сообщило, что число бедных в Индонезии из-за пандемии Covid-19 выросло больше чем на 2,7 млн. человек. Отмечается, что число бедных в Индонезии в сентябре 2020 г. достигло 27,55 млн., или 10,19 % населения, что на 2,76 млн. человек больше, чем в сентябре 2019 г. Рост бедности нельзя отделить от массовых увольнений в нескольких частных компаниях, пострадавших от ограничений, введенных во время пандемии.

Это согласуется с более ранним исследованием Фанинди и Мупиды,[27] пришедшими у выводу, что бедность стала одним из факторов поддержки террористического и радикального движения в Индонезии, хотя это не повлияло напрямую на распространение радикализма. Однако бедность легко влияет тех, кто ищет удовлетворения своих потребностей. Это позволяет применять экономичный подход к борьбе с радикализмом и религиозным экстремизмом. В условиях повсеместной бедности многие индонезийцы пытаются получить доход и материальную поддержку из разных источников. Радикальные группировки и террористы могут использовать это для распространения радикальных идей и вербовки, предлагая материальную поддержку.

Во-вторых, существуют проблемы политической несправедливости. Многие террористические и радикальные группы увидели в политике правительства во время пандемии возможность для нападок на правительство и влияния на умы индонезийцев. Из-за пандемии Covid-19 экономическое положение ухудшилось. Политику правительства сочли несправедливой и вредной для небольших общин, особенно для рабочих. Яхья в Kompas [28] в

---

[25] Fatkhuri, “Faktor Pendukung Terbentuknya Radikalisme dan Terorisme di Indonesia,” *Jurnal Universitas Pembangunan Veteran Jakarta* (2017), www.researchgate.net/publication/318054171_FAKTOR_PENDUKUNG_TERBENTUKNYA_RADIKALISME_DAN_TERORISME_DI_INDONESIA.

[26] Callistasia Wijaya, “Dampak Covid-19: 2,7 juta orang masuk kategori miskin selama pandemi, pemulihan ekonomi ‘butuh waktu lama’,” February 17, 2021, https://www.bbc.com/indonesia/indonesia-55992498.

[27] Fanindy and Mupida, “Pergeseran Literasi pada Generasi Milenial Akibat Penyebaran Radikalisme di Media Sosial.”

[28] Achmad Nasrudin Yahya, “Ramai-ramai Menolak UU Cipta Kerja dan Ancaman Nasional,” *Kompas.com*, June 10, 2020, https://nasional.kompas.com/read/2020/10/06/

октябре 2020 г. сообщил, что правительство и Палата представителей Индонезии на пленарном заседании приняли рамочный закон о создании рабочих мест. Однако много индонезийцев раскритиковало принятие этого закона. Многие партии осудили принятие Закона о создании рабочих мест. Законопроект назвали проблемным и способным нанести вред людям, особенно рабочим. Кроме того, законопроект был утверждён во время вспышки пандемии.

Валуё с коллегами [29] объяснили эту политическую несправедливость так: недовольство различных групп общества ведёт к возникновению террористических движений и проявлениям радикализма. Это чувство недовольства приводит к созданию радикальных группировок, а затем – к терроризму с целью противодействия правительству.

Кроме того, Чайдир [30] поясняет, что в BNPT пытались анализировать четыре взгляда на терроризм и радикальные группировки во время пандемии Covid-19, а именно:

1. Террористические и радикальные группировки продвигают идею о том, что распространение COVID-19 – это наказание неверных, и выступают против политики правительства по соблюдению медицинских протоколов.
2. Террористические и радикальные группировки пользуются периодом масштабных социальных ограничений для ведения пропаганды в соцсетях.
3. Террористические и радикальные группировки рассматривают пандемию Covid-19 как подходящий момент для терактов.
4. Террористические и радикальные группировки пользуются пандемией Covid-19 для наращивания сил, распространения своих нарративов и вербовки людей онлайн.

### *Угроза радикализма в соцсетях в Индонезии во время пандемии Covid-19*

Из предыдущих исследований Вахида [31] известно, что за словом «радикализм» часто следуют хэштеги (#), связанные с другими словами. К популярным словам, связанным с упоминанием радикализма, относятся #radicalism, #indonesia, #pancasila, #indonesiapeace, #indonesiahebat, #tolerance,

05545351/ramai-ramai-menolak-uu-cipta-kerja-dan-ancaman-mogok-kerja-nasional?page=all.

[29] Waluyo, Timur, and Susilawati, “Pengajaran Nilai Bela Negara Melalui Pendidikan Kewarganegaraan Sebagai Upaya Cegah Dini Terhadap Radikalisme.”

[30] Leski Rizkinaswara, “Pemblokiran dan Literasi jadi Langkah Kominfo Cegah Terorisme di Ruang Digital,” *Jakarta: Aptika Kominfo*, August 16, 2020, https://aptika.kominfo.go.id/2020/08/pemblokiran-dan-literasi-jadi-langkah-kominfo-cegah-terorisme-di-ruang-digital/.

[31] Wahid, Destitry, and Rakhmawati, “Radikalisme di Media Sosial: Penyebutan dan Konteks Sosial Penggunaannya.”

#bhinnekatunggalika и т.д. Кроме того, разное применение этих хэштегов в то или иное время бывает связано с разными событиями. Инес фон Бер с коллегами [32] поясняет, что Интернет и соцсети играют важную роль в продвижении радикализма в силу пяти причин, а именно:

1. Интернет и соцсети дают больше возможностей;
2. Интернет и соцсети работают как «резонаторы»;
3. Интернет и соцсети ускоряют процесс радикализации;
4. Интернет и соцсети создают возможность радикализации без физического контакта;
5. Интернет и соцсети увеличивают шансы саморадикализации.

По словам директора по вопросам контроля за информационно-коммуникационными приложениями Министерства связи и информатики Антониуса Малау (2020), терроризм и распространение радикализма во время пандемии Covid-19 всё ещё находились на высоком уровне. Данные с июля 2017 по июль 2020 гг. показывают, что 16 739 сообщений (в соцсетях и на веб-сайтах), касающихся терроризма и радикализма, были успешно заблокированы.

Там временем, по словам директора BNPT по вопросам защиты Хервана Чайдира, веб-сайт Kominfo [33] тоже зафиксировал рост случаев терроризма и радикализма. С февраля по июнь 2020 г. полиция обвинила в терроризме 84 подозреваемых. По словам Чайдира,[34] пандемия Covid-19 оставила 2 млн. человек в нищете и без работы. Предоставленные BNPT данные свидетельствуют об усилиях по борьбе с этими террористическими и радикальными группировками с тем, чтобы они не использовали пандемию для вербовки новых членов.

Что касается контента соцсетей, который может быть назван радикальным, то в справочнике BNPT по предупреждению радикализма в рабочей среде BUMN и частных компаний (2020) отмечены четыре индикатора, характеризующие группировку или человека как радикальные: нетерпимость, фанатизм, исключительность, и беззаконие. Вот примеры радикального контента, распространявшегося в соцсетях во время пандемии Covid-19, на основе индикаторов радикализма BNPT.

В Таблице 1 перечислены примеры, иллюстрирующие все четыре категории радикализма согласно определению BNPT – нетерпимость, фанатизм,

---

[32] Ines von Behr, Anaïs Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (RAND Europe, 2013).

[33] Rizkinaswara, “Pemblokiran dan Literasi jadi Langkah Kominfo Cegah Terorisme di Ruang Digital.”

[34] Rizkinaswara, “Pemblokiran dan Literasi jadi Langkah Kominfo Cegah Terorisme di Ruang Digital.”

**Таблица 1. Радикальные действия в соцсетях во время пандемии Covid-19.**

| № | Событие | Категория | Дата |
|---|---|---|---|
| **1** | Рейд по молельным домам в Чикаранге | Нетерпимость | 13.09.2020 |
| **2** | Фанатичная поддержка радикального движения FPI | Фанатизм | 30.12.2020 |
| **3** | Отказ в проповеди на языке минангкабау | Исключительность | 10.06.2020 |
| **4** | Инструкции по противодействию руководству 1-го командования FPI | Беззаконие | 26.06.2020 |

исключительность и беззаконие – с 2020 г. Согласно докладу *Kumparan.com*,[35] одним из примеров нетерпимых действий во время пандемии Covid-19 стало вирусное видео в соцсетях о нападении на христианский молитвенный дом в Чикаранге, Западная Ява. Полагают, что местные жители, напавшие на церковь, нарушили масштабные социальные ограничения.

Кроме категории нетерпимости, в данных, полученных от Warta Ekonomi, были выявлены фанатичные действия.[36] Трендом индонезийского твиттера стала новость о заморозке сообщества организации Фронт защитников ислама (FPI) с хэштегом #FPITerlarang. Многие пользователи сетей в Индонезии выразили поддержку фанатикам FPI, до сих пор пытающимся поддержать и защитить FPI в соцсетях. Члены и сторонники FPI распространяли твиты с признаками фанатизма по отношению к организации, в которой они участвуют и которую боготворят.

Вот один из примеров новости, в июне 2020 г. распространявшейся исключительно в соцсетях. Группа сообщества минангкабау возражала против публикации Библии на языке минангкабау. О неприятии заявляли в твитах и сообщениях соцсетей, где эта публикация была названа противоречащей обычаям и культуре народа минангкабау. Примером призыва в соцсетях к беззаконным действиям во время пандемии Covid-19 стал призыв к джихаду против коммунистической группировки Trisila в Индонезии. Сайт *Fajar.co.id* [37] цитирует указание генерального секретаря FPI Мунармана привести командование в первую степень готовности, призвав к джихаду для

[35] Anwar Saragih, “Intoleransi di Masa Pandemi,” *Kumparan.com*, April 20, 2020, https://kumparan.com/anwar-saragih/intoleransi-di-masapandemi-1tG7MN5ffb0.

[36] “FPI Dibubarkan, Warganet Pro-Kontra! Ada yang Bilang, ‘FPI Tetap di Hati!’,” *Wartaekonomi*, December 30, 2020, https://www.wartaekonomi.co.id/read320669/fpi-dibubarkan-warganet-pro-kontra-ada-yang-bilang-fpi-tetap-di-hati.

[37] Adi Mirsan, “Siaga 1, FPI Cs Serukan Jihad Qital Lawan Komunis,” *Fajar.co.id*, June 26, 2020, https://fajar.co.id/2020/06/26/siaga-1-fpi-pa-212-dan-gnpf-serukan-jihad-qital-lawan-komunis/.

сопротивления коммунистическим группировкам в Индонезии. Это стало ответом на действия группы Trisila после того, как альянс провел демонстрацию против законопроекта касательно идеологического направления Pancasila.

## Заключение

Соцсети стали важной платформой для информирования, развлечений и общения в сообществе и с другими людьми во время пандемии. В 2020 г. самыми популярными соцсетями в Индонезии были YouTube, WhatsApp и Instagram.

В период пандемии Covid-19 выросла угроза радикализма. Во время пандемии Covid-19 все больше членов общества радикализировались, по двум причинам: первая – это проблема обнищания, обострившаяся в ходе пандемии, а вторая – политическая несправедливость, которую ощущает общество. Многие люди были недовольны несправедливыми, по их мнению, мерами правительственной политики. Одной из причин возникновения этого чувства недовольства стала неэффективность борьбы с Covid-19 в Индонезии. В результате в 2020 г. зафиксировано немало случаев радикализма, в которых проявились нетерпимость, фанатизм, исключительность и беззаконие.

## Примечание

Представленные здесь взгляды принадлежат исключительно авторам и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

## Об авторах

**Атхтхаарик Ризки** – слушатель Программы изучения асимметричной войны в Индонезийском университете обороны, Богор.
*Электронная почта:* erikatorik@gmail.com

**Фаузиа Густарина Чемпака Тимур** – преподаватель Программы изучения асимметричной войны в Индонезийском университете обороны, Богор.
*Электронная почта:* fgcempaka@gmail.com

*Connections: The Quarterly Journal*
**ISSN 1812-1101, e-ISSN 1812-2973**

М. Балхи, *Connections QJ* 20, № 3-4 (2021): 97-112
https://doi.org/10.11610/Connections.rus.20.3-4.06

**Рецензированная статья**

# Отношения на основе взаимности: Как Талибан и мир видят друг друга

## *Мирваис Балхи*

*Высшая школа дипломатической службы Джорджтаунского университета, https://sfs.georgetown.edu/*

**Аннотация**: 15 августа 2021 г. 20-летняя война США, НАТО и Афганских сил обороны и безопасности с Талибаном закончилась драматическим приходом талибов к власти в Афганистане. Они во второй раз объявили о создании правительства в Кабуле. Возвращение Талибана на политическую сцену Афганистана требует анализа взглядов Талибана и стран-участниц афганского конфликта друг на друга. Каким будет характер взаимоотношений Талибана с этими странами? Как талибы смотрят на разные регионы, пытавшиеся влиять на Афганистан в последние 20 лет? Наконец, как видят Талибан в разных столицах – этот вопрос часто задают СМИ и аналитические центры? Сейчас мировые игроки смотрят на Талибан по-разному, а как будет в будущем? В этой статье мы попытаемся ответить на большинство из этих вопросов.

**Ключевые слова**: клановость, политизация религии, языковой национализм, международные отношения.

## Вступление

15 августа 2021 г. Талибан совершил поворот в истории Афганистана, во второй раз взяв власть и объявив временное правительство в Кабуле. Их первая победа и взятие Кабула привели к созданию режима, продержавшегося пять лет (1996-2001). Драматичное свержение проамериканского правительства и неожиданный приход Талибана к власти в 2021 г. поставил перед всеми региональными и международными игроками вопрос – призна́ют они действующий режим в Кабуле или выступят против него. Даже давние сторонники Талибана, такие, как Пакистан, Китай, Россия, Иран, Катар и Саудовская Аравия, не знают, как быть.

Традиционно ни Талибан, ни международные игроки не могли подумать, что силовая политика внутри Афганистана так быстро изменится. Руководство Талибана было озадачено тем, как хорошо оснащённая и поддерживаемая НАТО/США армия развалилась без особых усилий. За считанные недели Талибан вышел из подполья, атаковал основные города и обосновался в Кабуле. Международные НПО, сотрудники посольства, американские войска еще были в Кабуле, а так называемая передовая разведка была застигнута врасплох. Кабул погрузился в «естественное состояние», выстрелы грабителей эхом разносились по городу – таков был результат полного коллапса, произошедшего за несколько часов.

Афганский сценарий оставил тех, кто наблюдал за конфликтом извне, в аналогичной ситуации. Президенты, министры иностранных дел, представители, парламенты и оппозиционные партии стран, вовлеченных в афганский конфликт, оказались в ситуации беспрецедентного кризиса. Прошло более трех месяцев с тех пор, как Талибан захватил власть, но никто не смог принять решение и не осмелился выступить с инициативой дипломатических отношений с Талибаном. Талибан, все еще не совсем понимающий свою стратегию безопасности, в одночасье заменил сравнительно демократическое правительство в Афганистане. Хотя талибы говорили о национальной амнистии и установлении мирных отношений с миром, их словам трудно доверять. Что произойдет с демократическими ценностями, которые, вероятно, зачахнут при талибах? Поддержат ли они исламистскую группировку или будут настаивать на инклюзивном правительстве? Что будет с простыми жителями Афганистана, столкнувшимися с гуманитарной катастрофой? Это актуальные вопросы, которые требуют ответа.

Все игроки, вовлеченные в афганский конфликт, порознь и вместе анализируют режим Талибана, чтобы выработать контуры своей внешней политики. Многие ожидают, что США возьмут на себя роль лидера и представят стратегическую дорожную карту, чтобы устранить двусмысленность. Однако роль США, скорее всего, будет минимальной.

Поэтому надо изучить взгляды разных национальных и международных экспертов. Ожидается, что эти взгляды будут дополнять друг друга и представят информацию изнутри и извне о том, как мир воспринимает Афганистан. Реализуя этот подход, в этой статье мы проанализируем взаимоотношения Талибана с международными игроками.

## Что такое Талибан?

Термин «Талибан» происходит от множественного числа арабского/ персидского слова «студенты», имея в виду студентов религиозных медресе. В эту группу входит сельская молодёжь отдалённых районов Афганистана, не имеющая современного образования, навыков и связей в обществе. Это консервативная, радикализованная племенная группа, не способная конкурировать на современном рынке труда. Они приобрели влияние благодаря неприятию модернизма и недовольству афганским правительством, а

также поддержке Межведомственной разведки Пакистана (Inter-Services Intelligence, ISI) и других разведслужб региона. Талибан используют как стратегический актив для сохранения влияния и противодействия враждебным силам в Афганистане, что создаёт отношения взаимодействия группировки с этими разведслужбами. Поэтому Талибан нужно рассматривать в контексте национальной политики Афганистана и регионального интервенционизма.

Появление Талибана во время советского вторжения в Афганистан, закончившегося поражением от моджахедов, стало одним из самых важных событий в истории Афганистана. Когда руководители моджахедов вошли в Кабул и создали Исламское Государство Афганистан в главе с Бурхануддином Раббани, они строили межгосударственные отношения с региональными союзниками, включая Пакистан. Это было неприемлемо для пакистанских военных, надеявшихся на слабый марионеточный режим в Кабуле для сохранения главенствующего положения Пакистана в Афганистане и обеспечения прямого доступа пакистанского правительства к Средней Азии. Такие ожидания спровоцировал вакуум власти после падения просоветского режима в Афганистане. Воспользовавшись неразберихой в результате этнических столкновений и проблемами раздела власти в Кабуле, Пакистан настроил своих союзников в стране против кабульского правительства.

Пакистан не смог установить лояльное Исламабаду правительство в постсоветском Афганистане и не хотел участвовать в длительной войне там. В результате Пакистан не получил денег из-за рубежа для легитимизации боевых действий в Афганистане. Поэтому там разработали новую стратегию борьбы с режимом моджахедов в Кабуле, направленную на то, чтобы сменить новое руководство и получить международную поддержку. Они поддержали обиженных пуштунских лидеров на юге Афганистана, и в 1994 г. небольшая группировка под названием Талибан, объединившая студентов религиозных школ (медресе), объявила себя оппозицией кабульскому правительству и потребовала ото всех участников гражданской войны в Афганистане подчинения.

Однако некоторые аналитики считают, что Талибан, как маленькая самостоятельная группировка, появился в Кандагаре в 1994 г., выступив против действий верхушки моджахедов. Талибы утверждали, что моджахеды воюют за власть и используют ислам для оправдания своих действий. Чувствуя себя униженными и оскорбленными, они решили покончить с этой коррумпированной когортой. Возникает вопрос, как эта небольшая группа превратилась в столь мощную силу. Воспользовались ли они поддержкой ино-

странных игроков и вмешательством таких стран, как Пакистан, США и Саудовская Аравия?[1] Называя себя исламским движением, группировка нередко совершала преступные насильственные действия, включая торговлю наркотиками и жестокие убийства случайных людей.

С другой стороны, объявив себя исламистами, талибы явили миру неверную и жестокую картину ислама. Стали ли эти действия результатом религиозных учений фундаменталистов, или причину следует искать в социальном, культурном и этническом контексте страны? Социальные условия Афганистана проложили путь реакционным взглядам, идущим с Индийского субконтинента и Саудовской Аравии. Талибы явили себя нации под девизом «решения проблем, создаваемых людям афганскими моджахедами». Они заявили о своих целях: разоружить группы моджахедов, участвовавших в гражданских войнах, прекратить производство, распространение и оборот наркотиков, бороться с коррупцией властей и снизить преступность в обществе. Однако их конечной целью было исламское правление, основанное на неких негибких представлениях и интерпретациях ислама.[2]

## Триединая цель Талибана

Известно, что на действия игрока на международной арене влияет внутренняя политика. Без понимания значения и характера Талибана как регионального игрока анализ их отношений с другими странами будет затруднителен.

Стоит отметить, что вопреки общему мнению, «у Талибана нет внешней политики». Правильнее будет рассматривать «внешние отношения» движения, исходя из их «набора верований». Используя понятие внешней политики, мы можем непреднамеренно упустить из виду важные факты. Внешняя политика — это путь реализации государством своих интересов, но в случае Афганистана, увы, Талибан превратился в негосударственное образование с территориальными амбициями.

Отношение Талибана к международным связям и стратегиям до и после прихода к власти в Афганистане отличается. До прихода к власти их усилия были сосредоточены на поиске региональных и глобальных сторонников в войне против сил, возглавляемых США и их союзниками в Кабуле. Однако после прихода к власти они переключились на укрепление своих позиций в стране и получение поддержки региональных партнеров.

Характер движения Талибан определяет сочетание трёх принципов – клановости, языка и политизации религии. Помня об этом, проще понять отношения Талибана со странами мира и региона. Тот, кто поддерживает эти три цели, считается другом Талибана, а тот, кто выступает против них –

---

[1] Peter Marsden, *The Taliban: War, Religion and the New Order in Afghanistan* (Palgrave Macmillan, 1998), 169.

[2] Rohullah Shaikhzada, “An Assessment of the Security Challenges between 2001-2010,” MA Dissertation (Isfahan, Iran: University of Isfahan, 2011), 71-76.

врагом. Поэтому действия Талибана в Афганистане, основанные на трёх принципах племенного кодекса пуштунвали,[3] языкового национализма (использование в первую очередь пуштунского языка) и политизированной интерпретации ислама – деобанди, под влиянием неприятия империализма в начале XX века и во время последующего советского вторжения в Афганистан, могут отражать их отношение к региону и миру.

Поэтому такие страны, как Пакистан и Иран, вряд ли будут поддерживать дружеские отношения с Талибаном. Хотя Иран мог быть союзником Талибана до их прихода к власти и во время вторжения под руководством США, его нельзя считать другом Талибана во всех трёх аспектах. Несогласие Ирана с главными целями Талибана привело к конфликту интересов. Во-первых, Иран выступает против всеобщего применения пуштунвали. Во-вторых, иранские претензии на «культурный Иран», восточные пределы которого включают Афганистан и Среднюю Азию, противоречат экспансионистской стратегии Талибана по управлению Афганистаном. В-третьих, имеет место столкновение исторической памяти Талибана и Тегерана, поскольку династия Хотаки, правившая Исфаханом (современный Иран) в 1722-1738 гг., стала ярким антииранским историческим символом.

С лингвистической точки зрения Иран также мешает языковому национализму Талибана. Национализм пуштунов, больше проявляющийся в языке, чем в расе и религии (ибо они принадлежат к той же расе и религиозной секте ханафитов, что и таджики/парсиваны), видит в Иране главного спонсора персидского языка в Афганистане. Пуштуны считают, что если бы Иран не ввозил персидские книги в Афганистан, пуштуский язык был бы более распространён в стране. Поэтому политика Талибана в отношении Тегерана будет заключаться в том, чтобы помешать Ирану продвигать персидскую литературу и побудить Тегеран поддерживать и развивать культурные программы на языке пушту.

В сектантских и политизированных религиозных интерпретациях Талибана, основанных на деобанди, Иран рассматривают как государство рафидитов,[4] а антишиизм является исторической памятью сторонников радикального ислама. Талибан нападал на собрания шиитов и обезглавил представителей шиитского меньшинства в ряде центральных городов и провинций. Так называемый Вилаят Хорасан Исламского Государства точно так же настроен против шиитов. Поэтому Талибан видит в Иране угрозу исламу,

---

[3] Пуштунвали – традиционный образ жизни и кодекс чести пуштунского народа. Часто именуется «Путь Афганцев» и практикуется пуштунами в пуштунских районах Афганистана, Хибер-Пахтунхвы и севера Белуджистана, согласно учёным. См. Erinn Banting, *Afghanistan: The Land (Lands, Peoples & Cultures)* (Canada: Crabtree Publishing, 2003).

[4] Радида, или рафиди – мусульмане-шииты, отвергающие (rafḍ, ضفر) халифаты двух первых наследников исламского пророка Мухаммеда: Абу Бакра и Умара (Encyclopedia Britannica, 20 July 1998), которых сунниты считают правоверными халифами.

считая его шиитским государством. Придя к власти, Талибан не раз высказывал свои взгляды на права суннитского меньшинства.

То же самое касается отношений Талибана и Пакистаном. «Медовый месяц» талибов с Пакистаном был недолгим. «Пуштунский национализм» талибов вскоре был обращён против Пакистана, через пуштунов за линией Дюрана. Пакистан поддерживал Талибан как стратегический актив против пуштунских националистов в Кабуле, которые не раздували и не поддерживали сепаратизм белуджей и пуштунов в Пакистане. Однако племенная память о пакистанофобии вскоре настроила талибов против Исламабада. Этот сценарий сработал и во время правления в Афганистане моджахедов, пользовавшихся полной поддержкой Исламабада в борьбе с промосковским правительством в Кабуле. Тем не менее, оказавшись в Кабуле, они подвергли критике вмешательство и экспансионизм Пакистана.

Талибы считают, что исламского государства в Пакистане фактически нет; поэтому джихад должен быть продолжен и расширен на Пакистан. Второстепенные фигуры в руководстве талибов не раз критиковали неисламское правительство Пакистана. Эту устоявшуюся ментальность разделяют все исламисты в районе афгано-пакистанской границы. Десятилетний симбиоз афганских и пакистанских талибов повлиял на взгляды афганского Талибана. Верхушка может занимать дипломатичную консервативную позицию по отношению к Пакистану, но реалии на месте противоположны. Если *Pakistani Tahreki Taliban* (PTT) начнёт военные действия против пакистанского режима, тысячи афганских талибов присоединятся к ним. Многие афганские боевики Талибана делали такие заявления на видео и в интервью.[5]

Отношения Талибана со Средней Азией более предсказуемы, поскольку такие страны, как Таджикистан, Узбекистан и Туркменистан, руководствуются политическими соображениями и демонстрируют языковой национализм и клановость. При этнической и языковой общности с Афганистаном, они отвергают политизированную интерпретацию ислама – деобанди – которую исповедует Талибан, поддерживая вместо этого балхо-бухарскую теологическую школу, распространённую во всей Средней Азии. Поэтому Талибан рассматривает эти три страны и всю Среднюю Азию как угрозу своему существованию.

Хотя политика уступок Москвы по отношению к Талибану, как объективной реальности и антиамериканской силе, привела к консервативной политике по отношению к Талибану в Средней Азии, Талибан не рассматривает страны Средней Азии как союзников. Невзирая на три принципиальные цели Талибана, тысячи таджиков, узбеков и других граждан Средней Азии вместе с талибами воевали с НАТО и Афганскими национальными силами обороны и безопасности (ANDSF). Они базировались в Кабуле, ожидая возможности для проведения операций в Средней Азии, перейдя Амударью.

[5] Makhdoom Shahab-ud-Din, “Video|Taliban Chief Announcement After Cutting Fence Wire Erected by Pak Army at Durand line Border,” *Youtube.com*, 2021, https://www.youtube.com/watch?v=Y9mz8lliiOg.

Ранее мы видели, как таджикские террористические группировки заходят в удалённые районы Таджикистана через Бадахшан и отрезают головы военнослужащим таджикских сил безопасности.

Талибан тоже настороженно относится к этим нетерпимым и радикальным среднеазиатским боевикам. Если Талибан попытается депортировать или изгнать их из Кабула и других крупных городов, находящихся под их контролем, эти боевики могут присоединиться к Вилаяту Хорасан Исламского Государства и выступить против Талибана. Руководство Талибана знает, что их среднеазиатские союзники совершили множество нападений на международные силы и ANDSF. Поэтому у талибов отношения симбиоза с радикальными группировками из Средней Азии, что может помешать попыткам Талибана поддерживать тёплые отношения с Душанбе, Ташкентом и Ашхабадом.

Талибан не считает Королевство Саудовская Аравия естественным союзником. Согласно идеологии Талибана, Саудовская Аравия – союзник США с коррумпированным руководством, поддерживающим угнетение мусульман в мире.[6] Этот взгляд превалирует среди боевиков Талибана, особенно руководимых афгано-арабскими джихадистами, присоединившимися к джихаду в Афганистане в 1980-х гг. Одним из таких идеологов был видный афгано-арабский лидер Абдулла Азам. Тысячи арабских беженцев присоединились к талибам позже, в 1994-2001 и 2003-2021 гг., чтобы воевать с силами НАТО. Эти боевики еще больше укрепили антисаудовскую позицию Талибана в своих сочинениях, проповедях и выступлениях.

Созданию и первым победам Талибана помогли пакистанские и саудовские деньги и военные, но вскоре после захвата Талибаном власти в Кабуле в 1996 г. и радушного приёма Усамы бен Ладена Саудовская Аравия отвернулась от талибов. Это способствовало утрате Талибаном власти в конце века. Поэтому Талибан по-прежнему не поддерживает тёплых отношений с Эр-Риядом.[7]

Индия, Китай и Россия также выступают против третьего принципа идеологии Талибана – его радикальной интерпретации ислама (не включая языковой и пуштунский аспекты). Многие лидеры и командиры Талибана заключили союзы с кашмирскими боевиками в Индии, уйгурскими сепаратистами в Китае и российскими джихадистами на Кавказе. Они считают, что во всех трех странах мусульманские меньшинства угнетаются, и поддерживают движения за независимость Кашмира, Синьцзяна и стран Кавказа, которые они идеализируют со времен афганского джихада (1979-1992). Во время своего предыдущего правления (1996-2001) Талибан даже разрешил

---

6 Nawaf E. Obaid, "The Power of Saudi Arabia's Islamic Leaders," *Middle East Quarterly* (September 1999): 51-58, https://www.meforum.org/482/the-power-of-saudi-arabias-islamic-leaders.

7 Mirwais Balkhi, *Saudi Arabia's Foreign Policy Towards Afghanistan; 1991-2014* (Kabul, Afghanistan: Afghanistan Institute of Higher Education, University Афганистана, 2014), 113. – на персидском/фарси.

посольству Чечни работать в районе Вазир-Акбар-Хан в Кабуле. Многие боевики Талибана также присоединились к повстанцам в Кашмире и сражались против индийских сил безопасности.[8] Талибан имеет тесные связи с Исламским движением Восточного Туркестана (ETIM) в приграничных районах Пакистана и Афганистана и сообщалось, что Аль-Каида обучала боевиков Талибана и ETIM в одних и тех же лагерях. Поэтому союзники, которые сражались вместе с ними или присоединились к их джихаду, вряд ли утратят уважение или симпатию к режиму талибов после их прихода к власти.

Языковой принцип не влияет на политику Талибана по отношению к Западу – его политику на этом направлении определяет пуштунвали и радикальная интерпретация ислама. Согласно идеологии талибов, США, НАТО и Европейский Союз рассматриваются как империалистические колониальные державы, вторгавшиеся в Афганистан с целью вестернизации страны. Хотя они могут изменить свою дипломатическую позицию по отношению к Западу, чтобы добиться признания и гуманитарной поддержки афганского народа, оказавшемуся под их управлением, идеологически Талибан попрежнему отвергает Запад и придерживается джихадистского подхода. В их памяти остаётся горькая память о тяжёлом поражении от сил под руководством США в 2001 г., в результате которого они потеряли власть, а тысячи боевиков были убиты или заключены в тюрьмы. Талибы продолжат борьбу против доминирования Запада, предоставляя убежище и обучая мировых террористов, а также занимаясь контрабандой наркотиков. Они не верят, что Эмират может вести обычную войну против сил НАТО, и предпочли бы нетрадиционный подход с применением тактики террора и наркотиков.

## Региональные подходы к Талибану

В этом разделе статьи рассматривается, как заинтересованные страны – Пакистан, Иран, соседние государства Средней Азии, Индия, Китай и страны Запада – воспринимают Талибан и его интересы в регионе.

### *Пакистан*

Пакистан занимает особое положение среди прочих стран, вовлеченных в афганский конфликт. Вооруженные силы Пакистана разработали военные подходы и стратегии, а руководство Исламабада настойчиво пыталось стабилизировать и усилить военную мощь Талибана и легитимизировать его после падения Мазари-Шарифа в 1997 г. Это показательные примеры активной политики и дипломатических усилий Пакистана в отношении событий в Афганистане. Дипломатия Пакистана в Афганистане была успешной по

[8] Ijaz Khalid, "Sino-Russian Stance on Kashmir Issue," *Global Strategic and Security Studies Review* 5, no. 1 (Winter 2020): 47-56, https://gsssrjournal.com/papers/GVFULSIXTQ.pdf.

ряду внутренних и внешних причин. Внешняя политика Исламабада включает попытки повлиять на Афганистан и достичь ряда национальных целей.[9]

Пакистан сыграл решающую роль в создании и поддержке Талибана, используя его как политический, экономический и военный инструмент. С помощью разведслужб США и Великобритании, а также финансовой поддержки Саудовской Аравии Пакистан смог улучшить торговое сообщение со Средней Азией и решить проблему Пуштунистана, используя стратегическое расположение Афганистана. Пакистан последовательно выступает против сильного правительства в Кабуле, которое может поставить под угрозу его интересы или возобновить старые конфликты. Поэтому Пакистан предпочитает создавать и поддерживать в Афганистане такие правительства, как Талибан, которыми он может легко манипулировать для достижения стратегических целей.[10]

Интересы Пакистана в Афганистане можно разделить на три главных уровня:

1. Геополитические цели: Пакистан стремится установить в Афганистане слабое и послушное правительство, игнорируя спор о «линии Дюрана» и ослабляя национальную мощь и потенциал Афганистана, чтобы снизить риск способности Афганистана представлять какую-то угрозу интересам Пакистана или возобновить старые конфликты.
2. Геоэкономические цели: Пакистан стремится получить прямой доступ к Средней Азии и расчистить жизненно важный транзитный маршрут между Пакистаном и рынками Средней Азии. Он также хотел бы получить доступ к нефтегазовым ресурсам стран Средней Азии и превратить Афганистан в рынок потребительских товаров.[11] Насаждение талибов в Афганистане рассматривается как средство достижения этих целей.
3. Геостратегические цели: Стратегическое соперничество Пакистана с Индией определяет баланс сил в Южной Азии. Будучи соседом и посредником между Афганистаном и Индией, Пакистан намерен сохранить своё преимущество. Для этого он пытается помешать Индии

[9] Sayyid Abdul Qayoom Sajjadi, “Taliban, Iran and Pakistan: A Study of Foreign Policy of Iran, Pakistan and Saudi Arabia towards Talliban: Since Mazar-e-Sharif Fall Apart,” *Uloomi Siyasi Journal*, no. 2 (2009), 249, по состоянию на 20 декабря 2021, https://hawzah.net/fa/Article/View/84390/.

[10] Aqajari et al., “The Role of Regional Players in Post-Taliban State Building of Afghanistan,” *Pazhohishnamai Ravabit Bainulmilal*, no. 30 (2015): 57-104, 67.

[11] Nawzar Shafiee, “Power Politics in Afghanistan: Objectives and Behavioral Patterns,” *Mujala’i Siyasati Difah’i*, no. 20 (2002): 29-58, 35.

влиять на Афганистан и предотвратить формирование региональных союзов Ирана, России и Индии или Индии и США в отношении Афганистана.[12]

Контроль талибов над Афганистаном соответствует интересам Пакистана, обеспечивая дружественное правительство, которое поддерживает его цели геополитического, геоэкономического и геостратегического влияния в регионе. Если отстранить талибов от власти, это ограничит способность Пакистана достичь этих целей и потенциально может усилить позиции его соперников в регионе.[13]

### *Иран*

Исламская Республика Иран – важный игрок в Афганском конфликте. Приход талибов к власти в Афганистане был неожиданным и вызвал беспокойство в Иране. Иран рассматривает талибов как опасную группировку, получающую поддержку стран региона и мировых держав. В Иране считают, что Талибан стремится подорвать истинное учение ислама и ограничить региональную политику Ирана при помощи своего крайнего толкования религии и тактики репрессий.[14] Хотя Тегеран может видеть в Талибане союзника по борьбе с Америкой, он не забыл, как Талибан ранее разжёг войну с Ираном, убивая иранских дипломатов и угрожая его безопасности. Кое-кто первоначально считал вторжение в Афганистан под руководством США, которое привело к свержению Талибана, выгодным Ирану, поскольку оно устранило идеологического соперника и явную угрозу его безопасности. Эта общая цель Ирана и США предполагает потенциал сотрудничества и естественного союза.[15]

Тегеран занял выжидательную позицию после захвата власти талибами в Афганистане, но остаётся скептичным к своему бывшему союзнику. Внезапный и драматичный захват Кабула талибами заставляет Тегеран думать, как быть дальше. Несмотря на свою давнюю оппозицию кабульскому режиму, Иран не настроен на взаимодействие с Талибаном после мелких стычек боевиков Талибана с иранскими пограничниками в провинции Нимроз в декабре 2021 г. Иранские стратегические службы пытаются разрешить непредсказуемость ситуации, особенно в отношении расширения возможностей Талибана благодаря США и судьбы военной техники, захваченной Талибаном у США и Национальных сил обороны и безопасности Афганистана (ANDSF). Персидская поговорка о том, что «лучше с умным потерять, чем с

[12] Umul Banin Tawhidi, “Afghanistan Issues: the US and Others,” *Mah’awinat Pazhohishhai Siyasati Khariji*, no. 301 (2009): 64-87, 11.

[13] Shafiee, “Power Politics in Afghanistan,” 66.

[14] Ibrahim Ahmadi and Jawad Etahat, “A Geopolitical Analyses of Pakistan Relations with Others: Conflicts and Threads,” *Tahqiqat Bainulmilali Journal*, no. 24 (2015): 1-24, 17.

[15] Dehqani Firuzabadi and Sayyid Jalal, “Iran’s Foreign Policy Towards Afghanistan’s Crisis,” *Pazhohishi Hoqoq wa Siyasat*, no. 20 (2006): 7-22, 11.

дураком найти», вынуждает Тегеран занять оборонительную позицию и опасаться намерений Талибана.

### *Саудовская Аравия*

Будучи одним из главных экономических ресурсов суннитских джихадистских группировок и партий в рамках своей идеологической стратегии со времен афганского джихада 1994-1996 гг., Саудовская Аравия тем не менее не играла заметной роли в афганском конфликте. Политика поддержки талибов саудовцами достигла пика в 1996 г., когда Саудовская Аравия, как основной источник финансирования этой группировки, сыграла важную роль, помогая Талибану устранить все другие партии и группировки с военной арены в Афганистане. После визита директора Службы общей разведки Саудовской Аравии принца Турки аль-Фейсала в Пакистан в июле 1996 г. Саудовская Аравия стала главным финансовым спонсором Талибана.[16] Однако у Королевства есть опасения по поводу безопасности из-за антисаудовских исламистов, которые нашли убежище у талибов.

Кроме того, некоторые группы в религиозных кругах Саудовской Аравии реально воевали, поддерживая Талибан против альянса ANDSF/НАТО, хотя многие из них состояли в других радикальных джихадистских группировках, таких, как Вилаят Хорасан Исламского Государства. После вывода американских войск и падения афганского правительства они теперь благополучно живут в Кабуле и никак не задействованы. Они могут сосредоточиться на своей основной цели — организации терактов против Саудовской Аравии или любой другой цели в любой точке мира. Консервативная политика Саудовской Аравии в отношении Талибана и Афганистана, вероятно, станет более активной. Стоит отметить, что посольство Саудовской Аравии в Кабуле не входило в число четырех посольств, остававшихся открытыми и осуществлявшими консульскую деятельность 15 августа, когда талибы вошли в Кабул.[17] Хотя кое-кто в Пакистане может пытаться наладить отношения между Эр-Риядом и Талибаном, Саудовская Аравия не особо доверяет талибам.[18]

---

[16] Sajjadi, “Taliban, Iran and Pakistan: A Study of Foreign Policy.”

[17] В дни смятения и опасности продолжали работу четыре посольства – Пакистана, Ирана, Китая и России. Остальные покинули Афганистан за несколько недель или в день краха. Одним из первых было эвакуировано посольство Саудовской Аравии.

[18] Suhasini Haidar, “Taliban Have Responsibility to Exercise Good Governance, To Be Inclusive: Saudi Foreign Minister,” *The Hindu*, September 19, 2021, https://www.thehindu.com/news/national/saudi-foreign-minister-faisal-bin-farhan-al-saud-interview-taliban-have-responsibility-to-exercise-good-governance-to-be-inclusive/article36556729.ece.

### *Индия*

Приход Талибана к власти в Афганистане при помощи межведомственной разведки Пакистана в оба периода (1994–2001 и 2003–2021 гг.) вызвал обеспокоенность в Индии. Он был чреват нежелательными последствиями для страны. После того, как талибы 15 августа захватили Кабул, посольство Индии в Кабуле закрылось, а политические отношения с правительством талибов были прерваны, поскольку индийское правительство не признало легитимность Талибана. Более того, Индия рассматривает идеологию Талибана как угрозу своей безопасности, поскольку распространение их идей в Джамму и Кашмире угрожает безопасности и единству Индии.[19] Приход Талибана к власти с помощью Пакистана, давнего соперника Индии, ограничил любые потенциальные выгоды для Индии. Доступ к энергоресурсам Средней Азии критически важен для Индии, а создание военных баз в некоторых странах Средней Азии является одной из стратегических целей Индии.[20]

Индия была единственной представленной в Афганистане страной, не поддержавшей Талибан, но эта стратегия уже не актуальна. Прагматичная внешняя политика партии «Бхаратия Джаната» сосредоточена на ограничении влияния Пакистана, и поддержка афганского/пуштунского национализма является её важным приоритетом. Индия быстро признала псевдоправительство Мохаммада Ашрафа Гани, и индийское стратегическое сообщество советует политикам изучить возможность установления связей с Талибаном, используя антипакистанские настроения пуштунов. Индия стремится привлечь талибов к Дели и создать треугольник из талибов, пуштунских националистов в Хибер-Пахтунхве и Дели, чтобы оказать давление и, возможно, разорвать Пакистан.

## Взгляды на Талибан из-за пределов региона

### *США*

Нападение Аль-Каиды на башни-близнецы 11 сентября 2001 г. привело к нападению США на Афганистан. Нападение произошло, когда США находились на пике могущества и могли доминировать в новом мировом порядке после распада Советского Союза. Поэтому после 11 сентября Соединенные Штаты увидели новые угрозы и врагов, а борьба с терроризмом стала геополитическим приоритетом внешней политики США. Набор политико-географических представлений, определяющих внешнюю политику страны за её пределами, составляет геополитический код. Страны стремятся влиять на геополитические коды других стран для реализации своих целей и интере-

[19] Aqajari et al., “The Role of Regional Players in Post-Taliban State Building,” 74.

[20] Nawzar Shafiee et al., “India’s Approach towards Afghanistan after September 11,” *Geopolitical Journal*, no. 2 (2012): 91-126.

сов. Борьба с терроризмом стала приоритетом, а Афганистан, предоставивший убежище Аль-Каиде, был стратегически важен с точки зрения географии, экономики и геополитики.

В начале 2020-х гг. политика США в отношении Афганистана претерпела существенные изменения. Многие геополитические соперники, стремившиеся использовать Афганистан в своих интересах, включая Китай, Россию и Иран, поддерживали Талибан и выступали против присутствия США в Афганистане. Сообщалось даже о прямых нападениях Китая на вооруженные силы США.[21] Спустя 20 лет в США устали от войны и перешли к политике сдерживания и дипломатических союзов для защиты от потенциальных угроз со стороны Афганистана. Однако США продолжают внимательно следить за Талибаном и дали понять, что готовы при необходимости участвовать в нетрадиционной войне.

### *Россия*

Страны бывшего Советского Союза считаются влиятельными игроками в переменчивых условиях Афганистана. Ситуация в Афганистане оказывает серьёзное влияние на Таджикистан, а Туркменистан практически не способен влиять на Афганистан. Узбекистан уделяет приоритетное внимание своей национальной безопасности, а для этого важна стабильность Афганистана. Россия, как важнейший игрок Содружества Независимых Государств, стремится не допустить превращения исламизма в общую политическую базу региона Средней Азии. С точки зрения России, Афганистан является источником насилия и незаконной торговли, в том числе наркотиками и оружием, а также крупным экспортёром исламского экстремизма. Эта точка зрения подкреплена историческим опытом исламистских группировок, таких, как Исламское движение Узбекистана – экстремистской исламской группировки, подготовленной Талибаном в 1990-х гг. и до сих пор поддерживаемой им. Во время гражданской войны Партия исламского возрождения Таджикистана опиралась на военные базы и финансовые ресурсы в северо-западных районах Афганистана.

Москва поддерживала связи с Талибаном до ухода США из Афганистана. В то же время Россию беспокоила безопасность в связи с международными террористическими группировками, действующими вместе с Талибаном. Если в будущем вспыхнут столкновения из-за отсутствия у Талибана действенного контроля над северо-восточными границами Афганистана, эти отношения могут быстро ухудшиться и дестабилизировать регион. Россию также беспокоит уязвимость Талибана перед экстремистскими группировками, ибо она считает эти группировки самой серьёзной угрозой стабильности в Средней Азии. Кроме того, перемещение людей между странами

[21] اظهار بی‌اطلاعی چین از اخراج شهروندان‌اش از افغانستان به اتهام جاسوسی, *Deutsche Welle*, January 8, 2021.

Средней Азии и Афганистаном способствовало развитию экстремистских исламских идеологий в религиозных кругах.[22]

### *Европейский Союз*

Европейский Союз был вовлечен в конфликт в Афганистане, поскольку терроризм и организованная преступность признаны серьёзной угрозой для Европы. Афганистан важен для борьбы ЕС с терроризмом, и Евросоюз стремится расширить своё влияние как глобального игрока, предлагая свой подход к урегулированию конфликтов и установлению мира. Однако страны-члены ЕС имеют разные взгляды на свою роль в Афганистане. Некоторые государства, не слишком озабоченные терроризмом, обеспокоены тем, что поражение в Афганистане подорвёт авторитет НАТО и Запада. Другие страны присутствуют в Афганистане в силу глубоких стратегических связей со США. Некоторые считают, что их безопасность (за исключением Великобритании) зависит от ситуации в Афганистане, что толкает их к союзу со США. Хотя европейские правительства не играют доминирующей военной роли в Афганистане, они предлагают международную помощь в рамках Союза или двусторонних соглашений для обеспечения безопасности и стабильности Афганистана.[23]

## Что нужно делать дальше?

По мнению автора, как региональные, так и более далёкие страны, вовлечённые в афганский конфликт, должны занять выжидательную позицию в отношении Талибана. Нужна двойная стратегия с фундаментальным политическим подходом, направленным на поиск долгосрочного разрешения конфликта в Афганистане при одновременном оказании немедленной гуманитарной помощи населению. Вот некоторые предложения:

- Нынешние усилия Талибана направлены на получение признания, но всем государствам следует проявлять осторожность в этом отношении. Поддержка режима Талибана в долгосрочной перспективе никому не принесет пользы и может привести к потере стратегических друзей в Афганистане, особенно среди простых людей. С другой стороны, Талибан следит за поддержкой США, и вчерашние стратегические враги завтра могут попытаться стать друзьями.
- Международное сообщество может предоставить Афганистану гуманитарную помощь и поддержку. Страны, имеющие опыт работы с Талибаном, например, оказание денежной помощи в 1990-х гг. или

[22] Mohammad Darkhor, “Regional and Trans-Regional Strategic Approach towards the US Withdrawal from Afghanistan,” *Rahnama Siyasatguzari Journal*, no. 2 (2012): 53-67, 62.

[23] Yaser Nooralivand and Ali Khalilipour Roknabadi, “Multilateralism and Trans-Atlantic Relationship in Afghanistan,” *Strategic Studies Quarterly* 14, no. 51 (June 2011): 175-200, 187, https://doi.org/20.1001.1.17350727.1390.14.51.7.9.

применение мягких мер, могут поделиться своим опытом. Модель совместного обучения и подходы к образованию девочек в Пакистане, Иране, Саудовской Аравии и других странах региона дают хороший пример для подражания.

- Важно продолжать политику экспорта товаров из соседних стран в Афганистан, поскольку это критично для благосостояния населения и может помочь снизить напряженность на границе, а закрытие границ и прекращение торговли нанесут вред людям.

## Заключение

Появление и приход к власти Талибана в Афганистане привели к принятию региональными и трансрегиональными игроками различных стратегий. Пакистан и Саудовская Аравия поддерживали и финансировали Талибан, рассматривая его как инструмент продвижения своих региональных интересов, в то время как Иран, Индия и страны Средней Азии выражали обеспокоенность и восприняли Талибан как угрозу своим интересам в регионе. Межрегиональные подходы к приходу талибов к власти также существенно различаются. Поначалу США не считали эту группировку угрозой своим интересам. Однако теракты 11 сентября, укрывание Усамы бен Ладена в Афганистане и агрессивный характер группировки заставили Соединенные Штаты изменить свою позицию и попытаться разгромить и ликвидировать террористическую организацию. Политика Европейского Союза в отношении Талибана, основанная на применении НАТО статьи 5, также заслуживает внимания. Напротив, Россия рассматривает Афганистан как источник насилия, наркотиков и оружия, и экспортера исламского экстремизма, угрожающего её интересам и интересам соседних стран Средней Азии. Поэтому Россия, как трансрегиональный игрок в Афганистане, не приветствует Талибан.

В целом, существуют разные взгляды на Талибан на региональном и на межрегиональном уровне. Одни выражали оптимизм в связи с появлением этой группировки, другие придерживаются более пессимистической точки зрения. Выход Талибана на политическую арену Афганистана привел к формированию многомерной политики и изменению международных перспектив.

## Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

## Об авторе

Д-р **Мирваис Балхи** – приглашённый научный сотрудник, специалист в области международных отношений и ближневосточных исследований Джорджтаунского университета в Катаре. Имеет обширный опыт управленческой и научной работы: был министром образования Исламской Республики Афганистан с 2018 по 2020 гг. и заместителем посла Афганистана в Индии. Балхи получил степень доктора международных отношений со специализацией по Западной Азии в Университете Джавахарлала Неру в Дели, Индия. Плодовитый автор, опубликовавший множество научных трудов на английском и персидском языках. До прихода в Джорджтаунский университет в Катаре д-р Балхи преподавал на факультете права и политологии Американского университета Афганистана (AUAF) и на факультете международных отношений Института высшего образования Афганистана (UofA).
*Электронная почта*: mirwaisbalkhi@yahoo.com

# *Connections: The Quarterly Journal*
## Указания по подаче материалов и стилю

*Connections* принимает рукописи объёмом от 2000 до 5000 слов, написанные понятным языком для целевой аудитории информированных специалистов-практиков и учёных в области обороны и безопасности. Все рукописи следует подавать в редколлегию *Connections* на электронную почту PfPCpublications2@marshallcenter.org или загружать на веб-сайт журнала, https://connections-qj.org. В них должно быть указано имя автора, нынешнее место его работы и предварительное название вверху первой страницы, а также, при необходимости, ссылки. Кроме того, авторы должны представить аннотацию и ключевые слова рукописи.

Предпочтительные темы для будущих изданий журнала:

- Постконфликтное управление
- Противодействие гибридной войне
- Укрепление Североатлантического альянса
- Борьба за ресурсы и её влияние на безопасность
- Негосударственные игроки в киберпространстве
- Новые и прорывные технологии
- Цифровые трансформации и безопасность
- Строительство институтов обороны
- Борьба с коррупцией и формирование добропорядочности
- Совершенствование военного образования

По вопросам сносок и ссылок см. Chicago Manual of Style, http://www.chicagomanualofstyle.org/ tools_citationguide.html.

Инициативные рукописи принимаются в текущем порядке на усмотрение Редколлегии Консорциума ПрМ.

**Мнения, выраженные во всех публикациях Connections, являются исключительно точками зрения авторов и не являются официальными точками зрения Консорциума военных академий и институтов по изучению вопросов безопасности в рамках программы «Партнерство ради мира», участвующих организаций или редакторов Консорциума.**

**Оперативный отдел Консорциума военных академий и институтов по изучению безопасности в рамках программы «Партнерство ради мира» расположен в Европейском центре по изучению вопросов безопасности им. Джорджа К. Маршалла:**

**Partnership for Peace – Consortium**
**Managing Editor – LTC Ed Clark**
**Gernackerstrasse 2**
**82467 Garmisch-Partenkirchen, Germany**
**Phone: +49 8821 750 2259**
**E-Mail: PfPCpublications2@marshallcenter.org**

**ISSN 1812-1101**