CZU: 004.056.52
DOI: https://doi.org/10.53486/icspm2023.51

ORGANIZING A CYBER BLOCKADE
ОРГАНИЗАЦИЯ КИБЕРБЛОКАДЫ

OHRIMENCO Serghei
ORCID: 0000-0002-6734-4321
DSc, Professor, Laboratory of Information Security,
Academy of Economic Studies of Moldova, osa@ase.md
CERNEI Valeriu
ORCID: 0000-0003-3300-334X
PhD Student, Laboratory of Information Security,
Academy of Economic Studies of Moldova, valeriu.cernei@bsd.md

ABSTRACT. *Traditionally, experts considered several types of blockades, including sea, land, with the development of aircraft construction - air, with the advent of space technology and special satellites - space. With the rapid development of computer technology and communication tools, the information blockades have been introduced. Each type of blockade had its own historical characteristics; they differed in costs and, of course, efficiency. In the second half and at the end of the 20th century, scientists operated the term cyber blockade and restrictions in the field of cyberspace.*

A number of definitions of cyberspace are provided, since this category changes and is refined depending on the rapidly developing technical, technological, economic and social aspects of our life.

Because of the threat they pose, cyber-attacks and cyber warfare receive significant attention once society and business is developing. The growing dependence of countries on the cyberspace can play a negative role in the process of confrontation; the enemy can attack those areas where cyberspace is a decisive element.

KEYWORDS: *Cyber Domain, Cyberspace, Cyber Attacks, Cyber War, Cyber Blockade, Cyber Sanctions*

JEL CLASSIFICATION: *D74 D81 E26 F51 K24*

Введение

Еще не так давно человечество обладало только двумя физическими средами (доменами) – суша и море. Каждая их них имела совершенно разные физические характеристики. Море могло осваиваться людьми только с помощью специальных технологий в виде парусного судна, парохода, атомной подводной лодки. Землю можно было использовать только с помощью технических средств – колеса, плуга и т.д. Существенные перемены произошли столетие назад, когда к двум доменам была добавлена третья физическая область – авиакосмическая. С полетом первого спутника в 1957 году произошло добавление нового домена - космического пространства. Развитие отрасли по производству вычислительной и коммуникационной техники, а также создание государственных и частных информационных систем, и сетей послужило основой формирование еще одного домена – информационного.

Обзор литературы

Основными источниками, которые описывают исследуемые проблемы, являются следующие работы. В первую очередь, это относится к работам Allison Lawlor Russel [1,6], в которых впервые исследуются явления блокадных операций в киберпространстве, которые представляют собой крупномасштабные атаки на инфраструктуру или системы, направленные на то, чтобы помешать государству отправлять или получать электронные данные. Киберблокады могут осуществляться с помощью цифровых, физических и/или электромагнитных средств, и их появление в киберпространстве имеет серьезные последствия для международного права и нашего понимания кибервойны.

При изучении данной темы был проанализирован большой список источников, сгруппированных по нескольким категориям. Прежде всего это работы, направленные на исследование санкций как экономического и политического рычага давления на определенные государства. Некоторые известные примеры использования киберблокад, нашли отражение в работах [2,7,9-10,14-15]. Во вторую группу входят статьи, в которых исследуются традиционные и новые области конфликта, в частности, киберпространство [4,8,11-13]. В отдельную подгруппу можно выделить подходы военных исследователей к определению состава и структуры киберпространства [5,7].

Определение киберпространства

В настоящее время к указанным доменам добавили шестой – киберпространство. Аналитики предлагают множество определений киберпространства, в том числе такое, как – условная среда, в которой оцифрованная информация передается по компьютерным сетям. Или другое определение - киберпространство (cyberspace) — глобальный домен в пределах информационной среды, состоящий из взаимозависимых инфраструктур информационных сетей с хранящимися и циркулирующими в них данными, включая Интернет, сети передачи данных, компьютерные системы и используемые в них процессоры и контроллеры [5]. Анализ ряда определений киберпространства проведен в [2]. Но автор отмечает, что со временем эта категория будет меняться и уточняться в зависимости от бурно развивающихся технических, технологических, экономических и социальных аспектов нашей жизни. Другими определениями выступают:

1. Электронная (включая фотоэлектронные и пр.) среда, в (посредством) которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается [4].
2. Глобальная область информационного пространства, представляющая собой взаимосвязанную сеть инфраструктур информационных систем, включающих Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры [7].
3. Комплексная (сложная) среда, позволяющая осуществлять взаимодействие между людьми, программным обеспечением и службами, используя глобально распределённые устройства и сети информационных и коммуникационных технологий [3].
4. Программное обеспечение, которое работает в компьютерных устройствах, информация, которая сохраняется (и передается) в этих устройствах, или информация, которая создается этими устройствами. Оборудование и здания, в которых расположены эти устройства, также являются частью киберпространства [10].

Более точное определение кибепространства приведено в [12]. Киберпространство — искусственная неоднородная технологическая система с множеством разноуровневых органов оперативного и технологического управления, процесс создания и эксплуатации которой не предопределяется требованиями одной системы управления, а функционирует в интересах множества разнородных, в том числе антагонистических систем управления. При этом их свойства зависят как от характеристик собственных элементов, так и от объема и свойств реализуемых процессов в интересах внутренних и внешних потребителей.

Киберпространство — это физическая сеть, которой можно манипулировать, чтобы наказать злоумышленников, препятствуя их доступу к потоку данных, необходимому для безопасности и процветания, а киберблокировки — эффективное средство отказа или затруднения доступа к киберпространству.

Киберблокада, в условиях развития технологий и все более высокой зависимости государств от технологий, применяется для осуществления давления на страны (цели санкций/блокад). Аналогично санкциям и блокадам, относящихся к другим доменам, в текущей работе авторы прорабатывает действия, связанные с реализацией блокады в последнем домене – киберпространстве.

Определение киберблокады

Киберблокада представляет собой специально созданную ситуацию, вызванную атакой на киберинфраструктуру или информационные системы, что препятствует доступу государства к киберпространству, предотвращая передачу данных за пределы географических границ.

Следует обратить внимание на существенное отличие киберблокады от цензуры или других форм внутреннего контроля, которые имеют место в практике управления государством. В данном случае правительство не позволяет получать или передавать определенную информацию, как правило, из соображений внутренней стабильности.

Киберблокада должна быть эффективной для предотвращения передачи информации. Продолжительность блокады является второстепенным фактором, который имеет значение только с точки зрения создания и достижения желаемого эффекта. Например, блокада, которая длится всего несколько долей секунды, будет иметь относительно малое значение, но блокада в критическое время (день выборов, к примеру) или продолжающаяся в течение нескольких недель или месяцев может считаться весьма эффективной в зависимости от целей. Как и в случае с морской блокадой, поддержание киберблокады в течение определенного, заранее установленного периода времени не является обязательным. Важным является конечная эффективность блокады в достижении поставленных целей.

Считаем необходимым привести комплекс выводов и определений, сделанных по результатам анализа категории киберблокада в [6, с172-179].

Киберблокада – это ситуация, вызванная атакой на киберинфраструктуру или системы, препятствующие доступу госструктур к киберпространству, тем самым предотвращая передачу (вход-выход) данных за пределами географических границ. Киберблокада является законным инструментом международного государственного управления и, в соответствии с другими типами блокады, может считаться актом войны (хотя в конечном счете государство-мишень решает, хочет ли оно рассматривать ее как акт войны и потенциально обострить ситуацию). Киберблокада нацелена на государства целиком и пытается вызвать массовые сбои в работке элементов критической инфраструктуры. Целью киберблокад является предотвращение двухсторонней передачи данных за пределы географических границ посредством манипулирования, контроля или доминирования в киберпространстве и связанных с ним технологиях с целью нанесения политического, экономического, социального или психологического давления на противника.

Субъекты используют киберблокаду как инструмент международных отношений и санкций, потому что они являются эффективным и недорогим методом контроля доступа противника к современным сетям и могут осуществляться таким образом, чтобы повысить анонимность преступника или правдоподобное отрицание, тем самым снижая риск возмездия. Кроме того, существует несколько альтернативных вариантов действий для достижения того же результата, особенно для негосударственных акторов.

Государства, прокси-группы, негосударственные субъекты или отдельные лица могут проводить киберблокады, если у них есть возможности. Однако группы, не спонсируемые государством, также могут ввести киберблокады, если они обладают надлежащими техническими навыками для планирования и координации масштабной кибератаки, направленной на все государство. Физические атаки на киберинфраструктуру требуют мало ресурсов и небольшой опыт; как минимум, злоумышленники должны иметь возможность обнаруживать и уничтожать ключевую киберинфраструктуру. Электромагнитные атаки относятся к области государственной войны и требуют значительно больше ресурсов для достижения. Таким образом, в зависимости от того, как создается киберблокада (посредством цифровых, физических или электромагнитных атак), порог возможности проведения кибератаки может варьироваться от достаточно низкого (физическое уничтожение кабелей или терминалов) до высокого (электромагнитные атаки).

Киберблокады могут затронуть все аспекты технологий киберпространства, включая электрические сети, электростанции, услуги обычной телефонной связи и услуги мобильной связи, среди прочего. Киберблокады, как и другие блокады, по своей сути ненасильственны, но они могут привести к повреждению, разрушению или смерти, в зависимости от того, как они реализуются и их воздействия на цели. Цели, классифицируемые как «ограниченные» в соответствии с международным правом, такие как больницы, по-прежнему будут ограничены в киберпространстве.

Киберблокады можно создавать с помощью механических, электромагнитных или цифровых атак. Физические атаки являются жизнеспособной альтернативой цифровым атакам и представляют собой акт насилия в соответствии с международным правом, поскольку наносят ущерб физической инфраструктуре киберпространства. Электромагнитные атаки возможны, но менее вероятны, поскольку требуют больших ресурсов; тем не менее, они остаются эффективным способом осуществления киберблокировки.

Как грубые инструменты ведения войны, киберблокады очень эффективны для достижения конкретных результатов, но они не всегда могут быть предпочтительным инструментом для субъектов. В определенных ситуациях лица, принимающие решения, могут отдавать предпочтение более специализированным типам кибератак, которые являются очень изощренными и точными и могут достигать таких результатов, как шпионаж или уничтожение целевой системы при сохранении целостности других систем.

Киберблокады могут быть установлены относительно быстро и за низкую стоимость, в зависимости от используемого метода атаки. Скорость и стоимость варьируются в зависимости от различных типов киберблокады (например, электромагнитная блокада требует больше ресурсов, чем физическая блокада), но в целом дает злоумышленнику преимущества высокоскоростного и относительно недорогого варианта.

Киберблокады технически осуществимы против любой страны, но их легче достичь против географически меньших стран. Более крупные страны обычно имеют больше соединений с киберпространством, создавая более устойчивую сеть соединений между этой страной и другими странами. Таким образом, было бы сложнее ввести киберблокаду в отношении более крупной страны с хорошими связями, чем в отношении небольшой страны с меньшим количеством внешних киберподключений и потенциально менее устойчивой системой.

Киберблокады можно рассматривать как подмножество информационной блокады, потому что они нацелены на передачу информация. Однако информационные блокады не получили широкого признания, поэтому эта классификация может быть не самой полезной для политиков. Помимо того, что киберблокады являются подгруппой информационных блокад, их также следует рассматривать отдельно, поскольку они происходят в определенной области и, таким образом, могут быть полезны при сравнении между областями. Таким образом, киберблокады являются одновременно доменными блокадами киберпространства и подмножество информационных блокад.

Киберблокады могут быть, но не всегда должны считаться актами войны. Контекст имеет ключевое значение: в зависимости от обстоятельств киберблокада может считаться полной блокадой. Эволюция блокад в других областях показывает, что, хотя большинство блокад считались актами войны между воюющими сторонами, полные блокады не являются актами войны. Это следствие остается актуальным для киберпространства. Объявление войны по своей сути является политическим решением, мотивированным различными факторами. Поскольку киберблокировки нарушают государственный суверенитет, торговлю, связи, военные операции и другие действия, они могут по праву считаться актом войны, независимо от причиняемых ими физических разрушений. Однако мирная блокада является формой принудительной дипломатии, когда блокирующее государство заявляет, что оно не стремятся спровоцировать войну, а скорее заставить

блокадное государство уступить предъявляемым к нему требованиям. Есть примеры, когда международное сообщество пытается ввести киберблокаду в качестве формы санкций против государств, нарушающих международное право (например, запрет продажи лицензий на программное обеспечение или запрет предоставления услуг в облачном пространстве).

Киберблокады и киберзапретные зоны — это два различные виды операций. Киберблокады — это операции, препятствующие доступу, тогда как киберзапретные зоны — это операции по запрету доступа. Оба применимы к международной политике и праву, но это не одно и то же.

Увеличение количества и типов участников в киберпространстве представляет сложную ситуацию для присвоения авторства и делает возможным анонимность или правдоподобное отрицание на беспрецедентном уровне в кибервойне. Хотя это верно для всех аспектов киберпространства и усилий по кибербезопасности, это особенно актуально для блокад, поскольку их потенциальное воздействие очень серьезно. Государства не могут полагаться на традиционную модель сдерживания киберблокад, потому что они могут быть не в состоянии идентифицировать преступников, поэтому они должны больше сосредоточиться на разработке надежных, избыточных и устойчивых систем, способных противостоять или быстро восстанавливаться после киберблокады.

Государственно-частные партнерства имеют особое значение для киберблокировки, потому что область киберпространства не является чисто общественным благом — она принадлежит и управляется в основном частными корпорациями или отдельными лицами, однако правительствам поручено защищать ее как часть критической национальной инфраструктуры. Предыдущие типы блокад в разной степени затрагивали частный сектор (например, торговые суда, коммерческие самолеты или даже телеграфные кабели), но киберблокировки представляют собой первый случай, когда общественные и частные интересы переплелись до такой степени. В этой связи, будут полезны рекомендации СЭОР по цифровой безопасности, которые направлены на разработку политики цифровой безопасности социально-экономического сектора [18]. Цифровая безопасность — это собирательный термин, описывающий ресурсы, используемые для защиты сетевой личности, данных и других активов. Эти инструменты включают веб-сервисы, антивирусное программное обеспечение, SIM-карты для смартфонов, биометрические данные и защищенные персональные устройства. На первый взгляд, кибербезопасность и цифровая безопасность вступают в противоречия между собой, но на самом деле они дополняют друг друга. Цифровая безопасность защищает личную информацию, а кибербезопасность защищает инфраструктуру, системы, сети и информацию.

Возникает закономерный вопрос – почему термин «цифровая безопасность» стал использоваться вместо «кибербезопасности». Ответ достаточно прост – цифровая безопасность относится к экономическим и социальным аспектам кибербезопасности и в отличие от чисто технических аспектов, связанных с правоохранительной деятельностью или национальной и международной безопасностью. Категория «цифровая» полностью согласуется с такими категориями, как цифровая экономика, цифровая трансформация и и цифровые технологии. Данная категория трансформируется в основу для конструктивного международного диалога между заинтересованными сторонами через доверие и использование информационно-коммуникационных технологий. Данные процессы должны учитывать тренды в области кибербезопасности [19]. К ним следует отнести такие, как увеличение потенциала искусственного интеллекта, превращение мобильного телефона в новую цель киберпреступников, облачные технологии показали свою уязвимость, главная цель киберпреступников – личные данные, использование Интернета вещей и сетей 5G приводит к новой эре технологий и рисков, автоматизация и интеграция производства, целевые программы-вымогатели, небезопасность удаленной работы, атаки социальной инженерии, возможности мониторинга данных в реальном времени и др.

По мере изменения структуры киберпространства и состава участников изменяются возможности, связанные с организацией киберблокады. С одной стороны, технический прогресс уменьшает уязвимости в некоторых областях, а с другой, изменения в самом киберпространстве, скорее всего, порождают новые уязвимости, которыми могут воспользоваться злоумышленники.

Алисон Рассел в заключении своей книги [6], предлагает серьезные рекомендации, основанные на выводах исследований, которые можно разделить на две категории: политические и научные. Во многих отношениях усилия политического сообщества и ученых могут частично совпадать, что может быть полезно для продвижения исследований в области киберблокад, но в целях лучшей организации эти рекомендации представлены отдельно.

Первый комплекс рекомендаций разработан для академического сообщества. Поскольку академическое сообщество продолжает свои исследования в области киберпространства и кибербезопасности, важно, чтобы оно разработало общую терминологию для обсуждения событий и явлений в киберпространстве. В настоящее время научная литература разделена по определениям самых основных терминов, таких как киберпространство, кибератаки, кибервойна и применение силы. В некоторых областях начинает появляться консенсус, но важно, чтобы научное сообщество разработало последовательный набор терминов для обозначения всех аспектов и событий в киберпространстве.

В этом ключе ученые должны проявлять бдительность и осторожность при уточнении и определении того, как исторический опыт может подходить или не подходить для понимания киберпространства и обеспечения его безопасности. Это исследование в значительной степени опиралось на историческую эволюцию блокад и запретных зон в других областях, для определения блокады в киберпространстве и выявления общих черт в разных областях. Однако исторический опыт и междоменные сравнения не всегда идеально подходят для киберблокировок, и в оценке любых новых разработок, нужно знать, что существуют дополнительные факторы или инновации, которые не могут быть рассмотрены через историческую парадигму.

Для анализа и оценки категории «киберблокада», необходима информация о большом количество субъектов на разных уровнях анализа, роли анонимности, скорости/длительности кибератаки и стоимости киберблокировки — все это представляет собой значительное отклонение от прошлого опыта; их уникальность и важность необходимо учитывать, но не преувеличивать.

Таким образом, очень важно достигнуть точной балансировки уникальных атрибутов киберпространства с междисциплинарными теоретическими приложениями или историческим опытом, для понимания комплекса проблем в этой конкретной области. История и исторический экскурс могут многое предложить для постановки новых задач, но в погоне за пониманием нельзя ни забывать, ни преувеличивать уникальность области и ее атрибутов.

По мере достижения консенсуса в отношении терминологии киберпространства для научного сообщества также важно разрабатывать новые теории или модифицировать существующие теории для объяснения и прогнозирования событий в киберпространстве. Теории международных отношений полезны для прояснения ключевых элементов киберпространства, но всесторонний подход к разработке теории был бы нецелесообразен для решения всех аспектов домена. Комплексный подход позволил бы «отобразить» аспекты предметной области для будущих исследований и выделить связи с существующими научными исследованиями.

Второй комплекс рекомендаций ориентирован на политическое сообщество в виде трех рекомендаций. Первая рекомендация заключается в том, чтобы политики и государственные чиновники осуществляли планирование сценариев, при которых доступ к киберпространству будет запрещен в течение значительного периода времени. Отказ в

доступе может быть результатом несчастного случая или результатом преднамеренной атаки на критическую инфраструктуру страны.

Хотя ситуация, приведшая к массовому отказу в доступе, может быть маловероятной, но это будет серьезное, трудно предсказуемое и редкое событие — к которому подходит определение события «черный лебедь» («Чёрный лебедь» — теория, рассматривающая труднопрогнозируемые и редкие события, которые имеют значительные последствия). Учитывая зависимость общества и правительства от действий в киберпространстве для повседневной деятельности, и эти действия настолько обыденны и рутинны, что их часто игнорируют или упускают из виду. Поэтому очень трудно оправдать отсутствие процессов противостояния кризису, в условиях, когда доступ к киберпространству подвергается атакам.

Данная двусмысленность порождает некоторые трудности во время конфликтов, поскольку акторы не имеют четких границ и общих определений применения силы в киберпространстве. В результате этого, лица, принимающие решения в данной области, могут по-разному относиться к «красным линиям» при нападении, что может привести к непреднамеренной эскалации конфликта.

Во-вторых, для общего понимания конфликта решающее значение имеет использование международных норм относительно приемлемого поведения и применения силы. Эксперты высказывают мнение об отсутствии консенсуса относительно рамок допустимого использования киберпространства или кибертехнологий. Данный вопрос постоянно дискутируется на уровне международных и межправительственных организаций, но достигнуть консенсуса в отношении того, как должно и как не должно использоваться киберпространство государствами и негосударственными субъектами не достигнуто [19]. Эта двусмысленность порождает трудности во время конфликтов,

Все большую поддержку получает тезис о том, что киберблокада является инструментом управления государством. Она соответствует историческому опыту блокадных операций на море, в воздухе и на суше, а также международному праву о блокадных операциях. Учитывая исторические и юридические прецеденты, есть все основания считать киберблокаду частью логической эволюции военных действий в новом домене. Высказывается мнение, что в качестве законного инструмента международных отношений только государства будут иметь право применять блокады. Необходима разработка правил атрибуции, но с учетом того, что они не являются строго обязательными по аналогии с действиями подводных лодок. Кроме того, негосударственные субъекты не могут заниматься киберблокадами, так же как они не могут на законных основаниях проводить морскую, воздушную или наземную блокады. Кроме того, в соответствии с традиционным пониманием блокадных операций как комплекс военных действий, киберблокады могут быть признаны военными действиями. Соответствующие усилия по достижению внутреннего и международного консенсуса в отношении надлежащего использования киберпространства позволят создать правовые основы для сотрудничества. Необходимо исследовать вопрос о том, какие действия в киберпространстве представляют собой «применение силы» или «вооруженное нападение» для установления «красных линий» до начала конфликта и предотвратить непреднамеренную эскалацию. Подобные усилия должны касаться также активной и пассивной защиты и ответных мер для государства, ставшего жертвой кибератаки.

В-третьих, важной областью является форум частно-государственного партнёрства. В некоторых, в информационно развитых странах, частный сектор владеет и управляет более чем 80% критической инфраструктуры и технологиями киберпространства, но правительство играет ведущую роль в защите инфраструктуры. Это объясняется тем, что случае киберблокады против конкретной страны будут затронуты как национальная безопасность, так и коммерческие интересы. Никому не выгодно иметь критическую инфраструктуру и кибертехнологии, для которых не хватает безопасности и надежности и

безопасность домена может быть поставлена под угрозу из-за обременительных требований безопасности.

В любом случае, государственный и частный секторы проиграют в случае, если киберпространство не будет защищено должным образом. Поэтому бремя затрат и ответственности должно быть разделено между субъектами из двух секторов. Правительство обязано защищать собственную критическую инфраструктуру в виде сетей и систем, а также санкционировать, регулировать и применять меры для стимуляции частного сектора вкладывать средства в безопасность коммерческих систем.

Следует иметь в виду, что блокады не являются историческими событиями прошлого (например, морские блокады), они являются явлениями современными и будут происходить до тех пор, пока будут оставаться эффективным средством воздействия и кибероружием. В связи с этим, государствам необходимы разработки по планированию защиты от киберблокировок и планов восстановления после их реализации, необходимо разработать стратегии ответов на кибернападение.

Впереди огромные объемы теоретических исследований и практических разработок по интеграции знаний в теорию киберпространства с другими теориями о власти, коммуникациях, информационном обществе и роли информации в наступившем тысячелетии. Развитие и распространение негосударственных акторов требует рассмотрения множества вопросов о роли частных лиц и правах государства в будущих конфликтах. Негосударственные субъекты играют все большую роль в международной политике, поэтому возникает законный вопрос о необходимости модификации соответствующих законов о вооруженных конфликтах и возможности, и ответственности, за перенос действий в киберпространство.

Кибертренды

Нас будут интересовать перспективы будущих кибервойн, которые представлены в [16], коллективом автором из RAND Corporation. Тенденции будущих войн представлены в следующих разрезах: геополитические тенденции, военные тенденции, космические и ядерные тенденции, кибер тенденции и тенденции сдерживания. Считаем необходимым отметить тренды и ключевые тенденции в области киберпространства, которые представлены в следующей таблице.

Таблица 1. Кибертренды

Тренд	Кто будет сражаться	Как Соединенные Штаты будут сражаться	Где США будут сражаться	Почему Соединенные Штаты будут сражаться
Информационный контроль	Россия, Китай, Иран, Северная Корея и негосударственные субъекты	Информационные операции по противодействию нарративному киберпространству противника	Киберпространство	Не допустить, чтобы пропаганда влияла на общественность США и вызывала внутренние разногласия
Кибершпионаж	Китай, Россия и негосударственные субъекты	Усилить киберзащиту; продолжать разрабатывать более совершенные методы обнаружения кибер-вторжений	Киберпространство	Защищать национальную безопасность США, интеллектуальную собственность, исследования и разработки

Киберсаботаж	Россия, Иран, Северная Корея и негосударственные акторы	Создание отказоустойчивых сетей с резервированием	Киберпространство	Защита критически важной инфраструктуры и сетей связи, предотвращение уничтожения данных

Источник: Raphael S. Cohen, Nathan Chandler, Shira Efron, Bryan Frederick, Eugeniu Han, Kurt Klein, Forrest E. Morgan, Ashley L. Rhoades, Howard J. Shatz, Yuliya Shokh (2020). The Future of Warfare in 2030. RAND Corporation. ISBN: 978-1-9774-0295-0

Анализ содержания таблицы свидетельствует о полном совпадении объектов по всем трем трендам, с которыми предполагают противостоять США. Это РФ, Китай, Северная Корея и Иран, а также негосударственные субъекты. Возникает комплекс вопросов – какие ответы рассматривали США в ответ на киберкомпроментацию государственных информационных систем; удалось ли США существенно повлиять на поведение противника с помощью прошлых ответов; как следует реагировать на подобные инциденты в будущем? Ответ попытаемся найти в [17].

У аналитиков есть множество вариантов ответов, которые можно сгруппировать по следующим направлениям:

- экономические: санкции против государственных служащих, отдельных субъектов, частных организаций;
- ограничения на поездки физических лиц (применяются в одностороннем порядке или в коалиции с другими странами);
- политические/дипломатические меры: демарши, изгнание иностранных правительственных чиновников;
- разведка: отслеживание сложных постоянных угроз, контрразведывательные операции, скрытые действия, раскрытие вредоносного программного обеспечения и тактики противника;
- действия правоохранительных органов: конфискация активов, демонтаж инфраструктуры по решению суда, арест и судебное преследование;
- военные: кибердемонстрация силы, оборонительные кибероперации против правительственных систем и в «сером пространстве» (например, наступательные или оборонительные ответные действия), наступательные кибероперации.

Заключение

В заключение отметим, что киберблокады и киберзапретные зоны являются серьезными проблемами в современном мире. Они подразумевают угрозы национальной безопасности, коммерческим интересам и свободе слова. Поэтому государства должны развивать надежные системы защиты и резервирования информации, а также налаживать государственно-частное партнерство для эффективной борьбы с киберугрозами.

Однако по мере изменения топологии киберпространства и субъектов меняются возможности и уязвимости, связанные с киберблокадами. Поэтому необходимо постоянно совершенствовать и обновлять системы защиты и применять современные технологии для более эффективного противодействия киберугрозам.

ЛИТЕРАТУРА

1. Alison Shirin Lawlor Russell (2012). Cyber Blockades: Towards a Theory of Informational Warfare in the Digital Era. https://dl.tufts.edu/concern/pdfs/pv63gb62x (дата обращения: 12.04.2023)
2. Daniel T. Kuehl. From Cyberspace to Cyberpower: Defining the Problem. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-

Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210 (дата обращения 12.04.2023)

3. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity. https://www.iso.org/standard/44375.html (дата обращения: 14.04.2023)

4. James B. Godwin, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko (2014). The Russia-U.S. Bilateral on Cybersecurity–Critical Terminology Foundations, Issue 2. EastWest Institute and the Information Security Institute of Moscow State University. ISBN 978-0-9856824-4-6 https://www.files.ethz.ch/isn/178418/terminology2.pdf (дата обращения: 14.04.2023)

5. Joint Publication P3-12.Cyberspace Operations,8 June2018, p.100. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (дата обращения: 12.04.2023)

6. Russell Alison Lawlor (2014). Cyber blockades. Georgetown University Press. ISBN 978-1-62616-113-9

7. The Joint Publication (JP) 1-02,Department of Defense Dictionary of Military and Associated Terms. https://irp.fas.org/doddir/dod/jp1_02.pdf (дата обращения: 14.04.2023)

8. Зиновьева Е. С., Яникеева И. О. (2022). Эволюция взаимодействия России и США в области международной информационной безопасности в исторической ретроспективе //Вестник Санкт-Петербургского университета. Международные отношения. 2022. Т. 15. Вып. 2. С. 158–173. https://doi.org/10.21638/spbu06.2022.203 (дата обращения 12.04.2023)

9. Международная информационная безопасность: Теория и практика: В трех томах./Под общ. ред. А.В.Крутских.-М.: Издательство «Аспект Пресс, 2021.- 384 с. IBSN 97805-7567--1097-7

10. Международный Союз Электросвязи. Серия X: Сети передачи данных и взаимосвязь открытых систем. Безопасность электросвязи. Структура технологий безопасности для подвижной передачи данных от конца до конца. Рекомендации МСЭ-Т X.1121. https://www.itu.int (дата обращения: 12.04.2023)

11. Ю.И. Стародубцев, П.В. Закалкин, С.А. Иванов. Техносферная война как основной способ разрешения конфликтов в условиях глобализации. Военная Мысль · № 10 — 2020, с.16-21. https://vm.ric.mil.ru/Nomera/6/ (дата обращения: 12.04.2023)

12. Яковлева А.В. (2021). Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. – 2021. – Т. 11. – № 4. – С. 70-81. – DOI 10.33693/2223-0092-2021-11-4-70-81 (дата обращения: 12.04.2023)

13. Яникеева И.О. (2022). Российско-американские отношения в сфере обеспечения международной информационной безопасности // Мировая политика. – 2022. – № 4. – С. 1 - 15. DOI: 10.25136/2409-8671.2022.4.38897 EDN: JKNPZX : https://nbpublish.com/library_read_article.php?id=38897 (дата обращения: 12.04.2023)

14. Hakimdavar, G. (2014). A Strategic Understanding of UN Economic Sanctions International Relations, Law, and Development. Taylor & Francis Group. ISBN: 978-0-203-10946-5.

15. Lee Jones (2015). Societies Under Siege. Exploring How International Economic Sanctions (Do Not) Work. Oxford University Press. ISBN 978-0-19-874932-5

16. Raphael S. Cohen, Nathan Chandler, Shira Efron, Bryan Frederick, Eugeniu Han, Kurt Klein, Forrest E. Morgan, Ashley L. Rhoades, Howard J. Shatz, Yuliya Shokh (2020). The Future of Warfare in 2030. RAND Corporation. ISBN: 978-1-9774-0295-0

17. Quentin E. Hodgson, Yuliya Shokh, Jonathan Balk (2022). Many Hands in the Cookie Jar. Case Studies in Response Options to Cyber Incidents Affecting U.S. Government Networks and Implications for Future Response. RAND Corporation. ISBN: 978-1-9774-0901-0 DOI: https://doi.org/10.7249/RRA1190-1

18. Digital security is essential for trust in the digital age. https://www.oecd.org/digital/digital-security/ (дата обращения 12.04.2023)

19. Nikita Duggal (2023). Top 20 Cybersecurity Trends to Watch Out for in 2023. https://www.simplilearn.com/top-cybersecurity-trends-article (дата обращения 14.04.2023)