*Connections: The Quarterly Journal*
**ISSN 1812-1098, e-ISSN 1812-2973**

Пиотр Дела, *Connections QJ* 15, № 3 (2016): 59-69
https://doi.org/10.11610/Connections.rus.15.3.05

**Рецензированная статья**

# Киберпространство как среда, находящаяся под влиянием деятельности организованной преступности

## *Пиотр Дела*

*Академия национальной обороны, Варшава, Польша, http://www.akademia.mil.pl*

**Резюме**: В этой статье представлен обзор основных проблем, связанных с использованием киберпространства в качестве поля, на котором ведется информационная война. Также рассматривается роль деятельности организованной преступности. Идентифицированы основное влияние, место и роль распознавания и противодействия распознаванию в киберпространстве. Оценено экономическое влияние в смысле уровня развития киберпространства.

**Ключевые слова**: Киберпространство, информационная война, организованная преступность.

## Введение

По мере развития общества появляется ряд видов преступлений, которые связаны как с индивидуальной, так и с организованной преступностью. Уголовные методы и способы, с помощью которых организована преступность, напрямую связаны с технологическим развитием общества. По этой причине преступность развивается и во все большей степени переносит свою деятельность в киберпространство, идя рука об руку с развитием информационных и коммуникационных технологий (ИКТ), используемых в сфере киберпространства, являющимся широко распространенным понятием. Это относится как к индивидуальной преступности, так и к организованной преступности. Киберпространство стало идеальной средой как для совершения преступлений, так и для новых способов ведения дел в организованной преступности и управлении новыми формами борьбы за влияние. Это, в основном, имеет место в отношении влияния информации как

на враждебные преступные организации (соперничающие между собой), так и на государственные и международные институции, которые борются с организованной преступностью. Взаимодействия такого характера имеют признаки конфликта или войны за влияние, ведомой в киберпространстве, направлены на создание положительного образа преступной организации, на введение в заблуждение институций, ведущих борьбу с организованной преступностью и на подрыв потенциальной конкуренции – и все это средствами информационного взаимодействия. Масштаб этого явления будет увеличиваться по мере развития информационного общества, и взаимодействие с ним примет самые разные формы, как логические, так и кинетические.

Поэтому критически важно идентифицировать формы, методы и последствия деятельности организованной преступности в киберпространстве, а также способы противодействия ей. В киберпространстве будут иметь место конфликты, имеющие признаки войны, которые характеризуются участием оппонентов с асимметрическим весом, неограниченным охватом, неизвестными последствиями и неизвестными целями соперников.

Конфликты в киберпространстве отличаются по характеру от хорошо известных конфликтов в прошлом. Как говорят, каждая эпоха имеет свою собственную войну, соответствующую уровню технологического и социального развития общества. Действительно, это видно по способам ведения войны и в мерах, которые предпринимаются в ходе войны. Доступ к хранимой, обрабатываемой и передаваемой в киберпространстве информации дал обществу новое качество жизни, сделав возможными социальные функции, которые были просто мечтой и фантазией в не столь далеком прошлом. Это проявляется не только в быстром развитии общества, но имеет и важные экономические измерения, как показывает уменьшение стоимости функционирования общества при ускорении реализации этого функционирования.

С одной стороны, эти технологии способствуют развитию новых социальных форм, с другой, они порождают обоснованную озабоченность в связи с их использованием. В число самых ярких примеров влияния современных технологий на функционирование общества входит блокировка Интернета в Эстонии в 2007 и в Грузии в 2008. Это новое измерение, а именно – киберпространство, будет иметь огромное влияние на функционирование общества, на ход будущих конфликтов и на способы функционирования организованной преступности. Масштаб и последствия этого соревнования можно оценить только приблизительно, основываясь на упомянутых выше примерах.

Основной целью этой статьи является идентификация возможных способов, с помощью которых организованная преступность взаимодействует и осуществляет конкуренцию в киберпространстве, а также способы, с по-

мощью которых государственные и международные институции могут с ней бороться.

В отношении деятельности организованной преступности и ее влияния на глобальное сообщество важно идентифицировать характер современных конфликтов и определить саму сущность войны, поскольку деятельность организованных преступных групп в киберпространстве имеет признаки войны за влияние и за максимизацию прибыли. Саму войну как социальное явление трудно дефинировать в нынешних понятиях. Причиной тому являются разные факторы, имеющие отношение к войне, среди которых неимоверное ускорение глобального экономического развития, рост населения и политические изменения на международной арене. Часто упоминаются такие понятия, как *экономическая война, информационная война* или *политическая война*. Слово «война» стало термином, который используется разными политическими субъектами для выражения их отношения к конкретной ситуации. Это просто риторика на политической арене, направленная на произведение конкретного социального и международного впечатления. Трудно провести границу между тем, чем война является, и тем, чем война не является, особенно в последнее время, когда этот термин используется неправомерно некоторыми политиками и экспертами, рассуждающими на тему «глобальной войны с террором» или «войны против организованной преступности».

К примеру, Болеслав Бальцерович, признанный польский военный теоретик, считает, что современные определения войны раскрывают тесные отношения между политикой, государством, войной и контр-войной (тоже связанной с использованием насилия) в качестве инструмента политики.[1] Она представляет собой игру между силой, властью и людьми, или иными словами, между разведкой, силой и неким (слепым) компонентом. Война как форма разрешения конфликта между воюющими сторонами характеризуется использованием насилия, соответствующего ситуации, наличию способностей и социальному развитию. В этом отношении экономическая и социальная цена ведения войны, которую должны учитывать все власти в демократическом обществе, является важной в смысле функционирования государства. Поэтому подход к войне, в том числе и к борьбе с организованной преступностью, должен учитывать отношение между экономической ценой войны и достигнутыми результатами, а также учитывать социальную цену, т.е. неблагоприятные последствия для общества, которая играет все более важную роль. Все эти факторы дают основание понимания, что киберпространство используется как поле, на котором соперничают преступные организованные группы, не только совершая преступления против отдельных государств и международных институций, но и между собой. Так же важно обращать внимание на способы и методы, с

[1] Boleslaw Balcerowicz, *Czym jest współczesna wojna?* http://www.pl.ism.uw.edu.pl/images/stories/Publikacje/ebiblioteka/balcerowiczwspolczesnawoja.doc, по состоянию на 15 января 2016.

помощью которых можно вести борьбу с деятельностью такого характера в киберпространстве.

## Асимметрия информации

Асимметрия, означающая нарушение или полное отсутствие симметрии, имеет место во многих областях человеческой деятельности, в том числе – но не единственно – в уровне развития культурных, экономических и технологических сообществ. Государства пытаются передвинуться вверх по международной лестнице, основываясь на экономическим росте и с использованием последних технологий для повышения конкурентоспособности своей экономики и для дальнейшего развития своего общества. Одним из показателей современности государства является существование ИТ инфраструктуры, которая служит не только средством для общественного доступа к информации и для обмена информацией, но во все большей степени становится незаменимым элементом государственных функций.

Киберпространство так же нашло отражение в нормативных документах, которые определяют киберпространство разными способами, учитывая чисто технические или чисто человеческие аспекты. По мнению автора, сегодня киберпространство представляет собой среду, в которой отдельные лица и целые сообщества могут создавать новые формы отношений и новые методы сотрудничества и функционирования. Это тип пространства, в котором мы можем существовать независимо от окружающей среды. Основой киберпространства является информация. Поэтому мы можем попытаться определить киберпространство как пространство сотрудничества между людьми, использующими электронные устройства для создания, хранения, передачи и обработки информации. Данное определение требует соответствующего определения электронных устройств, рассматриваемых в качестве элементов в рамках ИТ инфраструктуры, которая создает среду для обмена и обработки информации. Такой средой является Интернет и другие телекоммуникационные сети, используемые для передачи, обработки и хранения информации. В общем смысле, а также имея в уме вопросы, связанные с теорией систем, Интернет является технической системой, создающей инфраструктуру для передачи, обработки и хранения информации. Киберпространство – это и социальная система, в которой самым важным элементом являются ее пользователи и которая базируется на технической системе Интернета и других ИКТ сетях.

Таким образом, определенное пространство становится ареной положительного сотрудничества, а именно, развития областей образования, общества, экономики и безопасности, а также ареной отрицательного сотрудничества в смысле кибернаблюдения, киберпреступности, кибертерроризма и кибервойны.

Проведенный анализ показал, что новые, дотоле неизвестные угрозы идут рука об руку с развитием новых технологий. В плане развития кибер-

пространства, похоже, основной угрозой является опора на технологию и невозможность возвращения к способу функционирования государства, имевшего места до введения этих технологий. Это подтверждается наблюдением отрицательных явлений в киберсфере. Степень зависимости от технологии будет зависеть от технологического развития государства и уровня его готовности к потенциально пагубным явлениям в киберпространстве. Чем выше фаза развития, тем более уязвимым является функционирование государства и общества от инцидентов, отказов или разрушения технологий. В киберпространстве организованная преступность становится еще более опасной.

Страны с хорошо развитой ИКТ инфраструктурой и совершенной системой защиты этой инфраструктуры будут иметь информационное преимущество по сравнению с менее развитыми странами. В свою очередь, отсутствие соответствующих систем защиты для развитых ИКТ инфраструктур может проявить себя в блокировке работы государственных органов, принимающих решения, и иметь тяжелые социальные последствия. С другой стороны, государства с недоразвитой ИКТ инфраструктурой (или даже неформальная организация преступного характера) с механизмами, процедурами и структурами, способными взаимодействовать с ИТ инфраструктурой другой страны, могут угрожать основам более развитой страны и подорвать ее экономическую, политическую, военную и социальную систему. Современный мир – это место, где существует информационная асимметрия.

Обладание правильными структурами механизмов защиты собственной ИТ инфраструктуры страны и ее информационных ресурсов сейчас является незаменимым элементом кибербезопасности и лежит в основе национальной безопасности. Другим важным аспектом, имевшей место в современном мире информационной асимметрии, является обладание инструментами, процедурами и структурами, способными распознать и вывести из строя противника, в данном случае – организованную преступность. Эти два элемента формируют картину защиты и нападения на кибераренe и, среди прочего, становятся нераздельной частью борьбы против организованной преступности. Качество этих элементов будет оказывать влияние на ход, цену и эффективность (степень реализации целей) предпринимаемых действий.

С точки зрения информационной асимметрии, необходимо классифицировать стороны, участвующие в конфликте, в смысле уровня развития инфраструктуры. В первую группу входят страны с хорошо развитой ИТ инфраструктурой, которые также обладают сетецентрическими способностями. Это означает, что они располагают интегрированными системами передачи данных и могут в полной степени предоставлять информационные ресурсы для общего пользования. Вторая группа охватывает страны, которые имеют хорошо развитую ИКТ инфраструктуру, но не располагают сетецентрическими способностями. Эти страны имеют полностью инте-

грированные ИКТ системы, но все еще не располагают системами, которые позволяют общее пользование всей информацией, которой они обладают. Эта категория может включать страны, которые находятся на стадии развития ИКТ инфраструктуры, на которой не все их ИКТ системы интегрированы, т.е. нет потока информации между системами. Четвертая категория стран включает те страны, которые не имеют ИКТ инфраструктуры, или те страны, в которых уровень развития ИТ инфраструктуры очень невысок, что не позволяет интеграцию. В отдельную категорию входят неформальные группы, в том числе сети организованной преступности, которые не имеют собственное законодательство и которые используют ИТ инфраструктуру, находящуюся на территории страны (или группы стран) для ведения своего бизнеса.

## Методы воздействия

Использование киберпространства в форме отрицательного сотрудничества является ничем иным, как борьбой за завоевание информационного превосходства над другой стороной. С одной стороны, оно включает желание скрыть информацию и собственные намерения, создать ложный образ в то время, как субъект стремится к получению информации о намерениях противной стороны; с другой стороны, оно включает обеспечение функциональности своей собственной информационной системы и нейтрализацию (выведение из строя) информационной системы противоположной стороны.

При таких конкретных целях в смысле отрицательного сотрудничества надо попытаться определить информацию как фактор, который определяет течение любого конфликта. Сегодня есть ряд разных подходов и определений этого понятия. Для многих теоретиков, принимавших участие в определении понятия информации, сама по себе информация считается исходным понятием, которое не подлежит определению. Некоторые авторы отказались от такого определения и довольствуются ее интуитивным и разговорным значением. Интересно, что в плане целей действий в киберпространстве определение информации было дано профессором Марианом Мазур, величайшим польским кибернетиком, который – в связи с психологической теорией отражения – утверждал, что информация – это «отношение между оригиналом и образом оригинала».[2] Другое определение информации было дано Пиотром Сиенкевичем, который понимает информацию как «набор фактов, событий, характеристик, объектов, представленных в такой форме, которая позволяет реципиенту реагировать на ситуацию и предпринимать адекватные умственные или физические действия».[3]

---

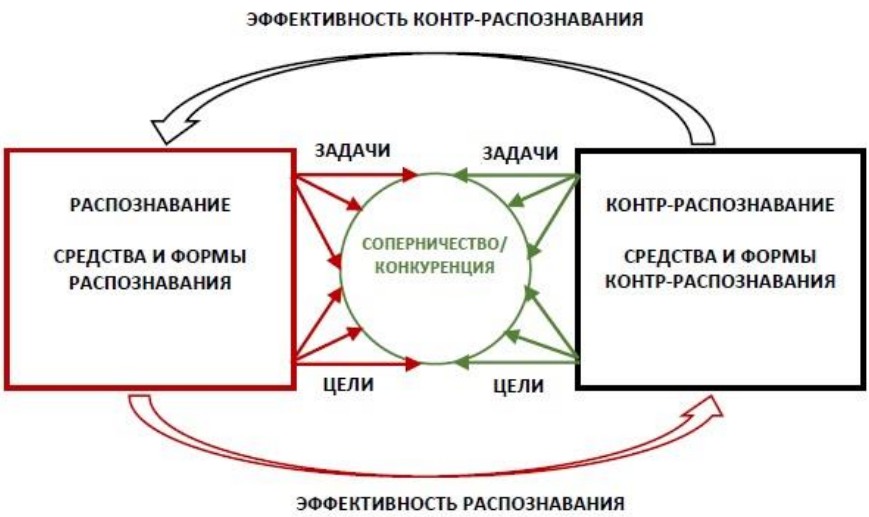
[2] Marian Mazur, *Cybernetic Theory of Autonomous Systems* (Warsaw: PWN, 1966), 35-37.

[3] Piotr Sienkiewicz, *Systemy kierowania* (Warsaw, 1989), 128.

Эти определения сфокусированы на идентификации информации в качестве зеркального образа наблюдаемой действительности, что не обязательно является отражением истины или фактов. На основе этого отражения в сочетании с рядом разных факторов (образование, опыт, убеждения наблюдателя и т.д.) строится знание. Если итоговая картина реальности в некоторой степени далека от истины, тогда созданное на этой основе знание не обеспечивает эффективное и результативное взаимодействие с реальностью.

Достоверность полученной информации зависит от качества системы распознавания и качества деятельности, которая этому мешает, или контр-распознавания. Эти два противоположных процесса, которые находятся в конкуренции в отношении информации, направлены на достижение информационного превосходства над оппонентом. Сторона, которая добивается преимущества в сфере информации, добьется своей цели при малых расходах, максимизируя расходы противоборствующей стороны. Эта система показана на фиг. 1.

При анализе распознавания надо отметить, что оно является процессом, посредством которого мы можем отличать основные материальные объекты и сущности. Субъектами этого процесса являются объект процесса распознавания и его контекст, физическая информационная среда и любые технические средства, используемые наблюдателем, который является анализатором и получателем информации. В свою очередь, в число субъектов распознавания входят все участники этого процесса, в том числе




**Фигура 1: Отношение между распознаванием и контр-распознаванием при отрицательном сотрудничестве.**

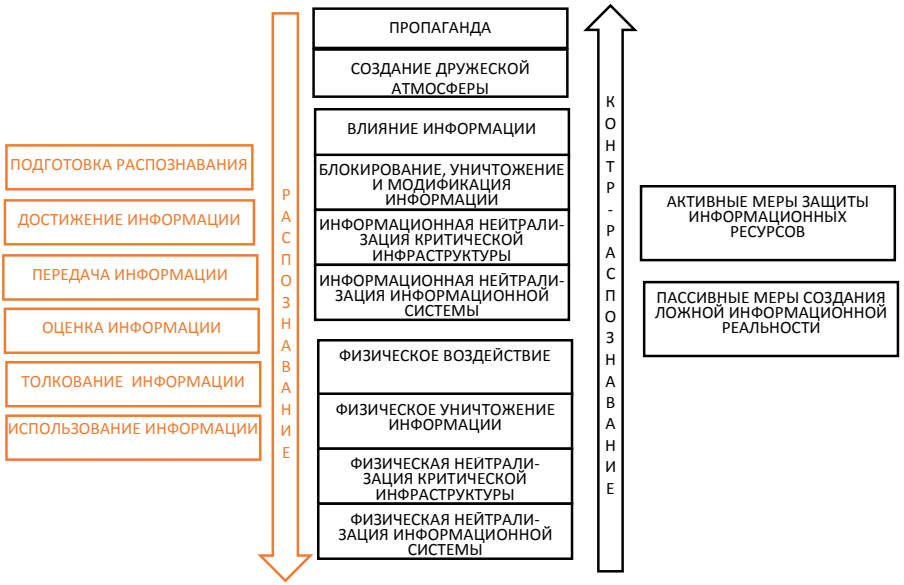
группы отдельных лиц и разведывательные органы на разных уровнях в организации.

Как было упомянуто выше, качество процесса распознавания в киберпространстве зависит от качества противодействия распознаванию, которое не только скрывает намерения (информацию), на также обеспечивает основной уровень защиты информационных ресурсов. Как часть борьбы в киберпространстве, информационное контр-распознавание включает как активные, так и пассивные меры.

Активные меры в плане контр-распознавания являются способом защитить корпоративную информацию, реализуются специальными группами с использованием ряда методов и инструментов. Их пассивный (превентивный) контрапункт подразумевает введение оппонента в заблуждение путем создания ложной картины.

Отрицательное сотрудничество в киберпространстве, понимаемое как информационная война, требует как наступательных, так и защитных действий, которые необходимы для достижения информационного превосходства над соперником и для достижения своих собственных целей. В настоящее время оно используется как прелюдия к действиям, осуществляемым вне киберпространства. По этой причине, до того, как будет иметь место физическая конфронтация между самими преступными группами или между преступниками и институциями, которые борются с ними, война ведется в сфере киберпространства, охватывая не только территорию сторон, напрямую вовлеченных в конфликт, но и киберпространство международного сообщества. Битва может протекать медленно или агрессивно. В первом случае воздействие противоположной стороны будет разворачиваться постепенно, без заметного начала нападения, может пройти незамеченным или на него могут не обратить внимание, приняв его за ежедневное онлайн явление. В свою очередь, агрессивное нападение характеризуется высокой степенью интенсивности взаимодействия в киберпространстве, и его последствия будут ощущаться более остро.

При идентификации манеры воздействия к киберпространстве это воздействие можно разделить на несколько фундаментальных этапов. Первый этап включает установление информационного превосходства через создание положительного образа сторон, вовлеченных в конфликт. Организованная преступность зависит от утаивания настоящей деятельности группы и создания благоприятной атмосферы для расширения сферы ее влияния. Следующим этапом является распознавание информационной системы оппонента (вражеской преступной группы или государственных институций в их борьбе против организованной преступности) с прицелом на ее компоненты, информационные ресурсы, процедуры и критическую инфраструктуру. Контр-распознавание – это стадия, эквивалентная диагностике, а именно действия, направленные на запутывание и введение в заблуждение соперника, а также защита своей собственной информационной системы. Последним этапом в этом графике отрицательного сотруд-




**Фигура 2: Распознавание и контр-распознавание в киберпространстве.**


**Фигура 3: Области борьбы в киберпространстве.**

ничества в киберпространстве является выведение из строя информационной системы соперника путем использования воздействия на информацию и, что вероятно, физическим (кинетическим) воздействием.

Целью описанных выше шагов, являющихся частью битвы в киберпространстве, является достижение информационного превосходства, переходящего к разработке и ведению преступной деятельности с позиции силы или подчинению противника в результате воздействия, которому он подвергся в киберпространстве. Фигуры 2 и 3 показывают области, в которых организованные преступные группы могут вести войну в киберпространстве.

## Заключение

В этой статье представлены определенные аспекты воздействия организованной преступности на киберпространство. Было раскрыто новое измерение организованной преступности и его влияние на развитие и ход потенциальных конфликтов, инициируемых в целях расширения влияния и увеличения прибылей. Были идентифицированы важные явления, наблюдаемые в современном мире, в частности неравенство между уровнями развития отдельных стран. Оно проявляет себя, среди прочего, в уровне развития ИТ систем и инфраструктуры, ассоциируемых со сторонами конфликта, и приводит к информационной асимметрии.

По мнению автора, война в киберпространстве и борьба за информационное превосходство станет новой формой соперничества на международной арене, в том числе и в борьбе за влияние между кругами организованной преступности. Ее последствия будут тяжелыми, оказывая влияние не только на экономическую сферу, но на первом месте, на социальную сферу.

## Библиография

Alberts, David S., John J. Garstka, Frederick P. Stein. *Network Centric Warfare*, 2nd Revised Edition. Washington, D.C.: DoD C4ISR Cooperative Research Program, 2000. Доступно на www.dodccrp.org/files/Alberts_NCW.pdf.

Balcerowicz, Bolesław, *Czym jest współczesna wojna?* Available at http://www.pl.ism.uw.edu.pl/images/stories/Publikacje/ebiblioteka/balcerowiczwspolczesnawoja.doc.

Balcerowicz, Bolesław. “Wojna. Kwestie nie tylko terminologiczne,” *Myśl wojskowa* 3 (2003): 53-74.

Balcerowicz, Bolesław. *Polskie wojny*. Available at www.pl.ism.uw.edu.pl/images/stories/Publikacje/ebiblioteka/balcerowiczPOLSKIEWOJNY.doc.

Cebrowski, Arthur K., and John J. Garstka. “Network Centric Warfare: Its Origins and Future,” *Proceedings Magazine* 124, no. 1 (January 1998): 28-35.

Gonzales, Daniel, Michael Johnson, Jimmie McEver, Dennis Leedom, Gina Kingston, and Michael S. Tseng, *Network-Centric Operational Case Study. The Stryker Brigade Combat Team*. Santa Monica, CA: RAND, 2005. Доступно на http://www.rand.org/pubs/monographs/MG267-1.html.

Kotarbiński, Tadeusz. *Traktat o dobrej robocie*. Wrocław: Ossolineum, 1969.

Mazur, Marian. *Cybernetic Theory of Autonomous Systems*. Warsaw: PWN, 1966.

Munkler, Herfried. *Wojny naszych czasów*. Kraków: Wydawnictwo WAM, 2004.

Sienkiewicz, Piotr. *Systemy kierowania*. Warszawa: Wiedza Powszechna, 1989.

Sun Tzu. *Sztuka wojny*. Warszawa: Przedświt, 1994.

## Об авторе

Полковник инженер Пиотр Дела, доцент, является выпускником Факультета Кибернетики Военно-технологического университета в Варшаве. С самого начала его работа была связана с Министерством национальной обороны и военным образованием. С 1998 года он является преподавателем в Национальном университете обороны в Варшаве. В настоящее время он работает в Институте инжиниринга систем безопасности Факультета национальной безопасности. Полковник Дела – один из авторов и организаторов серии военных учений в сфере ИТ безопасности. Он написал более 100 статей, работ, учебников, научных работ и монографий. В сферу его научных интересов входят системы поддержки принятия решений, коммуникационные и информационные системы, информационная безопасность, кибербезопасность. *E-mail*: p.dela@aon.edu.pl.