УДК 004.056.5
ББК 32.973.202

Дубов Дмитрий Владимирович*, заведующий отделом исследований информационного общества и информационных стратегий Национального института стратегических исследований, кандидат политических наук (Украина).

Кибермогущество как базис обеспечения "цифрового" суверенитета в современном мире: ключевые подходы

Стремительный рост количества и качества информационных потоков, тесно связанный с общим ростом роли информационно-коммуникационных технологий (ИКТ) в жизни общества, естественным образом трансформирует многие сущностные конструкты, базисы которых были заложены несколько сотен лет назад. Одним из таких конструктов является понятие "суверенитет".

Концепция суверенитета, которая лежит в основе всей современной системы международных отношений и вообще формата организации международной политической жизни, в последние годы подвергается систематическим и особо настойчивым "атакам" со стороны ряда мировых государств, которые рассматривают его как объективное препятствие для:

– перераспределения природных богатств стран;

– возможности бесконтрольного доступа на их рынки;

– завершения давних геополитических проектов, реализация которых существенно осложнилась ввиду экономического и политического усиления целого ряда международных игроков.

ИКТ тут выступают лишь одним из множества факторов, однако именно они приводят к всё более отчётливому формированию новой, критически важной для выживания государства составляющей – "цифровому" суверенитету. Для целей настоящей статьи понятие "цифровой" суверенитет будет употребляться в смысле "*возможности государства самостоятельно определять свои внутренние и внешние, политические и геополитические интересы в информационной сфере, самостоятельно определяться с курсом внутренней и внешней информационной политики, распоряжаться собственными информационными ресурсами и инфраструктурой национального информационного пространства и, соответственно, гарантировать "цифровую" безопасность государства, общества и гражданина*"[1].

* dubov@niss.gov.ua.

[1] Данное определение было сформулировано автором совместно с украинским учёным Н. А. Ожеваном.

Именно обеспечение "цифрового" суверенитета становится всё более сложным в глобализированном мире, поскольку большинство мировых игроков, ощущая его как объективную необходимость, ведут на поле усиления (своего) и деконструкции (чужого) "цифрового" суверенитета всё более активную деятельность. В то же время это парадоксальным образом накладывается на объективные сложности с формулированием его сущности, реальных параметров и методов обеспечения.

Дополнительной сложностью здесь выступает стремительное развитие ИКТ и информационной инфраструктуры, для которых характерна проблема двойственного юридического статуса. В самом простом случае если мы говорим о воздушном или морском пространстве той или иной страны, то имеем чёткий набор правил его использования. Более того, самовольное вторжение судов в любое из них может рассматриваться как военная угроза и повлечь за собой симметричный военный ответ.

Однако если мы говорим о цифровом пространстве, то правила во многом оказываются размытыми. И если классическое контентное пространство традиционных СМИ имеет давние традиции регулирования и контроля, то новые коммуникации существенно выходят за их рамки. Это касается и инфраструктурных составляющих цифрового пространства. Например, с одной стороны, физическая информационная инфраструктура (оптические кабельные сети) находится на территории одного государства, однако может относительно свободно использоваться практически любым субъектом – как государственным, так и негосударственным, в том числе и против интересов этого государства. Однако любые попытки власти навести порядок в этом вопросе и установить более или менее чёткие "границы" в этих новых пространствах наталкиваются на жёсткое сопротивление ряда мировых игроков и крупных ИТ-корпораций.

Между тем определение границ "цифрового" суверенитета, предпосылок его формирования и механизмов его обеспечения является жизненно необходимой задачей для любого государства, которое хочет защитить свою субъектность и в новом тысячелетии. Следует иметь в виду, что всё чаще в научных публикациях механизмы, обеспечивающие поддержание "цифрового" суверенитета, обозначаются как инструменты кибермогущества государства, что, в свою очередь, приводит к необходимости определить и это понятие, выявить его взаимосвязи с остальными.

Таким образом, актуальность нашего исследования обусловлена наличием противоречия между существующим состоянием концептуальной и правовой неопределённости "цифрового" суверенитета и необходимостью обеспечить его для полноценной субъектности государств на мировой арене.

Прежде чем приступить к содержательной части исследования, следует уточнить, что мы сознательно говорим именно о "цифровом", а неинформационном суверенитете. При этом мы полностью согласны с подходом, при котором "информационный" суверенитет рассматривается как понятие более широкое и сложное по сравнению с "цифровым". Объективно обеспечение информационного суверенитета подразумевает выполнение более масштабного объёма задач (среди которых и работа с контентной частью), чем "цифрового" суверенитета.

В то же время многие исследователи сегодня часто ставят знак равенства между понятиями "информационный" и "цифровой" суверенитет. Например, российский эксперт И. Ашманов, говоря об информационном суверенитете, называет его "цифровым", фактически расширяя это понятие до информационного: "Что такое *цифровой* суверенитет? Это право государства определять свою *информационную* политику самостоятельно, распоряжаться инфраструктурой, ресурсами, обеспечивать информационную безопасность и т.п. Цифровой суверенитет также можно поделить на несколько категорий. Одна из них – электронный суверенитет, который связан с защитой от кибератак"[2].

Во многом такое отождествление рационально и естественным образом произрастает из той сложной взаимосвязи, которая наблюдается между информационной (как преимущественно контентной) и цифровой (как преимущественно инфраструктурной) составляющими. Их действительно всё сложнее разделить, а чтобы обеспечить – требуются комплексные меры.

Например, защита от несанкционированного доступа к персональным данным граждан становится полиаспектной проблемой. С одной стороны, мы говорим об эффективном нормативно-правовом поле государства, которое обеспечивает необходимые юридические механизмы. С другой стороны, государство должно осуществлять комплекс мер технической безопасности. Однако при этом то же государство часто по объективным причинам не может гарантировать требуемый уровень сохранности, если данные циркулируют в сетях открытого или полуоткрытого типа, поскольку, как показали разоблачения Э. Сноудена, некоторые страны занимаются массированным съёмом информации на самих каналах связи, проконтролировать безопасность которых либо очень сложно, либо вообще невозможно. Опять же, часть персональных данных становится доступной иностранным субъектам и обрабатывается ими вне юрисдикций национального законодательства (например, данные, попавшие в социальные сети), поскольку все технические мощности (серверы) находятся за пределами юрисдикций большинства стран.

Ещё один пример похожей проблемы – зависимость от современных ИКТ. С одной стороны, государства продолжают массово закупать необходимые для развития их экономик современные технологии у относительно узкого круга поставщиков, что делает их уязвимыми перед решениями этих поставщиков (например, перед введением односторонних ограничений на поставки оборудования). *Другой стороной этой же проблемы часто является невозможность проверить безопасность этого оборудования на всех уровнях – как программном, так и техническом. В итоге большинство стран мира оказываются заложниками узкого круга компаний и тех специальных структур, с которыми эти компании сотрудничают.* Подобные угрозы вполне реальны, об этом говорят данные, указывающие на то, что по инициативе Агентства национальной безопасности (АНБ) США в продукты ИТ-компаний

[2] *Ашманов И.* Информационный суверенитет России: новая реальность / Игорь Ашманов / Игорь Ашманов // Россия навсегда : интернет-сайт. 2013. 13 мая. URL: http://rossiyanavsegda.ru/read/948/ (дата обращения: 31.12.2013).

встраивались закладки, в том числе в протоколы шифрования, и даже чипы[3]. И если раньше эта проблема волновала в основном молодые государства, которые только вступали на путь развития, то в последнее время об этом всё чаще начинают задумываться и страны развитые. Некоторые из них (например, Франция) уже проводили политику ограничения своей зависимости от критических для развития государства технологий, имея в своём распоряжении хотя бы минимальный запас "прочности" (скажем, наличие национального производителя мобильных терминалов во многом уменьшает прямую зависимость государства от поставок такой продукции от иных поставщиков), однако сейчас эта проблема становится особо актуальной.

И здесь, как мы уже говорили выше, сложно провести ту грань, которая смогла бы чётко и однозначно отделить информационный суверенитет от "цифрового". Возможным решением тут могло бы стать предложение того же И. Ашманова о выделении нескольких составляющих информационного суверенитета, среди которых:

– "электронный щит", который включает в себя собственную аппаратную платформу (сетевую и ПК); собственную или контролируемую программную платформу (сетевую и ПК); собственную/контролируемую мобильную платформу;

– "информационный щит", включающий собственную интернет-инфраструктуру, собственную медийную структуру СМИ, ТВ и Интернета, а также собственную систему и средства пропаганды и ведения информационных войн, развитую идеологию, законы и рынок идеологических услуг.

Однако как это разделение будет реализовано на практике – пока неясно.

Кроме того, в конечном итоге обеспечение любого суверенитета зависит от "могущества" страны, т.е. "способности политической единицы навязывать свою волю иным единицам"[4]. Понимая суверенитет прежде всего как независимость государства во внутренних и внешних делах, исходим из того, что эта независимость обеспечивается только необходимым потенциалом или совокупностью потенциалов государства, которые в целом как раз и приобретают вид "могущества".

Соответственно, для более полного рассмотрения проблемы обеспечения "цифрового" суверенитета целесообразно было бы оттолкнуться от понятия "кибермогущество" (в статье мы будем пользоваться именно этим понятием, поскольку по своей сути оно в целом идентично термину "цифровое могущество", однако значительно более разработано в научной литературе). Это понятие хотя и остаётся относительно новым, однако всё чаще становится предметом научного интереса. И в первую очередь в тех странах, которые чаще всего рассматриваются в качестве действующих или потенциальных информационных лидеров, – США, Китае и России.

---

[3] Сноуден пролил свет на ситуацию со взломом криптографии. Всё плохо // Хабрахабр : интернет-сайт. 2013. 6 сентября. URL: http://habrahabr.ru/post/192722/ (дата обращения: 03.01.2014).

[4] Приводится по: *Халецька Л.* Еволюція поняття "Могутність" у політичній думці Франції кінця XX – початку XXI століття / Л. Халецька // Дослідження світової політики : зб. наукових праць. 2011. Вип. 2. С. 177–188.

Говоря о кибермогуществе, коллектив авторов проекта Центра технологий и политики в сфере национальной безопасности Национального университета обороны Соединённых Штатов отмечает: "Кибермогущество является фундаментальной основой глобальной жизни… и США должны создать эффективные национальные и международные рамки для использования киберпространства как части общей стратегии национальной безопасности. Такие рамки, безусловно, будут иметь и геополитическое измерение… геополитическая деятельность будет направлена на усиление состояния национальной безопасности и оборонных усилий. Сюда же можно будет отнести и развитие идей сетецентричных операций, соответствующее комплексное планирование возможностей осуществления компьютерных атак, улучшения киберпланирования, создание соответствующих доктрин и образовательных программ"[5].

Про особенность кибермогущества с точки зрения военного компонента говорит учёный и дипломат Дж. Шелдон: "Основным стратегическим признаком кибермогущества, который и делает его настолько уникальным в современном мире, является возможность как в военное, так и мирное время манипулировать стратегической обстановкой, одновременно не давая противнику возможности сориентироваться в ней"[6]. Известный американский политолог Дж. Най, говоря о кибермогуществе, отмечает следующее его свойство: "Кибермогущество может продуцировать результаты как в киберпространстве, так и за его пределами"[7], – что роднит его со всеми классическими концепциями могущества – морским, воздушным, космическим или иными.

В то же время с самим определением термина "кибермогущество" существуют некоторые сложности, которые во многом являются продолжением сложностей, возникавших с определением понятия "могущество" как такового. Ведь большинство из тех, кто исследовал возможности военного (или любого иного важного для государств и наций) использования пространства, практически никогда не давали собственно понимания могущества в приложении к конкретной сфере: практически всегда это были некие общие формулировки.

Автор понятия "морское могущество" Т. Мехен так и не дал его определения, описывая факторы, которые приводят к военно-морскому преимуществу. Лишь в 1920 г. этот термин ориентировочно был сформулирован В. Стефенсом и А. Весткоттом как "способность страны проводить в жизнь свою волю на море"[8].

Б. Митчел, который посвятил свои труды проблеме военно-воздушных сил, тоже не дал чёткого определения "военно-воздушного могущества", описав его в целом как "способность делать что-либо в воздухе"[9].

---

[5] Cyberpower and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. Washington, D.C. : Potomac Books, 2009. P. 3.

[6] *Sheldon J. B.* Deciphering cyberpower strategic purpose in peace and war / J. Sheldon // Strategic Studies Quarterly. 2011. № 5 (2). P. 104.

[7] *Nye J.* Nuclear lessons for cyber security? / Joseph S. Nye // Strategic Studies Quarterly. 2011. № 5 (4). P. 19.

[8] *Stephens W., Westcott A.* A History of Sea Power / William Oliver Stephens, Allan Westcott // The Project Gutenberg eBook : website. URL: http://www.gutenberg.org/files/24797/24797-h/24797-h.htm (дата обращения: 15.09.2013).

[9] Приводится по: *Clodfelter M.* The limits of air power: the American bombing of North Vietnam / Mark Clodfelter. Lincoln : Univ. of Nebraska Press, 2006. P. 212.

С учётом относительной новизны всей киберпроблематики и начала исследований в сфере кибермогущества представляется маловероятным, что в ближайшее время мы сможем получить действительно чёткое и всеобъемлющее определение. Однако некоторые наработки в этом направлении всё же существуют. Например, американский исследователь С. Старр предлагает в целом адекватное общее представление о том, чем является кибермогущество (по крайней мере, на нынешнем этапе). По его мнению, это "способность к использованию киберпространства для создания преимуществ и влияния на всех иных операционных пространствах через инструменты могущества"[10]. Заключительную часть этого определения – "инструменты могущества" – исследователь предлагает понимать следующим образом: "В то время как киберпространство как среда просто существует, кибермогущество всегда является мерой способности использовать эту среду. Технологии являются одним из очевидных факторов, поскольку обеспечивают базовую возможность "войти в киберпространство", а значит, возможность его использовать"[11].

Однако, вновь говоря о проблеме определений, стоит согласиться с тем же С. Старром, который отмечает: "Теория кибермогущества всё ещё находится на начальных этапах своего становления и, скорее всего, до более-менее однозначного понимания будет немало неудач. Современная теория физики развивалась на протяжении сотен лет, начиная с оригинальных трудов Г. Галилея и И. Ньютона. Хотя в этой дисциплине и наработана общая база знаний, есть варианты для конкретных субнаправлений (например, в квантовой механике, классической динамике или теории относительности). Кроме того, существуют тесные связи с другими дисциплинами, такими как математика, химия и биология. И хотя значение основных терминов и понятий, как правило, установлено, однако следует отметить, что на этом пути было немало неудачных попыток. И даже в наше время остаются вопросы, связанные с фундаментальными определениями материи"[12].

Говоря о конкретных элементах, позволяющих лучше понять сущность кибермогущества, стоит отметить несколько исследований, которые, на наш взгляд, сегодня наиболее точно отражают позиции основных подходов к этой проблематике.

Прежде всего обращает на себя внимание исследование, проведённое совместно Китайской академией современных международных отношений (КАСМО) и японским Институтом международных социально-экономических исследований[13]. Их работа на тему "Гегемония в эпоху Интернета" предложила некое обобщённое ви́дение проблемы кибермогущества как способности государства вести кибервойны. По мнению исследователей, понятие "кибермогущество" относится к "возможности страны осуществлять мероприятия и влиять на киберпространство", что обеспечивается

[10] См.: Cyberpower and National Security. P. 38.
[11] Ibid. P. 39.
[12] Ibid. P. 44.
[13] Fiscal 2009 Japan-China joint research project: Internet hegemony and governance – final study session // Institute for International Socio-Economic Studies : website. 2010. January 28. URL: http://www.i-ise.com/en/study/study_20100128.htm (дата обращения: 11.10.2013).

благодаря использованию ряда важных факторов, которыми в разной степени обладает или не обладает любая страна[14].

1. *Возможности Интернета и информационных технологий* – это прежде всего инновационный потенциал страны, её возможности осуществлять исследования и внедрять разработки для функционирования промышленности. Также важным является то, насколько современные ИТ трансформируют (модернизируют) индустриальную составляющую.

2. *Возможности ИТ-индустрии*, есть ли в стране такие ИТ-лидеры, как IBM, Microsoft, Intel, Google или Apple.

3. *Возможности интернет-рынка*, который зависит от общего размера страны, развитости внутренней сетевой инфраструктуры, корреляции степени взаимоинтегрированности ключевых ИТ-инфраструктур, численности интернет-пользователей, количества компьютеров и т.п.

4. *Влияние интернет-культуры*. Является ли национальный язык одним из тех, которым в основном пользуются в Интернете, каким обычно является язык веб-сайтов в стране, каково количество таких ресурсов и их контента, каков общий уровень влияния веб-сайтов на жизнь страны.

5. *Интернет-дипломатия/внешнеполитические возможности* – возможность государства влиять на позицию организаций, которые занимаются администрированием Интернета (ICANN, Форум по управлению Интернетом, Международный союз электросвязи и др.).

6. *Киберсоставляющая военной силы* – возможности страны защитить ключевую национальную и военную ИТ-инфраструктуры от атак, осуществлять сетевое сдерживание и проводить наступательные сетевые акции, в том числе похищать секреты у других стран и предупреждать такую деятельность относительно собственных секретов.

7. *Желание государства создавать стратегии для участия в борьбе за киберпространство*. Недостаточно иметь только возможность осуществлять всё то, что перечислено в предыдущих пунктах. Необходима последовательная, теоретически обоснованная политика (киберстратегия), а на её базе должны быть разработаны нормы поведения, критерии деятельности и соответствующие стратегические планы.

Как отмечает директор Института исследований информационного и социального развития при КАСМО Ли Джанг, если анализировать показатели кибермогущества по этим параметрам, то мы неизбежно придём к выводу, что наиболее кибермогущественной страной сегодня являются США[15].

Свой подход к пониманию кибермогущества предложили и американские исследователи. Г. Раттрей[16] считает, что базовой рамкой исследований любого "могущества" (в том числе и кибермогущества) является анализ четырёх ключевых параметров: (1) технического прогресса, (2) скорости и масштаба операций, (3) контроля ключевых элементов и (4) национальной мобилизации.

---

[14] *Li Zhang*. A Chinese perspective on cyber war / Li Zhang // International Review of the Red Cross. New Technologies and Warfare. 2012. June. P. 801–807.

[15] Ibid. P. 801–807.

[16] См.: Cyberpower and National Security. P. 642.

В соответствии с *первым параметром* было определено, что само появление киберпространства и нового качества зависимости нашей жизни от него породило новые вызовы и опасности, которые ежечасно влияют на нашу деятельность. Соответственно, скорость инновационного развития и масштабы научно-технического прогресса становятся определяющими для тех, кто хочет достичь в этом пространстве существенных позиций.

Аналогично по *второму параметру* констатируется, что киберпространство привело к существенному увеличению скорости и расширению масштабов операций, которые проводятся уполномоченными структурами. Более того, в отношении возможностей использования киберпространства для военных действий практически все эксперты и учёные согласны с тем, что атаки посредством киберпространства осуществляются практически мгновенно и останавливаться должны в таком же режиме реального времени. И если даже скоротечный обмен ракетными ударами всё же даёт операторам время для принятия контрмер, то кибератака в большинстве случаев такой возможности не предоставляет.

Третий параметр – контроль над ключевыми элементами – роднит эту проблему с понятиями могущества государства на иных театрах действий. Если в классической военно-морской теории такими "ключевыми элементами" были, например, проливы (или любые узкие места), а для теории "космического могущества" – контроль над геостационарной орбитой, то для кибермогущества такими "узкими" элементами стали некие узлы, которые созданы самим человеком (в противоположность всем иным пространствам). К ним относятся сгруппированные и взаимопроникающие телекоммуникационные элементы. В физическом мире они могут быть сосредоточены вокруг мощных центров данных или важных для функционирования киберпространства элементов инфраструктуры.

Следует сказать, что эти "теоретические" подходы явным образом используются Соединёнными Штатами и на практике. Из данных, озвученных Э. Сноуденом, видно, что АНБ США самым активным образом подключалось к базовой инфраструктуре Всемирной сети (врезки в магистральные кабели), работало с центрами данных наиболее крупных ИТ-корпораций и т.п. То есть *де-факто* подобный подход борьбы за "ключевые точки" идёт уже сейчас.

Четвёртый параметр – национальная мобилизация – приобретает особое значение, поскольку сама особенность киберпространства во многом зависит от человеческого ресурса и того, как государство может направить этот ресурс на достижение поставленных задач.

Ещё США крайне серьёзно относятся к этому аспекту наращивания кибермогущества. Из года в год увеличиваются заявки на ИТ-специалистов, которые требуются военным, правоохранительным и специальным органам для обеспечения кибербезопасности страны. По подсчётам экспертов, в 2013 г. количество таких специалистов только в военном секторе США составляло от 53 до 58 тыс. человек[17]. И это без учёта профильного персонала таких структур, как Агентство национальной безопасности,

[17] *Reed J.* How many cyber troops does the U.S. have? / John Reed // The Foreign Policy : website. 2013. March 7. URL: http://killerapps.foreignpolicy.com/posts/2013/03/07/how_many_cyber_troops_does_the_military_have (дата обращения: 08.09.2013).

Федеральное бюро расследований, Центральное разведывательное управление, Министерство внутренней безопасности, Разведывательное управление Министерства обороны США и др.

Примечательно, что, сравнивая азиатский (китайский) и американский подходы к вопросам кибермогущества, обнаруживаются как показательные совпадения, так и разительные отличия. Очевидная схожесть – это принципиально военно ориентированный подход. В обоих случаях кибермогущество рассматривается преимущественно как военный аспект развития государства.

Однако при этом американский подход практически игнорирует те базовые факторы, которые необходимы для усиления кибермогущества, – развитую инфраструктуру, инновационную экономику, международное влияние или конкурентоспособных национальных ИТ-производителей. И это логично, поскольку большая часть этих факторов и так сосредоточена в руках США или развита в этой стране на высоком уровне. Китай же как развивающийся лидер вынужден отражать эти аспекты отдельно, показывая, что всё это ещё предстоит обрести.

На фоне представленных выше двух подходов к кибермогуществу интересным выглядит ещё один, который изложил австрийский исследователь А. Климбург. Для понимания рассматриваемого феномена он предлагает пользоваться комплексным подходом, основанном на использовании возможностей нескольких заинтересованных сторон на правительственном, национальном (общественном) и международном уровнях – так называемых подходах "полное правительство" – *whole of government*, "вся система" – *whole of system*, "вся нация" – *whole of nation*. Первый из них – *whole of government* – приобрёл популярность во время событий в Косове вместе с необходимостью отойти от сугубо военных методов решения конфликтов (или решать проблему восстановления стран после них) к более широкому пониманию этого процесса, что предполагает привлечение и негосударственных игроков. Традиционно подход "полное правительство" базируется на другом подходе – "3D" (где "D" – англ. *development, diplomacy, defend,* т.е. развитие, дипломатия, оборона)[18]. С приходом на президентский пост Б. Обамы этот же подход был принят за основу внешней политики США на период его президентства (вместе с другой концепцией, которая во многом является наследием "3D"-подхода, а именно "умная сила" – *smart power*).

А. Климбург предлагает рассматривать понятие "кибермогущество" через некую совокупность подходов. В частности, построить "интегрированную модель возможностей кибермогущества" (Integrated Capability Model of Cyberpower). По его мнению, именно она является "наиболее качественной основой для того, чтобы определить, какие, собственно говоря, возможности могут быть использованы для доставки разнообразных инструментов национального могущества"[19].

---

[18] *Евтихевич Н., Исраелян Е.* Концепция "безопасности личности и общества": канадский подход / Н. Евтихевич, Е. Исраелян // Институт мировой экономики и международных отношений : интернет-сайт. С. 43. URL: http://www.imemo.ru/files/File/magazines/puty_miru/2013/13008_02.pdf (дата обращения: 23.11.2013).

[19] *Klimburg A.* The Whole of Nation in Cyberpower / Alexander Klimburg // Austrian Institute for International Affairs : website. P. 173. URL: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/News/The_Whole_of_Nation_in_Cyberpower_AK.pdf (дата обращения: 01.12.2013).

Сама интегрированная структура (которую А. Климбург иногда называет "измерением кибермогущества") состоит из трёх компонентов.

1. "*Интегрированные правительственные возможности*" (Integrated Government Capability). Речь идёт о способности государства эффективно распределять свои ресурсы в киберсфере, чётко формулировать политику относительно киберпространства, согласованно осуществлять в нём свои действия. Акцент делается на наличие разработанных и согласованных с частным сектором планов реагирования на чрезвычайные события в киберпространстве, возможность использовать киберпространство для защиты или нападения.

2. "*Интегрированные системные возможности*" (Integrated Systems Capability). Это способность государства использовать формализированные структуры для достижения своих целей. Автор выделяет международные альянсы и партнёрства (ООН, НАТО), неправительственные организации (FIRST) или гибридные структуры (ICANN). Прежде всего речь идёт о внешних усилиях государств и о том, какое место в общей структуре приоритетности внешнеполитических вопросов занимает проблематика кибербезопасности.

3. "*Интегрированные национальные возможности*" (Integrated National Capability). Это способность государства построить действительно эффективное сотрудничество с негосударственным сектором, действия которого в дальнейшем были бы направлены на те же цели, которые преследует и государственная политика в киберпространстве. В первую очередь речь идёт о возможности более эффективно влиять на разработку новых технологических стандартов, на направление разработок и защиту критической инфраструктуры от кибератак (поскольку значительная её часть находится в частной собственности).

Конечным же результатом всех этих измерений является создание совокупности эффектов, которые и дают представление о кибермогуществе государства: скоординированность (*coordination* – эффект первого измерения), сотрудничество (*collaboration* – эффект второго измерения), кооперация (*cooperation* – эффект третьего измерения)[20].

Предпринимаются и попытки измерить показатели кибермогущества стран. В частности, американская компания Booz Allen Hamilton, в которой работал разоблачитель Э. Сноуден и которая является подрядчиком АНБ США по многим вопросам кибербезопасности, предложила собственную методику определения и подсчёта показателей кибермогущества. По мнению её специалистов, к таким показателям относятся[21]:

– нормативно-правовое регулирование киберпространства;
– экономический и социальный контекст;
– технологическая инфраструктура;

---

[20] Формально в английском языке *collaboration* и *cooperation* похожи по содержанию, но первое чаще понимается как сотрудничество на базе общих интеллектуальных интересов и целей, тогда как второе – получение взаимной экономической прибыли.

[21] Приводится по: Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз / [Бик В. В., Климчук А. А., Панченко В. Н., Петров В. В.]. Киев : Академпресс, 2013. С. 49.

– промышленное применение информационно-телекоммуникационной инфраструктуры в разных сферах.

Каждый из показателей определяется через совокупность субпоказателей (их около 40), среди которых: участие государства в развитии киберпространства, продуманность политики кибербезопасности, степень цензуры, степень проникновения инноваций в бизнес-среду, открытость торговли, расходы на ИКТ, уровень качества используемых технологий, развитость электронного правительства и др.

В целом же важным уточнением к любому из вышеперечисленных подходов является следующий принципиальный момент: в любых обстоятельствах кибермогущество будет иметь два измерения – теоретическое и реальное.

Первое – это, собственно, то, как именно государство видит своё кибермогущество через предложенную систему отдельных направлений и индикаторов. Действительно, большинство из них может быть измерено, а в отдельных случаях и полностью сформировано при помощи целенаправленной государственной политики.

Второе – реальный потенциал кибермогущества, может быть выявлен лишь в условиях чрезвычайной ситуации, когда государство (само или совместно с частным сектором) будет вынуждено применить все обозначенные элементы своего кибермогущества на практике. При этом следует понимать, что они могут существенно отличаться от теоретических, что объясняется, с одной стороны, всё ещё более чем приблизительными подходами к пониманию самого концепта кибермогущества, а с другой – принципиально латентным характером ведения борьбы в киберпространстве.

Говоря о приоритетности тех или иных подходов с точки зрения реального их применения и использования при формировании стратегий развития государства, по нашему мнению, для большей части государств именно китайско-японский подход является той базой, от которой следует отталкиваться в первую очередь. В то же время эта схема лишь частично предусматривает целую группу важных элементов, без которых говорить о кибермогуществе, а уж тем более о "цифровом" суверенитете не приходится. Например, сюда можно отнести проблему наличия необходимых ресурсов и технологий для построения собственного высокотехнологического производства (импортозамещение) или наличия адекватного национального законодательства, которое обеспечивает достижение подобных целей. Также в китайско-японской схеме лишь бегло упомянут фактор человеческого потенциала, что является существенным упущением.

Между тем в рамках политики импортозамещения всё больший акцент делается на национальных производителей, что является абсолютной доминантой обновлённого суверенитета в новом столетии. Причём на первый план выходят как видоизменённые традиционные факторы (например, обеспечение экономики редкоземельными металлами), так и менее привычные – создание полностью "национальных" высокотехнологических продуктов по всем сферам деятельности.

Более того, масштабы кибершпионской деятельности отдельных стран делают актуальными те проекты, которые ещё 10–15 лет назад казались

невозможными или неоправданными. К ним можно отнести предложения стран БРИКС по созданию фактически альтернативной инфраструктуры Всемирной сети. Осенью 2013 г. президент Бразилии Д. Роуссефф заявила о планах создания независимой от США всемирной сети, которая предполагает прокладывание совершенно нового кабеля по маршруту Владивосток (Россия) – Шаньтоу (Китай) – Ченнаи (Индия) – Кейптаун (Южная Африка) – Форталеза (Бразилия)[22].

Ещё одним направлением являются попытки государств минимизировать (насколько это вообще возможно в глобализированном мире) присутствие иностранных продуктов как можно в большем числе сфер, где используются высокотехнологические элементы, или там, где они обеспечивают работу объектов, относящихся к критически важной национальной инфраструктуре. Эти попытки активно дискредитируются развитыми государствами (как неэффективные и абсолютно бесперспективные), однако они являются жизненно важным приоритетом для тех стран, которые хотят сохранить свою субъектность на мировой арене.

Впрочем, говоря о "цифровом" суверенитете, следует обратить внимание ещё на один фактор, который будет оказывать долговременное влияние на глобальное перераспределение кибермогущества между основными игроками. *Маловероятно, что все страны, которые сейчас являются значимыми геополитическими игроками (или претендуют на этот статус), действительно смогут исключительно своими силами обеспечить свой "цифровой" суверенитет. Тем более этого не смогут сделать меньшие страны. Это приводит к логичной ситуации усиления (восстановления) существующих кооперационных связей или формирования новых между теми странами, взаимоотношения которых выходят за рамки простого делового партнёрства.*

Ярким примером подобного объединения является программа "Пять глаз", которая объединяет США, Великобританию, Канаду, Австралию и Новую Зеландию в некий альянс, обменивающийся между собой информацией и технологиями более свободно, чем с остальными игроками. Стоит предположить, что аналогичные альянсы будут появляться и в других регионах (в том числе на постсоветском пространстве), группируясь как вокруг более технологически развитых и сильных игроков, так и формируя объединения "средних" стран. Впрочем, для этого потребуется несколько иной уровень взаимного "политического доверия", которое является весьма изменчивой величиной, подверженной заметным колебаниям (например, при изменении политической стабильности).

* *
*

Таким образом, можно констатировать ряд принципиальных моментов.

В первую очередь проблема обеспечения "цифрового" суверенитета перестаёт быть сугубо теоретической конструкцией, становясь полноценной

[22] Конкретные параметры нового кабеля неизвестны, но ориентировочно речь идёт о 34 тыс. км кабеля мощностью 12,8 Тбит/сек.

темой при обсуждения приоритетов обеспечения общего суверенитета государства в современном мире. Как следствие – *борьба вокруг формирования собственных эффективных "цифровых" суверенитетов и максимальной деконструкции аналогичных суверенитетов иных стран будет лишь набирать обороты, становясь всё более ожесточённой.*

Государства, которые хотят сохранить свою субъектность на мировой арене хоть в сколько-нибудь отдалённой перспективе, будут вынуждены обратиться к вопросу обеспечения "цифрового" суверенитета уже в самое ближайшее время.

Базой его построения и дальнейшего обеспечения будет обретение государствами необходимого для этого кибермогущества. Ведущие страны уже сейчас проводят активные научные исследования в сфере концептуализации этого понятия и определения ключевых параметров, достижение которых будет способствовать повышению кибермогущества государств. Отдельные страны в этих вопросах уже переходят от теоретических конструкций к внедрению этих концепций на практике. Можно предположить, что *те страны, которые в силу разных причин проигнорируют данную проблему на нынешнем этапе, могут вновь оказаться в роли догоняющих, пропустив важный момент усиления своей субъектности на мировой арене, а при менее благоприятных условиях – потерять существенную часть своего суверенитета (не только цифрового, но и общего).*

Следует понимать, что большей части стран (даже тех, которые сейчас относятся к разряду развитых и успешных), скорее всего, не удастся самостоятельно выстроить полноценные комплексы "цифрового" суверенитета – для этого потребуется кооперация с теми странами, отношения с которыми характеризуются повышающимся уровнем политического доверия. Примером такого альянса уже сейчас является программа "Пять глаз" под эгидой США. Схожие альянсы будут и дальше формироваться как реакция на объективный вызов суверенитетам большинства стран. Подобные цифровые альянсы будут создаваться как из нескольких небольших стран (возможно, даже вне тех региональных политико-экономических интеграционных проектов, в которых они сейчас участвуют), так и вокруг более явных лидеров.

Ключевые слова: *"цифровой" суверенитет – кибермогущество – концепции – США – Китай.*

Keywords: *"Digital" sovereignty – cyberpower – concepts – US – China.*