Может ли шифрование спасти жизни? Безопасный обмен сообщениями и его инфраструктура как точки соприкосновения кибервойны и обычной войны: случай Украины

Ксения Ермошина, Франческа Мусиани

Этот документ является предварительным отпечатком

Ксения Ермошина, Франческа Мусиани, 2024, «Может ли шифрование спасти жизни? Безопасный обмен сообщениями и его инфраструктура как точки соприкосновения кибервойны и обычных боевых действий: случай Украины», Медиа, война и конфликт, OnlineFirst.

Для цитирования или ссылки обращайтесь к опубликованной версии.

Может ли шифрование спасти жизни? Безопасный обмен сообщениями и его инфраструктура как точки соприкосновения кибервойны и обычной войны: случай Украины

Ксения Ермошина и Франческа Мусиани
Центр Интернета и общества, Национальный центр научных исследований (CNRS), Париж, Франция

Абстрактный

Споры вокруг права на неприкосновенность частной жизни людей в гиперсвязанном мире являются давними дебатами, где особое внимание уделяется технологиям шифрования, которые кодируют информацию, преобразуя ее исходные представления в альтернативные формы, которые компьютеры не могут расшифровать, тем самым обеспечивая безопасность коммуникаций. Эти технологии находятся в центре публичной полемики, в которой конфиденциальность выступает за столкновение с утверждениями о том, что шифрование представляет собой угрозу общей безопасности как средство подрывных действий. Недавние события в вооруженном конфликте на Украине открывают или возобновляют такие вопросы, как: какова роль шифрования и технологий конфиденциальности во время войны? Как вооруженный конфликт бросает вызов существующим моделям угроз, каковы новые риски для гражданского общества? Может ли шифрование спасти жизни? В этой статье рассматриваются эти вопросы, показывая, что зашифрованные сообщения являются предметом конвергенции между информационными и физическими аспектами «в поле» войны в 21 веке. Цель состоит в том, чтобы показать, как эти инструменты обмена сообщениями и цифровая экосистема, которая делает возможным их развертывание (интерфейсы, поставщики доступа, операторы связи), теперь являются неотъемлемой частью инфраструктуры войны и сопротивления, где границы между кибервойной и обычной войной становятся все более размытыми. Однако мы также подчеркнем ограничения подхода, ориентированного на инструменты, и продемонстрируем, как в случае войны в Украине физические угрозы гражданским лицам и повреждение инфраструктуры означают, что зашифрованные сообщения являются одной из нескольких инновационных технических и социальных практик целостной самообороны, применяемых украинцами.

Ключевые слова
вооруженный конфликт, кибервойна, шифрование, инфраструктура, интернет, управление интернетом, физическая война, Россия, Украина

Введение

Думать об инфраструктурной политике сегодня — значит рассматривать, как интернет-инфраструктуры определяют современный геополитический конфликт.1 В частности, споры вокруг права на неприкосновенность частной жизни отдельных лиц, связанные с их все возрастающей зависимостью от цифровых технологий, являются давними дебатами. В ходе этих дебатов особое внимание уделяется технологиям шифрования, которые кодируют информацию путем преобразования ее исходных представлений

в альтернативные формы, которые компьютеры и несанкционированные третьи лица в принципе не способны расшифровать, что обеспечивает безопасность коммуникаций.

Эти технологии находятся в центре публичного спора, в котором приватность выступает за столкновение с теми, кто утверждает, что шифрование представляет угрозу общей безопасности, поскольку оно допускает терроризм и другие формы подрывной деятельности. Ранее мы анализировали этот и другие споры в недавней публикации (Ermoshina & Musiani, 2022). В этой публикации мы изложили нелинейную историю шифрования, которая привела в последнее десятилетие (в частности, после разоблачений Сноудена и их переосмысления шифрования как вопроса общественного интереса) к рождению четкого — и порой запутанного и фрагментированного — ландшафта инструментов для удовлетворения проблем пользователей. Это означало, что ряд пользователей с разными профилями не уверены в том, какой сервис обмена сообщениями использовать и, возможно, к нему приспособиться; разработчики, со своей стороны, находятся в состоянии «постоянства» и занимаются компромиссами между различными проблемами дизайна, чаще всего в отсутствие формальных процессов стандартизации (Ermoshina & Musiani, 2022: 23). Протоколы и приложения в области зашифрованных сообщений имеют общую цель, которая заключается в обеспечении некоторой степени цифровой маскировки для повышения свободы отдельных лиц и групп в осуществлении деятельности или профессий; однако их разнообразие раскрывает (и выполняет) воображаемые публики, ценности или цели. Безопасные инструменты и протоколы обмена сообщениями задуманы, разработаны, созданы и повторно присвоены; таким образом, существует необходимость в критическом допросе самого процесса «маскировки» (Уилан, 2024).

Развитие вооруженного конфликта в Украине делает еще более актуальным ответ на вопросы, которые эта публикация начала открывать: какова роль шифрования и технологий конфиденциальности во время войны? Как вооруженный конфликт бросает вызов существующим моделям угроз, каковы новые риски для гражданского общества? Может ли шифрование спасти жизни? В этом вкладе предлагается рассмотреть эти вопросы, показав, что технологии зашифрованных коммуникаций и сокрытия трафика являются предметом конвергенции между информационными и физическими аспектами «в поле» войны в 21 веке.2

В этой статье разрабатывается двухчастный аргумент. Во-первых, мы покажем, как эти инструменты обмена сообщениями и подключения, а также цифровая экосистема, которая делает возможным их развертывание (интерфейсы, поставщики доступа, операторы связи), теперь являются неотъемлемой частью инфраструктуры войны и сопротивления, где границы между кибервойной и обычной войной становятся все более размытыми. Во второй части мы подчеркнем ограничения подхода, ориентированного исключительно на инструменты, и покажем, как в случае войны в Украине физические угрозы гражданским лицам и повреждение инфраструктуры делают так, что зашифрованные сообщения являются лишь одной из нескольких инновационных технических и социальных практик комплексной самообороны, применяемых украинцами. Использование зашифрованных сообщений во время войны включает мобилизацию как инструментов повышения конфиденциальности последнего поколения, так и технологий до Web 2.0, которые смещают фокус с инноваций на наладку, ремонт, обслуживание и переработку. Случай Украины, в частности, демонстрирует сосуществование этих различных инструментов, стратегий и проблем, на которые они отвечают, поскольку сама страна разделена, а использование зашифрованных инструментов различается не только в зависимости от профилей пользователей, но и от ее оккупированных и неоккупированных территорий.

Эта статья стремится внести ценный вклад на трех уровнях. Во-первых, она предлагает перспективу, основанную на «материальном повороте» и инфраструктурных исследованиях течений в области исследований науки и технологий (STS), для изучения использования и развития средств массовой информации и коммуникации во время войны. Во-вторых, она выносит на научное обсуждение эмпирический материал, полученный из недостаточно изученных (и труднодоступных) полевых исследований, включая интервью с украинскими военными журналистами, тренерами по цифровой безопасности, интернет-провайдерами

(ISP) и пользователи средств связи с высоким уровнем риска. В-третьих, предлагается аргумент и набор выводов, которые — помимо внутреннего интереса изучения украинского случая — могут быть использованы и применены исследователями в других контекстах, чтобы увидеть, как стратегии использования сходятся или различаются.

Структура статьи

В первом разделе будет представлена литература, которую мы использовали в этом исследовании и которая легла в основу более длительного исследования зашифрованных сообщений с точки зрения социальных наук, начатого в 2016 году; за этим следует краткое введение в нашу методологию. Затем статья переходит к размещению предмета нашего исследования в более широкой истории и историях того, как устройства связи используются стратегически и/или как инструмент выживания во время войны. Последующие два раздела являются ядром статьи; в первом мы обсуждаем, как инструменты зашифрованных сообщений использовались в контексте российского вторжения в Украину не только как устройство экстренной связи, но и как «элемент пазла» более широких стратегий выживания и военного преимущества. Во втором мы рассматриваем, как такие инструменты, несмотря на их известность, являются лишь частью более широкой инфраструктуры информации и коммуникации во время войны, которая часто прибегает к «более простым» и более базовым устройствам и процессам связи, которые не менее стратегически важны, а иногда и более адаптированы к конкретным военным контекстам, чем передовые технологии повышения конфиденциальности. Статья завершается кратким рассмотрением данного исследования в более широком контексте «глобальной войны за управление Интернетом», которую ДеНардис (2014) изначально использовал как метафору, но которая в наши дни приобретает вполне «материальное» значение.

Взгляд социальных наук на шифрование и его инфраструктуру3

За эти годы ученые в области STS разработали методологические инструменты, позволяющие читать и описывать инфраструктуры, такие как «этнография инфраструктуры» Стара (1999), призывающая к повышенной этнографической чувствительности, чтобы отслеживать то, что в противном случае находится на заднем плане, невидимо и принимается как должное, чьи процессы проектирования, если их эмпирически проверить, могут раскрыть страстные и иногда конфронтационные истории диссонансов и привязанностей (Стар и Руледер, 1994). Боукер и Стар (1999) обозначили как «инфраструктурную инверсию» двойной методологический жест, состоящий из взгляда «за кулисы» практик, чтобы проследить то, что было разрешено или ограничено дизайном, и взгляда «в глубину», чтобы позволить обозначениям и смыслу возникнуть из технических стандартов, устройств и аппаратов, чтобы понять, где возникают конфликты и противоречия и как они формируются с помощью инфраструктур и посредством них .

В рамках этой работы особое внимание уделяется трансформациям, связанным с внедрением цифровых технологий в различных социальных мирах (Edwards, 2010). Действительно, когда речь идет об Интернете и цифровых технологиях, а также информационных системах в целом, ученые признали – и эмпирически проанализировали – что инфраструктура также охватывает более абстрактные (и априори нематериальные) артефакты, такие как протоколы, стандарты (Bowker et al., 2010), программное обеспечение и код (например, Blanchette, 2011; Fuller, 2008), наряду с физической инфраструктурой, поддерживающей функционирование цифровых сетей, такой как подводные кабели, центры обработки данных, точки обмена интернет-трафиком (IXP) и т. д. Развивая эту идею – пожалуй, наиболее известное выражение, сформулированное юристом Лоуренсом Лессигом, — «кодекс — это закон»: что технические устройства могут быть инструментами социального контроля наряду с другими нормативными системами, ряд авторов уточнили наше понимание механизмов власти, присущих и проявляемых техническими инфраструктурами и архитектурами Интернета и

цифровые/сетевые технологии. Примерами этого исследования являются вдохновленная Фуко работа Гэллоуэя (2004) о протоколах TCP/IP и DNS как средстве контроля, анализ ДеНардиса (2009) «политики протоколов», пронизывающей переход от IPv4 к IPv6, анализ Джиллеспи (2014) «значимости алгоритмов» в управлении интернет-контентом, а также — что особенно актуально в контексте этой статьи — совокупность работ, посвященных «конфиденциальности по замыслу» и степени, в которой защита конфиденциальности может быть встроена и вписана в технологию (Кавукян, 2012).

Зашифрованные инструменты, а также инфраструктура, которая их поддерживает и обеспечивает их функционирование, все чаще рассматриваются с точки зрения STS и инфраструктурных перспектив, чтобы пролить свет на технические компоненты и процессы, которые «тяжелы» с точки зрения политических последствий. Действительно, как это вряд ли можно оспорить сейчас, откровения Эдварда Сноудена 2013 года стали знаковым событием в развитии области защищенных коммуникаций (см. Snowden, 2019). Шифрование коммуникаций в больших масштабах и удобным способом стало предметом общественного беспокойства, и возникло новое криптографическое воображение, которое рассматривает шифрование как необходимое предварительное условие для формирования сетевых обществ (Myers West, 2018). Наряду с превращением шифрования в полноценный политический вопрос, откровения Сноудена стали катализатором давних дебатов в области протоколов защищенных сообщений. Криптографическое сообщество (в частности, академические и свободно-программные коллективы) возобновили свои усилия по созданию протоколов защищенных сообщений следующего поколения, чтобы преодолеть ограничения существующих протоколов. Протоколы являются жизненно важной частью функционирования Интернета, обеспечивая его концептуальную модель, а также набор спецификаций, которые объясняют, как данные должны перегруппировываться в пакеты, адресоваться, передаваться, маршрутизироваться и приниматься; Как ясно показала Лора ДеНардис (2009) в своей книге «Политика протоколов», выбор и принятие конкретных протоколов имеет важные политические и экономические, а также технические последствия.

Кроме того, точки инфраструктурного контроля, выходящие за рамки их изначально предполагаемой функции, могут служить доверенными лицами для различных субъектов, чтобы восстановить (или получить) контроль или манипулировать потоком денег, информации и рынком идей в цифровой сфере — то, что было названо «поворотом к инфраструктуре в управлении интернетом» (Musiani et al., 2016). Это может привести к полноценной политизации инфраструктур IG, где широкий круг частных и государственных субъектов стремится использовать определенные социально-технические функции, заложенные в цифровых инфраструктурах, включая инфраструктуры, поддерживающие шифрование, в качестве инструментов власти (DeNardis, 2009). Этот вопрос особенно важен в деликатных контекстах, включая информационные и/или вооруженные конфликты, поскольку использование инфраструктуры интернета для выполнения функций, отклоняющихся от их изначальной предполагаемой цели, может привести к значительному сопутствующему ущербу стабильности и безопасности интернета и защите гражданских свобод в Интернете (DeNardis and Musiani, 2016).

В течение довольно долгого времени «шифрование» как предмет исследования в основном было прерогативой компьютерных ученых, а более «социальные» вопросы, касающиеся его, часто ограничивались дебатами о пригодной безопасности, т. е. обсуждениями, проходящими в сообществе компьютерных ученых и основанными на исследованиях типа опросов, направленных на поиск способов сделать зашифрованные инструменты более простыми в использовании (см., например, Abu-Salma et al., 2017). Несколько исследований пошли дальше в социологической перспективе относительно конкретных групп пользователей определенных зашифрованных инструментов или протоколов (см., например, исследование Брауна и Оствина [2018] характеристик и мотивов программного обеспечения для шифрования Pretty Good Privacy).
После разоблачений Сноудена зашифрованные сообщения становятся предметом широких публичных дебатов, наряду с целями конфиденциальности и безопасности, которые они стремятся улучшить; социальные науки взяли на себя задачу глубокого изучения того, как зашифрованные инструменты обмена сообщениями задуманы и разработаны, прин

по разным профилям пользователей – иногда непреднамеренными или непредвиденными способами – как они вдохновляют и вдохновляются разными образами и как они в конечном итоге становятся целью управления. Таким образом, они бросают вызов таким понятиям, как «линейность» разработки протоколов или присущая «хорошесть» конкретных инструментов повышения конфиденциальности или безопасности; вместо этого они предлагают реляционный подход, который выходит за рамки натурализации отношений между цифровыми инструментами, их базовой архитектурой и разнообразием их использования. При этом они дают представление о продолжающейся борьбе вокруг ежедневного «создания» шифрования и раскрывают, как управление и оспаривание могут происходить в разных областях и с помощью различных технических средств.

Как показала недавняя попытка проследить историю зашифрованной коммуникации, «ландшафт рисков двадцать первого века стал бесконечно более сложным, когда Сноуден указал гражданам на риски для гражданских прав, которыми необходимо управлять наряду с рисками терроризма, преступности и национальных государств» (Джарвис, 2020: 390); действительно, шифрование — это вопрос конкурирующих воображаемых представлений и видений, проектов и реализаций, которые они совместно создают, как утверждала Сара Майерс Уэст (2018). Люди думают о шифровании через шифры (которые переставляют буквы алфавита) и через коды (которые заменяют слова) в различных социальных, культурных и политических контекстах. Шифрование приобрело различные значения в сфере национальной безопасности и секретности, а также в сфере демократических систем, в каждой из которых оно обеспечивает частную коммуникацию и позволяет избегать слежки и потенциальных социальных или политических санкций. Исследование Майерс Уэст воображаемых представлений о шифровании проиллюстрировало, как похожие технологии могут приобретать различные значения и роли в различных культурных условиях. Историческое измерение этих социально-культурных контекстов и их эволюция с течением времени также должны быть рассмотрены, как указывает Айседора Хеллегрен (2017) в своей работе. В предыдущем исследовании мы описали криптографические воображаемые как технологические проекции «худшего из всех возможных миров», и, как таковые, к ним следует подходить динамически, в отношении так называемых «моделей угроз» — разработки упреждающей структуры, которая позволяет точно идентифицировать противников, их сильные и слабые стороны, а также способы борьбы с ними — и к постоянному развитию технических возможностей противника (Ермошина и Мусиани, 2018).

Таким образом, многогранное значение шифрования развивается не только в сообществах разработчиков и пользователей, но и с течением времени, и понимание того, как различные субъекты сконструировали конкретные значения свободы в отношении таких технологий, как шифрование, имеет важное значение для историков Интернета, хакеров, программистов и политиков, поскольку все эти субъекты участвуют в создании формы, функции, меры и значения свободы Интернета. Более того, шифрование — и дебаты вокруг него и поддерживающей его инфраструктуры — являются результатом множества общественных сфер и экспертных кругов, встроенных в более широкие вопросы интернета и общества, такие как контроль сетевых СМИ, наблюдение и защита персональных данных (Monsees, 2019). Раннее исследование (Dizon, 2024) того, как определяются и расставляются по приоритетам значения, принципы и ценности шифрования между различными категориями заинтересованных сторон (широкая общественность, бизнес и правительство), показало общие черты между участниками (конфиденциальность в целом считается наиболее значимым принципом и ценностью шифрования). Однако после конфиденциальности показано, что несколько других ценностей, процессов и проблем составляют мозаику создания и значения шифрования, включая защиту данных, информационную безопасность, доверие, национальную безопасность и общественную безопасность, право на собственность, а также тайну переписки, правоохранительные органы и законный доступ, право против необоснованного обыска и изъятия и право против самооговора (стр. 12).

Эта множественность значений, практик и опыта шифрования, в дополнение к информационно-коммуникационной инфраструктуре, которая позволяет и поддерживает его, особенно заметны при рассмотрении в контексте войны. Действительно, понимание того, что является наиболее подходящим решением для обеспечения безопасности и конфиденциальности в этих наиболее чувствительных контекстах, становится из вопроса демократии и построения общественной сферы вопросом жизни и смерти. Степень, в которой технологии шифрования были и остаются инструментом в том, что было названо «информационной войной», изучалась в отношении цифровых технологий с середины 1990-х годов (Klopfenstein, 1999; Libicki, 1995), с общей тенденцией к выводу, что «информационная» война представляет собой отдельный набор процессов и имеет отдельный набор целей по отношению к войнам, ведущимся с использованием «физического» оружия на поле боя.

Оставшаяся часть этой статьи и ее эмпирическое ядро стремятся предоставить недавнюю аналитическую иллюстрацию того, как информационные и коммуникационные технологии становятся локусами, где сходятся информационная война и вооруженный конфликт. Мы стремимся показать это на примере Украины, рассмотренной как до, так и после полномасштабного российского вторжения, начавшегося в начале 2022 года.

Методология

Данная статья основана на полевых исследованиях, проведенных сначала в рамках проекта NEXTLEAP, а затем проекта ResisTIC (более подробную информацию об обоих проектах см. в разделе «Финансирование»). Эти два проекта позволили провести несколько лет полуструктурированных интервью с разработчиками и пользователями защищенных сообщений в различных национальных контекстах и на разных уровнях риска, включая Украину и Россию (основное направление ResisTIC). Несколько моментов полевой работы состоялись в Украине, включая месячные исследовательские периоды в Киеве в 2016, 2017 и 2018 годах. Помимо интервью, эти исследовательские периоды включали наблюдение за четырьмя тренингами по цифровой безопасности и тремя конференциями, посвященными безопасности журналистов и НПО в контексте войны. Всего за эти исследовательские периоды было проведено 50 интервью (60–90 минут) с активистами украинских НПО, тренерами по цифровой безопасности, военными репортерами, техническими экспертами и политиками. Эти интервью в основном были сосредоточены на восприятии риска, моделях угроз и стратегиях цифровой самообороны украинцев, чья работа включала общение с временно оккупированными территориями или посещение их.

Контакты, установленные в эти периоды, позволили после февраля 2022 года продолжить взаимодействие и последующие интервью, которые были сосредоточены на практиках разработки и использования различных инструментов обмена сообщениями и тренингов по цифровой безопасности в свете полномасштабного вторжения. Этот второй раунд интервью включал семь последующих бесед с тренерами, журналистами и техническими экспертами. Целью было определить, как изменились модели угроз и методы самообороны с полномасштабным вторжением.

В статье также использованы анализ документов, касающихся правовых и нормативных документов, а также руководства по цифровой безопасности, разработанные Digital Security Lab Ukraine и службой поддержки Nadiyno, а также технические документы, связанные с разработкой безопасных средств коммуникации (отчеты об ошибках, заметки о выпуске, запросы на включение внесенных изменений и т. д.).

Кроме того, мы провели веб-этнографию с упором на каналы Telegram, поддерживаемые украинскими интернет-провайдерами4 , которые помогли собрать визуальные и текстовые свидетельства о влиянии войны на коммуникационные инфраструктуры, технологии обхода и методы ремонта и обслуживания. Отчеты об отключениях интернета, подготовленные AccessNow, Netblocks, а также данные IODA и Mozilla Network Outages Data Project также использовались в качестве ценных источников информации о подключении в Украине во время войны.

Зашифрованные сообщения: стратегический инструмент

Мобильные технологии были неотъемлемой частью оборудования во время конфликтов в течение многих лет. Приведем показательный пример: в 2011 году, когда в Сирии началась гражданская война, на больших территориях страны было бесперебойное покрытие сети, и телефоны имели первостепенное значение (Rohde et al., 2016). Вооруженные бойцы использовали свои телефоны для связи друг с другом, отправляя важную информацию о местоположении и передвижениях своих противников. Телефоны с камерами также стали необходимыми для передачи во внешний мир изображений, которые обнажали реалии войны, например, фотографий, раскрывающих последствия применения химического оружия против мирных жителей. Тревожные кадры такого рода, снятые гражданскими журналистами и размещенные на веб-сайтах крупных международных СМИ, привели к санкциям, введенным США против высокопоставленных сирийских чиновников в 2017 году (Cliff et al., 2013).

Во время одной из наших полевых поездок на Украину в 2018 году, путешествуя в компании испанского коллеги на поезде из Харькова в Киев, мы встретили украинского офицера лет 50-ти.
Заинтригованный присутствием молодого иностранца, который также имел опыт войны (в качестве военного журналиста, освещавшего движение сопротивления в Рожаве), офицер быстро стал разговорчивым.
Он поделился своим военным опытом и с энтузиазмом показал нам фотографии с передовой, которыми он делился с сослуживцами по Viber. Офицер не знал о слабостях шифрования Viber или о том, что Viber разместил часть своих серверов в России в 2015 году, чтобы соответствовать российскому законодательству.5 Он признался, что использовал Viber для общения с российскими офицерами, которых знал по чеченской войне, куда он отправился служить контрактником. Они использовали Viber для переговоров об организации обмена пленными с обеих сторон. Для этого офицера, как, должно быть, и для многих других, удобство, надежность и скорость общения по Viber приобрели большую значимость, чем сомнительная политика безопасности и конфиденциальности этой системы связи.

В 2014 году Viber набрал 1 из 7 баллов по (ныне устаревшей) «Secure Messaging Scorecard» Electronic Frontier Foundation6 из-за отсутствия сквозного шифрования. Это означало, что сообщения, отправленные через Viber, были зашифрованы только при передаче, но не на серверах компании. Scorecard, разработанная весьма уважаемой НПО, в течение нескольких лет служила инструментом перформативного измерения (Musiani & Ermoshina, 2017) и привела к внедрению нового протокола шифрования в 2016 году на основе современного протокола, разработанного командой Signal. Он использовал механизм «Double Ratchet», который генерирует ключи для каждого сеанса связи, установленного между двумя устройствами. Протокол Viber не был стандартизирован и открыт до недавнего времени, что делало этот мессенджер непопулярным выбором для технически подкованной аудитории.

Этот полевой анекдот раскрывает несколько аспектов использования шифрования во время войны. Во-первых, это показывает, что свойства безопасности приложения для обмена сообщениями не всегда определяют выбор пользователей. В случае Viber это популярность инструмента (это самое популярное приложение для обмена сообщениями в Украине) и последующие сетевые эффекты, которые эта популярность порождает. Во-вторых, если рассматривать это в перспективе с недавней эволюцией украинско-российской войны, это проливает свет на трудности разработки согласованной культуры безопасности и организационной политики для регулирования коммуникаций в армии во время открытых боевых действий. Действительно, как показывают наши интервью с тренерами по цифровой безопасности, солдаты на местах привыкли возиться с разнообразным набором приложений и полагаться на него для внутренних коммуникаций, а также для отношений с семьей и друзьями. Когда война переросла в полномасштабное вторжение, для украинских сил обороны были разработаны более строгие рекомендации, предписывающие использование Threema, швейцарского мессенджера со сквозным шифрованием и закрытым исходным кодом, который также используется самой швейцарской армией.

Однако для многих подразделений Вооруженных сил Украины, помимо приложений для обмена сообщениями, социальные сети, такие как Instagram или YouTube, стали важнейшим инструментом сбора средств на оборудование и беспилотники, а также важным инструментом внешней коммуникации об успехах украинской армии. Кадры и фотографии военных в действии циркулируют по платформам социальных сетей с небольшими или вообще без мер по анонимизации. Для российской армии, с другой стороны, Telegram стал основным средством коммуникации, несмотря на отсутствие сквозного шифрования по умолчанию.

Наряду с военными, зашифрованные чаты и приложения для обмена сообщениями стали важными инструментами общения для гражданских лиц, оказавшихся в центре насильственного конфликта, и для тех, кто живет при авторитарных режимах. Для сторон конфликтов эти приложения предоставили критически важную информацию об общественной безопасности и последние новости о местонахождении вторгшихся сил. Для людей, живущих в авторитарных странах, зашифрованные сообщения облегчили канал связи, который избегает наблюдения шпионских программ, что дает этим правительствам кладезь информации, позволяющей арестовывать и заключать в тюрьму политических оппонентов. Эти службы электронной почты предлагают сквозное шифрование, чтобы никто, кроме отправителя и получателя, не мог мониторинг коммуникаций. Информация, отправляемая через эти приложения, преобразуется в набор случайных знаков и символов, что делает исходное сообщение полностью защищенным с помощью специального ключа для его разблокировки. Службы коротких сообщений (SMS), с другой стороны, обычно не зашифрованы, оставляя пользователей во власти хакерского программного обеспечения, которое может быть развернуто для чтения всех сообщений, отправляемых через эту среду.

Зашифрованные сообщения оказались жизненно важными в конфликте на Украине. Viber и Telegram были особенно полезны: эти два инструмента имеют самые высокие показатели проникновения — 98 процентов и 86 процентов соответственно. Их широкое использование во многом объясняется тем, как Министерство здравоохранения Украины полагалось на эти приложения для передачи критически важных медицинских сообщений во время пандемии COVID-19, но, что интересно, эти службы обмена сообщениями были переориентированы после российской эскалации. Основной канал Telegram, посвященный надежной информации о коронавирусах в Украине, управляется частной компанией, но тесно сотрудничает с правительством и проверяется Telegram: канал связи, который изначально был аполитичным, может развиться, «чтобы стать важным инструментом гражданства общения во время войны» (Trauthig, 2022). Украинский пример, возможно, является самым последним и ярким примером, но не единственным, демонстрирующим растущую важность приложений и служб для обмена зашифрованными сообщениями в вооруженном конфликте.

Например, украинцы, проживающие на оккупированных территориях, сталкиваются с такими проблемами, как слежка со стороны российских оккупантов, для которой шифрование кажется очевидным решением. Они также сталкиваются с интенсивной цензурой, дезинформацией и пропагандой в Интернете. С января 2023 года интернет-провайдеры (ISP) на временно оккупированных территориях должны устанавливать так называемые промежуточные устройства СОРМ для законного перехвата и хранения метаданных своих клиентов. Это было расценено нашими респондентами как одно из основных больших изменений в ландшафте угроз после полномасштабного вторжения:

Что определенно увеличилось, если сравнивать 2014–2022 и 2022–2023 годы, так это блокировки сайтов и сервисов, например, мессенджеров, через которые люди могли передавать и передавали информацию о местонахождении военной техники, мониторинг интернет-активности, проверка содержимого смартфонов на наличие украинской символики, проукраинского контента, фотографий военных (оккупантов) и всего, что с этим связано. (П., тренер по цифровой безопасности, подключенный к горячей линии Надийно, интервью 27 декабря 2023 г.)

Таким образом, как специализированные организации, такие как DSL Ukraine или Nadiyno helpline, так и peer dynamics способствуют распространению использования определенных безопасных приложений для обмена сообщениями, которые способствуют защите содержания сообщений от третьих лиц с помощью передовых криптографических протоколов, таких как сквозное шифрование. Виртуальные частные сети (VPN), которые как скрывают некоторые действия пользователя в браузере, так и помогают обойти цензуру, являются другими важными инструментами. Учитывая, что многие украинцы на оккупированных территориях участвуют в передаче конфиденциальной информации, например, сведений о дислокации российских войск,
Значительные усилия были приложены для продвижения инструментов шифрования для этой группы украинцев и изучения особенностей трудностей, с которыми они сталкиваются.

Тренеры по цифровой безопасности разработали специальные рекомендации для украинцев, живущих в условиях оккупации, в которых подчеркивается важность использования псевдонимных мессенджеров, не привязанных к номеру телефона.7

Например, канадская НПО eQualit.ie запустила инициативу под названием dComms с серверами в нескольких крупных городах Украины, в том числе в местах, которые ранее находились под российской оккупацией (а именно, в Херсоне). Этот проект позволяет людям общаться локально, используя федеративные сквозные зашифрованные инструменты, такие как Element8 или Delta Chat.9 Использование зашифрованных звонков VoIP (например, через Signal или WhatsApp) вместо простых звонков GSM быстро стало обычной практикой и рекомендацией10 для избежания слежки на оккупированных территориях.
территории.

Местные интернет-провайдеры и международное техническое сообщество прилагают особые усилия для того, чтобы оккупированные украинские территории оставались подключенными11 к украинскому и международному киберпространству, включая бесцензурный доступ к украинским и зарубежным СМИ и отсутствие российской слежки. Однако практика цифровой безопасности пользователей с высоким уровнем риска в Украине показывает, что шифрование имеет решающее значение в конфликтных ситуациях, и в то же время, в определенных контекстах, менее важно, чем можно было бы подумать. Например, многие рекомендации сосредоточены на защите аккаунта с использованием двухфакторной аутентификации или других некриптографических рекомендаций:

Мы все еще напоминаем людям о тех же вещах, основах, таких как включение 2FA, выбор надежных паролей и так далее... очевидные вещи, такие как защита телефона паролем вместо биометрии. Новое — это отключение электроэнергии, постоянное наличие внешних аккумуляторов и зарядных устройств и готовность к чрезвычайным ситуациям в целом. (M, тренер по цифровой безопасности, дополнительное интервью, ноябрь 2023 г.)

Удивительно, но многие из мер безопасности украинцев не претерпели радикальных изменений перед лицом полномасштабного российского вторжения, даже если инфраструктура интернета становится важным полем битвы за власть. В ряде случаев физические и материальные аспекты цифровой экосистемы, в частности доступ к любому виду связи, становятся более важными во время войны, чем доступ к передовому шифрованию.

За пределами шифрования: коммуникационные инфраструктуры как инструменты выживания в военное время

Несмотря на свою известность, методы зашифрованной связи являются лишь частью более широкой инфраструктуры информации и связи во время войны, которая часто прибегает к «более простым» методам.
и более базовые коммуникационные устройства и процессы, которые не менее стратегически важны, а иногда и более адаптированы к конкретным военным контекстам, чем передовые технологии повышения конфиденциальности.

С самых ранних стадий вторжения России в Украину российская армия продемонстрировала склонность к атакам на информационные и коммуникационные инфраструктуры. Управление трафиком и захват протокола BGP в прифронтовых зонах активно использовались Россией в качестве стратегии информационной войны. Один из наших собеседников, украинский военный фотограф, поделился своим опытом миссии, которую он выполнял в 2017 году недалеко от линии разграничения в Донецкой области (на украинской стороне). Он использовал Wi-Fi-соединение в одном из немногих работающих кафе, чтобы загрузить фотографии, которые он только что сделал, в облачное хранилище и поделиться некоторыми из них с редакцией, с которой он работал. Однако он заметил, что веб-сайт его СМИ был заблокирован, и ему показали российскую страницу блокировки. Проверив информацию о своей сети, он обнаружил, что он был перенаправлен через российского провайдера восходящего потока.

Эта ситуация является примером более широкой стратегии контроля информации, которую мы называем «трафиковыми войнами» (Ермошина, 2024). С 2022 года Россия неоднократно захватывала инфраструктуры украинских интернет-провайдеров на оккупированных территориях и перенаправляла трафик конечных пользователей через свои восходящие каналы, некоторые из которых были созданы с этой целью; а именно, печально известный оператор Miranda-Media, дочернее предприятие российского Ростелекома, введенное в 2014 году для взятия на себя маршрутизации в Крыму (как подробно описано в специальной публикации; см. Fontugne et al., 2020). Для украинских гражданских лиц и военных это означает российскую цензуру, дезинформацию и слежку с более высоким риском деанонимизации и отслеживания онлайн-активности. Отсюда необходимость в более надежной защите всех онлайн-коммуникаций (а для некоторых военных — строгий запрет на все публичные действия в социальных сетях).

В начале 2022 года на временно оккупированных территориях Украины развернулась интенсивная борьба за контроль над информационными инфраструктурами Украины, включая стационарные линии связи, кабели и вышки сотовой связи. Кульминацией этой борьбы стал период с мая по ноябрь 2022 года, когда российский оператор Miranda-Media взял на себя маршрутизацию на территориях, контролируемых Россией. Это включало в себя физический захват оборудования интернет-провайдеров, а также важные изменения в настройках BGP, которые заставили небольших местных интернет-провайдеров использовать российский восходящий трафик. Для граждан, проживающих на оккупированных территориях, это означает установление цензуры и слежки, при этом надежная цифровая безопасность становится для них все более важной.

В других случаях российская армия, по-видимому, по крайней мере частично не осознавала, к чему приведет уничтожение ею конкретных и чувствительных компонентов инфраструктуры связи Украины для ее собственных военных усилий. Действительно, по данным группы проверки фактов Bellingcat (переданным несколькими другими СМИ), в начале марта 2022 года российские военные были вынуждены использовать незашифрованные коммерческие телефонные линии после того, как их собственные атаки на украинские вышки 3G помешали использованию созданного российским правительством криптофона «Эра», которому для работы необходимы сети 3G и 4G, и который был предназначен для безопасной связи войск друг с другом. Это нарушение безопасности в конечном итоге позволило украинскому разведывательному управлению подтвердить, что российский генерал Виталий Герасимов был убит.12

После российского вторжения в феврале 2022 года украинцы живут в условиях «асимметричного риска», то есть риск неравномерно распределен среди населения. Многие украинцы покинули страну, другие присоединились к армии и остаются в эпицентре событий, большинство живет под постоянным риском авианалетов, а большая группа украинцев сталкивается с тяготами жизни в условиях российской оккупации. Все рискуют остаться без связи.
В этой «асимметрии» рисков нет консенсуса относительно предпочтительных инструментов зашифрованной коммуникации или «лучшей тактики» цифровой самообороны. Вместо этого мы наблюдаем множество контекстов, требующих различных инструментов и наборов рекомендаций.

Отключения Интернета, полные или частичные, происходят очень часто (см. Рисунок 1);13,14 инфраструктуры становятся мишенью для бомбардировок, поскольку подключение является стратегическим ресурсом во время войны. Отключение может означать разницу между жизнью и смертью, когда цифровые средства связи являются ключевыми для запроса продовольственной помощи, медицинской помощи, электричества и других ключевых услуг. Конфликт разворачивается через инфраструктуру Интернета.

Рисунок 1. Инфографика на основе проекта Mozilla Network Outages Data Project, созданного на Хакатоне без границ в Берлине 29–30 апреля 2023 года.

В то же время некоторые украинские пользователи сталкиваются с более высокими рисками, чем другие. Например, журналисты или гуманитарные работники, чьи миссии проходят на передовой, или гражданские лица, которые активно поддерживают Вооруженные силы Украины, находясь под российской оккупацией. Из-за разнообразия профилей и уровней риска этих пользователей шифрование не всегда является или не является единственным решением. Наши исследования использования систем зашифрованных сообщений в Украине, проведенные в период с 2016 по 2019 год, были сосредоточены на пользователях с особенно высоким уровнем риска, таких как журналисты, правозащитники и жители ключевых полей сражений, таких как Крым или Донецкая и Луганская области (Ермошина и Мусиани, 2022). Практики цифровой безопасности этих пользователей включали безопасные

Инструменты обмена сообщениями и другие технологии повышения конфиденциальности. Но вместо того, чтобы сосредоточиться на объяснении передовых инструментов, таких как The Onion Router (Tor) или PGP (Pretty Good Privacy), тренеры по цифровой безопасности, которые консультировали их, вместо этого сосредоточились на разработке индивидуальных и иногда контринтуитивных ответов. Тренеры понимали риск как в высшей степени контекстуальный и быстро меняющийся, а «безопасность» как многоуровневый процесс (Ermoshina & Musiani, 2018; см. также Kazansky, 2021). Это локализованное и целостное понимание угрозы привело к выводу, что большее или лучшее шифрование не всегда является ответом для пользователей, в отличие от того, что считают многие сторонники технологий повышения конфиденциальности.
В недавнем раунде интервью с украинскими пользователями, тренерами по цифровой безопасности и техническими операторами мы обнаружили, что с февраля 2022 года тренеры по цифровой безопасности подчеркивают важность коммуникационной автономии и физической безопасности. Внешние аккумуляторы, солнечные батареи, дополнительные телефоны, зарядные устройства и кабели, мобильные роутеры и даже антенны Starlink стали новым фокусом учебных сессий, наряду с психологическими уроками самопомощи и курсами оказания первой медицинской помощи. Шифрование отошло на второй план, в то время как простая доступность любого вида средств связи стала жизненно важной.

Многие усилия интернет-провайдеров были направлены на своевременный ремонт поврежденной инфраструктуры (что сопряжено с риском для жизни при работе под бомбежками) и на то, чтобы донести Wi-Fi до бомбоубежищ. Роль интернет-провайдеров в состоянии войны стала предметом публичных споров и проблемой для управления интернетом. С начала полномасштабного вторжения украинские интернет-провайдеры часто работали под бомбежками, чтобы восстановить свою инфраструктуру. Местные, малые или средние провайдеры были одними из первых, кто отреагировал и восстановил связь в городе. Украинская ассоциация интернет-провайдеров пыталась запросить у украинского правительства вооруженные автомобили для провайдеров, но могла получить только помощь в каждом конкретном случае, и провайдерам приходилось самим собирать средства, чтобы купить лучшие и более безопасные автомобили.

Частые отключения электроэнергии существенно повлияли на работу украинских интернет-провайдеров, сделав доступ к электричеству главным приоритетом. Международный фонд «Keep Ukraine Connected» и канадская неправительственная организация eQualit.ie оказывали адресную помощь украинским интернет-провайдерам на неоккупированных территориях, отправляя им генераторы и аккумуляторы. Отключения электроэнергии оказали глубокое влияние на интернет-инфраструктуру в Украине, заставив сетевых инженеров искать новые решения для экономии электроэнергии или даже находить способы предоставления интернета без электричества. Это привело к популяризации технологии PON (пассивная оптическая сеть). Архитектура PON представляет собой точку-многоточку, что позволяет провайдеру обслуживать множество клиентов, подключающихся к ним напрямую через оптоволоконные кабели, которые не зависят от электричества. Если в офисе интернет-провайдера есть ток, клиенты будут иметь доступ к интернету, даже если их дома отключены от электричества. Наш анализ каналов Telegram украинских интернет-провайдеров показал, что это сообщество было весьма инновационным и поддерживало своих клиентов за пределами чисто коммерческого отношения. Таким образом, некоторые поставщики электроэнергии организовывали электростанции внутри или снаружи своих офисов, чтобы предоставить людям доступ к розеткам и дать им возможность заряжать свои устройства.

Однако доступ к интернет-подключению на оккупированных территориях является предметом публичных споров: в то время как технические специалисты продолжают поддерживать своих клиентов, чья жизнь и свобода зависят от подключения, они также формально сотрудничают с российской оккупационной администрацией. Случай провайдера из Херсона, SkyNet, стал примером этой двойной роли интернет-провайдеров во время войны. SkyNet обслуживал людей в Херсоне на протяжении всего времени российской оккупации и организовал местный форум для своих клиентов, которые могли общаться друг с другом даже без подключения к глобальной сети. Они также установили электростанцию, чтобы клиенты могли заряжать свои телефоны. Однако с окончанием оккупации им пришлось закрыться, поскольку их посчитали «коллаборационистами».

Хотя вероятность отключения электроэнергии существует на всей территории Украины (даже если она распределена неравномерно), использование устройств и связанные с этим риски различаются на территориях, контролируемых Украиной, и на оккупированных территориях. В Херсоне, важном портовом городе, находившемся под российской оккупацией с апреля по ноябрь 2022 года, украинские пользователи подвергались высокому риску случайного контроля личности и допросов со стороны российских военных, включая изъятие устройств. Как следствие, использование менее распространенных или более технически сложных зашифрованных мессенджеров считалось риском само по себе. Сам факт наличия определенных приложений на телефоне (таких как Signal, Tor, VPN или даже Telegram) мог вызвать подозрения и привести к телесным повреждениям или даже опасным для жизни ситуациям во время плановых проверок телефонов, проводимых российскими солдатами.

На оккупированных территориях повсюду блокпосты, у людей отбирают телефоны, а приложения и чаты тщательно проверяются. Поэтому вы можете использовать только те приложения, которые не вызывают подозрений: конечно, Signal не входит в сферу действия, за его использование вас могут арестовать. Возможны только Viber, WhatsApp или Telegram. И снова, вы должны быть очень осторожны с тем, как вы пишете и кому. В основном пользователи полагаются на самоцензуру, исчезающие сообщения и иногда даже на самодельные шифры. (D, тренер по цифровой безопасности, Украина, интервью 12 апреля 2024 г.)

Контекст военной оккупации возвращает старые доинтернетовские практики запутывания, такие как шифры или эзопов язык. Он переопределяет роль шифрования и показывает, как каждое приложение для обмена сообщениями фактически относится к определенным коммуникативным культурам и группам пользователей. Используя стратегию, которая на первый взгляд может показаться нелогичной тем, кто не находится в военных ситуациях, тренеры по цифровой безопасности, осведомленные в этом контексте, советуют своим пользователям из группы высокого риска использовать WhatsApp и Gmail вместо Signal или зашифрованной с помощью PGP формы электронной почты.

С тех пор как WhatsApp принял сквозное шифрование, мы обычно не тратим так много времени на шифрование мгновенных сообщений [во время тренингов] и рекомендуем оставаться с WhatsApp, если люди уже им пользуются. Так они могут по-прежнему общаться со всеми своими друзьями, и также... это выглядит знакомым и не шокирует их. И люди говорят [во время тренингов], что если они используют WhatsApp, это менее подозрительно, чем если они используют специальное приложение для активистов. («Я», женщина-тренер по информационной безопасности, Украина, 2017)

В этом контексте, внекриптографические факторы, такие как «эфемерные» (исчезающие) сообщения, оказались ключевыми в определении практик общения людей. Или, говоря проще, когда дело дошло до обеспечения безопасной коммуникации для оккупированных народов Херсона, знакомство с определенными инструментами и их незаметность взяли верх над сложными технологиями повышения конфиденциальности. Вдобавок ко всему, низкая кривая обучения, связанная с уже популярными инструментами, а также тот факт, что эти инструменты уже имеют встроенную сеть опытных пользователей, оказываются более важным преимуществом, чем защита конфиденциальности, гарантированная за счет более совершенных технологий шифрования.

Украинский подход к безопасности подчеркивает, что риск является относительным и локальным. Поэтому не существует единого мнения относительно «лучшего зашифрованного приложения для обмена сообщениями». Безопасность следует рассматривать как многослойный сложный процесс, в котором цифровой уровень является лишь одним из многих. Практика украинских пользователей учит нас, что защитный потенциал шифрования всегда и неразрывно связан с физической, психологической и операционной политикой, а также с инфраструктурными проблемами.

Заключение и будущие исследования: шифрование между «войной за управление Интернетом» и новой войной(ыми)

Развертывание защищенного обмена сообщениями в качестве стратегического инструмента во время войны приглашает себя в более широкие дебаты, касающиеся расширения регулирования цифровых технологий государствами, одного из центральных вопросов того, что Лора ДеНардис (2014) назвала «войной за управление Интернетом». Ссылаясь на важность зашифрованного обмена сообщениями в зонах конфликта, таких как Украина, несколько аналитических документов подтвердили15 необходимость надежного шифрования, в то время как сторонники его ослабления говорят, что такая технология затрудняет правоохранительным органам мониторинг приложений на предмет нарушений прав человека и преступлений. Эксперты отрасли указывают на возможность того, что может открыться дверь для усиления правительственного надзора, а также эксплуатации хакерами, пытающимися украсть конфиденциальные финансовые данные. Компании, которые используют зашифрованный обмен сообщениями, знают, что их платформы используются в качестве жизненно важных спасательных кругов некоторыми субъектами и используются для распространения пропаганды другими, но их ответы до сих пор были непоследовательными. В условиях приватизации регулирования и необходимости цифровой и физической защиты шифрование коммуникаций все еще остается спорным вопросом и демонстрирует, как управление Интернетом все чаще оказывается втянутым в конфликты XXI века.
В то же время уникальный характер войны в Украине переопределяет роль шифрования, а также выбор, который делают субъекты относительно того, когда на него полагаться и какие инструменты выбирать. Поскольку страна остается частично оккупированной, это создает неравенство в плане доступа к онлайн-услугам и рисков, с которыми сталкивается ее население. Зашифрованные мессенджеры по-прежнему предпочитаются незашифрованным на всей территории, но реалии войны обуславливают выбор мессенджеров отдельными лицами и группами, делая их более склонными выбирать более надежные и популярные. Другие методы, такие как самоцензура или самодельные шифры, все еще сохраняются, что демонстрирует важность личных связей, групповых соглашений и специальных практик в качестве дополнения (или даже замены) к сложным цифровым инструментам во времена крупных кризисов.

В этой статье, посвященной особенно чувствительному сценарию ответа Украины на вторжение, на перекрестке информационной и физической войны, мы предлагаем обратить внимание на «повседневные практики», которые ежедневно создают неформальные структуры управления информацией и Интернетом (Эпштейн и др., 2016). В конечном счете, мы предлагаем, чтобы будущие исследования уделяли более пристальное и частое внимание способам, которыми эти практики раскрывают то, что делает «хорошую» безопасность в сегодняшнем сетевом (и чреватом войнами) обществе.

Финансирование

Это исследование получило поддержку сначала европейского проекта NEXTLEAP (nextleap.eu, 2016–2018), затем проекта ResisTIC (resistic.fr, 2018–2022), финансируемого Французским национальным агентством по исследованиям (ANR), а совсем недавно — Французского фонда социальных наук (Fondation pour les sciences sociales, sous l'égide de la Fondation de France, 2023–2024) и проекта ANR DIGISOV (https://cis.cnrs.fr/digisov/, 2024–2027).

Примечания

1. Значительно более короткая версия этой статьи была опубликована в качестве главы в издании (2023), ориентированном на широкую читательскую аудиторию (см. Ермошина и Мусиани, 2023).
2. Данное исследование получило поддержку сначала европейского проекта NEXTLEAP (nextleap.eu, 2016–2018), затем проекта ResisTIC (resistic.fr, 2018–2022), финансируемого Французским национальным агентством по исследованиям (ANR), а совсем недавно — Французского фонда социальных наук (Fondation pour les sciences sociales, sous l'égide de la Fondation de France, 2023–2024) и проекта ANR DIGISOV (https://cis.cnrs.fr/digisov/, 2024–2027).

3.Часть этого раздела была переработана из введения (Ермошина и Мусиани, 2022).

4.Например, см.
https://t.me/tk_group; https://t.me/fifthua; https://t.me/kyivlink; https://t.me/skynet_ks_inf
o; https://t.me/ponKabzdec https://t.me/lanetua и т. д.
5.См.: https://www.neweurope.eu/article/viber-moves-data-storage-to-russia/ 6.См.: https://
www.eff.org/pages/secure-messaging-scorecard
7.См., например, эту статью, рекомендующую использовать защищенный мессенджер Threema вместо
Signal: https://nadiyno.org/chomu-threema-krashhe-za-signal-v-okupacziyi/
8.См.: https://element.io
9.См.: https://delta.chat/
10. Горячая линия цифровой безопасности Надийно опубликовала несколько статей, посвященных выбору
приложений для безопасного общения на временно оккупированных территориях, см.,
например, https://nadiyno.org/yak-zahystyty-golosovi-povidomlennya-cherez-mesendzher-na-okupovanij-
terytoriyi/#
11.См., например, инициативу Keep Ukraine Connected , https://nogalliance.org/our-task-forces/keep-ukraine-
connected/
12.См.: https://www.datacenterdynamics.com/en/news/ukraine-russian-militarys-own- encrypted-phones-
impacted-after-destroying-3g4g-towers-allowing-comms-to-be-intercepted/
13.См.: отчет Access Now https://www.accessnow.org/who-is-shutting-down-the-internet-in-ukraine/

14.См. также интерактивную карту отключений в Украине,
https://public.tableau.com/app/profile/nika.aleksejeva/viz/InternetOutages_UA_RU_
DE/Карты_DB
15.См.: https://www.bcs.org/articles-opinion-and-research/removing-end-to-end-encryption-
would-do-more-harm-than-good-says-poll-of-it-professionals/

Ссылки

Абу-Салма Р. и др. (2017, май) Препятствия к внедрению безопасных средств связи.
В: Симпозиум IEEE по безопасности и конфиденциальности 2017 г. (SP), май: 137–153.
Бланшетт Дж. Ф. (2011) Материальная история битов. Журнал Ассоциации информационной науки и
технологий 62: 1042–1057.
Боукер GC и Стар SL (1999) Сортировка вещей: классификация и ее последствия.
Кембридж, Массачусетс: Издательство MIT.
Bowker GC et al. (2010) На пути к исследованиям информационной инфраструктуры: способы познания в
сетевой среде. В: Hunsinger Jet al. (ред.) Международный справочник по исследованиям Интернета.
Берлин: Springer, 97–117.
Браун С. и Ооствин А.М. (2018) Шифрование для масс? Анализ использования ключей PGP.
Исследования медиатизации 2: 69.
Кавукян А. (2012) Конфиденциальность по замыслу: истоки, значение и перспективы обеспечения
конфиденциальности и доверия в информационную эпоху. В: Йи Г. (ред.) Меры и технологии
защиты конфиденциальности в бизнес-организациях: аспекты и стандарты. Херши,
Пенсильвания: IGI Global, 170–208.
Клифф Д., Моул Р. и Жюжье А. (2013) Обнаружение химического оружия: проверка Сирии.
VERTIC BRIEF 22: 1–7.
ДеНардис Л. (2009) Политика протоколов: глобализация управления Интернетом. Кембридж, Массачусетс:
Издательство MIT.
ДеНардис Л. (2014) Глобальная война за управление Интернетом. Нью-Хейвен, Коннектикут: Издательство Йельского университета.

DeNardis L и Musiani F (2016). Введение: Управление с помощью инфраструктуры. В: Musiani F et al. (ред.)
Поворот к инфраструктуре в управлении Интернетом. Нью-Йорк: Palgrave-Macmillan, 3-21.

Dizon MAC (2024) Социально-правовое исследование технологий: подход к законодательству и политике в области взлома и шифрования с точки зрения норм и ценностей. Computer Law & Security Review 52: 105958.
Эдвардс П. Н. (2010) Огромная машина: компьютерные модели, климатические данные и политика глобального потепления. Кембридж, Массачусетс: Издательство MIT.
Эпштейн Д., Катценбах К., Мусиани Ф. (2016) Осуществление управления интернетом: практика, противоречия, инфраструктуры и институты. Обзор политики Интернета 5(3): 1-14.
Ермошина К (2024) «Голоса с острова»: Информационная аннексия Крыма и трансформации журналистских практик. Журналистика 25(3): 528-546.
Ермошина К, Мусиани Ф (2023) Шифрование как поле битвы на Украине. В: Cath C (ред.), Eaten by the Internet. Манчестер (Великобритания): Meatspace Press, 82-88.
Ермошина К., Мусиани Ф. (2022) Сокрытие ради свободы: создание шифрования, безопасного обмена сообщениями и цифровых свобод. Mattering Press.
Ермошина К и Мусиани Ф (2018) От кого прячутся? Модели угроз и разрабатываемые технологии шифрования. Интермедиальности: история и теория искусств, литературы и техники 32. DOI: 10.7202/1058473ar.

Fontugne R, Ermoshina K, Aben E (2020) Интернет в Крыму: исследование случая маршрутизации Interregnum. В: IFIP Networking Conference 2020 (Networking). IEEE, 809-814.
Фуллер М. (ред.) (2008) Исследования программного обеспечения: Лексикон. Кембридж, Массачусетс: Издательство MIT.
Гэллоуэй AR (2004) Протокол: как осуществляется контроль после децентрализации. Кембридж, Массачусетс: Издательство MIT.
Gillespie T (2014) Актуальность алгоритмов. В: Gillespie T et al. (ред.) Медиатехнологии: очерки о коммуникации, материальности и обществе. Кембридж, Массачусетс: The MIT Press.

Хеллегрен З.И. (2017) История криптодискурса: шифрование как место борьбы за определение свободы Интернета. Истории Интернета1(4): 285–311.
Джарвис С. (2020) Криптовойны: борьба за конфиденциальность в цифровую эпоху: политическая история цифрового шифрования. Лондон: CRC Press (Тейлор и Фрэнсис).
Казанский Б. (2021) «Это зависит от вашей модели угрозы»: упреждающие измерения сопротивления наблюдению на основе данных. Большие данные и общество 8(1).
DOI: 10.1177/2053951720985557.
Клопфенштейн DR (1999) Расшифровка дебатов о шифровании: конституционный анализ текущих правил и прогноз на будущее. Emory Law Journal 48: 765.
Libicki MC (1995) Что такое информационная война? Отчет, Национальный университет обороны, Центр передовых концепций и технологий командования. Доступно по адресу: https://apps.dtic.mil/sti/tr/pdf/ADA367662.pdf (дата обращения: 13 ноября 2024 г.).
Монси Л. (2019) Криптополитика: шифрование и демократические практики в цифровую эпоху. Абингдон: Routledge.
Майерс Уэст С. (2018) Криптографические воображаемые и сетевая общественность. Обзор политики Интернета 7(2). DOI: 10.14763/2018.2.792.
Мусиани Ф. и др. (2016, ред.). Поворот к инфраструктуре в управлении Интернетом. Нью-Йорк: Palgrave-Macmillan.

Мусиани Ф. и Ермошина К. (2017) Что такое хороший инструмент безопасного обмена сообщениями? Система показателей безопасного обмена сообщениями EFF и формирование цифровой (пригодной для использования) безопасности. Вестминстерские документы по коммуникации и культуре 12(3).
Rohde M et al. (2016) Из Сирии: использование мобильных медиа во время гражданской войны. Международный журнал взаимодействия человека и компьютера 32(7): 515–531.
Сноуден Э. (2019) Постоянная запись. Нью-Йорк: Henry Holt and Company.
Star SL (1999) Этнография инфраструктуры. American Behavioral Scientist 43(3): 377–391.

Star SL и Ruhleder K (1994) Шаги к экологии инфраструктуры: сложные проблемы в проектировании и доступе для крупномасштабных совместных систем. В: Труды конференции по компьютерной поддержке совместной работы. Чапел-Хилл, Северная Каролина: ACM Press, 253–264.

Trauthig IC (2022) Чат и приложения для обмена зашифрованными сообщениями — новые поля битвы в пропагандистской войне. Lawfare, 27 марта. Доступно по адресу: https://www.lawfareblog.com/chat-and- encrypted-messaging-apps-are-new-battlefields-propaganda-war (дата обращения: 13 ноября 2024 г.).

Уилан А. (2024) Обзор книги «Сокрытие ради свободы: создание шифрования, безопасного обмена сообщениями и цифровых свобод» (Ксения Ермошина и Франческа Мусиани, 2022). Internet Histories 8(1/2): 208–212.

Биографии авторов

Ксения Ермошина — доцент-исследователь (chargée de recherche) Национального центра научных исследований Франции (Centre national de la recherche scientifique, CNRS) и член Centre Internet et Société (CIS). Научные интересы Ксении лежат на стыке инфраструктурных исследований, исследований наблюдения, STS, политической социологии и исследований удобства использования. Она интересуется разработкой протоколов шифрования, а также трансформацией инфраструктур Интернета в геополитических конфликтах.

Франческа Мусиани — научный профессор (directrice de recherche) в CNRS и заместитель директора CIS. Последние исследования Франчески были сосредоточены на использовании искусственного интеллекта в проектах публичных действий, разработке и использовании технологий шифрования в защищенных сообщениях и «цифровом сопротивлении» цензуре и слежке в российском Интернете. Теоретическая работа Франчески исследует подходы STS к управлению Интернетом, уделяя особое внимание социально-техническим противоречиям, а также управлению «посредством архитектуры» и «посредством инфраструктуры».