УДК 004+327+327.8 Вестник СПбГУ. Международные отношения. 2024. Т. 17. Вып. 3

Kuberpolitik — власть в цифровую эру

В. В. Григорьевский

Национальный исследовательский институт мировой экономики
и международных отношений им. Е. М. Примакова РАН,
Российская Федерация, 117997, Москва, ул. Профсоюзная, 23

Для цитирования: *Григорьевский В. В.* Kuberpolitik — власть в цифровую эру // Вестник Санкт-Петербургского университета. Международные отношения. 2024. Т. 17. Вып. 3. С. 362–381. https://doi.org/10.21638/spbu06.2024.308

В статье исследуются информационно-коммуникационные технологии (ИКТ) как инструмент международного влияния. Цель статьи — определить предметную область науки о международных отношениях, в которой бы изучались мировые политические процессы, использующие ИКТ или основанные на ИКТ. Автор проанализировал существующие определения киберполитики и выявил причины, по которым они не отражают исследуемый предмет в полном объеме. Используя методологию общей теории систем (включая системный анализ и кибернетику), структурный функционализм, положения неореализма и неолиберализма, а также методики структурного анализа, абстрагирования и моделирования, автор разработал системную модель для анализа киберполитики как многоаспектного и многоуровневого явления, включающего в себя социотехнические и социотехнологические подсистемы, а также их иерархии, показал связь с уровнями социальной системы, каждый из которых выполняет различные функции и имеет определенную значимость с точки зрения кибернетического управления. Предложены и обоснованы формула и функция влияния, которые определяют ключевые переменные, определяющие как природу влияния в общем виде, так и каждый конкретный случай влияния. Автор описал ключевые компоненты технических и технологических ИКТ-систем, чтобы дать представление как об их структуре, так и о процессах их создания и использования. Рассмотрены понятие глубоких технологий и их возможная роль в усилении международной конкуренции и технологической взаимозависимости в современном мире. В результате были типологизированы объекты и субъекты политических отношений в данной сфере, сформулирован предмет международной киберполитики как относящийся к политической науке, изучающей как существующие, так и возможные аспекты мировой политики в сфере ИКТ, для чего предложен новый термин — «комплексная киберполитика», или *Kuberpolitik*. Разработана матрица для оценки потенциальных моделей влияния, приведен пример прогнозирования с помощью этой матрицы, даны рекомендации по направлению дальнейших исследований (составление детальных матриц для каждого типа субъекта, описание всех возможных моделей влияния).

Ключевые слова: киберполитика, комплексная киберполитика, Kuberpolitik, информационно-коммуникационные технологии, «глубокие технологии», цифровая эра, цифровая экономика, цифровизация, системный анализ.

Введение

В связи со стремительным развитием глобальной индустрии информационно-коммуникационных технологий (ИКТ), особенностями их предоставления

© Санкт-Петербургский государственный университет, 2024

на международном рынке (осуществляемого зачастую без физического проведения импортно-экспортных операций в их традиционном виде), а также проникновением ИКТ в большинство сфер жизнедеятельности возникает необходимость исследовать ИКТ как инструмент международного влияния.

Как и многие другие сферы, которые созданы прежде всего частными международными компаниями и изначально фактически регулировались рынком, сфера ИКТ становится не просто новым фокусом внимания государств и региональных интеграционных объединений как субъектов мировой политики — она политизируется и оказывается инструментом политического регулирования, прямого или опосредованного влияния на других — государственных и негосударственных субъектов, включая индивидов, частные предприятия и ТНК.

Развитие данного феномена привело к тому, что в конце 1990-х годов начали появляться первые определения киберполитики. Тем не менее до настоящего времени не было проведено системного анализа описываемого явления.

Цель статьи — определить предметную область науки о международных отношениях, в которой бы изучались мировые политические процессы, использующие ИКТ или основанные на ИКТ.

Исследование опирается на методологию общей теории систем (включая системный анализ и кибернетику) и структурного функционализма Т. Парсонса, положения неореализма и неолиберализма (для определения субъектов), а также методики структурного анализа (для декомпозиции объекта), абстрагирования и моделирования (для графического представления результатов).

В первом разделе автор сравнил существующие определения киберполитики и выявил причины, по которым они не отражают исследуемый предмет в полном объеме. Во втором разделе приведена авторская методология определения предмета киберполитики, далее следуют разделы с детальным описанием субъектов и объектов этого предметного поля. В последнем разделе систематизируются методы международного влияния в сфере ИКТ. В конце статьи представлены результаты исследования, в которых дается определение предложенному автором понятия «комплексная киберполитика», или *Kuberpolitik*.

Киберполитика: сложности концептуализации

С конца 1990-х годов в научной литературе было дано много различных определений киберполитики, которые описывают этот феномен с разных сторон. Автор проанализировал существующие определения с целью поиска того из них, которое бы наиболее точно отражало суть рассматриваемого предмета.

Итогом детального анализа литературы стал сводный обзор 42 прямых или опосредованных определений киберполитики, были выявлены ключевые причины, по которым эти определения не могут считаться достаточно полными: 1) они охватывают лишь незначительную часть предмета (участие индивидов в политических процессах, политические коммуникации и СМИ, регулирования интернета, кибервойны и пр.); 2) для определения используются слишком широкие понятия.

Бóльшая часть исследований в области киберполитики рассматривает влияние ИКТ на участие индивидов в политических процессах. Примерами могут стать работы таких авторов, как К. Хилл и Дж. Хьюз [1], М. Меккель [2], Б. Гронбек

и Д. Визе [3], Ш.-Д. Лю [4], А. Шехаби и М. Джонс [5], Х. Гусфа и Ф. Каджуанд [6], С. Ю, Ц. Ван и Ю. Лю [7]. Киберполитика в этих работах трактуется как «возможности интернета предоставлять обществу бесплатную удобную платформу для получения политической информации и участия в политической жизни» [7].

Особое внимание при изучении киберполитики уделяется политическим коммуникациям и роли СМИ в политических процессах. Именно такой логики придерживаются Д. Халлин и П. Манчини [8], Э. Чедвик [9; 10] и Ф. Говард [11; 12], М. Тури [13], С. Коулман и Дж. Блумлер [14], П. Де Ла Гарса Монтемайор, Д. Ибаньес и П. Лопес-Лопес [15]. Киберполитика в этом случае предстает как «способы, которыми политические деятели используют новые технологии», а также «политические махинации по установлению телекоммуникационных стандартов и принятию решений о том, как проектировать информационную инфраструктуру» [12].

Помимо этого, киберполитика изучатеся в таких ее аспектах, как:

- влияние интернета и его регулирование: Р. Дейберт [16; 17] и Э. Финберг [18];
- кибервойны: Л. Янчевский и Э. Коларик [19], Я. Лимнелл [20];
- определение силы в киберпространстве: М. Вайс [21] и Б. Банта [22];
- роль и влияние Big Tech: Л. Шэн [23];
- использование, обмен и хранения информации и данных: Ю. Суда [24];
- связь с процессами глобализации: Д. Кельнер [25];
- философский и пр. аспекты: А. Роза, К. Фернандес, К. Трон, Х. Бенсусан, Ф. Луиг, Ж. Юнг, Х. Килиси-Гонсалес, М. Гонсалес, М. Броенс, М. Мэллори, Н. Матуччи, Д. Валентини, В. Романини, Р. Гуарда, Р. Седдон, М. Паванини и В. Лубрано [26].

Частой причиной неполноты определения является использование широких или абстрактных понятий, которые «размывают» предмет исследования: «политические цели», «политическая коммуникация», «политическое поведение», «кибертехнологии», «политическая сила» и «цифровая сфера». В таких категориях рассуждают Д. Роткопф [27], Н. Шукри [28–30], Т. Джордан [31], Р. Хейг и Б. Лоадер [32], Ким Ён Чхоль [33], Ф. Крамер, С. Старр и Л. Венц [34], К. Мартинс [35; 36], Дж. Най и Д. Уэлч [37]. В качестве примера можно привести одно из наиболее цитируемых определений киберполитики, данное профессором политологии Назлы Шукри: совокупность двух процессов или реальностей — тех, которые относятся к взаимодействиям между людьми (политике), определяющим, кто что, когда и как получает, и тех, которые возникают в результате использования виртуального пространства (киберпространства) в качестве новой арены для споров с его собственными условиями и реалиями [29].

Среди наиболее удачных, по мнению автора, описаний имеет смысл отметить три.

Первое предложил в 2019 г. доцент университета из Джакарты (Universitas Pembangunan Nasional Veteran Jakarta) Дж. Индраван, который хотя и не дал точного определения «киберполитики», перечислил множество ее различных аспектов: политические кампании и коммуникации, активизм, кибербезопасность и кибервойны, определение киберпространства, роль образования и пр. [38].

Второе описание в 2019–2020 гг. дали аргентинские исследователи М. Вила-Сеоане и М. Сагье, рассмотревшие «конфликт и сотрудничество между группой соответствующих акторов в области киберполитики в четырех конкретных областях, представляющих интерес для международных отношений: кибербезопасность, управление мировой торговлей и финансами, права человека и гражданство

в интернете, пространство» [39]. Также вместо одного «пространства» они упоминают множество «пространств… для основных арен, на которых происходят споры о построении цифрового миропорядка» [40].

Наиболее полное описание киберполитики дали в 2013 г. американские исследователи — профессор политологии Назлы Шукри и информатик и пионер интернета Дэвид Кларк — в статье «Кто контролирует киберпространство» [41]. Они определили как уровни киберпространства (физический, интернет, сервисный, приложений, информационный, человеческий), так и типы субъектов (индивидуальный, государственный, международный, глобальный, некоммерческий и коммерческий), задействованных в киберполитике.

Тем не менее даже в этих детальных определениях не рассмотрены потенциальные инструменты влияния, а также не раскрыта в полной мере суть самих информационных технологий.

На основании проведенного анализа можно сделать вывод, что хотя термин «киберполитика» используется в различных контекстах, на данный момент отсутствует его универсальное определение. Каждый исследователь рассматривает, как правило, какой-то конкретный аспект этой сравнительно новой политической реальности и деятельности, отдельных субъектов (государства, организации, индивиды и т. д.), конкретные инструменты влияния (выборы, информационные войны, экономическая зависимость, культурное влияние и т. д.) или лишь определенные части или сферы ИКТ (интернет, контент, цифровые сервисы и пр.).

Возникает проблема уточнения понятийно-категориального аппарата этого нового предметного поля исследования политической науки. Есть потребность наиболее точно определить предмет киберполитики, чтобы изучать тенденции развития.

Методология

Автор разработал системную модель, которая позволяет рассмотреть киберполитику масштабно — как многоаспектное и многоуровневое явление — и выделить как уже исследованные аспекты этого явления, так и потенциальные, а также увидеть возможности, контуры и предлагаемые практики многоуровневого управления данным явлением в условиях все более жесткой международной конкуренции.

Автор предложил назвать этот сложный феномен во всем своем многообразии комплексной киберполитикой (*comprehensive cyberpolitics*, или *Kuberpolitik,* для отличия от множества существующих и рассмотренных выше определений — *cyberpolitics*), по аналогии с «комплексной геополитикой» (*comprehensive geopolitics*, подходом к изучению геополитики, который учитывает широкий спектр факторов за пределами традиционной политической географии и политики в категориях силы). Такое название позволяет очертить рамки исследуемого предмета, а также предложить инструменты прогнозирования сценариев развития мировой кибирполитической системы.

Для исследования данных процессов автор предлагает использовать структурный анализ социальных систем и подсистем: социотехнических и социотехнологических.

Социотехническая система (СТС) в узком смысле — это система, состоящая из индивидов и технических средств, с которыми человек взаимодействует для выполнения какой-либо операции. Это может быть как личное повседневное

использование (двое людей коммуницируют между собой через мобильные устройства по интернету), так и профессиональная деятельность (сотрудник предприятия работает на компьютере в программе для бухгалтерского учета).

Социотехнологическая система (СТлС) — это система, деятельность которой направлена на создание (проектирование, разработку, реализацию, поддержку и пр.) технических систем. Например, это группа инженеров и набор программно-аппаратных средств, используемых для создания программного обеспечения (для коммуникации через интернет или для ведения бухгалтерского учета) либо аппаратного обеспечения (мобильное устройство, компьютер).

Особенностью ИКТ является то, что они используются как в СТС, так и в СТлС, тогда как другие технологии, к примеру технологии добывающей и обрабатывающей промышленности, используются только в СТлС (см. рис. 1).

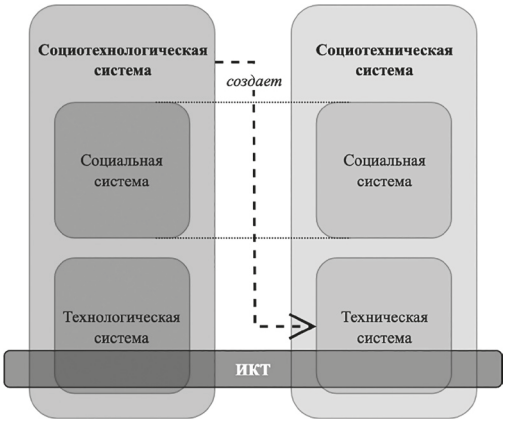

Рис. 1. Связь социотехнической и социотехнологической систем

При этом существует иерархия СТлС, так как одна СТлС может создавать средства производства другой СТлС более низкого уровня (например, процессор как продукт и как средство производства) (см. рис. 2).

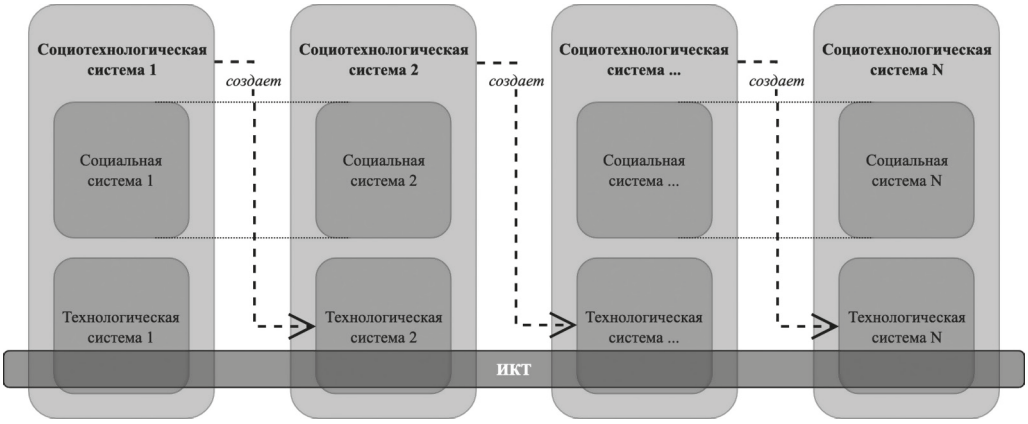

Рис. 2. Иерархия социотехнологических систем

Для анализа рассматриваемых систем и их иерархий автор обращается к науке об общих закономерностях процессов управления и передачи информации в машинах, живых организмах и обществе [42] — кибернетике. Кибернетику как науку следует рассматривать шире, чем просто сферу ИКТ. Поскольку ее объектом являются все управляемые системы, кибернетика рассматривает любые СТС и СТлС как кибернетические системы (КС). Но когда объектом управления становится сама кибернетическая система, можно также говорить об иерархии кибернетических систем и формировании КС более высокого уровня.

Аналогичный подход был применен американским социологом Талкоттом Парсонсом для анализа социальных систем. В частности, им была разработана методология структурного функционализма с использованием понятия социальной системы, которая имеет свою структуру и механизмы взаимодействия структурных элементов, каждый из которых выполняет собственную функцию.

Определения СТС / СТлС, приведенные выше, из непосредственно социальной системы используют лишь один элемент — человека. Безусловно, социальная система является более сложным образованием, поэтому рассмотрим ее более детально, особенно те ее части, которые влияют на поведение человека.

Т. Парсонс предложил четыре функции социальной системы — сохранение образца, интеграции, достижение цели и адаптации, которые можно соотнести к социальным подсистемам, через которые эти функции реализуются: правовая, культурная, политическая и экономическая. Данные функции приведены Парсонсом в порядке убывания значимости с точки зрения кибернетического управления процессами действия в системе рассматриваемого типа [43].

Правовая система, по мнению Т. Парсонса, имеет наибольшую значимость с точки зрения управления процессами в социальной системе, так как зачастую невозможно в короткий срок радикально изменить нормативную и судебную системы общества (здесь, конечно, не идет речь о революционных изменениях). Культурная система в стране может меняться быстрее, чем законы, но медленнее, чем политическая система, что обуславливает степень влияния этих систем на условия функционирования общества. Экономическая же система, выполняющая функцию адаптации, призвана оперативно реагировать на изменение рыночной конъюнктуры для обеспечения жизнедеятельности общества разного рода ресурсами (см. рис. 3).

Рис. 3. Структура социальной системы (на основе модели Т. Парсонса)

Техническую/технологическую систему нельзя непосредственно включить в социальную систему, но можно предположить, что такая система является продуктом

социальной системы и зависит от нее. Это дает возможность не только связать все эти системы, но и исследовать их взаимозависимость в категориях власти.

Кибернетика изучает процессы управления (control). Но для выполнения управляющего воздействия субъекту управления необходимо иметь средства и возможности управления. Другими словами, субъекту управления необходимо обладать соответствующей властью (power) в достаточном объеме. Таким образом формируется отдельная научная проблема, неразрывно связанная с предметом политической науки: как работают процессы обретения, удержания, распределения и использования власти в кибернетических системах.

Так как отдельные кибернетические системы в наше время достигают не просто государственного масштаба (электронное правительство, критическая инфраструктура, электронный документооборот), но и глобального (интернет, социальные сети, облачные сервисы и пр.), возникает необходимость исследовать данную проблему на международном уровне.

Предлагаемая автором методика анализа власти в международной кибернетической системе сводится к двум этапам: выбор и обоснование элементов функции власти в международном киберпространстве.

Необходимыми и достаточными элементами функции власти в первом приближении являются наличие субъекта власти (актора), объекта власти (ресурса), а также возможности и/или фактов использования такой власти (влияния). В контексте данного исследования такие понятия, как «методы влияния», «формы власти» и «способы контроля», используются взаимозаменяемо и по своей сути описывают потенциал воздействия субъектов на объекты. Следовательно, автор предлагает использовать следующую упрощенную формулу влияния:

$$(s \overset{m}{\rightarrow} o),$$

где субъект *s* воздействует методом влияния *m* на объект *o*.

Контроль над ресурсами как источник власти — это, пожалуй, одно из немногих утверждений в политической теории, с которым согласны представители абсолютно разных времен, концепций и парадигм: Сунь-Цзы, Фукидид, Аристотель, Н. Макиавелли, Т. Гоббс, Дж. Локк, В. Парето, Г. Моска, Г. Моргентау, Дж. М. Бьюкенен-мл., Г. Киссинджер, С. Ф. Хантингтон, Р. Кохейн и др.

Данный подход справедлив для уже ставших классическими сфер мировой политики: геополитики (США имеют стратегическое расположение между двумя океанами), политики нефти (ОПЭК регулирует цены на нефть), политики космического пространства (США обладает наибольшим количеством искусственных спутников Земли), политики воды (Эфиопия владеет ГЭС Хыдасе) и т. д. Следовательно, его можно применить и для киберполитики.

Следует отметить, что, очевидно, конечной целью влияния является не контроль над ресурсами как объектами власти, а влияние на других субъектов, поэтому объекты становятся инструментом влияния, а функция влияния может быть представлена в следующем виде:

$$p = f(s_1, s_2, m, o),$$

где p — множество всех возможных вариантов влияния; s_1 — множество всех возможных типов субъектов, оказывающих влияние; s_2 — множество всех возможных

типов субъектов, на которых оказывается влияние; m — множество всех возможных методов влияния; o — множество всех возможных объектов влияния.

Соответственно, формула влияния выглядит как

$$(s_1 \overset{m}{\rightarrow} o) \overset{p}{\rightarrow} s_2,$$

где субъект s_1, воздействуя методом влияния m на объект o, тем самым оказывает влияние p на субъект s_2.

Каждая форма международных отношений — это сложная, многогранная и динамичная система, а реальные процессы влияния часто нелинейны и зависят от множества факторов, которые сложно свести к одной формуле. Вышеуказанные функция и формула влияния являются упрощенными моделями, описывающими ключевые параметры (переменные) влияния и их взаимосвязь с целью их последующего анализа в рамках данной статьи.

Выявление и изучение инструментов влияния в международной кибернетической системе должны установить детальное определение конкретного предмета, который описывается предлагаемым автором понятием Kuberpolitik.

При рассмотрении субъектов фокус делается в первую очередь на те их типы, которые в большей степени наделены возможностями во властных процессах, — это государства, международные организации и крупные ТНК. Так, участниками данных процессов прямо или косвенно являются акторы на всех уровнях системы международных отношений. Для определения субъектов исследования автор основывается на положениях неореализма (государства и их союзы как ключевые акторы), но также принимает во внимание парадигму неолиберализма для учета основных участников процессов использования ИКТ (индивиды, частные и транснациональные компании).

Объектами Kuberpolitik выступают различные компоненты и подсистемы глобальной иерархии СТС / СТлС в сфере ИКТ, все, что может прямо или опосредованно использоваться в таких системах. При этом анализируются как материальные (или физические) объекты, так и нематериальные (виртуальные объекты и логические ресурсы).

Методы влияния реализуются через социальные подсистемы: правовые, культурные, политические и экономические.

Весь диапазон воздействий установленных субъектов на установленные объекты, а также влияние одних субъектов на других являются предметом Kuberpolitik.

В данной статье автор не рассматривает цели воздействия и/или влияния, так как их природа может иметь различный характер — от целей индивидов до целей международных организаций и союзов. В фокусе исследования — ответ на ключевой вопрос о том, как такое влияние может реализовываться или реализуется в международной среде.

Субъекты Kuberpolitik

Исследуемая система представляет собой многоуровневое функциональное пространство, в рамках которого действуют различные типы субъектов и наблюдается формирование контуров многоуровневого управления. В рамках проведенного анализа автор выделил отдельные их типы.

Государства (включая их союзы и коалиции, (суб)региональные интеграционные объединения) остаются ключевыми субъектами мировой системы, имея наибольшее количество формальных инструментов реализации своей политики. Более того, государства способны определять условия функционирования других акторов, инициировать создание новых, определять их курс либо ограничивать, направлять или стимулировать деятельность других. Примерами наиболее активных субъектов этого типа выступают США, Европейский союз, Китай, Россия.

Тип «международные организации и институты глобального управления» включает формальные организации, которые в большей степени зависят от государств, так как они создаются либо государствами-участниками (международные межправительственные организации, или ММПО, которые по сути являются методом реализации ее членами их институциональной власти), либо в рамках действующего законодательства (международные неправительственные организации, или МНПО), т. е. опосредованно зависят от государств. Примерами ММПО и МНПО являются Международный союз электросвязи и Корпорация по управлению доменными именами и IP-адресами (ICANN) соответственно.

Коммерческие организации имеют свободу реализации своих в первую очередь экономических интересов, а крупнейшие ТНК еще и обладают большим потенциалом для этого. Бесспорно, наблюдается усиление роли ТНК в глобальных процессах: возможности лоббирования своих интересов в органах государственной власти, интеграционных объединениях и международных организациях и институтах, прямые иностранные инвестиции, разработка и внедрение новых технологий. Однако ТНК по-прежнему функционируют в рамках действующего законодательства, как национального (в странах, где они ведут бизнес), так и международного права, что накладывает определенные ограничения на них. Примерами таких ТНК являются омпании Big Tech: Apple, Google, Microsoft, Amazon.

Неформальные объединения и движения сетевого типа действуют вне рамок конкретного юридического поля и могут реализовывать свою деятельность в том числе посредством ИКТ, т. е. виртуально, — интернет-сообщества, сети активистов и хактивистов[3], прочие социальные движения, имеющие отношения к функционированию ИКТ. Примером таких объединений является современная международная сеть активистов и хактивистов «Анонимус» (Anonymous).

Частные лица являются наиболее численной группой акторов, но при этом наименее влиятельной с точки зрения реализации возможности изменения структуры или условий функционирования международной ИКТ-системы. Всех людей можно условно поделить на три подгруппы: пользователи (частные и бизнес), разработчики ИКТ-решений и интернет-активисты. К пользователям можно отнести людей, коммуницирующих через мобильный телефон посредством сети интернет, пользующихся компьютером в бытовых и рабочих целях (например, и бухгалтерскими программами). Примерами разработчиков ИКТ-продуктов являются разработчик мобильной операционной системы и инженер-конструктор персонального переносного компьютера (ноутбука). В пример известного интернет-активиста можно привести Джулиана Ассанжа, австралийского журналиста и основателя сайта WikiLeaks.

[3]Хактивизм (англ. hacktivism; словослияние от «хакер» и «активизм») — использование незаконными способами компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации [44].

Ресурсы как объекты власти

В сфере ИКТ объектом власти является все то, что используется при производстве ИКТ-товаров и услуг, сами эти ИКТ-товары и услуги, а также продукты (результаты) их функционирования. Каждая СТС и СТлС состоит из набора объектов — элементов системы. Для построения общей модели любой СТС / СТлС автор определил стандартные типы объектов и представил их графически. Рамки данного анализа охватывают лишь те системы, в составе которых используются ИКТ.

Рис. 4. Общая модель социотехнической или социотехнологической системы

Таким образом, все объекты СТС / СТлС (ИКТ) можно поделить на две большие группы и выделить следующих их типы:

- основные объекты (непосредственно ИКТ): программное обеспечение (ПО), данные, информация и знания (ИКТ-часть), клиентское оборудование, серверы, сети и сетевое оборудование;
- вспомогательные объекты: человеческий капитал, данные, информация и знания (не ИКТ-часть), добывающее, обрабатывающее и энергетическое оборудование, сырье и энергоресурсы.

Тип «программное обеспечение» включает в себя широкий спектр различных решений: исходный код (языки разработки, компиляторы, интерпретаторы), программные компоненты (библиотеки, двоичные файлы), веб-серверы, базы данных, операционные системы, браузеры, среды разработки и пр. Важно отметить, что ПО также может отличаться и по прикладному принципу — как показано на рис. 4, ПО имеет свою специфику для работы добывающего, обрабатывающего и энергетического оборудования, для сетей и сетевого оборудования, для серверов, а также для клиентского оборудования.

Тип «данные, информация и знания» также включает в себя различные подтипы: структурированные и неструктурированные данные, данные приложений, персональные данные, информация о физических и виртуальных ресурсах и процессах, интеллектуальные активы (технологии, патенты, международные стандарты, копирайт и торговые марки) и пр. Как и ПО, данный тип объектов зависит от их прикладного характера. Например, данные о сырье и энергоресурсах нельзя отнести к классу ИКТ-объектов, а данные о добывающей промышленности можно отнести частично. Данные о технологии добычи не являются ИКТ, но если для добычи используются автоматизированные средства, управляемые программно, то данные об этой программе имеют непосредственное отношение к ИКТ. Данные называют «новой нефтью» [45], подразумевая их особую ценность как ресурса.

Тип «клиентское оборудование» состоит из рабочих станций (компьютеров), портативных (мобильные телефоны, смартфоны, планшеты и пр.) и носимых («умные часы», «интерактивные очки» и пр.) устройств, периферийных устройств и сенсоров, точек доступа к сети, а также специализированных устройств (киоски самообслуживания, сканеры штрих-кодов и пр.), компьютеризированных рабочих мест операторов различных профессий (оборудование для утразвуковой диагностики и пр.).

Тип «серверы» включает в себя физические дата-центры (или центры хранения и обработки данных) и размещенную в них инфраструктуру (информационную, телекоммуникационную и инженерную), обеспеченные системами подачи электроэнергии, охлаждения, автоматизированного пожаротушения, резервного копирования и пр.

Тип «сети и сетевое оборудование» состоит из магистральных сетей связи, проводных и радиоканалов передачи данных, оборудования (базовые станции, сетевые коммутаторы, маршрутизаторы и пр.), кабелей (медные, коаксиальные, витые пары, оптоволоконные), автоматизированных телефонных станций, систем длинноволновой и спутниковой связи, что в совокупности составляет физическую часть ресурсов данного типа. Логические ресурсы представлены IP-адресами, доменами, системой доменных имен (DNS).

Тип «человеческий капитал» сам по себе не является частью ИКТ-системы, а определение подтипа зависит от сценариев работы людей с ИКТ-системами. Человек может быть частью СТлС, и тогда он выступает разработчиком ИКТ-систем следующего порядка, например может выполнять роль инженера ПО или технического дизайнера новых микропроцессоров. Если же человек сам использует ИКТ, то он выполняет роль пользователя и, соответственно, относится к одноименному подтипу. Данный тип является уникальным, так как в исследуемой системе люди одновременно могут быть и объектом, и субъектом.

Тип «добывающее, обрабатывающее и энергетическое оборудование» также не является частью ИКТ-системы, но имеет большое влияние на процессы формирования этой системы, так как все ее физические компоненты создаются из материалов, которые необходимо произвести, а сырье для которых необходимо добыть и обработать.

Тип «сырье и энергоресурсы» включает базовое сырье (литий, кобальт, графит, индий, ванадий и пр.), редкоземельные ресурсы (церий, диспрозий, европий, лантан, иттрий, скандий и пр.) и источники энергии (нефть, уголь, природный газ, ядерная энергия, гидроэнергия, возобновляемая энергия и пр.).

В контексте исследования киберполитики отдельное внимание следует обратить на особые технические и технологические системы, существующие или еще разрабатываемые, которые принято называть обобщенным термином «глубокие технологии» (Deep Technology, Deep Tech, Hard Tech) — глобальные технологические решения, требующие решения фундаментальных научных и/или инженерных задач, крупных инвестиций и длительных научных исследований, например передовые материалы и методы производства, искусственный интеллект, биотехнологии, блокчейн, робототехника, фотоника, электроника и квантовые вычисления.

Так, искусственный интеллект называют «новым электричеством» [46], подразумевая его потенциальную возможность трансформировать общество, обеспечить многие технологические достижения и стимулировать инновации, эффективность и производительность во всех отраслях и секторах.

В свою очередь, НАТО планирует обеспечить «квантовую готовность», о чем было заявлено в принятой в январе 2024 г. «Квантовой стратегии», в которой в числе прочих ставятся следующие цели: определение наиболее перспективных квантовых приложений военного и двойного назначения, разработка и внедрение политик и стандартов программного и аппаратного обеспечения, сотрудничество с союзниками по разработке квантовых технологий [47].

Важность «глубоких технологий» обусловлена их связью с понятием технологического сюрприза — внезапным появлением новых технологий или неожиданным развертыванием существующих технологий, что оказывает существенное влияние на стратегический баланс, национальную безопасность или другие критические факторы в международных отношениях.

Методы международного влияния

Так как выше были проанализированы социальные системы, с одной стороны, и СТС / СТлС — с другой, можно представить развернутую структуру СТС / СТлС и выявить методы влияния в международном киберпространстве через призму подсистем социальной системы.

Применительно к киберполитике в рамках обозначенных подсистем можно выделить следующие методы влияния:

- правовая система: судебные, санкционные;
- культурная система: цивилизационные/идеологические, коммуникационные, информационные;
- политическая система: демографические (миграционные), военные, институциональные;
- экономическая система: торгово-производственные, финансовые.

Судебные методы влияния рассматривают нормативную или судебную систему, при которой в случае судебных разбирательств решение принимается с учетом национальных интересов. Поменять правила функционирования системы на данном уровне сложнее относительно других уровней, а поэтому такие правила являются индикатором долгосрочной стратегии государства. Примером такого влияния может быть законопроект о введении налога на цифровые услуги, принятый парламентом Франции в 2019 г.

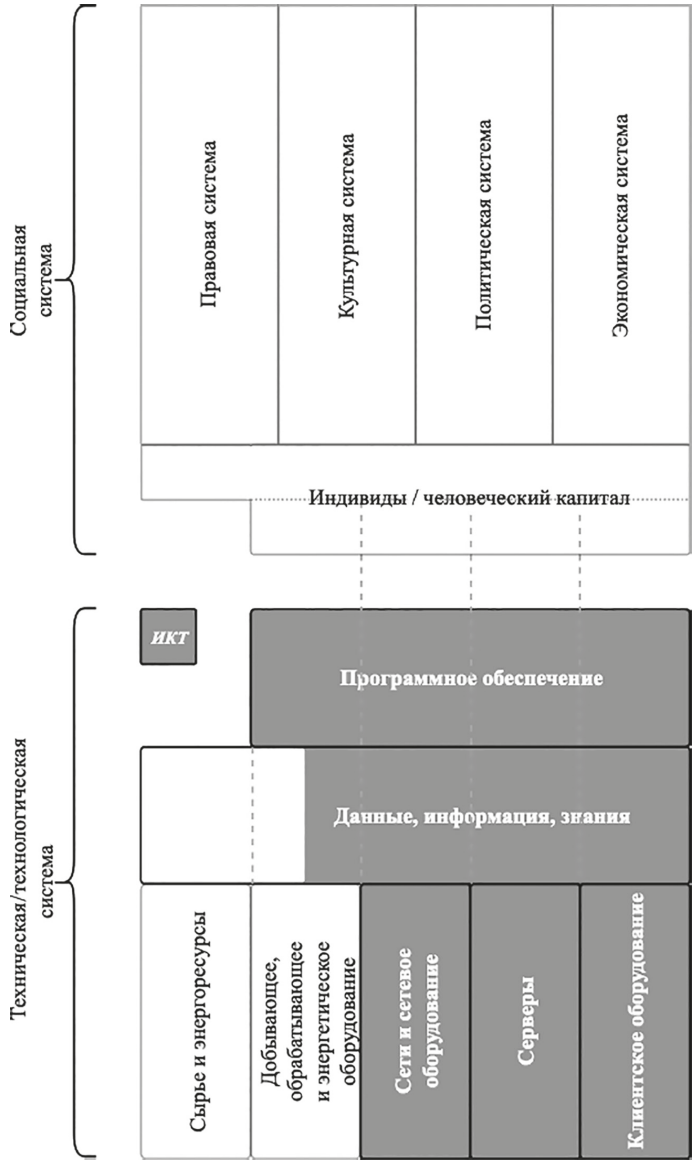

Рис. 5. Структура социотехнической/социотехнологической системы

Санкционные методы включают как низкоуровневые акции воздействия, направленные против иностранных физических и юридических лиц, так и высокоуровневые специальные директивы против целых стран и их союзов. В качестве примеров могут быть приведены санкции США, рассматриваемые или наложенные по подозрениям или обвинениям в кибершпионаже и/или кибератаках.

Цивилизационные (или идеологические) методы влияния заключаются в формировании некоторого идеального образа общества и индивида в нем и либо последующего «экспорта» такого образа, либо его охраны путем запрета «импорта» других культурных образов. Так, например, последствиями распространения западной

культуры могут являться изменение исторически традиционных обществ, отказ людей от занятости в первичном секторе экономики в пользу третичного, их стремление к урбанизации или эмиграции, риски утраты аутентичности местной культуры и традиционных ценностей ее носителей.

Коммуникационные методы включают увеличение количества каналов распространения своей (или желаемой) культуры и/или идеологии. Например, инвестиции в развертывание коммуникационных сетей пятого поколения (5G) или разработка спутникового интернета (система Starlink).

Информационные методы обеспечивают создание инструментов распространения своей (или желаемой) культуры и/или идеологии поверх установленных каналов коммуникации или противодействие им. Такие методы включают стимулирование развития и продвижения дружественных СМИ, включая видеохостинги (YouTube), социальные сети (Facebook*), системы мгновенного обмена сообщениями (WhatsApp*) заграницей, или же, наоборот, блокировку таких иностранных сервисов внутри страны (как это реализовано в КНР по отношению к вышеперечисленным сервисам). Помимо распространения каналов доставки контента, страны могут стимулировать или ограничивать сам контент (например, осуществлять финансирование или блокировку отдельных аккаунтов).

Демографические методы дают возможность стимулировать развитие человеческого капитала, предотвращать или ограничивать «утечку мозгов», а также создавать условия для иммиграции иностранных специалистов. Например, США, Великобритания и Саудовская Аравия имеют программы по предоставлению виз иностранным высококвалифицированным работникам в сфере ИКТ.

Военные методы влияния имеют много различных аспектов применения и включают разведывательные (киберразведка, слежение), оборонительные (кибербезопасность) и наступательные (кибератаки) инструменты. Примерами могут служить разведывательный альянс «Пять глаз» (Five Eyes, FVEY), Департамент кибербезопасности Офиса цифровой трансформации Президента Турции и кибератака Stuxnet в 2010 г. (предположительно направленная против ядерного проекта Исламской Республики Иран) соответственно.

Институциональные методы включают создание международных союзов, организаций, соглашений, проектов и т. д., направленных как на расширение и укрепление собственного влияния, так и на потенциальное уменьшение влияния иностранных государств или их союзов. В качестве примера можно назвать созданное в 2020 г. Глобальное партнерство по искусственному интеллекту (Global Partnership on Artificial Intelligence).

Торгово-производственные методы обеспечивают реализацию рыночной силы и включают возможности по наращиванию либо ограничению экспорта, импорта или производства конкретных товаров и услуг, возможности тарифного и нетарифного регулирования по отношению к конкретным компаниям, странам и/или их союзам (например, торговая война между США и Китаем, начавшаяся в 2018 г.).

Финансовые методы позволяют производить воздействие на иностранных субъектов как за счет предоставления международных кредитов и инвестиций, так и путем ограничения использования иностранных финансовых инструментов

* Продукт компании Meta, деятельность которой признана экстремистской в Российской Федерации.

внутри страны. Так, в период с 2006 по 2021 г. американская ТНК Intel проинвестировала около 1,5 млрд долл. США в строительство завода по сборке и тестированию микросхем в Сайгонском парке высоких технологий во Вьетнаме.

С 2022 г. начинают появляться примеры системной реализации методов Kuberpolitik. Например, в США было создано Бюро киберпространства и цифровой политики (Bureau of Cyberspace and Digital Policy, CDP) [48], которое определяет свою миссию как «продвижение национальной и экономической безопасности США, проводя, координируя и совершенствуя внешнюю политику в области киберпространства и цифровых технологий» [49].

Автор привел лишь некоторые примеры международного влияния в сфере ИКТ с целью обоснования связи предмета международных отношений с ИКТ. Полный анализ системы международного влияния в сфере ИКТ должен включать

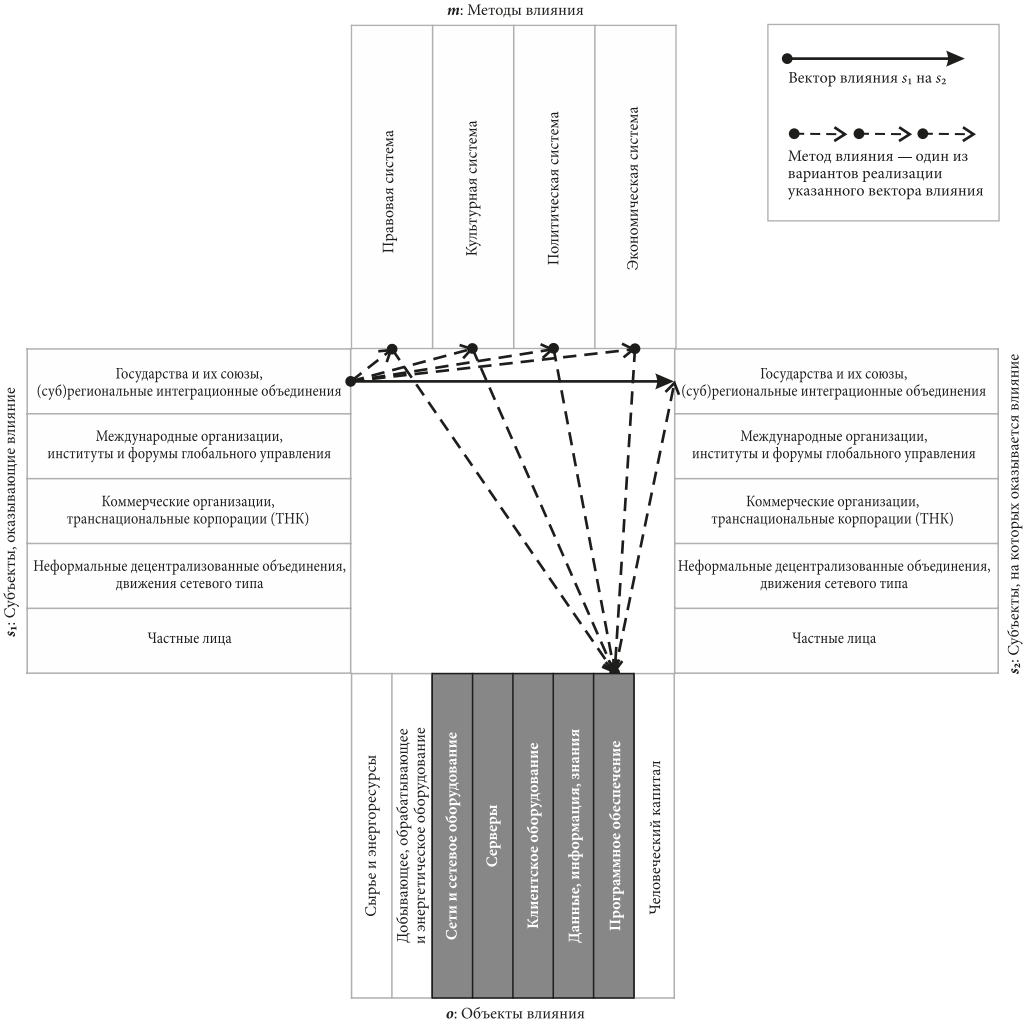

Рис. 6. Пример матрицы методов влияния Kuberpolitik на основе потенциального прогноза

построение матрицы, в которой описаны варианты реализации вышеуказанных методов влияния для каждого субъекта и объекта СТС / СТлС.

В качестве шаблона такой матрицы, а также для графического представления матрицы влияния автором рассмотрен один из примеров прогнозирования потенциальных методов влияния — например, если s_1 США хочет воздействовать на s_2 КНР, то нужно найти такой объект o, который может оказать влияния на s_2 КНР (например, программное обеспечение), а также такой метод влияния m, который может быть оказан s_1 США и который при этом способен воздействовать на выбранный объект o.

Так, последовательно анализируя методы влияния (справа налево, по возрастанию сложности применения), можно предположить следующие сценарии:

- экономические: государственные органы США перестают приобретать (или использовать) любое программное обеспечение, разработанное в КНР;
- политические: правительство США ведет активную работу со своими международными партнерами по совместному сокращению объемов потребления ПО КНР; или правительство США финансирует внутренние проекты по кибератакам, направленным на ПО КРН;
- культурные: правительство США разворачивает государственную информационную кампанию против использования ПО КНР или финансирует разработку и продвижение соответствующих сюжетов при производстве продуктов массовой культуры;
- правовые: правительство США принимает законы о запрете использования ПО КНР на разных уровнях.

Данный пример демонстрирует, что предложенный прогноз покрывает всего лишь четыре модели влияния, тогда как полная матрица Kuberpolitik допускает использование всех вариантов комбинаций, что в итоге составляет 800 моделей влияния: любой из пяти типов субъектов влияния, используя любой из четырех методов влияния, оказывая влияние на любой из восьми объектов влияния, влияет на любой из пяти типов субъектов.

Результаты и выводы

В статье приведено краткое описание предпосылок формирования современной системы международных отношений в сфере ИКТ в целом и цифровой эры в частности, проведен анализ 42 определений киберполитики, составленных разными исследователями за период с 1998 по 2022 г., предложена классификация этих дефиниций и характеристика причин, по которым существующие определения не отражают исследуемый предмет в полной степени.

Методология исследования построена на системном анализе критериев власти рассматриваемой международной кибернетической системы: определены субъекты, объекты и методы влияния. На основании этого сформулирована предметная область киберполитики, укзаны ее характеристики, составные части, аспекты анализа и задачи прогнозирования, разработана матрица для оценки потенциальных моделей влияния.

Автором предложено понятие Kuberpolitik (от др.-греч. κυβερ — «управлять» + нем. politik — «политика»), или Куберполити́к, комплексная киберполитика

(comprehensive cyberpolitics) — раздел политической науки, изучающий мировую политику в сфере информационно-коммуникационных технологий, в частности как разные типы международных субъектов, используя различные методы воздействия на разные объекты социотехнических (использующих ИКТ) и социотехнологических (разрабатывающих ИКТ) систем, могут оказывать прямое или опосредованное влияние на другие международные субъекты.

Kuberpolitik представляет собой дисциплину, расположенную на пересечении трех наук — политологии, информатики и кибернетики.

На уровне международных отношений Kuberpolitik есть метод изучения внешней политики для понимания, объяснения и прогнозирования международного политического поведения с помощью характеристик ИКТ. К таким характеристикам относятся свойства как социотехнических (СТС), так и социотехнологических систем (СТлС), которые включают технологии ИКТ, топологии информационных сетей, человеческий капитал, интеллектуальные активы и специфические полезные ископаемые оцениваемой страны или региона.

Автором приведено несколько актуальных примеров того, как Kuberpolitik реализуется и на страновом уровне (США), и на уровне международных организаций (НАТО).

Сферой анализа Kuberpolitik также могут выступать международные договоры в сфере ИКТ, национальное и международное право в киберпространстве, международное информационное влияние, международные сотрудничество и конфликты в сфере ИКТ, международная экономика в сфере ИКТ.

Помимо этого, Kuberpolitik включает анализ гипотетического политического влияния разработок в сфере «глубоких технологий» (Deep Tech) — передовые материалы и методы производства, искусственный интеллект, биотехнологии, блокчейн, робототехника, фотоника, электроника и квантовые вычисления.

Kuberpolitik фокусируется на отношении между интересами международных субъектов и их политической власти, связанной с киберпространством, как в физической, так и в виртуальной среде, что в совокупности формирует международную киберполитическую систему.

По мнению автора, глобальные процессы цифровизации будут все больше стимулировать развитие Kuberpolitik — и как раздела политической науки, и как практических инструментов международного влияния.

Литература/References

1. Hill, K. A. and Hughes, J. E. (1998), *Cyberpolitics: Citizen Activism in the Age of the Internet*, Lanham, MD: Rowman & Littlefield Publishers, Inc.

2. Meckel, M. (1999), Cyberpolitics und Cyberpolity, *Elektronische Demokratie?*, ed. by Kamps, K., Wiesbaden: VS Verlag für Sozialwissenschaften, pp. 229–244.

3. Gronbeck, B. E. and Wiese, D. R. (2005), The Repersonalization of Presidential Campaigning in 2004, *American Behavioral Scientist*, vol. 49, no. 4, pp. 520–534.

4. Liu, S.-D. (2013), The cyberpolitics of the governed, *Inter-Asia Cultural Studies*, vol. 14, no. 2, pp. 252–271.

5. Shehabi, A. A. and Jones, M. O. (eds) (2015), *Bahrain's Uprising: Resistance and repression in the Gulf*, London: Zed Books.

6. Gusfa, H. and Kadjuand, F. E. D. (2020), Political Agonism for Indonesian Cyberpolitic: Critical Cyberculture to Political Campaign of 2019 Indonesian Presidential Election in Twitter, *Nyimak: Journal of Communication*, vol. 4, no. 2, pp. 211–232.

7. Yu, X., Wang, J. and Liu, Y. (2021), Civic Participation in Chinese Cyberpolitics: A Grounded Theory Approach of Para-Xylene Projects, *International Journal of Environmental Research and Public Health*, vol. 18, no. 23, art. 12458.

8. Hallin, D. C. and Mancini, P. (2004), *Comparing Media Systems: Three Models of Media and Politics*, 1st ed., Cambridge: Cambridge University Press.

9. Chadwick, A. (2006), *Internet Politics: States, Citizens, and New Communication Technologies*, Oxford; New York: Oxford University Press.

10. Chadwick, A. (2017), *The Hybrid Media System*, vol. 1, New York: Oxford University Press.

11. Chadwick, A. and Howard, P. N. (eds) (2008), *Routledge Handbook of Internet Politics*, London; New York: Routledge 2008.

12. Howard, P. (2011), *Cyberpolitics. Communication*, Oxford University Press.

13. Karatzogianni, A. (ed.) (2009), *Cyber-conflict and global politics*, Oxfordshire; New York: Routledge.

14. Coleman, S. and Blumler, J. G. (2009), *The Internet and Democratic Citizenship: Theory, Practice and Policy*, 1st ed., Cambridge: Cambridge University Press.

15. De La Garza Montemayor, D. J., Ibáñez, D. B. and López-López, P. C. (2021), Crisis of Democracy, Social Media and the Digital Age: The Narrative of Specialists from Spain, Mexico and Peru, in: Rocha, Á., Ferrás, C. and Paredes, M. (eds), *Information Technology and System,* vol. 1331, Cham: Springer International Publishing, pp. 169–178.

16. Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. L. (eds) (2008), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press.

17. Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. L. (eds) (2010), *Access controlled: the shaping of power, rights, and rule in cyberspace*, Cambridge: MIT Press.

18. Feenberg, A. (2019), The Internet as network, world, co-construction, and mode of governance, *The Information Society*, vol. 35, no. 4, pp. 229–243.

19. Janczewski, L. and Colarik, A. M. (eds) (2008), *Cyber warfare and cyber terrorism*, Hershey: Information Science Reference.

20. Limnéll, J. (2018), Developing Political Response Framework to Cyber Hostilities, in: Lehto, M. and Neittaanmäki, P. (eds), *Cyber Security: Power and Technology,* vol. 93, pp. 31–48.

21. Weiss, M. (2020), Who Should Be in Charge of Cyberspace? The European Union, Member States and the Constitution of Structural Power*, Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS 2020/22*, http://dx.doi.org/10.2139/ssrn.3634542

22. Banta, B. R. (2020), International Cyberpolitics, in: *Oxford Research Encyclopedia of International Studies*. Oxford University Press. Available at: https://oxfordre.com/internationalstudies/display/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-553 (accessed: 25.06.2023).

23. Sheng, L. (2022), Cyber-Politics in U.S. – China Relations: Big Tech and the Trade War, in: *Big Tech Firms and International Relations*, Singapore: Springer Nature Singapore, pp. 43–70.

24. Suda, Y. (2021), Cybersecurity and the politics of data, in: *Security and Safety in the Era of Global Risks*, Routledge, pp. 24–38.

25. Kellner, D. (2002), Theorizing Globalization, *Sociological Theory*, vol. 20, no. 3, pp. 285–305.

26. Pereira Martins, C. (ed.) (2001), *Cyberpolitics*, Coimbra: Instituto de Estudos Filosóficos. https://doi.org/10.5281/zenodo.5137400

27. Rothkopf, D. J. (1998), Cyberpolitik: The Changing Nature of Power in the Information Age, *Journal of International Affairs*, vol. 51, no. 2, pp. 325–359.

28. Choucri, N. (2000), Introduction: CyberPolitics in International Relations, *International Political Science Review*, vol. 21, no. 3, pp. 243–263.

29. Choucri, N. (2012), *Cyberpolitics in International Relations*, Cambridge, MA: MIT Press.

30. Krieger, J. (ed.) (2013), *The Oxford companion to comparative politics*, New York: Oxford University Press.

31. Jordan, T. (2001), Language and Libertarianism: The Politics of Cyberculture and the Culture of Cyberpolitics, *The Sociological Review*, vol. 49, no. 1, pp. 1–17.

32. Hague, B. N. and Loader, B. D. (eds) (2005), *Digital Democracy: Discourse and Decision Making in the Information Age*, London: Routledge.

33. Kim, Yong Cheol (2009), Research Trends and Tasks of Cyberpolitics in Korea, *Studies in Humanities and Social Sciences,* vol. 1, no. 25, pp. 93–128.

34. Kramer, F. D., Starr, S. H. and Wentz, L. K. (eds) (2009), *Cyberpower and national security*, 1st ed., Washington, D. C.: National Defense University Press; Potomac Books.

35. Estudos, R., *Potência e Impotência na Ciberpolítica, por Constantino Pereira Martins | Revista Estudos Hum(e)anos*. Available at: http://revista.estudoshumeanos.com/potencia-e-impotencia-na-ciberpolitica-por-constantino-pereira-martins/ (accessed: 25.06.2023).

36. Martins, C. P. (2021), What Is Cyberpolitics?, *ResearchGate*. Available at: https://www.researchgate.net/publication/348995429_WHAT_IS_CYBERPOLITICS (accessed: 25.06.2023).

37. Nye, J. S. and Welch, D. A. (2017), *Understanding global conflict and cooperation: An introduction to theory and history*, 10th ed., Boston: Pearson.

38. Indrawan, J. (2019), Cyberpolitics Sebagai Perspektif Baru Memahami Politik di Era Siber, *Jurnal Politica*, vol. 10, no. 1, pp. 1–16.

39. Vila Seoane, M. and Saguier, M. (2019), Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional, *Relaciones Internacionales,* no. 40, pp. 113–131. Available at: https://repositorio.uam.es/bitstream/handle/10486/686767/RI_40_6.pdf?sequence=1&isAllowed=yn (accessed: 25.06.2023).

40. Seoane, M. V. and Saguier, M. (2020), Cyberpolitics and IPE: towards a research agenda in the Global South, in: *The Routledge Handbook to Global Political Economy,* London: Routledge, pp. 702–718. Available at: https://www.researchgate.net/profile/Marcelo-Saguier/publication/333380898_Cyberpolitics_and_IPE_towards_a_research_agenda_in_the_Global_South/links/608c0964299bf1ad8d6b5b68/Cyberpolitics-and-IPE-towards-a-research-agenda-in-the-Global-South.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 (accessed: 25.06.2023).

41. Choucri, N. and Clark, D. D. (2013), Who controls cyberspace?, *Bulletin of the Atomic Scientists*, vol. 69, no. 5, pp. 21–31.

42. Wiener, N. (2019), *Cybernetics or Control and Communication in the Animal and the Machine*, Cambridge; London: MIT Press.

43. Parsons, T. (2018), *Social system*, transl. from English, Moscow: Akademicheskii proekt Publ. (In Russian)

44. Krapp, P. (2005), Terror and Play, or What was Hacktivism?, *Grey Room*, no. 21, pp. 70–93.

45. Arthur, C. (2017), Tech giants may be huge, but nothing matches big data, *The Guardian*, August 23.

46. *Andrew Ng: Why AI Is the New Electricity*. Available at: https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity (accessed: 25.06.2023).

47. *Summary of NATO's quantum Technologies strategy*. Available at: https://www.nato.int/cps/en/natohq/official_texts_221777.htm (accessed: 01.02.2024).

48. *Establishment of the Bureau of Cyberspace and Digital Policy — United States Department of State*. Available at: https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/ (accessed: 01.02.2024).

49. *Bureau of Cyberspace and Digital Policy — United States Department of State*. Available at: https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/ (accessed: 01.02.2024).

Статья поступила в редакцию 2 апреля 2024 г.;
рекомендована к печати 15 мая 2024 г.

Контактная информация:

Григорьевский Валентин Валентинович — аспирант; v.grigoryevskiy@gmail.com

Kuberpolitik — power in the digital age

V. V. Grigoryevsky

Primakov National Research Institute of World Economy
and International Relations of the Russian Academy of Sciences,
23, ul. Profsoyuznaya, Moscow, 117997, Russian Federation

For citation: Grigoryevsky V. V. Kuberpolitik — power in the digital age. *Vestnik of Saint Petersburg University. International Relations*, 2024, vol. 17, issue 3, pp. 362–381.
https://doi.org/10.21638/spbu06.2024.308 (In Russian)

This article explores the role of information and communication technologies (ICT) in exerting international influence. The aim is to pinpoint a specific area within the science of international relations that examines global political processes involving ICT. The author assessed existing definitions of "cyberpolitics" and highlighted their inadequacy in capturing the subject under scrutiny. Employing methodologies such as systems theory (including systems analysis and cybernetics), structural functionalism, neorealism, neoliberalism, as well as structural analysis, abstraction, and modelling, the author devised a comprehensive model for analysing cyberpolitics. This model views cyberpolitics as a multidimensional and multi-level phenomenon with sociotechnical and socioecological subsystems and their hierarchies, demonstrating their link to social system levels. The article introduces a formula and function of influence, delineating key variables that determine the nature of influence in general and in specific cases. All components of technical and technological ICT systems are described, providing a thorough understanding of their structure and processes. The concept of "deep technologies" and their potential role in international competition and technological dependence is explored. The typology of objects and subjects of political relations in this realm is presented, defining international cyberpolitics as a subset of political science. The term "comprehensive cyberpolitics" (Kuberpolitik) is proposed. A matrix is developed for evaluating potential influence models, with an illustrative forecasting example. The article concludes with recommendations for future research, including detailed matrices for each subject type and a comprehensive exploration of influence models.

Keywords: cyberpolitics, comprehensive cyberpolitics, Kuberpolitik, information and communication technologies, "deep technologies", digital age, digital economy, digitalisation, systems analysis.

Received: April 2, 2024
Accepted: May 15, 2024

Author's information:

Valentin V. Grigoryevsky — Postgraduate Student; v.grigoryevskiy@gmail.com