offset the importance of traditional energy sources at the present stage. The struggle for control over countries with large hydrocarbon reserves remains a factor of geopolitical instability.
Keywords: *energy resources, energy, international relations, expansion, oil, LNG*

ЦАРЁВ Матвей Александрович – *аспирант кафедры дипломатии Московского государственного института международных отношений (университет) МИД России (119454, Россия, г. Москва, пр-кт Вернадского, 76; carev_m_a@my.mgimo.ru); ORCID: 0000-0002-0754-2705; ResearcherID: IRZ-1212-2023; SPIN-код: 2844-1251*

ГЛОБАЛЬНОЕ РЕГУЛИРОВАНИЕ РАЗВИТИЯ ИКТ И ИНФОРМАЦИОННО-КОММУНИКАЦИОННОГО ПРОСТРАНСТВА: ПОДХОДЫ ВЕЛИКИХ ДЕРЖАВ (РОССИЯ, КНР И США)

Аннотация. *В условиях кризисного характера формирования мирового порядка актуализируется проблематика глобального регулирования. Развитие информационно-коммуникативных технологий (ИКТ), будучи одним из мегатрендов мирового развития, не является исключением. В настоящее время регулирование глобального информационно-коммуникационного пространства затруднено ввиду ряда различных причин, таких как его секьюритизация государствами, отсутствие аккомодации между великими державами и гомогенности в определении угроз, сущностных терминов, идей и подходов. В статье рассматривается роль ИКТ как ресурса атрибутивной и релятивной силы, подходы России, США и КНР к глобальному регулированию развития ИКТ и информационно-коммуникационного пространства, а также основные проблемы на этом пути. В заключение делается вывод о необходимых шагах в этом направлении, которые следует предпринять России для достижения лидерства в этом функциональном «досье».*
Ключевые слова: *кибербезопасность, глобальное управление, сдерживание, информационно-коммуникационные технологии (ИКТ), великие державы, мегатренды, нормативный активизм, суверенитет*

В настоящее время происходит формирование современного мирового порядка [Шаклеина 2022]. На фоне этого актуализируется нормативный и коммуникационный аспекты взаимодействия между субъектами, а также вопрос о механизмах принятия решений на глобальном уровне [Лебедева 2020]. Несмотря на то что черты нового мирового порядка до конца еще не оформились, вполне можно констатировать недостаточную степень аккомодации в отношениях между великими державами, размывание международных режимов и несоблюдение норм, а также кризис институтов глобального регулирования. Сегодня мир можно описать либо как «осыпавшийся»[1], либо как «опять разделенный», в котором выделяются три центра силы, отождест-

[1] Мир осыпался: что дальше? Четвёртый день ежегодного заседания клуба «Валдай». – *Международный дискуссионный клуб «Валдай»*. 28.10.2022. Доступ: https://ru.valdaiclub.com/events/posts/articles/mir-osypalsya-chto-dalshe/ (проверено 09.05.2024).

вленные тремя великими державами – Россией, США и КНР [Богатуров 2020: 10].

ИКТ: от инструмента «коммуникации во благо» до ресурса «войн будущего»

С развитием информационно-коммуникационных и цифровых технологий (ИКТ) изменилось само пространство международных отношений: из трехмерного (суша, вода и воздух) оно трансформировалось в четырехмерное (киберпространство/информационная сфера[1]). И если в начале его активного освоения (1990-е гг.) оно рассматривалось как неподконтрольное государствам, то уже в нулевых годах постепенно стало приходить понимание, что оно имеет свои политические границы, отражающие существующую карту мира [Зиновьева 2015: 112]. Глобальное регулирование этого пространства становится прерогативой национальных государств [Drezner 2004], поскольку информационные технологии рассматриваются как проблема обеспечения их национальной безопасности.

Если на заре развития ИКТ и становления понимания информационного пространства как «коммуникационного» виделась возможность междержавной кооперации в информационной среде для достижения общего блага, то в дальнейшем данная среда стала рассматриваться как потенциально конфликтная, включенная в пространство войны [Истомин 2022: 105; Конышев 2022: 186], в которой возникают и развиваются различные типы кибер-/кибернетических/кибернетизированных (*cybered*) конфликтов [Demchak 2020] как внутри национальных государств (в т.ч. в результате вмешательства извне), так и между ними. Складывается дихотомия, в рамках которой ИКТ рассматриваются как обоюдоострый меч: усиливая то или иное государство и позволяя ему стать лидером, они одновременно становятся орудием для нанесения ему вреда со стороны тех, кто стремится его разрушить[2]. Эти технологии также рассматриваются с точки зрения их возможного двойного и военного назначения, в т.ч. как инструмент ведения гибридных войн [Конышев, Парфенов 2019], и одной из особенностей природы и методов ведения «войн будущего» [Сучков, Тэк 2019]. Более того, угрозы и вызовы в информационном и киберпространстве стали восприниматься через призму обеспечения безопасности ядерного комплекса государств [Футтер 2016]. Закономерным итогом стала милитаризация глобального информационного пространства [Зиновьева 2015: 114-115], а информационно-коммуникационные и цифровые технологии стали ресурсом как атрибутивной, так и релятивной силы.

Причины кризиса глобального регулирования информационно-коммуникационного пространства

В настоящее время эффективное глобальное регулирование информационно-коммуникационного пространства отсутствует по нескольким причинам.

Во-первых, как уже упоминалось выше, в настоящее время наблюдается недостаточная степень аккомодации между тремя ключевыми великими державами. Во-вторых, каждая из великих держав стремится предложить свое в*и*дение будущего мирового устройства и глобального регулирования. Такие попытки нередко направлены на обретение статуса лидера/гегемона, сдержи-

[1] Киберспространство — американский термин, информационная сфера — российский.

[2] 2010 National Security Strategy. – *Historical Office. Office of the Secretary of Defense*. May 2010. P. 24. URL: https://history.defense.gov/Portals/70/Documents/nss/NSS2010.pdf?ver=Zt7IeSPX2uNQt00_7wq6Hg%3D%3D (accessed 18.06.2024).

вание других держав, программирование системы международных отношений на междержавную конкуренцию. Особенно это характерно для внешнеполитической деятельности США [Шаклеина 2020]. В-третьих, по-прежнему сохраняется дискурс относительно того, стоит ли передавать больше полномочий на уровень глобальных институтов или идти по пути укрепления роли национальных государств в различных сферах [Сафранчук, Лукьянов 2021а: 15]. Для современного состояния системы международных отношений характерны опасения государств относительно углубления взаимозависимости, которая воспринимается как средство вмешательства во внутренние дела, а также «суверенизация повесток», являющаяся как инструментом обретения собственных выгод, так и средством конкуренции с другими игроками, в результате чего подрывается доверие между ними, и достижение баланса сил и гомогенизация идей становятся невозможными [Сафранчук, Лукьянов 2021б: 57, 66-67].

В*и*дение глобального регулирования информационно-коммуникационного пространства отличается у трех держав. ИКТ обретают еще одну грань – они становятся ресурсом нормативной силы государств.

Подходы великих держав

Россия подразумевает под таким пространством «информационную среду/пространство» (отсюда термин «информационная безопасность»)[1], а США – «киберпространство» («кибербезопасность»)[2]. Понимание пространства Китаем можно описать как «сетевое пространство» [Понька, Рамич, У 2020: 384] («сетевая безопасность»[3]). В то же время достаточно распространенным термином в китайских документах остается «информационная среда» [Creemers 2024: 175] и «информационная безопасность»[4] [Понька, Рамич, У 2020: 384]. Также встречаются термины «цифровая сфера»[5] и «кибербезопасность»[6]. Отличаются и подходы государств к глобальному регулированию информационного пространства.

Россия выступает с позиции необходимости институционализации информационной сферы, признания всеми игроками существования национальных сегментов информационного пространства и принципа суверенитета наци-

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Доступ: http://kremlin.ru/acts/bank/41460 (проверено 09.05.2024).

[2] 2023 National Cybersecurity Strategy. – *The White House*. March 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf (accessed 09.05.2024).

[3] Как указывает исследователь Р. Кримерс, термин «кибербезопасность», обычно использующийся при переводе китайских текстов, на самом деле означает «сетевую безопасность». Этот термин является новым и призван заменить используемый ранее термин «информационная безопасность» [Creemers 2024: 175].

[4] The Internet in China. – *Information Office of the State Council of the People's Republic of China*. 08.06.2010. URL: http://iq.china-embassy.gov.cn/ara/zt/zgzfbps/201206/t20120621_2518854.htm (accessed 09.05.2024).

[5] China's Positions on Global Digital Governance (Contribution for the Global Digital Compact). – *Ministry of Foreign Affairs of the People's Republic of China*. 25.05.2023. URL: https://www.fmprc.gov.cn/eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202305/t20230525_11083607.html#:~:text=China%20supports%20the%20leading%20role,international%20consensus%20in%20this%20regard. (accessed 09.05.2024).

[6] International Strategy of Cooperation on Cyberspace. – *Ministry of Foreign Affairs of the People's Republic of China*. 01.03.2017. URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html (accessed 09.05.2024).

ональных государств над своей частью пространства, означающего невмешательство при помощи ИКТ во внутренние дела суверенных государств. Более того, российский подход не только затрагивает проблематику безопасности компьютерных систем и иных средств связи, но также рассматривает политико-идеологические аспекты безопасности и направлен на обеспечение безопасности социально-гуманитарного развития общества. По мнению России, интернационализированное глобальное регулирование информационного пространства – ключ к кооперационной модели существования государств. Россия в 2004 г. выступила инициатором создания Группы правительственных экспертов ООН (ГПЭ), на базе которой в 2018 г. вновь по предложению России была создана Рабочая группа открытого состава (РГОС). Создание РГОС было обусловлено возникновением во второй половине 2010-х гг. серьезных противоречий между членами ГПЭ [Шакиров 2021] по вопросу применения международного права относительно действий держав в информационном/киберпространстве. Но несмотря на принятие в 2021 г. доклада РГОС, ставшего символом «триумфального успеха российской дипломатии»[1], и упразднение параллельно возрожденного США формата ГПЭ, по-прежнему затруднено внедрение принятых предложений и норм в реальную практику. На это есть как минимум две принципиальные причины. Во-первых, между странами по-прежнему отсутствует единая позиция относительно механизмов применения международного права в информационном/киберпространстве. Во-вторых, ООН не является инструментом глобального регулирования (необходимыми атрибутами обладает лишь Совет Безопасности) [Худайкулова 2022: 62, 63].

Китай выступает с позиции многосторонней централизованной модели [Дегтерев, Рамич, Пискунов 2021: 21], суть которой заключается в распространении суверенитета[2] государства в вопросах, относящихся к глобальному регулированию информационного/интернет-пространства [Ребро и др. 2021: 55] (роль негосударственных акторов сводится лишь к консультативной функции). Китай в своей внешнеполитической стратегии рассматривает «традиционные международные институты», например систему ООН, как структуру, в которой он не может достичь лидирующей роли и конструктивного сотрудничества с другими державами, считая, что его интересы не будут удовлетворены в результате ограничительных действий других влиятельных игроков. Это объясняется тем, что они создавались в то время, когда Китай еще не был одним из системообразующих акторов. Следовательно, в них он видит свою роль в качестве «участника», действия которого лишь направлены на поддержку этих институтов. Это, впрочем, вовсе не означает, что его роль в них в качестве «участника» выработки глобальных норм и создания международных режимов не будет активной. Напротив, в «модифицированных», или «улучшенных», а тем более в «инновационных» международных институтах (ШОС+, БРИКС+), созданных, когда Пекин уже стал одной из ключевых глобальных держав, влияющей на систему международных отношений, он видит свою роль в качестве «созидателя», «лидера» и «направляющего» [Грачиков, Сюй 2022: 17, 18]. Поэтому предполагается, что

[1] В РФ заявили, что рабочая группа ООН по информационной проблематике начнет работу в июне. – *ТАСС*. 13.03.2021. Доступ: https://tass.ru/politika/10895625 (проверено 09.05.2024).

[2] Global Initiative on Data Security. – *Ministry of Foreign Affairs of the People's Republic of China*. 08.09.2020. URL: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/202009/t20200908_679637.html (accessed 09.05.2024).

именно эти институты Китай будет рассматривать как перспективные для своей нормативной деятельности и активизации сотрудничества в области глобального регулирования развития ИКТ и информационно-коммуникационного пространства.

США рассматривают глобальное регулирование киберпространства как децентрализованную модель [Дегтерев, Рамич, Пискунов 2021: 21], основную роль в которой играют частные структуры (на которые, впрочем, могут оказывать влияние американские власти, т.е. речь идет о государственно-частном режиме управления, или принципе мультистейкхолдерности). Что касается категории суверенитета, то она по-прежнему не употребляется в американских документах, предназначенных для глобального уровня. Это может интерпретироваться как «желание распространить нормы и практики внутренней политики США на своих союзников» [Зиновьева, Шитьков 2023: 47]. Это вовсе, однако, не означает, что США не секьюритизируют эту проблематику (например, они вводят рестриктивные меры в отношении иностранных цифровых платформ). США заинтересованы в экстратерриториальном глобальном регулировании, т.е. расширении собственной юрисдикции «на международный уровень системы Интернета в целом», что позволит им ограничить суверенитет других держав и укрепить свой статус гегемона-лидера [Зиновьева 2022: 14]. Таким образом, для них неприемлем российский и китайский подходы, поскольку они видят в них укрепление примата государственного контроля над киберсредой. В области обеспечения кибербезопасности Вашингтон институционализирует сотрудничество со странами НАТО. США продвигают Группу независимых экспертов под эгидой НАТО, ключевым проектом которой является Таллинское руководство, целью которого стало регулирование киберпространства с точки зрения международного гуманитарного права. На сегодняшний день Руководство уже охватывает два принципиальных вопроса – *jus ad bellum* и *jus in bello,* давая понять, что США рассматривают киберпространство как настоящий театр военных действий. Более того, США в своих стратегических документах отмечают, что на кибератаки они будут «реагировать всеми соответствующими инструментами национальной мощи»[1]. В целом, стратегия США в киберсреде направлена на сдерживание России и Китая [Себекин 2023], что не только мешает конструктивному диалогу между великими державами, но и «обостряет дилемму безопасности» [Зиновьева 2019: 59].

В рамках глобального регулирования в области информационно-коммуникационных и цифровых технологий заметны те же тенденции, которые характерны для многих других сфер: постепенное смещение акцента на «два конкурирующих мирорегулирующих блока («глобальное НАТО» и «ШОС+») [Худайкулова 2022: 63], а также повышение статуса БРИКС+. В настоящее время отсутствие международного режима со своими работающими институтами во многом является следствием нежелания США лишать себя особого положения в этом функциональном «досье». Все это не ведет к снижению конфликтности между игроками на международной арене и элиминации глобальных угроз в информационной и цифровой среде.

---

[1] 2022 National Security Strategy. – *The White House*. October 2022. P. 34. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (accessed 09.05.2024).

Заключение

На этом фоне возможным положительным сценарием для России может стать углубление взаимодействия в рамках данной проблематики с Китаем, а также с Индией, Бразилией и другими заинтересованными державами в рамках ООН, ШОС+, БРИКС+, ОДКБ и других глобальных и региональных форматов, альтернативных западным институтам. Иными словами, России крайне важно сохранить гибкость, рационализм и инклюзивность своего подхода по формированию всеобъемлющего и универсального международно-правового режима регулирования информационно-коммуникационного пространства. Для этого России необходимо продолжать активно выступать на международной арене в качестве нормативного актора, манифестируя свои намерения в рамках глобального публичного пространства.

Помимо дискурсивных практик, не менее важным для России является онтологическое наполнение ее цифрового суверенитета. В существующих реалиях экономического давления западных стран и их попыток сдержать ее технологическое развитие добиться этого становится весьма нетривиальной задачей. Однако достижение ощутимых результатом в рамках этой деятельности, на наш взгляд, будет являться стратегической целью для России, поскольку от этого будет зависеть ее развитие и ее мощь.

Цифровой и технологический суверенитет России позволит ей помешать складыванию американо-китайской дуополии в информационном/сетевом/киберпространстве. Заключение двусторонних и многосторонних договоров в области обеспечения региональной и глобальной информационной безопасности позволит ей не допустить своей изоляции и сдерживания со стороны какой-либо державы.

Активная и самостоятельная политика России на этом направлении будет встречать критику и, возможно, даже неприятие со стороны стран Запада. В то же время именно независимость внешней политики России и стремление развивать глобальное регулирование в области информационно-коммуникационных и цифровых технологий в логике кооперации с другими государствами с целью построения инклюзивного (справедливого) и равноправного для национальных государств и суверенного для каждого из них коммуникационного пространства будет укреплять роль Москвы как ответственной великой державы, позволяя ей продвигаться на пути лидерства как минимум в этом функциональном «досье» глобального регулирования, оказывающего влияние на формирование нового мирового порядка.

Список литературы

Богатуров А.Д. 2020. Введение. Попытка построения «однополярной безопасности» и современная трехполюсная система. – *Системная история международных отношений. Опять разделенный мир. 1980–2018*: учебное пособие для вузов. 3-е изд., перераб. и доп. М.: Юрайт. С. 10-17. EDN: WFDKWR.

Грачиков Е.Н., Сюй Х. 2022. КНР и международная система: формирование собственной модели мироустройства. – *Вестник международных организаций: образование, наука, новая экономика*. Т. 17. № 1. С. 7-24. DOI: 10.17323/1996-7845-2022-01-01. EDN: ZDZJNP.

Дегтерев Д.А., Рамич М.С., Пискунов Д.А. 2021. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе». – *Вестник международных организаций: образование,*

наука, новая экономика. Т. 16. № 3. С. 7-33. DOI: 10.17323/1996-7845-2021-03-01. EDN: RHBSFR.

Зиновьева Е.С. 2015. Глобальное управление Интернетом: российский подход и международная практика. – *Вестник МГИМО Университета*. № 4(43). С. 111-118. DOI: 10.24833/2071-8160-2015-4-43-111-118. EDN: UDUNML.

Зиновьева Е.С. 2019. Киберсдерживание и цифровая дилемма безопасности в американском экспертном дискурсе. – *Международные процессы*. Т. 17. № 3(58). С. 51-65. DOI 10.17994/IT.2019.17.3.58.4. EDN: LVKPIA.

Зиновьева Е.С. 2022. Формирование цифровых границ и информационная глобализация: анализ с позиций критической географии. – *Полис. Политические исследования*. № 2. С. 8-21. DOI: 10.17976/jpps/2022.02.02. EDN: AJDIQL.

Зиновьева Е.С., Шитьков С.В. 2023. Цифровой суверенитет в практике международных отношений. – *Международная жизнь*. № 3. С. 38-51. EDN: HBTQYT.

Истомин И.А. 2022. Войны будущего в свете опыта прошлого. – *Мировая экономика и международные отношения*. Т. 66. № 11. С. 101-114. DOI: 10.20542/0131-2227-2022-66-11-101-114. EDN: IRAVWZ.

Конышев В.Н. 2022. Изучая природу войны: взгляд из России и Европы. – *Полис. Политические исследования*. № 6. С. 182-188. DOI: 10.17976/jpps/2022.06.13. EDN: MIYBGV.

Конышев В.Н., Парфенов Р.В. 2019. Гибридные войны: между мифом и реальностью. – *Мировая экономика и международные отношения*. Т. 63. № 12. С. 56-66. DOI: 10.20542/0131-2227-2019-63-12-56-66. EDN: NQTLHW.

Лебедева М.М. 2020. Новый мировой порядок: параметры и возможные контуры. – *Полис. Политические исследования*. № 4. С. 24-35. DOI: 10.17976/jpps/2020.04.03. EDN: DNORYR.

Понька Т.И., Рамич М.С., У Ю. 2020. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация. – *Вестник Российского университета дружбы народов*. Сер. Международные отношения. Т. 20. № 2. С. 382-394. DOI: 10.22363/2313-0660-2020-20-2-382-394. EDN: UANODL.

Ребро О.И., Гладышева А., Сучков М.А., Сушенцов А.А. 2021. Категория «Цифрового суверенитета» в современной мировой политике: вызовы и возможности для России. – *Международные процессы*. Т. 19. № 4(67). С. 47-67. DOI: 10.17994/IT.2021.19.4.67.6. EDN: QPXXVU.

Сафранчук И.А., Лукьянов Ф.А. 2021а. Современный мировой порядок: адаптация акторов к структурным реалиям. – *Полис. Политические исследования*. № 4. С. 14-25. DOI: 10.17976/jpps/2021.04.03. EDN: JVPZJB.

Сафранчук И.А., Лукьянов Ф.А. 2021б. Современный мировой порядок: структурные реалии и соперничество великих держав. – *Полис. Политические исследования*. № 3. С. 57-76. DOI: 10.17976/jpps/2021.03.05. EDN: XOYUIZ.

Себекин С.А. 2023. Система международной информационной безопасности в условиях политической турбулентности. – *Вестник Санкт-Петербургского университета. Международные отношения*. Т. 16. № 2. С. 170-190. DOI: 10.21638/spbu06.2023.205. EDN: JQHKPU.

Сучков М.А., Тэк С. 2019. Будущее войны: доклад международного дискуссионного клуба «Валдай». – *МДК «Валдай»*. 24 с. EDN: JZOFUG.

Футтер Э. 2016. Ядерное оружие в век информационных технологий. – *Россия в глобальной политике*. Т. 14. № 6. С. 146-159. EDN: XAELEH.

Худайкулова А.В. 2022. К вопросу о глобальном управлении в XXI в.: подходы РФ, КНР и США. – *Социальные и гуманитарные знания*. Т. 8. № 1(29). С. 56-69. DOI: 10.18255/2412-6519-2022-1-56-69. EDN: CYFJSX.

Шакиров О.И. 2021. Широкий киберконсенсус. – *Российский совет по международным делам*. 23.03.2021. Доступ: https://russiancouncil.ru/analytics-and-comments/analytics/shirokiy-kiberkonsensus/?sphrase_id=131721305 (проверено 18.06.2024).

Шаклеина Т.А. 2020. Политика США в отношении России: конкуренция, сдерживание и управление. – *Вестник РГГУ*. Сер. Политология. История. Международные отношения. № 4. С. 10-26. DOI: 10.28995/2073-6339-2020-4-10-26. EDN: FOEVRX.

Шаклеина Т.А. 2022. Переломный момент в мировом развитии. Сохранит ли Запад преобладающее влияние на формирование мирового порядка XXI века? – *Международные процессы*. Т. 20. № 4(71). С. 6-22. DOI: 10.17994/IT.2022.20.4.71.2. EDN: IGCAUV.

Creemers R. 2024. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. – *Journal of Contemporary China*. Vol. 33. Is. 146. P. 173-188. DOI: 10.1080/10670564.2023.2196508.

Demchak C.C. 2020. Cybered Conflict, Hybrid War, and Informatization Wars. – *Routledge Handbook of International Cybersecurity*. Routledge. P. 36-51.

Drezner D.W. 2004. The Global Governance of the Internet: Bringing the State Back in. – *Political Science Quarterly*. Vol. 119. Is. 3. P. 477-498. DOI: 10.2307/20202392.

TSAREV Matvei Akeksandrovich, *postgraduate student at the Chair of Diplomacy, Moscow State Institute of International Relations, University of the Ministry of Foreign Affairs of Russia (76 Vernadskogo Ave, Moscow, Russia, 119454; carev_m_a@my.mgimo.ru)ж ORCID: 0000-0002-0754-2705ж ResearcherID: IRZ-1212-2023; SPIN-код: 2844-1251*

GLOBAL ICT GOVERNANCE: APPROACHES OF THE GREAT POWERS (RUSSIA, THE PRC, AND THE U.S.)

Abstract. *Nowadays, the global governance of ICT resembles a pitchfork or a mirror reflecting the dynamics and zeitgeist of a new world order formation. On the one hand, its relevance is growing due to the impact of this megatrend on the global development. However, instead of becoming a tool for achieving common good, ICTs are often seen as a means of future warfare and as potential offensive and defensive capabilities. Hence, ICT is a source of attributive and relational power of states. On the other hand, ICT development affects the key principle of the Westphalian system – national sovereignty. States, being interested in its preservation or expansion, act within the framework of global institutions as normative actors in the field of international information and cyber security. Thus, ICTs also become a source for states' normative power. This article contains examination of Russian, American and Chinese approaches to global ICT regulation and the main challenges encountered along the way. Its conclusion provides the necessary steps that Russia should take in this direction to achieve leadership in this domain and avoid being constrained and degraded by other powers.*

Keywords: *cybersecurity, global governance, constraint, ICT, great powers, megatrends, normative activism, sovereignty*