EURASIAPEACE

Центр Изучения и Прогнозирования Мира в Евразийском пространстве

# Киберпространство в Евразии

## Новые уязвимости - Законодательная база- Информационная борьба

Досье, координируемое Мари Корсель, Энцо Падованым и Морганом Кайле - в партнерстве с OERI

апрель 2023 г

# ДИСКЛЕЙМЕР

**EurasiaPeace - Centre de Réflexion et de Prospective sur la Paix en Eurasie первый французский аналитический центр, занимающийся вопросами построения мира на евразийском пространстве. В центре ведутся исследования, программы обучения и различные публикации.**

**Данное досье было подготовлено в партнерстве со студенческим центром международных отношений - OERI - Observatoire Étudiant des Relations Internationales в Сен-Жермен-ан-Ле. Цель этого партнерства - пробудить интерес молодых людей к современным геополитическим проблемам и внести свой вклад в анализ мира, в котором мы живем:** http://www.oeri.fr/

**Авторы досье– Мари Корсель, Энцо Падован, Енте Тьеппон, Клер Танги, Лара Бабска, Шарлотта Мазе и Морган Кайе.**

**Интервью Реми Сабатье, Лоик Трегурес, Клеман Барнье, Лара Аиди, Навмай Опалински и Селестина Рабуам**

**Картография - Люси Симоно Хоанг Фото на обложке - Капуцин Корсель**

**перевод: Дарья Кузьмина, Жереми Леклер, Констанс Демарке, Анна Боронина, Елизавета Каменская и Анаис Жакен**

**Ссылаться на эту работу можно, указывая следующие элементы :**

**Морган Кайле, Мари Корсель, Энцо Падован, *Киберпространство в Евразии - Новые уязвимости - Законодательная база-Информационная борьба*, EurasiaPeace, Ньон, апрель 2023 года.**

**Авторы и исследователи, которые приняли участие в этой работе несут ответственность за свои слова.**



**61, Avenue Henri Rochier 26110 Nyons**

**Электронная почта : morgan.caillet@eurasiapeace.org**

**Сайт : https://eurasiapeace.org/**

# Содержание


Вступительные слова....1
Киберугрозы и новые уязвимости....3
Упрощенная классификация киберугроз....3
Основные цели кибератак и методы их осуществления....5
дополнительная лексика….....7
Карта - доступ к интернету в евразийском пространстве....9
Интервью с Реми Сабатье....10
Карта - уровень кибербезопасности стран ЕС и Евразии....22
Интервью с Лоиком Трегуром....23
Карта — несколько примеров недавних кибератак....35
Карта - основные атаки на евразийском пространстве с 2000-х годов....36
Законодательные базы : сравнение положений в Европе и Центральной Азии....37
ОРЗД: Единая правовая основа....37
Мари Корсель....37
Защита персональных данных: ОРЗД Европейского союза....37
Содержание и функционирование....39
Достигнутые результаты....41
ЕС и кибербезопасность: разработка общеевропейской стратегии....42
Енте Тьенпон и Лара Бабска....42
Совет ЕС – главный участник в борьбе с киберугрозами....43
Киберпространство на стыке многочисленных проблем....46
Развитие политики информационной безопасности в Центральной Азии....48
Основные законодательные акты....49
Государственный контроль над Интернетом....51
Интернет все же остается инструментом развития....54
Карта - цифровая свобода и защита данных на евразийском пространстве....57
Борьбы за информацию и киберпространство в Иране и Пакистане....58
Интервью с Клеман Барнье и Ларой Айдиной об иранском киберпространстве....59
Интервью с Намвайом Опалинским о пакистанском киберпространстве....71
Вопрос киберпространства в Арктике....87
Интервью с Селестиной Рабуам об арктическом киберпространстве....87
Заключение....99

# ВВЕДЕНИЕ

Киберпреступность, права на изображение, шпионаж, саботаж, фишинг, вирусы, отказ в обслуживании, программы-вымогатели, это целый словарный запас, который теперь является частью повседневной жизни интернет-пользователей.

Тем не менее, значения значение этих терминов остаются довольно размытыми для большинства пользователей - что же именно они означают? Как все это работает? Как защититься от этих многочисленных угроз?

Война в Украине снова привлекла внимание к киберугрозам, и показала, что эти вопросы имеют сугубо геополитический характер. Можно отметить некоторые тенденции: попытки территориализации киберпространства или технологического разделения и вопрос о цифровом суверенитете; различные национальные зависимости от поставок полупроводников и редких металлов, от хранения данных или подключения к различным кабелям; вопрос о международно-правовом арсенале и судебных мерах, которые необходимо принять; вопрос информационной борьбы, распространения опасных нарративов для хрупкого демократического равновесия и демократизации доступа к шпионским инструментам…

Все эти вопросы рассматриваются в этом досье с помощью статей или интервью с исследователями и/или специалистами по кибербезопасности. Также исследование сопровождается геополитическими картами, позволяющими оценить ситуацию на евразийском пространстве.

Речь здесь пойдет не о том, что некоторые уже называют «кибервойной» между Украиной и Россией, которая уже широко освещается в других местах, а скорее об усвоении главных ключей к общему пониманию геополитических проблем киберпространства, сосредоточив внимание на менее известных киберпространствах, таких как, Пакистан, Иран или Арктика.

“EurasiaPeace” предлагает вам пересмотреть в пояснительной манере новые кибер-уязвимости, анализирует правовую модель ЕС по сравнению с моделью Центральной Азии, а также предлагает вам ознакомиться с двумя малоизвестными киберпространствами, Иран и Пакистан. В качестве дополнения вам также предлагается увлекательное интервью со специалистом по арктическому киберпространству и его новым вызовам.

**Морган Кайе**
**основатель EurasiaPeace**

## Киберугрозы и новые уязвимости

В отношении киберугроз развивается относительно новая лексика, которая понятна не всем. Соответственно, в этой части усилия направлены на представление в образовательной форме (с помощью диаграмм, карт и вставок) понятия киберуязвимости, под которое попадают государства и частные лица евразийского пространства.

Также слово предоставляется профессионалу кибербезопасности и специализированному исследователю из IHEDN, чтобы дальше углубится в анализ этого нового конфликтного контекста, который теперь имеет важное значение для нашей повседневной жизни.

## Упрощенная классификация киберугроз

**Енте Тьеннпон и Лара Бабска**

Вопросов, связанных с кибератаками, довольно много. Кибератаки воздействуют на информационные системы (ИС) или организации, опирающиеся в своей деятельности на использование технологий и сетей, с целью их повреждения, уничтожения или кражи содержащихся на них данных. Французское правительство выделяет четыре вида угроз в сфере информационной безопасности: **кибермошенничество, нанесение ущерба репутации, кибершпионаж и компьютерный саботаж**.

Однако для более глубокого понимания феномена кибератак, необходимо различать методы их осуществления, возможные прямые и косвенные последствия, а также понимать цели атакующих. Установить связь между одним из методов атаки с определенной целью на практике оказывается невозможным, так как злоумышленник может использовать одновременно несколько методов для

достижения одной определенной цели, точно так же как и один и тот же метод может использоваться для достижения сразу нескольких целей. Несмотря на то, что предоставленная нами информация по этому вопросу не будет исчерпывающей, мы тем не менее попытаемся проиллюстрировать различия между типами кибератак, представив основные методы их осуществления, цели атакующих и последствия для жертв.


**NB :** Следует отметить, что разные средства компьютерных атак могут приводить к разным целям и последствиям. Например, при атаке вредоносного программного обеспечения вредоносные агенты получают доступ к данным, которые они могут изменять и удалять. Получив эти конфиденциальные данные, они могут влиять на ключевые функции компьютера или отключать их и/или тайно шпионить за его работой. В результате жертва, в конечном счете, может понести значительный ущерб (вред имиджу, кража данных, потеря денег и т.д.).

## Основные цели кибератак и методы их осуществления

Выделают две основных цели кибератак : **доступ к данным и их эксплуатация или кибершпионаж**, позволяющий получить несанкционированный доступ к данным для их дальнейшего использования тем или иным способом, и **компьютерный саботаж**, целью которого является выведение компьютерной системы из строя. **Методы осуществления кибератак:**

### *Доступ к данным и их эксплуатация/ кибершпионаж*

Кибератака данного типа включает в себя ряд действий, осуществляемых через киберпространство, и заключается **в незаконном проникновении в компьютерные системы** организации или физического лица **с целью похищения информации для её дальнейшего использования**.

Кибершпионаж осуществляется преимущественно посредством вредоносных или шпионских программ, целевых кибератак или за счет использования уязвимых мест в компьютерных системах. Речь идет о социальной инженерии (фишинг, хакерский взлом) или вредоносных программах.

**Фишинг**

Вид интернет-мошенничества, который заключается в обмане пользователей интернета, заставляя их думать, что они взаимодействуют с организациями, с целью получить идентификационные данные пользователей, такие как пароли, номера кредитных карт, банковских счетов и другую конфиденциальную информацию.

Как правило, фишинговая атака представляет собой мошенническое сообщение или уведомление, отправленное по электронной почте, которое похоже на достоверные источники, такие как банки, провайдеры или сайты электронной торговли. В данных сообщениях получателей просят перейти по ссылке, которая затем перенаправляет их на мошенническую веб-страницу, где нужно ввести конфиденциальную информацию.

**Вредоносная программа** охватывает все вредоносные коды или компьютерные программы, которые могут быть опасны для компьютерной системы.

Эти программы направлены на вывод из строя и нанесение вреда компьютерам и компьютерным системам, сетям, мобильным устройствам и другим серверам.

Как правило, они позволяют киберпреступникам, которые их используют, удаленно взять управление над устройством и вмешаться в его работу. Вредоносные программы могут заражать устройства несколькими способами: по электронной почте, через сети обмена или через браузер.

**Компьютерный вирус -** это тип вредоносных программ, связанный с файлами, которые загружается на компьютер без согласия и разрешения владельца (до тех пор, пока не установлен соответствующий антивирус). Попав в компьютер, вирус может бесконтрольно распространять свои копии. Фактически он может разрушить функциональность системы и удалить или повредить определенные папки. Как правило, эти папки представляют собой исполняемые файлы.

### *Компьютерный саботаж*

Компьютерный саботаж заключается **в выводе из строя всей или части информационной системы** организации при помощи компьютерной атаки. Данный тип кибаратаки можно сравнить с «подготовленным сбоем», поражающим всю систему или ее части, в зависимости от типа ожидаемого повреждения : продолжительности, степени огласки, стоимости восстановления. Существует множество методов осуществления данного типа кибератак, так как зачастую организации недостаточно подготовлены, чтобы противостоять действиям злоумышленников. **Следует помнить о двух основных методах : «отказ в обслуживании» (DoS) и использование вредоносных программ-вымогателей.**

**DoS-атака или отказ в обслуживании -** совокупность действий, направленных на блокировку или замедление работы отдельных серверов или целой информационной системы, с целью вывести её из строя или затруднить доступ. Это достигается путем активного использования сети, чтобы попрепятствовать функционированию, в результате нарушения связи между двумя компьютерами, предотвращая доступ к определенному сервису или за счет блокирования доступа к услугам конкретного человека.

**Программа-вымогатель –** наиболее распространенный тип вредоносных программ в последнее время. В частности, программа-вымогатель блокирует компьютер, угрожая удалить все его содержимое, а затем от пострадавших требует выкуп за то, чтобы разблокировать его.

## дополнительная лексика…

**Компьютерное пиратство**– несанкционированный доступ к ресурсу компьютера лицом, не являющимся его законным владельцем. Целью компьютерного пиратства является получение контроля над ресурсом или похищение конфиденциальных, личных или секретных данных для злонамеренного использования. О компьютерном пиратстве можно говорить только при условии проникновения в компьютерные сети при его отсутствии, невозмножно говорить о нем. (France.gouv).

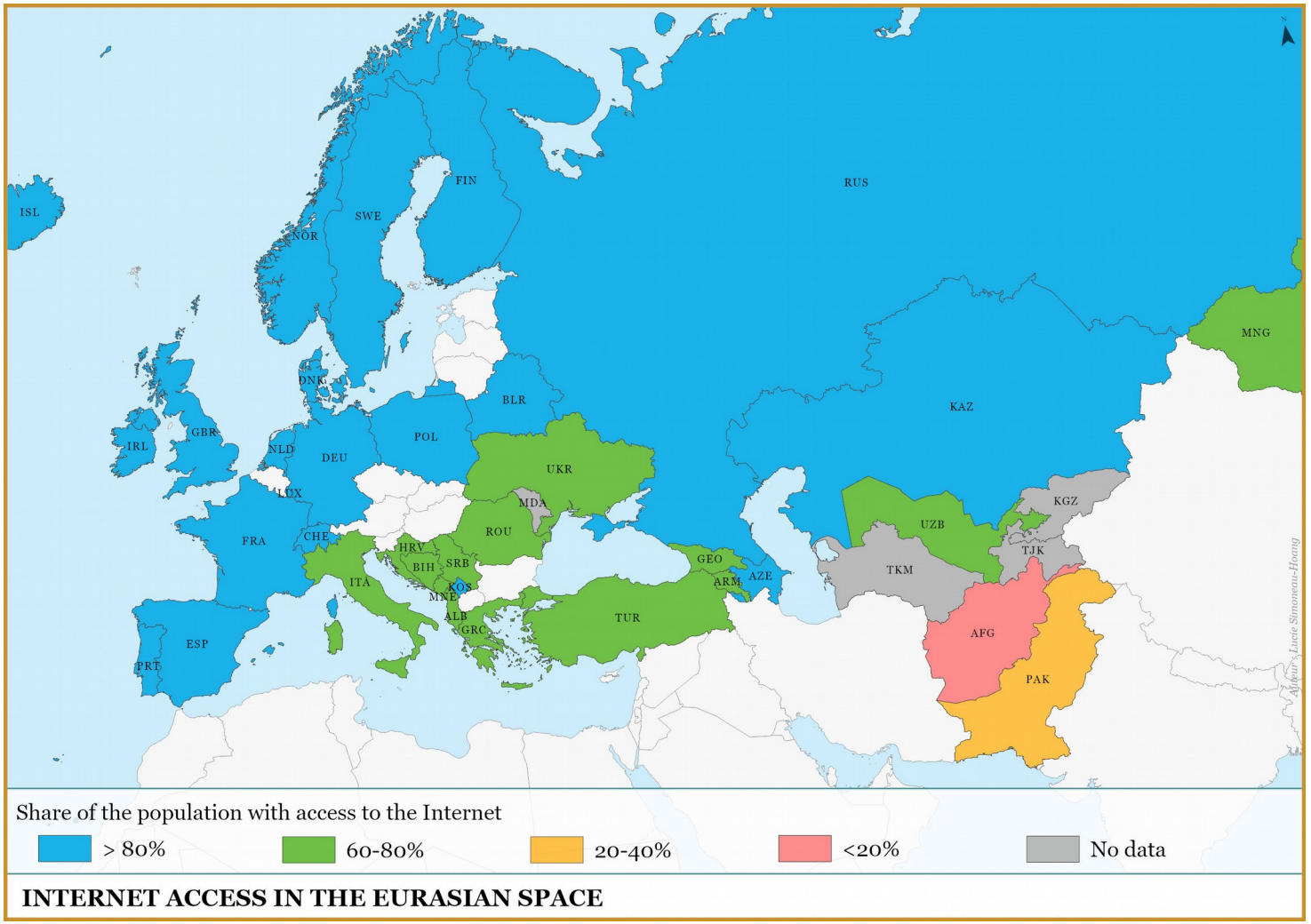
**Доступ к данным** относится к способности для пользователя получать доступ или извлекать данные, хранящиеся в базе данных или другом хранилище. Пользователи, имеющие авторизованный доступ к данным, могут хранить, извлекать, перемещать или ими манипулировать по необходимости. Эти данные могут храниться на самых разных жестких дисках или внешних устройствах.

**Белый или этичный хакер** - это специалист по компьютерной безопасности или хакер, который проводит тесты на проникновение для безопасности компьютерных систем, таким же способом как это делают обычные взломщики. Однако это делается по этическим соображениям с целью помочь структуре устранить недостатки безопасности и, таким образом, усилить защиту компьютерных систем и данных.

**Бэкдоры –** программы скрытого доступа пользователя к программному обеспечению. Производители иногда намеренно оставляют некоторые, чтобы облегчить обслуживание программного обеспечения или заблокировать его работу, например в случае неуплаты лицензии. Бэкдоры также могут быть созданы злоумышленниками, которые затем могут украсть или уничтожить личные данные, отслеживать действия пользователей, получить контроль над компьютером или всеми объектами, подключенными к сети.

**Атака на цепочку поставок** - это очень эффективный метод нарушения безопасности путем внедрения вредоносных программ в компьютерные сети через разработчика программы или пользователя. Это позволяет злоумышленникам украсть конфиденциальные данные, получить доступ к очень много других информаций и управлять определенными системами даже дистанционно. Крупные компании по разработке программных обеспечений и продавцы аппаратного обеспечения подвергаются особому риску, так как они полагаются на своих поставщиков в производстве и поставке оборудований, которые они потом, используют для разработки собственных оборудований.

## Карта - доступ к интернету в евразийском пространстве



## Интервью с Реми Сабатье

**предоставлен Энцо Падован при содействии Мари Корсель и Морган Кайе**

Реми Сабатье –выпускник факультета геополитики, геоэкономики и стратегической разведки, специалист по области международной стратегии. Он много лет работает в **качестве аналитика по вопросам, связанным с киберпреступностью в CERT (Компьютерная группа реагирования на чрезвычайные ситуации) крупной французской компании.** Он принял участие в написании нескольких книг по стратегическим вопросам (геополитика, дипломатия, оборона, редкие металлы).

***« Для достижения эффективного уровня киберберзащиты в будущем потребуется как усиленное развитие французской автономии в этой области, так и укрепление сотрудничества. »***

**Энзо Падован (Э.П): Можете ли вы объяснить нам, в чем заключается ваша работа и каковы ваши задачи? Можете ли вы рассказать подробнее о группе компаний, в которой вы работаете?**

**Реми Сабати (Р.С):** Я уже шесть лет работаю в крупной французской группе компаний в качестве аналитика по киберпреступности. Я отвечаю за мониторинг кибербезопасности крупных компаний - CAC 40 или европейских компаний - в интересах их клиентов. В рамках подразделения по борьбе с мошенничеством CERT (Computer Emergency Response Team) мы работаем над чрезвычайными киберситуациями наших клиентов. В частности, мы боремся с фишингом (особенно при работе с банками), чтобы как можно быстрее закрывать мошеннические сайты, нацеленные на наших клиентов. Мы обеспечиваем круглосуточный веб-мониторинг, в частности, благодаря нашим зарубежным филиалам (Монреаль и Сингапур), которые позволяют нам работать в три смены, что очень важно для наших клиентов, которые сталкиваются с постоянными кибератаками.

Также мы работаем над анализом электронной почты: мы установили кнопки отчетности на электронных почтовых ящиках наших клиентов для потенциально подозрительных писем – наша роль заключается в анализе этих писем, чтобы определить, представляют ли они угрозу. Если да, то мы должны распределить их по категориям и выявить индикаторы компрометации, которые содержит письмо (IP-адреса, адреса электронной почты, доменные имена и т. д.), что в конечном итоге позволяет нам пополнять базу данных о вредоносных артефактах.

В рамках подразделения CERT, занимающегося угрозами, мы преимущественно работаем в Даркнете, чтобы определять утечки данных, которые могут нанести ущерб нашим клиентам. Это важная работа по оповещению: как только мы обнаруживаем утечку данных или, в более общем смысле, угрозу, мы информируем наших клиентов, предоставляя им как можно больше деталей о том, что могло быть украдено, чтобы они могли управлять ситуацией изнутри. Таким образом, мы постоянно следим за видимой, глубокой сетью и Даркнетом. **Видимая сеть - это поверхностная сеть, составляющая от 4 до 5% всемирной паутины, та, которая индексируется поисковыми системами. Глубокая сеть не индексируется поисковыми системами, в нее входят, например, внутренние сети компаний, для доступа к которым необходимо идентифицировать себя. Даркнет тоже не индексируется, более того, она еще и является незаконной: там можно найти все запрещенные виды деятельности.**

**Э.П : Какие самые распространенные типы кибератак? Откуда ведутся эти атаки, и в чем они заключаются? Каковы мотивы хакеров?**

**Р.С : Спектр кибератак очень широк. Прежде всего, есть те, которые относятся к области киберпреступности,** их цель - **получение финансовой выгоды . Они относятся к организованной преступности**, к мафии. Иногда мы встречаем новых участников, которые работают в одиночку и только начинают действовать на этом рынке.

Помимо денежного аспекта, **существуют также политические мотивы, связанные с использованием государствами киберсредств для защиты своих интересов: здесь в дело вступают спецслужбы или военные министерства**, использующие киберсредства для защиты или нападения. К ним относится шпионаж, так как это скрытые атаки, целью которых является сбор конфиденциальных данных. Часто используются шпионские программы. **Саботаж также является одним из основных видов деятельности и иногда осуществляется с использованием вредоносного ПО Wiper, как это было в российско-украинском конфликте.** Другим примером государственных кибероперацій является применение вредоносной программы Stuxnet, которая, как считается, была нацелена на Иран в 2010 году в рамках операции "Олимпийские игры", проводимой Израилем и США с целью замедлить реализацию ядерной программы Ирана путем нарушения работы центрифуг на заводе по обогащению урана. **Существует также целый ряд кибератак, осуществляемых так называемыми "хактивистами"**. Хотя у них может быть разное происхождение и разные способы действий, их обьединяет одно - они действуют в защиту идей. В основе их действий лежит целая идеология: встречаются как религиозные террористические организации, так и защитники окружающей среды. Что касается методов, они, как правило, схожи с теми, что применяет большинство киберпреступников : проникновение в информационные системы с целью получения данных, атаки на отказ в обслуживании (DDoS) и т.д. Но здесь это не люди, которые пытаются скрытся, это скорее люди, которые имеют претензии к действиям государств.

***«Видимая сеть - это поверхностная сеть, составляющая от 4 до 5% всемирной паутины, та, которая индексируется поисковыми системами. Глубокая сеть не индексируется поисковыми системами, в нее входят, например, внутренние сети компаний, для доступа к которым необходимо идентифицировать себя. Даркнет тоже не индексируется, более того, она еще и является незаконной: там можно найти все запрещенные виды деятельности».***

**Э.П : Способно ли большинство французских компаний сегодня противостоять кибератакам или это касается только крупных компаний? Можно ли утверждать, что некоторые компании несерьезно относятся к защите своих данных? Какие меры предосторожности следует предпринять для наилучшей защиты от кибератак? Чего следует избегать? Как реагировать, если вирус заражает компьютерную систему?**

**Р.С :** В большинстве случаев это скорее отсутствие бдительности, чем серьезности. Мы говорим о человеческих недостатках в области кибербезопасности. За последние годы был достигнут определенный прогресс, но предстоит сделать еще больше. Сейчас все крупные компании имеют специальные программы для обеспечения кибербезопасности и получают поддержку от внешних поставщиков услуг. **Основная борьба приходится на малые и средние предприятия: в этой сфере меньше возможностей, ресурсов и осведомленности в этом вопросе. Крупные компании действительно чаще становятся мишенью для кибератак из-за своего статуса, они также имеют, больше возможностей для самозащиты. На самом деле, небольшие компании страдают гораздо меньше, но когда это происходит, вероятность того, что в случае кибератаки они столкнутся с серьезными неприятностями, гораздо выше.**

На случай взлома информационной базы все крупные компании имеют процедуры обеспечения непрерывности бизнеса, которые выходят далеко за пределы киберсферы. Существует много подготовительных мероприятий, которые проводятся заранее. Но все равно необходимо работать со специалистами по кибербезопасности внутри компании, выделяя человеческие и финансовые ресурсы, или прибегая к помощи внешних поставщиков услуг. Но опять же, это гораздо сложнее для небольших компаний, у которых не всегда есть дополнительные средства и которые не всегда воспринимают угрозу всерьез.

**Э.П : В этой области у вас многолетний опыт. Видели ли вы в последние годы какие-либо особые изменения, связанные с киберугрозами? Какие структуры на данный момент являются наиболее подверженными**

**атакам? Каковы причины? Мы видели, что атакуют больницы, аэропорты...**

**P.C :** Больницы все чаще подвергаются атакам, потому что киберпреступники понимают, что имеют дело с важными, но слабо защищенными структурами. Больница похожа на университет: это открытое место, предназначенное для приема людей. Поэтому культура безопасности лежит не в основе работы больниц, а в самом конце цепочки, даже если инфраструктура для этого постепенно создается. Мы также наблюдаем большую осознанность в этой области со стороны крупных организаций.

**Что касается целевой направленности, то программы-вымогатели и вредоносные программы *infostealer*, которые крадут данные, в значительной степени атакуют поставщиков и провайдеров услуг, поскольку они сталкиваются с повышенной безопасностью со стороны более крупных компаний. В этом случае речь об атаке на цепочку поставок (supply-chain attack).** Появление такого типа атак свидетельствует о значительном развитии в сфере киберпреступности. Эти кибератаки особенно опасны тем, что компания, которая первоначально подверглись нападению (поставщик товаров или услуг), в конечном итоге не является целью злоумышленников. Злоумышленники сначала атакуют поставщика услуг, чтобы впоследствии легче проникнуть в бузу данных крупной компании-клиента. Первая атака может заключаться в нападении на разработчика программного обеспечения с целью заражения его продукта, которое затем продают компаниям-клиентам. Она также может быть связана с перехватом договорных и персональных данных у поставщика услуг для проведения целевых фишинговых атак (*spear phishing*) при помощи полученных данных. Например, в 2021 году группа злоумышленников REvil провела кибератаку на программное обеспечение VSA, разрабатываемое американской компанией Kaseya. В результате этой кибератаки пострадали многие компании по всему миру, использующие программное обеспечение производства Kaseya. Другой пример - атака на компанию SolarWinds в 2020 году со стороны группировки APT29 под псевдонимом Cozy Bear, якобы действующая под эгидой СВР (Служба внешней разведки Российской Федерации).

Эта кибератака была направлена на профессиональное программное обеспечение Orion, продаваемое американской компанией SolarWinds. Она позволила бы нарушить работу информационных систем нескольких сотен организаций, компаний и прежде всего правительственных учреждений и ведомств США.

***«Основная борьба приходится на малые и средние предприятия: в этой сфере меньше возможностей, ресурсов и осведомленности в этом вопросе. Крупные компании действительно чаще становятся мишенью для кибератак из-за своего статуса, но тем не менее имеют больше возможностей для самозащиты. На самом деле, небольшие компании страдают гораздо меньше, но когда это происходит, вероятность того, что в случае кибератаки они столкнутся с серьезными неприятностями, гораздо выше».***

**Э.П : Какие отношения существуют между частным сектором кибербезопасности и государством во Франции? Наблюдаются ли между ними какие-либо формы сотрудничества? В какой степени государство может обеспечить кибербезопасность субъектов частного сектора?**

**Р.С** : Да, сотрудничество есть. Например, Французское агентство безопасности информационных систем (ANSSI) играет важную роль в обеспечении безопасности операторов жизненно важных услуг (OIV - *opérateurs d'importance vitale*), которые являются компаниями или организациями, работающими в стратегических секторах - энергетике, транспорте, обороне и т.д. Поэтому для обеспечения безопасности этих операторов необходимо государственное вмешательство. Например, государству пришлось вмешаться во время нападения на TV5 Monde несколько лет назад.

Также следует отметить сотрудничество между частными компаниями и государством в области обмена информацией, но многое еще предстоит сделать,

поскольку мы сталкиваемся с информационными барьерами, что свойственно вопросам безопасности в целом. Это означает, что иногда приходится работать с двухуровневой системой, в рамках которой мы сталкиваемся с вопросами, требующими срочного решения, и субъектами, которые не всегда заинтересованы к обмене информацией.

Нельзя не отметить, что целью компаний, занимающихся кибербезопасностью, остается получение прибыли, как и у любой другой компании, что частично объясняет некоторую сдержанность в обмене информацией и полезным опытом. Но в любом случае, у государства нет возможности обеспечить кибербезопасность всех компаний до единой, и я не уверен, что это именно его задача.

**Э.П : Как вы думаете, чем объясняются различия в уровне кибербезопасности между такими странами, как Болгария, Румыния, Чехия, Словения и остальными европейскими странами? Какие формы сотрудничества существуют здесь? Можем ли мы обеспечить кибербезопасность Франции самостоятельно? Возможна и/или желательна ли автономная и самодостаточная кибербезопасность?**

**Р.С :** В этих странах в области кибербезопасности работают очень талантливые люди, но они, в большинстве случаев, эмигрируют в Западную Европу или другие страны. Поэтому сложно судить об уровне отдельных стран, а реальная ситуация зависит от размера государства и имеющихся средств... Самое главное – это работать вместе, чтобы строить все совместными усилиями в европейском масштабе.

**Франция не действует в одиночку в области кибербезопасности,** она, безусловно, сотрудничает с другими государствами. Это необходимо для того, чтобы получать как можно более подробную информацию и эффективно бороться с угрозами. **Но Франции необходимо стать более автономной: систематическая зависимость от инструментов, программного обеспечения и информации из-за рубежа - это не очень хорошо, поскольку это ограничивает нас в выборе,**

**оценке угроз и т.д.** Важно иметь собственные возможности для обеспечения кибербезопасности. Но быть полностью независимыми и автономными кажется невозможным. **Поэтому ключевыми словами здесь являются автономия и сотрудничество.**

***«Франция не действует в одиночку в области кибербезопасности [...] Но Франции необходимо стать более автономной: систематическая зависимость от инструментов, программного обеспечения и информации из-за рубежа - это не очень хорошо, поскольку это ограничивает нас в выборе, оценке угроз и т. д. [...] Поэтому ключевыми словами здесь являются автономия и сотрудничество».***

**Э.П : Стоит ли нам опасаться "кибервойны" в ближайшие годы? Считаете ли вы этот термин уместным?**

**Р.С** : О кибервойне говорят уже давно, и еще чаще - с начала российско-украинского конфликта. Если рассматривать ситуацию в последнем случае, то мы наблюдаем не кибервойну, а кибератаки. У понятия «война» есть точное определение, и я довольно осторожен с терминологией. Но я считаю, что в будущем место кибернетики в конфликтах будет гораздо значительнее, так как она будет более активно присутствовать в обществе в целом, как это происходит сегодня с искусственным интеллектом.

В Украине наблюдается наблюдается рост кибератак, но конфликт вызвал разногласия среди злоумышленников, промышляющих в этой сфере. Например кибермафия Conti разделилась на два лагеря в связи с конфликтом. Некоторые из членов Conti встали на сторону России, а другие, не согласные с такой позицией участники группировки слили в сеть ряд сведений, что привело к распаду группы.

**Э.П : Есть ли другие страны помимо России, США, Китая и Израиля, показывающие значительный прогресс в области кибербезопасности? И почему эти страны имеют большее влияние в этой области, чем страны Европы?**

**P.C** : Страны, которые вы упомянули, являются самыми авторитетными в плане развития кибербезопасности. **Что касается кибератак, также можно назвать Иран или Северную Корею, потому что американцы очень заинтересованы ситуацией в этих странах, а значит, мы чаще слышим о них в СМИ, что также отвечает политическим интересам некоторых стран**: очень легко добровольно разместить свои домены и серверы в другой стране. Аналогичным образом, злоумышленники без колебаний намеренно оставляют ложные улики, чтобы ввести в заблуждение следователей и специалистов по анализу компьютерных вирусов. Атрибуция - это всегда политический выбор, хотя есть атаки, совершенные конкретными правительствами. **СМИ гораздо больше говорят об атаках наших врагов; чем о наших, но не стоит забывать, что союзники тоже шпионят друг за другом, как например, это было в случае с делом Сноудена.**

Например, особенность атак со стороны Северной Кореи заключается в том, что они очень агрессивны: у Пхеньяна есть государственные хакеры, но они ведут себя как киберпреступники, что довольно удивительно, поскольку традиционные методы действия государственных хакеров - это шпионаж и саботаж. Здесь мы сталкиваемся с более злонамеренными методами работы: атака на банки с целью захвата средств и т.д. Но это характерно именно для Северной Кореи, которая нуждается в деньгах из-за своей дипломатической изоляции.

**Япония упоминается мало, но она обладает реальными возможностями в области кибербезопасности благодаря своей эффективной производственной и технологической структуре, как и Южная Корея**, которая все еще официально находится в конфликте со своим северным соседом, в следствии чего она нарастила реальный потенциал в этой области по геополитическим причинам. **Индия также располагает большим резервом инженеров и технических специалистов в области информационных технологий в целом и кибербезопасности в частности**. Многие компании, которые занимаются информационной безопасностью, решают перенести часть своей деятельности в Индию, поскольку рабочая сила здесь дешевая и достаточно

квалифицированная, даже если лучшие специалисты стремятся эмигрировать в Северную Америку, Европу или страны Персидского залива.

**Бывшие советские страны с их академическими традициями (особенно в области математики и инженерии) также обладают большим потенциалом в сфере кибербезопасности.** К этой же категории можно отнести и государства, которые не остались без внимания России, например, Украину. В состоянии войны возможности увеличиваются в десятки раз, поскольку перенесенные атаки способствуют наоаплению опыта. Таким образом, Киев постепенно становится ведущим игроком в области киберзащиты.

Израиль, в свою очередь, является лидером в области разработки программного обеспечения для компьютерной безопасности, а также в области кибербразведки. Мы часто забываем про Латинскую Америку, хотя она не только обладает потенциалом в сфере кибербезопасности, но и является родиной многих киберпреступных групп, особенно это касается **Бразилии**.

На африканском континенте киберпреступники встречаются довольно часто, что объясняется развитием центров кибербезопасности и увеличением числа университетских программ, подготавливающих специалистов в этой области. **Во Франции наблюдается довольно высокий уровень эмиграции студентов из стран Магриба и Африки к югу от Сахары, которые проходят обучение по техническим специальностям в области кибербезопасности** и приезжают сюда для завершения обучения после получения степени бакалавра или магистра. Для нас эти выпускники очень важны, поскольку мы испытываем трудности с набором кадров в этой сфере: слишком большая потребность в специалистах по сравнению с количеством доступных учебных курсов. Многие из них приезжают работать в Центр мониторинга информационной безопасности (Security Operations Centres, SOC, прим. редактора), где востребованы технические специальности, и охотно нанимают молодых иностранных выпускников.

***«СМИ гораздо больше говорят об атаках наших врагов, чем о наших; но не стоит забывать, что союзники тоже шпионят друг за другом, как например, это было в случае с делом Сноудена».***

**Э.П : По вашему мнению, какие пути достижения прогресса в области кибербезопасности существуют во Франции?**

**Р.С** : **По моему мнению, добиться прогресса в области кибербезопасностия Франция сможет, развивая следующие области: высшее образование в этой сфере, повышение уровня осведомленности сотрудников и граждан, разработка и интеграция искусственного интеллекта в инструменты кибербезопасности, укрепление французской автономии и сотрудничество.**

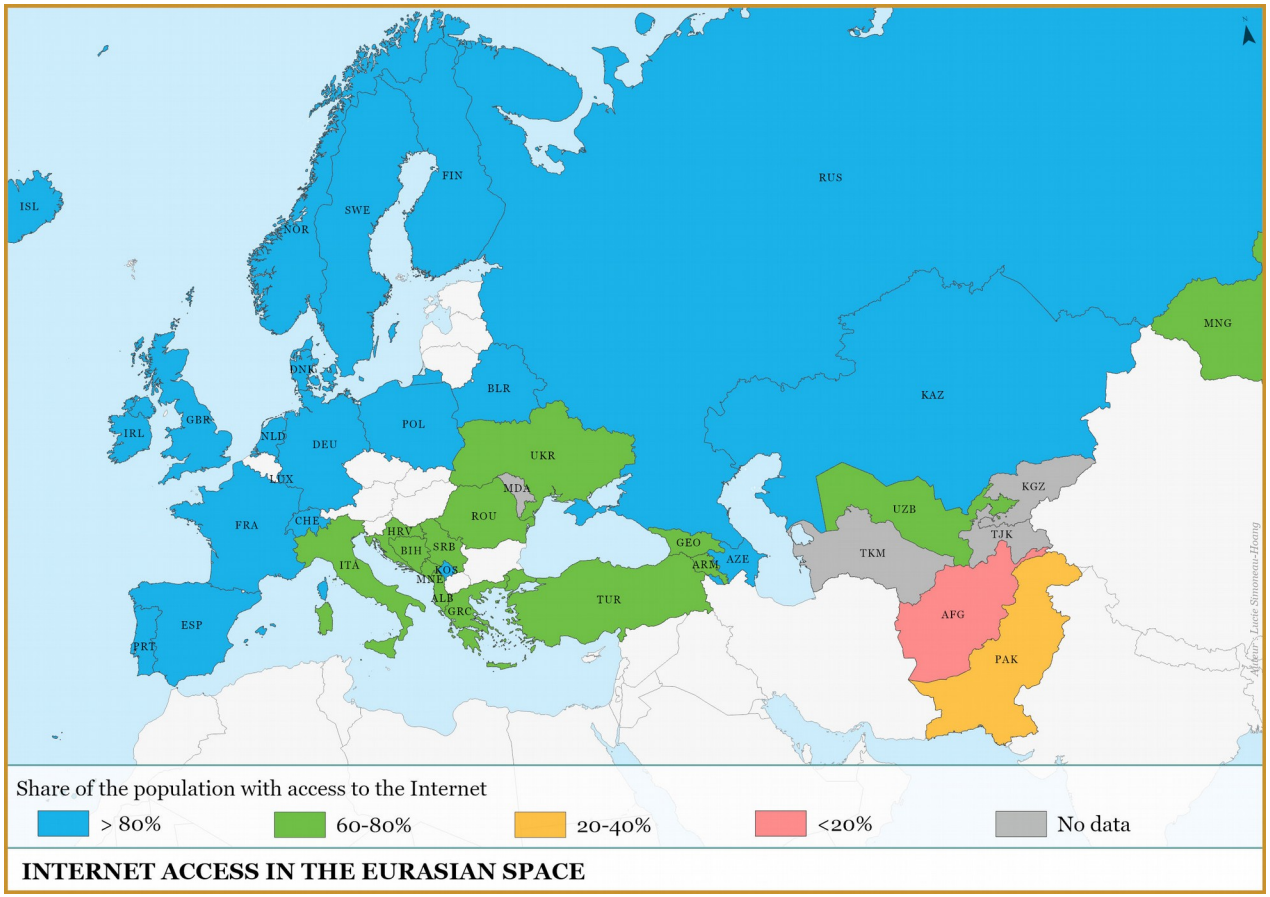
Университетское образование остается ключевым вопросом, поскольку наши потребности в кибербезопасности значительно превышают количество молодых выпускников, выходящих на рынок труда. Во Франции создаются новые учебные программы, но необходимо ускорить развитие и увеличить количество университетских программ по компьютерной безопасности.

Что касается осведомленности в области кибербезопасности, то здесь наблюдается определенный прогресс. ANSSI и платформа Cybermalveillance.gouv.fr делают многое в этом отношении, как и некоторые другие компании. Тем не менее нам еще предстоит большая работа. Миллионы французов продолжают ежедневно пользоваться компьютерами, планшетами и смартфонами, не зная и не соблюдая "кибергигиену". Но разве можно их в этом винить? В отличии от правил дорожного движения, где существует водительское удостоверение, для работы в Интернете подобного документа не существует. Однако риски и угрозы в сфере информационных технологий вполне реальны. Компьютерная безопасность дорожной безопасности : это дело напрямую касается каждого из нас и требует особой бдительности!

Последние разработки в области искусственного интеллекта являются настоящим прорывом. Они сулят большие перспективы во многих областях в целом и, в частности прогресс в кибербезопасности, но они также предвещают появление серьезных проблемы, поскольку киберпреступники уже используют возможности искусственного интеллекта при разработке своих кибератак. Уже началась новая гонка за ИИ между киберзащитниками и киберзлоумышленниками.

**Наконец, как мы уже говорили, для достижения эффективного уровня киберзащиты в будущем потребуется как усиленное развитие французской автономии в этой области (обучение, стартапы, разработчики программного обеспечения, компании, занимающиеся обеспечением кибербезопасности), так и укрепление сотрудничества. Открытый в 2022 году Киберкампус (Campus Cyber), святилище кибербезопасности во Франции, является символом такого сотрудничества между малыми и средними предприятиями (МСП), крупными корпорациями, стартапами, школами и, конечно же, государством в области ИТ-безопасности.** Модель, которую необходимо воспроизвести для того, чтобы вывести кибербезопасность во Франции на новый уровень и создать безопасное цифровое сообщество.

# Карта - уровень кибербезопасности стран ЕС и Евразии



# Интервью с Лоиком Трегуром

**предоставлен Мари Корсель, Клер Танги и Морган Кайе**

Лоик Трегурес (Loïc Tregoures) – преподаватель политологии в Католическом институте Парижа, специалист по Балканам, **ответственный за специализацию «Цифровой суверенитет и кибербезопасность» в Институте высших исследований национальной обороны (IHEDN).**

**EurasiaPeace (E.P) :** Что подразумевает под собой понятие «киберпространство»? Является ли оно пространством, управляемым так же, как и физическое пространство, то есть территорией в строгом смысле этого слова, и, таким образом, подпадающим под те же вопросы (границы, завоевание, национальный суверенитет, монополия государства на легальное применение силы и т.д.)? Другими словами, существует ли «французское киберпространство» ?

**Лоик Трегурес (Л.Т)** : Если вспомнить высказывания пионеров в этой области, например, декларацию Джона Барлоу 1996 года, под киберпространством понимается некий мир без границ, свободный от контроля государств и основанный на саморегулировании его пользователей. Затем властям государств пришло осознание, что такая «территория» была неподконтрольна им и, таким образом, находилась вне закона. В итоге государства пришли к соглашению, что закон должен распространяться и на киберпространство. **Обратимся к международному праву: согласно логике закона о цифровых услугах (*Digital Service Act*), являющегося частью законодательства Европейского сообщества, все то, что запрещено в «реальной жизни», должно быть запрещено и в Интернете. Однако возникает закономерный вопрос о компетенции судьи рассматривать дела по всем видами деятельности в Интернете (информация, торговля, развлечения, работа), которых становится все больше в нашей повседневной жизни, в частности это ставит под вопрос полномочия калифорнийского судьи, фигурирующего в пользовательских соглашениях веб-**

**гигантов GAFAM**. В 2013-1015 годах во Франции также были дебаты о регулировании высказываний в Интернете, в частности опубликованных на Facebook, касающихся терактов и войны в Сирии. Вопрос был следующий: как во Франции обеспечить соблюдение закона о свободе слова компаниями, находящимися под юрисдикцией американского законодательства? Исследователи Aude Géry и Alix Desforges написали статью, в которой подробно рассматривается вопрос о том, можно ли сегодня говорить о киберпространстве без границ, поскольку государства все чаще пытаются его территориализовать.

Таким образом, киберпространство тесно связано с геостратегическими вопросами, поскольку оно более не является (а было ли оно когда-нибудь?) пространством вне мира, но представляет собой продолжение геополитических отношений государств. **Один из этих вопросов заключается в том, существует ли одно уникальное киберпространство или же их несколько : в этом и заключается идея Балканизации Интернета или Сплинтернет (*Splinternet*). Таким образом, мы будем иметь дело не с одним единым Интернетом, а несколькими: с одной стороны, китайский и российский Интернет, каждый из которых характеризуется стремлением к абсолютному контролю над контентом, а с другой – свободный Интернет, регулируемый западным законодательством.** До тех пор, пока государства регулируют Интернет в соответствии со своим законодательством, будут существовать разные концепции. Китайский Интернет не имеет ничего общего с нашим, даже в отношении одного и того же приложения, например, такого как TikTok.

**Е.Р : Что подразумевается под термином «цифровой суверенитет»? Что конкретно означает для страны возможность осуществления, защиты и/или продвижения такой концепции? Являются ли какие-либо конкретные страны суверенными в этой области или находятся на пути к тому, чтобы стать таковыми?**

**Л.Т :** Если считать, что государство не наделяется суверенитетом (государство, признанное другими суверенными государствами, является суверенным по закону), а осуществляет его (государство, которому

удается осуществлять свой суверенитет по отношению к другим государствам во всех областях, является суверенным), то это означает, что **под суверенитетом, если его следует отличать от автаркии, на которую ни одно государство не может по-настоящему претендовать в цифровой сфере, хотя Китай, Россия и США пытаются достичь этого различными способами, подразумевается умение выбирать, как и от кого зависеть.** Другими словами, следует расставить приоритеты и понять, что необходимо освоить самим, а что можно доверить другим, будь то на инфраструктурном, логическом или семантическом уровне. Хранение, управление и обработка данных, например, облачные хранилища, поставщики кабелей, полупроводников и прочее.

**Не следует забывать и о контроле над информационным пространством: Франция сделала создание цифрового суверенитета своей целью, в то время как многие другие страны ЕС не видят в этом необходимости.** Можно также отметить усилия Тьерри Бретона, еврокомиссара по вопросам внутреннего рынка, по превращению ЕС в цифровую державу с помощью инвестиций в полупроводники, батареи, усиление системы регулирования цифровых гигантов на уровне рынка и контента и т. д. Для Франции это означает возможность на европейском уровне не зависеть от иностранных частных компаний, таких как Microsoft, Amazon и т.д. Это касается довольно обширных областей – от национального образования и облачных хранилищ до системы здравоохранения (например, Национальная система данных о здоровье, *Health Data Hub*).

***« Один из этих вопросов заключается в том, существует ли одно уникальное киберпространство или же их несколько : в этом и заключается идея Балканизации Интернета или Сплинтернет (Splinternet). Таким образом, мы будем иметь дело не с одним единым Интернетом, а несколькими: с одной стороны, китайский и российский Интернет, каждый из которых характеризуется стремлением к абсолютному контролю над контентом, а с другой – свободный Интернет, регулируемый западным законодательством ».***

**<u>E.P</u> : Каковы особенности киберпреступности в сравнении с преступностью в целом? С какими видами киберугроз может столкнуться государство, и в частности Франция, в настоящее время? Не могли бы вы сделать для нас быстрый обзор видом киберугроз?**

**Л.Т**: Когда речь заходит о киберпреступности, мы думаем о взломе банковских счетов или банкоматов как в старые времена, или о программах-вымогателях, другими словами, о преступлениях, которые происходят без применения физического насилия и не имеют большого риска для преступников, часто являющихся иностранцами и/или действующими из-за рубежа. Сотрудничать с некоторыми странами, в частности с Россией, в этом отношении очень сложно. Киберпреступность становится все более структурированной, происходит разделение задач между теми, кто находит уязвимые места, теми, кто их использует, теми, кто ведет переговоры с жертвами, теми, кто отмывает деньги, выплачиваемые в криптовалюте через сложные схемы, и т.д. Реальность далека от клишированного образа суперагента, способного в одиночку взломать систему ЦРУ.

Чтобы противостоять этому, необходимы специализированные следователи и судьи, а также тесное международное сотрудничество. **Во Франции существует особое командование жандармерии киберпространства (COMCyberGEND), а также подразделение судебной полиции и еще одно подразделение, подведомственное префектуре полиции Парижа. В то же время на судебном уровне наша система довольно слаба, поскольку в отделе прокуратуры J3 (отдел по борьбе с киберпреступностью Парижского суда), которая отвечает за крупные дела, работают всего три должностных лица.** Что касается международного сотрудничества, то принятая Советом Европы Будапештская конвенция о компьютерных преступлениях, направленная на регулирование и содействие международному сотрудничеству в борьбе с киберпреступностью, и ее протоколы являются незаменимыми инструментами в этом отношении.

**По данным Генерального секретариата по обороне и национальной безопасности (SGDSN) и Национального**

**агентства по безопасности информационных систем (ANSSI), киберугрозы, с которыми сталкивается Франция, безусловно, носят преступные характер, однако все сложнее становится определить, имеем ли мы дело с независимыми или действующими в интересах другого государства бандами киберпреступников. Другое дело – кибершпионаж. Согласно последнему отчету SGDSN и результатам, предоставленным ANSSI, Китай очень активен в этой области.**

**Наконец, некоторые из участников информационного пространства стремятся распространить свое видение, идущее вразрез с интересами Франции, но находящее отклик среди ее граждан (например, Россия, Китай, Турция). Это непростая тема, так как в основе этой проблемы лежит потеря доверия граждан к государству, что открывает путь альтернативным позициям.** Таким образом, чем больше государственная власть воспринимается народом как инструмент цензуры и запрета определенных высказываний, тем менее эффективной она будет. Так было в случае с законом Avia, направленным на борьбу с ненавистническим контентом в Интернете: этот закон оказался заведомо неосуществимым, так как большая его часть подверглась серьезному осуждению со стороны Конституционного совета за нарушение свободы слова.

**Франция приняла решение создать VIGINUM – государственный орган, задачей которого является не реагирование, а прежде всего мониторинг.** Также французское военное киберкомандование (Comcyber) приняло доктрину о борьбе за влияние в киберпространстве. Министерство иностранных дел, в свою очередь, увеличило численность сотрудников соответствующего отдела под руководством Шарля Тепо.

**Касательно последних двух пунктов, необходимо помнить о распространении кибероружия за пределы государства.** Дело Pegasus (шпионское программное обеспечение, используемое государствами для слежки за журналистами, политическими оппонентами, главами государств и т.д.), а также дело, раскрытое сетью журналистов Forbidden Stories в отношении Team Jorge

(израильская организация, которая специализируется на кампаниях по дезинформации), показывают, что **создается особая «серая зона», где шпионаж и влияние продаются как услуги, которые будет становиться все более и более доступными для негосударственных субъектов.**

**Е.Р : В какую категорию можно отнести таких людей, как Джулиан Ассанж, осужденный американской судебной системой, или хакерские группы как Anonymous, которые, утверждают, что ведут борьбу за повышение информационной прозрачности?**

**Л.Т :** На этот вопрос очень трудно ответить, так как здесь не существует конкретной «объективной» классификации, с которой все согласны. Ассанж пролил свет на преступления, совершенные и скрываемые американскими военными. Он также подверг опасности свои источники и местных жителей (например, афганцев, работавших с американскими военными) и, безусловно, сделал из Wikileaks канал влияния для российских спецслужб в рамках президентской кампании 2016 года в США. В этом отношении он отодвинул на второй план заслуживающую одобрения борьбу за прозрачность ради сотрудничества с властью, о которой он сам с иронией говорит, что нет никакой необходимости в Wikileaks, потому что там все прозрачно, политическая оппозиция и пресса могут свободно работать и выражать свое мнение.

Война в Украине поднимает вопрос об «IT Army» (своего рода «цифровая армия» Украины, которая собирает добровольцев для противодействия вторжениям в украинское киберпространство). Это люди обладают соответствующими навыками и привержены справедливому делу. Как относиться к ним с точки зрения международного права? Являются ли они кем-то вроде современных каперов? Они не работают с прямого разрешения своего государства, и страны обязаны проявлять должную осмотрительность, в том числе и в киберпространстве.

Прозрачность информации опирается, с одной стороны, на демократическую традицию предоставления доступа к данным и документам, которой, несомненно, не хватает во

Франции, где информация быстро становится конфиденциальной (Совет обороны и безопасности выносит решения по ситуации с эпидемией COVID-19), а с другой стороны, на возможность свободной работы прессы. Что делается для того, чтобы разрешить или воспрепятствовать работе журналистов, будь то в случае с капиталистическим контролем, осуществляемым над печатными изданиями (карикатурный пример – Венсан Боллоре), или, например, законодательным (дело Патрика Драи о коммерческой тайне; доступ к историческим архивам)?

Наконец, ведутся дебаты о пределах возможностей OSINT (Разведка по открытым источникам, *Open source intelligence*). Паспортные данные из системы ГРУ, полученные Bellingcat (НПО, специализирующаяся на OSINT), помогли доказать участие России в перевороте в Черногории, разоблачить шпиона, базирующегося в Неаполе рядом с командованием НАТО, раскрыть дело Скрипаля (отравление бывшего офицера российской разведки, который перешел на сторону Великобритании) и идентифицировать отравителей Навального. Однако эта база данных не является, строго говоря, открытым источником. Эта дискуссия может продолжаться бесконечно до тех пор, пока цель остается справедливой. А она должна быть справедливой, как и используемые средства должны быть ей сопоставимы.

***« Во Франции существует особое командование жандармерии киберпространства (COMCyberGEND), а также подразделение судебной полиции и еще одно подразделение, подведомственное префектуре полиции Парижа. В то же время на судебном уровне наша система довольно слаба, поскольку в отделе прокуратуры J3 (отдел по борьбе с киберпреступностью Парижского суда), которая отвечает за крупные дела, работают всего три должностных лица ».***

**<u>Е.Р</u> : Прежде всего, что такое киберзащита ? Что это значит с точки зрения конкретных действий и систем ?**

**<u>Л.Т</u> :** Процитирую определение, данное Cattaruzza, Taillat и Danet, которое близко к английскому термину «cyber warfare»: *«концепция действий на, в или через цифровые сети и видов деятельности, которые они поддерживают».* Она носит как оперативный, так и стратегический характер и в значительной степени входит в ведение военных и разведывательных служб. Это государственная задача, в осуществление которой свой вклад может внести и частный сектор.

Армия, в частности военное киберкомандование, опирается на три доктрины: оборонительная киберборьба(LID), наступательная киберборьба(LIO) и борьба за влияние в киберпространстве(L2I).

**<u>Е.Р</u> : Какие страны наиболее успешны с точки зрения киберзащиты? Обязательно ли успешная стратегия киберзащиты сочетается с сильным кибернаступательным потенциалом? Какие страны в настоящее время можно считать кибердержавами и по каким критериям об этом можно судить?**

**<u>Л.Т</u> :** Наличие наступательных возможностей является необходимым условием для того, чтобы считаться кибердержавой.

Можно обратиться к Национальному индексу кибер-мощи (*National Cyber Power Index*), составляемый Белферским центром Гарвардского университета, который ежегодно публикует рейтинг кибердержав. Он дает наглядное представление о ситуации и включает страны, о которых не так активно говорят (Австралия, Нидерланды, Иран), хотя можно удивиться, что Израиль не входит в первую десятку.

**<u>Е.Р</u> : Стало ли использование киберпространства в так называемых гибридных войнах неотъемлемым элементом современных конфликтов такого типа? Считаете ли вы возможным начало «кибервойны» в ближайшие годы? И что означает термин «кибервойна»?**

**<u>Л.Т</u>: «**Гибридная война» означает одновременно все и ничего. Киберпространство – это еще одно поле сражения,

что, конечно, становится очевидным во время войны, но прежде всего это очень эффективный инструмент для того, чтобы оставаться вне войны, а также для подрывной деятельности, шпионажа и саботажа. Еще предстоит пройти долгий путь, прежде чем «кибер» станет основным оружием в конфликтах высокой интенсивности. Некоторые считают, что ключевые элементы, из которых и состоит явление «война», не позволят кибернетике стать чем-то большим, чем просто «помощником» в такой концепции. Другие, как Эвиатар Матания, считают, что сегодня кибернетика — это то, чем была авиация в межвоенный период, и поэтому киберреволюция на поле боя еще только впереди благодаря прогрессу искусственного интеллекта, развитию робототехники, квантовых технологий и т.д. Сложно сказать наверняка.

**Тем не менее я не верю в «кибервойну», если под этим подразумевается противостояние между державами, которое происходит вне реального поля сражения и ведется только с использованием кода. На мой взгляд, этот термин употребляется неверно, но он служит для наибольшего вовлечения и повышения осведомленности, как и термины «кибер Перл-Харбор» или «кибер 11 сентября».** Такая возможность потенциально существует, потому что у всех государств есть критические уязвимости, и нельзя быть на сто процентов уверенными, что они не используются прямо сейчас или однажды не будут использованы. Все, что можно сделать – это повышать защиту, чтобы увеличить стоимость атак и оспаривать классическое представление о чрезвычайной эффективности кибероружия благодаря внутреннему преимуществу, которое оно дает атакующему за счет скрытности, теоретически низкой стоимости и возможности отрицать собственную причастность к делу.

**Е.Р : Какова военная киберстратегия Франции? Существует ли вероятность разработки общеевропейской политики киберзащиты или создания единого европейского киберпространства? Как развивается сотрудничество между странами ЕС ?**

**Л.Т :** Я отсылаю вас к следующим документам: стратегический обзор киберзащиты SGDSN 2018 года, далее элементы доктрин LIO, LID и L2I. Идея состоит в том, чтобы сделать общедоступным наше понимание

самообороны, четко обозначить то, что мы считаем нападением, какие степени нападения выделяем, и как мы будем вынуждены реагировать в зависимости от них. Это снижает цену неопределенности для наших потенциальных оппонентов.

На европейском уровне, особенно под влиянием Франции, наблюдается определенный прогресс в области кибербезопасности, поэтому все, что касается военного аспекта, можно опустить (директива NIS2, Европейская сеть организаций связи по киберкризисам (EU-CyCLONe), закон о киберустойчивости (CRA), повышение роли ENISA и т.д.). **Основной задачей является установление солидарности между членами ЕС в случае атаки и отправка групп реагирования, даже если большинство стран предпочли бы двустороннее партнерство, в частности, с США, если они когда-либо столкнутся с системной атакой, как это недавно произошло в Черногории и Албании.**

***« Тем не менее я не верю в "кибервойну ", если под этим подразумевается противостояние между державами, которое происходит вне реального поля сражения и ведется только с использованием кода. На мой взгляд, этот термин употребляется неверно, но он служит для наибольшего вовлечения и повышения осведомленности, как и термины "кибер Перл-Харбор" или "кибер 11 сентября" ».***

**<u>Е.Р</u> : Можно ли считать балканские страны, известные своей политической нестабильностью, главной мишенью для кибератак ? Здесь можно упомянуть об атаке, приписываемой российским властям в Черногории в августе 2022 года, или об атаке в Албании, предположительно совершенной Ираном.**

**<u>Л.Т</u> :** Балканские страны не более или менее известны своей политической нестабильностью, чем, например, Великобритания (три премьер-министра в 2022 году) или Италия, где правительство никогда не находятся у власти более 18 месяцев.

Киберпространство отражает сложившийся геополитический баланс сил и существующие напряженности между странами. В этой связи балканские страны, как и любые другие, могут стать жертвами кибератак. Я не думаю, что в этом смысле можно говорить о какой-то особой специфике Балкан, за исключением того, конечно же, что они ограничены в возможностях защиты.

***« Основной задачей является установление солидарности между членами ЕС в случае атаки и отправка групп реагирования, даже если большинство стран предпочли бы двустороннее партнерство, в частности, с США, если они когда-либо столкнутся с системной атакой, как это недавно произошло в Черногории и Албании ».***

**<u>Е.Р</u> : Вызвала ли война в Украине рост числа кибератак в регионе ? Какие существуют механизмы для защиты от них?**

**<u>Л.Т</u>:** Насколько мне известно, нет. Франция и другие развитые кибердержавы в целом могли наблюдать, что российский киберпотенциал был обращен на Украину и на собственную защиту. Мы ожидали, что придется столкнуться с волной атак, а произошло обратное – их количество уменьшилось. Просто стало меньше рабочей силы, а также мобилизация отпугнула разбирающихся в компьютерах специалистов. Так что страны Балканского полуострова не были объектом целенаправленных атак, если не считать Черногорию.

**Тем не менее следует отметить, что речь не идет об информационной борьбе. Это другой вопрос, и здесь пророссийская повестка находит сильный отклик благодаря усилиям сербских СМИ. Сильнее всего это проявляется там, где есть сербы, а именно в Сербии, Черногории и Боснии. Такие высказывания**

**совершенно не популярны, например, в Косово и Албании.**

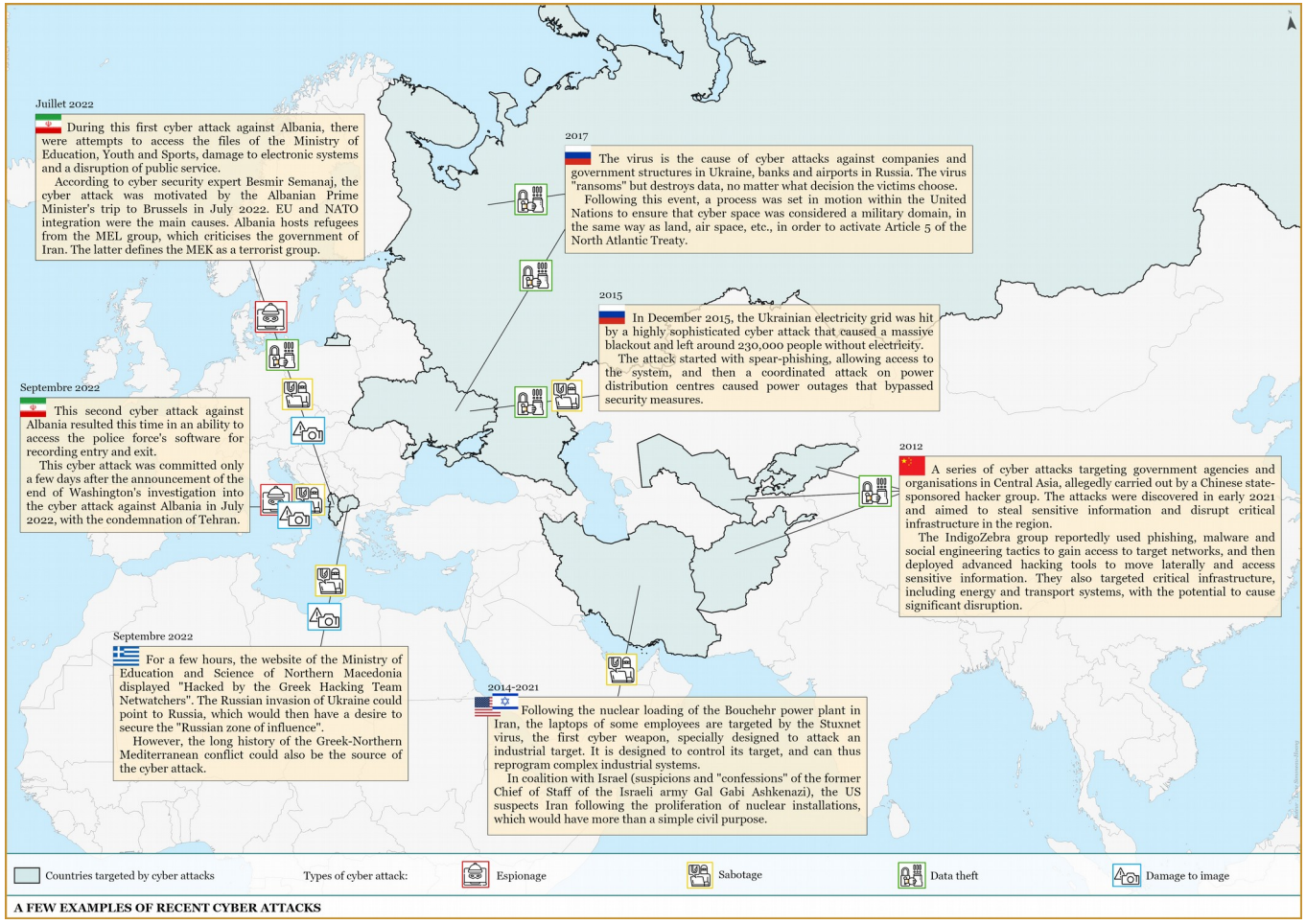
Для стран региона, входящих в НАТО, решение простое: обратиться к американцам. Именно это мы наблюдали в Албании и Черногории, где присутствовали как государственные американские структуры – АНБ, ФБР, так и частные компании, такие как Mandiant (частная компания, специализирующаяся на кибербезопасности, дочерняя компания Google).

**<u>Е.Р</u> : Вывело ли присоединение части балканских стран к ЕС и НАТО развитие сотрудничества в области кибербезопасности на более значительный уровень? Существуют ли или предусматриваются ли программы сотрудничества для государств, не входящих в эти две организации?**

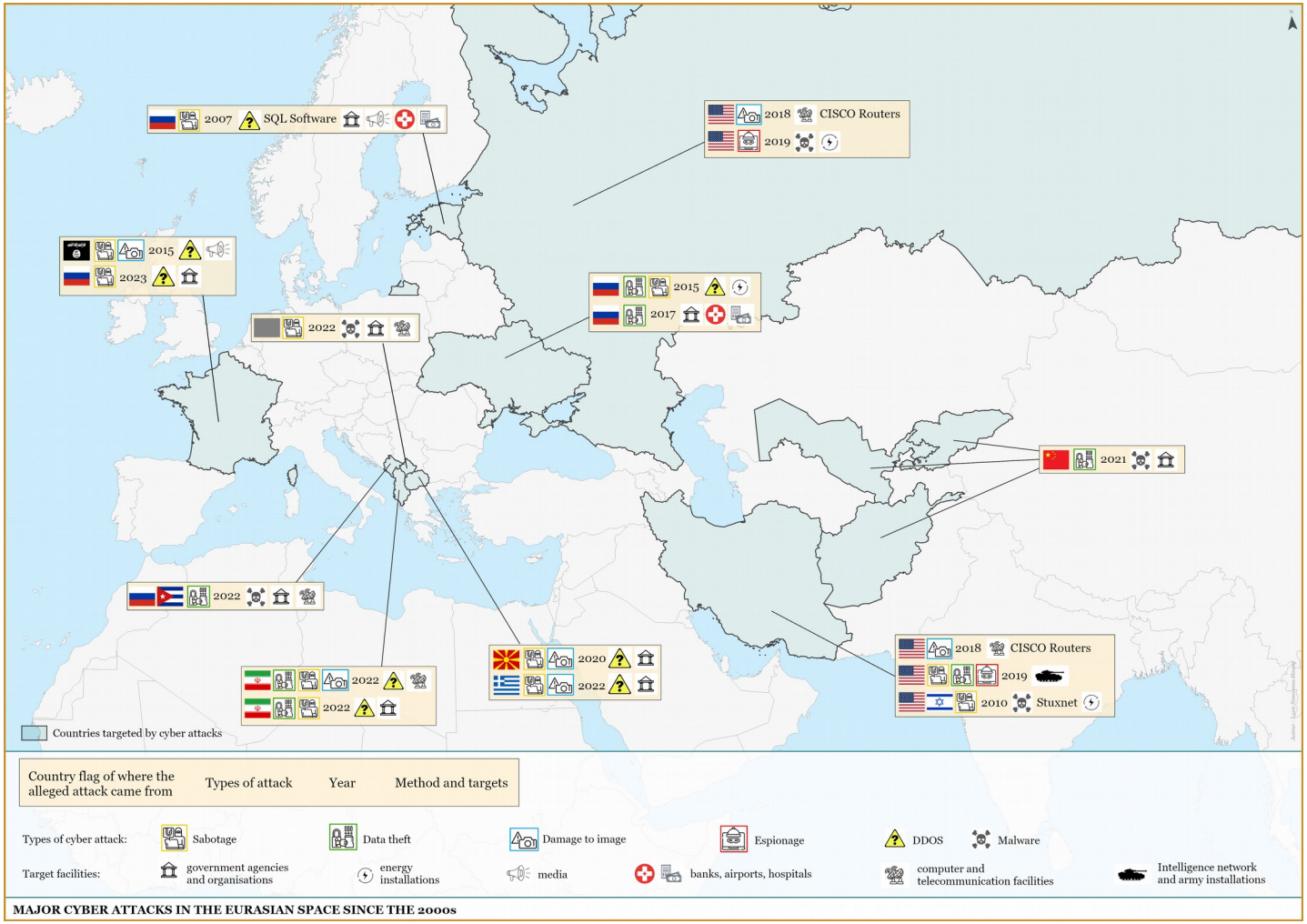
**<u>Л.Т</u>:** Развиваются возможности для наращивания потенциала в области инфраструктуры, права, человеческих ресурсов, кризисного управления и т.д. В частности, благодаря Академии электронного управления (*e-Governance Academy*) в Таллинне в Эстонии.

**Франция совместно со Словенией откроет региональный центр киберсотрудничества в Подгорице (Черногория) для подготовки кадров в регионе. Страны-кандидаты в члены ЕС в любом случае обязаны принимать так называемые *acquis communautaire* (с фр. — «достояние Сообщества») в этой области. Это один из элементов глобального реагирования.**

# Карта — несколько примеров недавних кибератак



# Карта - основные атаки на евразийском пространстве с 2000-х годов



# Законодательные базы : сравнение положений в Европе и Центральной Азии

Европейские новости в последние месяцы в основном были посвящены укреплению правового арсенала против различных угроз, тяготеющих над ЕС, у которого теперь есть уникальная в мире структура, которая кстате допустила наложения санкции против GAFAM: RGDP. Санкции – один из ответов на уязвимости Европы в этой области. Таким образом, следует проанализировать построение европейской кибербезопасности и представить ее последние разработки, такие как «Закон о цифровых услугах» или «Закон о цифровом рынке», принятые в октябре прошлого года. Мы сравним это с ситуацией в Центральной Азии, где Интернет является инструментом развития, но до сих пор сильно попадает под государственный контроль

## ОРЗД: Единая правовая основа

**Мари Корсель**

« *ОРЗД (Общий регламент по защите данных) - новый закон о защите персональных данных. Новый закон делает Европу главным в мире органом по надзору за технологиями* », можно прочесть в газете New York Times 24 мая 2018 года. Это одна из многих газет, приветствующих европейскую инициативу, и не зря: Брюссель, благодаря ОРЗД, не только пытается утвердить свой суверенитет в киберпространстве, но и предлагает правовую базу, которая является уникальной в мире с точки зрения защиты персональных данных.

### Защита персональных данных: ОРЗД Европейского союза

Но Брюссель не дожидался конца 2010-х годов, чтобы заняться темой защиты персональных данных. Первая директива ЕС "О защите физических лиц при обработке персональных данных и о свободном обращении таких

данных " была запущена еще в 1995. Однако возникла проблема: текст был директивой, что означало, государствам был представлен крайний срок, чтобы перенести его в национальное законодательство. Поэтому в разных странах могли существовать различия в законодательстве. В связи с этим, институты ЕС решили предложить новый текст. В 2010 году, пятнадцать лет спустя, Европейская комиссия запустила процедуру, которая стала тем, что сегодня известно как ОРЗД.

Параллельно с этим право на защиту персональных данных было закреплено с 2009 года в статье 8 Хартии Европейского Союза об основных правах, а также в статье 16§1 Договора о функционировании Европейского союза (или Лиссабонского договора). Со своей стороны, Центральный суд ЕС разработал прецедентное право в этой области, благодаря решениям, вошедшим в историю, выводы из которых будут перенесены в ОРЗД. Одним из примеров является решение по делу Google в Испании от 2014 года, где суд закрепил право на забвение. В другом постановлении 2016 года - в развитие постановления 2014 года о цифровых правах - государства-члены должны воздержаться от наложения на поставщиков услуг электронных коммуникаций общих обязательств по хранению данных, как они делали это ранее: они должны быть ограничены по времени и соответствовать мерам строгой необходимости.

Однако, чтобы уяснить, из чего состоит ОРЗД, который представляет собой длинный текст (почти сто страниц) и выглядит техническим, необходимо вернуться к нескольким понятиям, которые нужно объяснить, прежде чем вдаваться в детали его работы.

Во-первых, — это европейский закон (установленный Регламентом 2016/679), направленный на лучшую защиту персональных данных граждан ЕС. Он применяется во всех государствах-членах ЕС с 25 мая 2018 года и является обязательным для компаний, администраций и ассоциаций, которым приходится обрабатывать персональные данные.

Персональные данные, согласно определению, Европейской комиссии – это *«любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу».* Например, « *имя и фамилия; домашний адрес; адрес электронной почты; номер удостоверения личности; данные о местонахождении; данные, хранящиеся в больнице или у врача, которые позволяют однозначно идентифицировать человека, и т.д.».* Обработка персональных данных состоит из любых операций, связанных с такими данными: запись, хранение, передача и т.д.

## Содержание и функционирование

ОРЗД имеет широкое применение. В действительности, государственные или частные организации (компании, администрации, ассоциации...), обрабатывающие персональные данные европейских граждан, обязаны соблюдать это постановление. Следует отметить, что постановление действует не только на территории государств-членов: организации, не созданные в ЕС, которые должны обрабатывать персональные данные европейских граждан, обязаны применять законодательство сообщества, даже если обработка таких данных происходит за пределами их территории. Таким образом, иностранная компания обязана выполнять требования ОРЗД : законодательство ЕС применяется, как только обработка данных касается гражданина Европы.

Это требование соблюдать ОРЗД фактически влечет за собой **ряд поручений** для организаций. Компании обязаны информировать людей о собранной информации, а также обеспечивать ее конфиденциальность с помощью защищенных сайтов (хранение и размещение). Кроме того, их веб-сайты должны использовать систему cookie-файлов, где имеется подлинное согласие пользователя на те из них, которые собирают, например, данные о предпочтениях и навигации. Иными словами, с юридической точки зрения, согласие должно быть свободным и информированным. Именно поэтому при посещении веб-сайта почти систематически появляются баннеры,

где пользователь может выбрать, принимать или нет эти известные файлы cookie, которые будут собирать (или не собирать) его личную информацию. Однако некоторые данные не могут обрабатываться и собираться (за некоторыми исключениями), которые известны как *конфиденциальные данные*: этническая принадлежность, сексуальная ориентация, политические или религиозные убеждения и т.д. Компании также обязаны удалять данные лиц, которые больше не являются клиентами, в течение периода, не превышающего трех лет.

Благодаря ОРЗД пользователи получают информацию о своих правах: веб-сайты должны предоставлять пользователям разделы под названием "Правовое уведомление" или "Политика конфиденциальности", в которых говорится о том, каковы эти права и, прежде всего, как их отстаивать. Что касается пользователей и их клиентов, то их права были усилены и могут быть сгруппированы следующим образом: право на возражение, переносимость, стирание, исправление и доступ. Любой человек может попросить организацию удалить или изменить хранящиеся у нее данные. Клиент также может отказаться от использования компанией определенных данных и попросить вернуть своиданные. В случае нарушения своих прав европейские граждане могут подать иск в национальные суды своего государства для получения возмещения или подать жалобу в соответствующий надзорный орган. Во Франции таким органом является CNIL *(Национальная комиссия по информатике и свободам)*. К организации, не соблюдающей европейское законодательство, могут быть применены различные санкции: административные санкции (штрафы до 2 миллионов евро или даже эквивалент 4% годового оборота компании), уголовные санкции (в случае неправомерного использования персональных данных, Штраф в размере 300 000 евро), возмещение убытков (в зависимости от нанесенного ущерба, в дополнение к административным или уголовным санкциям), а также обязательство организации обнародовать санкцию, наложенную на нее (так называемая санкция потери престижа).

## Достигнутые результаты

Многие пользователи во Франции подали жалобы в Национальную комиссию по информатике и свободам (CNIL) о нарушении их персональных данных на основе ОРЗД : в 2018 году их было почти 11 000, а в 2022 году их число достигло

14 000. Но наиболее показательными являются постановления Суда Европейского союза, против Big Tech-корпораций. Например, решение по делу Schrems II от 16 июля 2020 года. Максимилиан Шремс в 2013 году подал жалобу в Комиссию по защите данных Ирландии (Data Protection Commissioner, DPC), требуя, чтобы DPC запретила "Facebook Ireland" передавать его личные данные в США, считая, что там нет надлежащего уровня защиты из-за действующего в США законодательства ("Privacy Shield"). В своем решении Суд Европейского союза пришел к выводу, что законы США о доступе американских спецслужб к данным интернет-провайдеров и телекоммуникационных компаний чрезмерно нарушают неприкосновенность частной жизни. Действительно, статья 44 ОРЗД гласит, что уровень защиты персональных данных в случае передачи должен быть эквивалентным. Таким образом, в результате этого нарушения, а также из- за недостаточных средств защиты в отношении обработки персональных данных, Европейский суд признал недействительным решение Европейской комиссии о адекватности " Privacy Shield ". В действительности, передача персональных данных третьей стране, может осуществляться, только *если Комиссия приняла решение о том, что третья страна, обеспечивает достаточный уровень защиты* (согласно ст. 45 (1) ОРЗД).

В то время как решения Европейского суда по правам человека вызвали широкий резонанс, штрафы, наложенные органами по защите данных на Big Tech-корпорации за нарушение ОРЗД, также получили широкую огласку: в январе 2021 года Комиссия по защите данных Ирландии (DPC) оштрафовала компанию Meta на 390 миллионов евро ( в том числе 210 миллионов евро для Facebook и 180 миллионов евро для Instagram). Несколько месяцев спустя, в августе 2021 года, настала очередь надзорного органа

Люксембурга обязать Amazon выплатить сумму в размере 746 миллионов евро. В сентябре 2022 года Европейский совет по защите персональных данных наложил на Instagram рекордный штраф в размере 405 миллионов евро. Однако, по мнению некоторых, эти штрафы, кажущиеся огромными суммами для обычного человека, являются незначительными для компании, если учесть, что оборот Google в 2022 году достиг почти 180 миллиардов долларов.

**В то время как ОРЗД является первопроходцем в сфере защиты персональных данных, ЕС также пытается развивать эффективную единую политику в области кибербезопасности с помощью различных учреждений и проектов. В декабре 2020 года Европейская служба внешних действий представила новую стратегию кибербезопасности ЕС.**

## ЕС и кибербезопасность: разработка общеевропейской стратегии

**Енте Тьенпон и Лара Бабска**

Учреждения приняли на себя обязательство предоставить (и выполнить) решения, которые способны снизить риски кибербезопасности, чтобы противодействовать угрозам, наносящим ущерб киберпространству в Европейском Союзе.

Главным европейским участником в области кибербезопасности является Совет ЕС. нередко называемый просто «Совет». Он является соавтором законопроектов вместе с Европейским парламентом.
Наряду с предложениями о принятии новых законов, министры в Совете ЕС принимают окончательные решения по практической реализации мер кибербезопасности.

22 марта 2021 года Совет утвердил выводы по стратегии кибербезопасности, в которых министры ЕС определили

ключевую цель достижение стратегической автономии при сохранении открытой экономики.
Речь идёт в частности о повышении способности принимать самостоятельные решения в области кибербезопасности в целях укрепления цифрового лидерства и стратегических возможностей ЕС.

В то же время Европейская комиссия принимает решения по внешней политике, включая кибердипломатию, и отвечает за меры по выделению бюджетных средств на мероприятия, помогающие бороться с киберугрозами. Например, в декабре 2020 года Европейская комиссия представила новую Стратегию кибербезопасности ЕС, целью которой является укрепление устойчивости Европы к киберугрозам.

На уровне ЕС деятельность институтов подкрепляется специализированными агентствами по киберзащите. Первым из них является ENISA (Агентство Европейского Союза по кибербезопасности), бывшее Европейское агентство по сетевой и информационной безопасности. Его задача заключается в оказании помощи государствам-членам, институтам ЕС и другим заинтересованным сторонам в борьбе с кибератаками. Существует также Европейское оборонное агентство (EDA), которое работает в сотрудничестве с ENISA и Европолом: его основной функцией является поддержка проектов оборонного сотрудничества между государствами-членами, а в киберсфере оно помогает государствам-членам создать квалифицированный военный персонал киберзащиты и обеспечить наличие технологий проактивной и реактивной кибербезопасности.

## Совет ЕС – главный участник в борьбе с киберугрозами

Как упоминалось выше, компетенции Совета ЕС позволяют ему проявлять наибольшую инициативу в борьбе с киберугрозами. В мае 2022 года Совет ЕС совместно с Парламентом пришли к временному соглашению о принятии поправок в Директиву о безопасности сети и информационных систем *(NIS)*, принятую в 2016 году. На фоне нарушения ключевой инфраструктуры - как это произошло в случае нападения

на Украину в 2015 году - необходимо было отреагировать и предложить меры, которые привели бы к повышению безопасности такой инфраструктуры. Таким образом, обзор 2022 года установил обязательства по обеспечению безопасности для операторов, предоставляющих основные услуги (в критически важных секторах, таких как энергетика, транспорт, здравоохранение и финансы), и для поставщиков цифровых услуг (онлайн-рынки, поисковые системы и облачные сервисы). Новое законодательство также должно обеспечить укрепление системы управления рисками и расширить сферу применения норм.

Кроме того, министры Совета ЕС выразили надежду укрепить доверие потребителей в безопасности цифровых технологий. В этом случае, учреждение приняло новую директиву, цель которой бороться с мошенничеством при оплате банковскими картами или чеками, а также обеспечение безопасности новых методов оплаты, появившихся в последние годы: электронный кошелек, мобильные платежи, виртуальные валюты и др. Эти новые меры должны быть закреплены государствами – членами в их национальном законодательстве. Наряду с этим, Совет ЕС стремится повысить эффективность средств по борьбе с киберпреступностью, пытаясь тем самым облегчить доступ к электронным доказательствам, шифрованию и хранению данных. В связи с этим Европейский союз работает над *новыми правилами*, которые смогут улучшить трансграничный доступ к электронным доказательствам судебными органами, которые, в свою очередь, все больше полагаются на электронные доказательства (тексты, электронные письма, приложения для обмена сообщениями). В этой области Совет ЕС сотрудничает с Европейской комиссией, которая ведет переговоры о заключении двустороннего соглашения с США для облегчения трансграничного доступа к электронным доказательствам в уголовном процессе.

К тому же, Совет ЕС сосредоточен на поиске баланса между дальнейшим использованием технологий шифрования и гарантией того, что судебные и правоохранительные органы имеют одинаковый доступ к информации, как онлайн, так офлайн. В связи с этим Совет

подчеркивает необходимость обеспечения безопасности одновременно и посредством шифрования и, независимо от шифрования.

Также в рамках борьбы с киберпреступностью Совет ЕС расширил санкции по отношению к киберпреступникам. В мае 2019 года была создана структура, позволяющая ЕС вводить целенаправленные санкции для сдерживания кибератак, представляющих внешнюю угрозу для ЕС или его государств-членов. Целевыми лицами являются люди, непосредственно ответственные за кибератаки или оказывающие любую поддержку (финансовую, техническую или материальную). *Меры*, принятые Советом ЕС, в частности включают запрет на поездки в Европейский Союз для лиц, признанных виновными в киберприступлениях.

Европейская комиссия- главный игрок в области кибербезопасности за пределами ЕС.
Чтобы обеспечить более эффективное управление киберрисками, Европейская комиссия создала сертификацию кибербезопасности, которая гарантирует высокие стандарты кибербезопасности для продуктов, процессов и услуг ИКТ. В настоящее время в ЕС используются различные схемы сертификации безопасности, что приводит к фрагментации рынка и создает нормативные барьеры. Учитывая это, ЕС ввел в действие единую для всего ЕС систему сертификации, которая создаст доверие, будет способствовать росту рынка кибербезопасности и облегчит торговлю на всей территории ЕС. Хотя на сегодняшний день единой сертификации все еще нет, принятие в июне 2022 года Закона ЕС о кибербезопасности приближает Брюссель к этой цели.

Поскольку компетенции Комиссии ЕС позволяют ей вносить предложения по бюджету, она может принимать решения о распределении инвестиций, за которые затем голосуют Совет и Парламент. В 2020 году Комиссия ЕС предоставила проекту «Горизонт Европа» (*Horizon Europe*) 49 миллионов на увеличение инноваций в системах кибербезопасности и конфиденциальности. ЕС также обязался инвестировать 1,6 млрд евро в развитие инфраструктуры и инструментов кибербезопасности по

всему Евросоюзу для государственных администраций, предприятий и частных лиц.

## Киберпространство на стыке многочисленных проблем

Несмотря на то, что роли различных органов ограничены, участники должны работать в тесном сотрудничестве. В действительности же, киберриски находятся на стыке многочисленных проблем и многочисленных сторон. В качестве примера мы приведем Закон о цифровых рынках (DMA)и Закон о цифровых услугах (DSA).

Стремясь обрести стратегическую независимость, попытки ЕС направлены на избавление от иностранных цифровых платформ и поощрение европейских.

Именно поэтому в октябре 2022 года Совет ЕС принял Закон о цифровых услугах (DSA) и Закон о цифровых рынках (DMA). Прежде всего, они формируют набор правил и стандартов для защиты пользователей. К тому же, они направлены на стимулирование инноваций, роста и конкурентоспособности европейского единого рынка в этой области.

Более конкретно, *Закон о цифровых услугах (DSA)* нацелен на цифровые услуги по типу онлайн- платформ, интернет сайтов, онлайн-услуг.

Также это касается социальных сетей, виртуальных магазинов, платформ обмена контентом, онлайн-рынков, платформ для путешествий и размещения. Закон о цифровых услугах (DSA), вступивший в силу в ноябре 2022 года, предназначен для непосредственного применения государствами-членами ЕС начиная с 2023 года. Таким образом, положения закона касаются компаний, а также государств-членов и самих органов ЕС с различными эффектами.

В свою очередь, Закон о цифровых рынках (**DMA**) относится к «привратникам Н.323» онлайн-платформ. Они выступают в качестве связующего звена между компаниями и потребителями важных цифровых услуг, проверяя компьютерную идентичность сайтов и пользователей и разрешая или не разрешая соединения. Они оказывают влияние на цифровые рынки и зачастую устанавливают частные стандарты, которые могут быть

несправедливыми для компаний и ограничить выбор потребителей. Это может включать запрет пользователям удалять определенные приложения или запрет предприятиям заключать контракты за пределами платформы. Для принятия данного текста, который вступит в силу в ноябре 2022 года (как и DSA) и в соответствии с положениями Закона о цифровых рынках (DMA), Комиссия ЕС составит список «привратников», к которым будет применяться данный текст. Этот список находится в стадии разработки и ожидается в сентябре 2023 года.

Оба устройства (механизма), и Закон о цифровых рынках (DMA) и Закон о цифровых услугах (DSA),позволяют бороться с незаконными рынками, с распространением дезинформации, или же отстаивать основные права пользователей. Данное законодательство хорошо показывает, насколько вопросы кибербезопасности пересекаются с многочисленными проблемами. К тому же, эти законодательства также требуют пересечения множества участников, поскольку для *их реализации* задействованы не только различные европейские институты, но и бизнес, а также национальные институты государств-членов.

**Таким образом, стратегия кибербезопасности ЕС включает в себя Совет ЕС, Европейскую комиссию, Европейский парламент и специализированные учреждения, включая государства-члены на национальном уровне. Каждый участник имеет свои собственные полномочия, но призван сотрудничать с другими. Данное сотрудничество крайне необходимо, что позволяет отвечать на киберугрозы комплексно: например, юридически, через тексты и правовые механизмы, финансовыми средствами, а также человеческими и технологическими ресурсами посредством помощи, предоставляемой государственными органами и мерами поддержки.**

## Развитие политики информационной безопасности в Центральной Азии

**Энцо Падован**

На момент 2023 года лишь в нескольких странах мира использование сетей VPN (*Virtual Private Network* – Виртуальная частная сеть) считается преступлением. В их число входит Северная Корея и Беларусь, а также одна из пяти бывших союзных республик СССР, расположенных в Центральной Азии – Туркменистан. Как оказалось, власти Ашхабада уже на протяжении нескольких лет ведут агрессивную политику против использования сетей VPN. В действительности же к помощи этих виртуальных частных сетей прибегает значительная часть интернет-пользователей страны. Более того, как сообщает « Радио Свобода», начиная с 2021 года жители Туркменистана обязаны приносить клятву на Коране не использовать сети VPN при работе с Интернетом. Эти запреты сопровождаются значительными ограничениями доступа к неправительственным сайтам. В настоящий момент в Туркменистане, где индивидуальный доступ к Интернету стал разрешен лишь с 2008 года, полностью заблокированы такие сайты как Facebook, Instagram и Twitter, а остальные находятся под сильным контролем властей.

Тем не менее высокая степень контроля властей Туркменистана над населением страны не является показательной для всего региона: в последние годы Интернет здесь становится всё более доступным. По мере того, как роль новых технологий в политике и стратегии государств начала возрастать, местным правовым системам также пришлось приспосабливаться. Новые законы, зачастую вдохновленные зарубежными правовыми текстами, такими как всемирно известный Общий регламент защиты персональных данных (*General Data Protection Regulation*, GDPR) Европейского Союза или желанием предоставить контроль за использованием Интернета широкой общественности, отражают особое, характерное для Центральной Азии понимание киберпространства. Таким образом, подробный анализ правовой базы, касающейся использования Интернета и новых технологий, позволяет узнать немало важных подробностей о местных политических режимах и применении информационных технологий в регионе.

## Основные законодательные акты

**Один из первых законов, регулирующих использование интернет-пространства в Центральной Азии, был принят в Кыргызстане.** Благодаря закону КР «Об информации персонального характера» от 14 апреля 2008 года №58, в который в ноябре 2021 года были внесены поправки, в Кыргызской Республике впервые появилась правовая основа для защиты персональных данных. Данный правовой акт содержит первое определение понятия персональных данных : « *зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности* ».

Данное определение положило начало правовому регулированию использования персональных данных граждан Кыргызстана. Интересно также отметить схожесть этого определения с тем, что содержится в регламенте GDPR, вступившем в силу лишь в 2016 году. Таким образом, даже если некоторые сведения остаются в свободном доступе (например, телефонные номера граждан Кыргызстана, давшие свое согласие на внесение их в общедоступный справочник), все данные личного характера защищены законом. Любая частная организация, располагающая или собирающая такие данные на территории Кыргызстана, должна получить соответствующее разрешение от действующего правительства. Более того, после вступления в силу данного закона Бишкек учредил официальный реестр организаций, уполномоченных осуществлять обработку персональных данных граждан, который находится в свободном доступе.

Закон КР от 14 апреля 2008 года является первым в серии правовых актов, принятых в течение последующих лет. **В 2013 году подобный закон, схожий по содержанию со своим кыргызским аналогом, был принят в Казахстане (№94-V, «*О персональных данных и их защите*»)**. Аналогичные правовые документы были разработаны

также в Туркменистане и Таджикистане в 2017 и 2018 году соответственно, что свидетельствует о постепенном распространении законодательного закрепления защиты персональных данных по всему региону. Продолжая эту тенденцию, также входящие в регион Узбекистан и Монголия в 2021 году примут собственные законы о правовом регулировании в интернет-пространстве.

**Принятый сравнительно недавно в Монголии закон о персональных данных является одним из наиболее полных в регионе и обеспечивает куда более эффективную защиту, чем его ранние аналоги из Кыргызстана и Казахстана.** Уникальной стороной этого закона является то, что он передает правовые полномочия по защите данных сразу двум организациям. В отличие от Европейского Союза, возложившего обязанность по надзору за соблюдением регламента GDPR на Европейский совет по защите данных (*European Data Protection Board*, EDPB), вместо создания специализированного учреждения Улан-Батор передал задачу по правовому регулированию интернета двум уже существующим органам. Первым из них стала Национальная Комиссия по правам человека Монголии, созданная в начале 2000-х годов. Данная комиссия является полуавтономным государственным учреждением, осуществляющим надзор за соблюдением прав человека в стране, а также в рассмотрение жалоб, связанных с нарушениями в данной сфере. Не удивительно, что именно на данную организацию также была возложена обязанность расследовать случаи использования персональных данных в злонамеренных целях, ведь право человека на неприкосновенность частной жизни является одним из основополагающих. Кроме того, Комиссия имеет право вносить предложения правительству, когда считает, что защита персональных данных может быть осуществлена более эффективным образом. С другой стороны, Министерство цифрового развития и коммуникации отвечает за другой аспект защиты персональных данных, а именно следит за соблюдением закона при работе с частными организациями. Данное министерство также занимается утечками данных и их ликвидацией. Таким образом, **принятый в Монголии закон о защите персональных данных свидетельствует о довольно несвойственном**

**для данного региона стремлении** разделить полномочия по контролю между несколькими государственными органами.

**В Узбекистане орган, занимающийся вопросами защиты персональных данных – Государственный центр персонализации**, **находится в непосредственном ведении Кабинета Министров** и, таким образом, является полноценным правительственным учреждением. Аналогичным образом в **Кыргызстане Государственное агентство по защите персональных данных** находится в подчинении органов исполнительной власти. Однако на сегодняшний день агентство еще вынесло никакого официального решения по вопросу правового регулирования в киберспространстве.

Таким образом, Монголия выступает одним из немногих примеров стран, разделяющих полномочия властей в сфере защиты персональных данных, как правило, осуществляемых напрямую правительством. Это подводит нас к другому, более сложному вопросу, касающемуся роли интернет-пространства в законодательстве стран Центральной Азии, а именно о степени контроле государств над информационными технологиями и Интернетом.

## Государственный контроль над Интернетом

2 января 2022 года в Казахстане было принято решение снять ограничение на цены на природный газ, на который приходится почти четверть потребления электроэнергии в стране. После этого по всей Республике вспыхнули массовые акции протеста. Почти неделю забастовки и беспорядки сотрясали политическую жизнь Казахстана, что привело к тяжелым человеческим жертвам : в результате этих событий сотни людей получили ранения (как среди протестующих, так и среди сотрудников правоохранительных органов), около 250 человек погибли, согласно данным неправительственной организации Human Rights Watch. Порядок в стране удалось восстановить лишь после объявления чрезвычайного положения и вмешательства сил Организации Договора о коллективной безопасности (ОДКБ), одним из членов которой является Россия.

Иностранные и казахские военные оставались в состоянии боевой готовности до конца января, несмотря на протесты со стороны Европы, решительно осудившей применение насилия в отношении демонстрантов.

Тем не менее один из самых важных фактов, касающихся этого события, не затронул ни военнослужащих, ни международное сообщество. На протяжении пяти дней, когда беспорядки достигли своего апогея, в Казахстане был массово ограничен доступ к Интернету, не затронув лишь некоторые отдельные районы страны. Безусловно, это не первый случай, когда часть или все население страны оказалось лишено возможности выхода в Интернет: в ноябре 2020 года жители региона Тыграй в Эфиопии пережили почти полное отключение Интернета в рамках вспыхнувшего в стране конфликта между федеральными войсками и властями автономии. Однако в Казахстане действия властей носят законный характер. В отличие от правительства Франции, не располагающего полномочиями контролировать общий доступ к интернет-пространству, в Казахстане существуют законодательные акты, позволяющие Нур-Султану управлять подключением жителей страны к Интернету.

Доступ к Интернету в Казахстане находится под строго централизованным контролем, усилившемся после внесения ряда поправок к закону о национальной безопасности в 2011 и 2017 году. Столкнувшись с массовыми политическими протестами, подобными тем, что прошли в стране в 2022 году, правительство Казахстана одобрило возможность отключения доступа к Интернету в случае угрозы национальной безопасности. Власти Нур-Султана сравнили протестующих, вышедших на улицы в 2022 году, с участниками террористических группировок, что позволило им отключить доступ к Интернету по соображениями государственной безопасности.

Однако Казахстан – это далеко не единственное государство, где интернет-пространство полностью или в значительной степени остается под контролем правительства. Жители Туркменистана, где 20 декабря 2014 года был принят закон о правовом регулировании в интернет-пространстве, также являются жертвами

усиленного государственного контроля над новыми технологиями. Появление данного закона указывало на заинтересованность властей Ашхабада в демократизации использования Интернета в стране, однако в нём также имелся ряд запретов и ограничений. Например, в стране запрещены сайты, предлагающие продажу алкоголя или табака, а также платформы, распространяющие порнографию. Кроме того, закон предусматривает уголовную ответственность за оскорбление президента Туркменистана, в том числе в сети Интернет. Учитывая тот факт, что эти критерии могут быть интерпретированы совершенно по-разному (законодательство Туркменистана не позволяет определить наверняка, где проходит граница между оскорблением и критикой), нет ничего удивительного в том, что большинство социальных сетей в стране находится под запретом. Подобные меры контроля привели к тому, что у местного интернет-пространства даже появилось специальное название. Туркменское интернет-сообщество прозвали «Туркменет», поскольку правительство по-прежнему стремится усовершенствовать интернет-фильтрацию в стране. Агрессивная политика в отношении пользователей сетей VPN, о которой упоминалось в начале статьи, является лишь одной из последних попыток правительства Туркменистана сохранить контроль над местным интернет-пространством.

Тем не менее государством Центральной Азии, где ситуация вызывает наибольшую обеспокоенность, остаётся Афганистан. На сегодняшний день в Кабуле нет ни закона о защите персональных данных, ни государственного органа, регулирующего надлежащее использование информации личного характера. В условиях этого правового вакуума, сохраняющегося и после прихода к власти талибанов в августе 2021 года, угрозы нарушения прав человека становятся весьма реальными. Во время американской оккупации, а позже после установления Исламской Республики в стране были созданы специальные базы данных, содержащие информацию о жителях Афганистана, в частности для наблюдения за личностями, враждебно относившимися в вооруженным силам США, или, наоборот, для выявлениях их сторонников. С уходом сил коалиции с территории страны большая часть этих данных попала в руки

фундаменталистов; таким образом, эти группировки имеют неограниченный доступ к конфиденциальной и компрометирующей для части населения информации. В течение последних двух лет гуманитарные неправительственные организации (НПО) предупреждают о серьёзных последствиях, к которым могут привести эти базы данных, и о важности предостережения Афганистана касательно вопроса кибербезопасности.

Таким образом, некоторые государства использовали и до сих пор продолжают использовать интернет-пространство как инструмент контроля над населением, в том числе применяя механизмы информационной фильтрации. Все чаще правительства стран Центральной Азии определяют развитие кибербезопасности одним из основных направлений их национальных стратегий. Более того, эта тенденция также закрепляется в законодательстве, поскольку государства осознали важность тех преимуществ, которые современные технологии предоставляют для их собственной политической власти.

## Интернет все же остается инструментом развития

В последние годы в Центральной Азии все быстрее происходит внедрение современных технологий в различные сферы жизни. По всему региону растёт количество амбициозных национальных планов. Так, президент Узбекистана поставил перед государством цель к концу 2022 года произвести около 20 000 километров волоконно-оптических кабелей. Эти стремление развивать использование новых технологий также отражается в повышенном внимании к сфере кибербезопасности. Центральная Азия является одним из регионов, наиболее предрасположенным к атакам злоумышленников и интернет-мошенников, пытающихся получить доступ к конфиденциальным данным: предположительно со стороны Китая в июне 2021 года была предпринята попытка атаковать Совет национальной безопасности Афганистана при помощи электронных писем, содержащих вирусы. Столкнувшись с этой ещё малознакомой широкой общественности

угрозой, многие государства принялись подготавливать собственные планы реагирования.

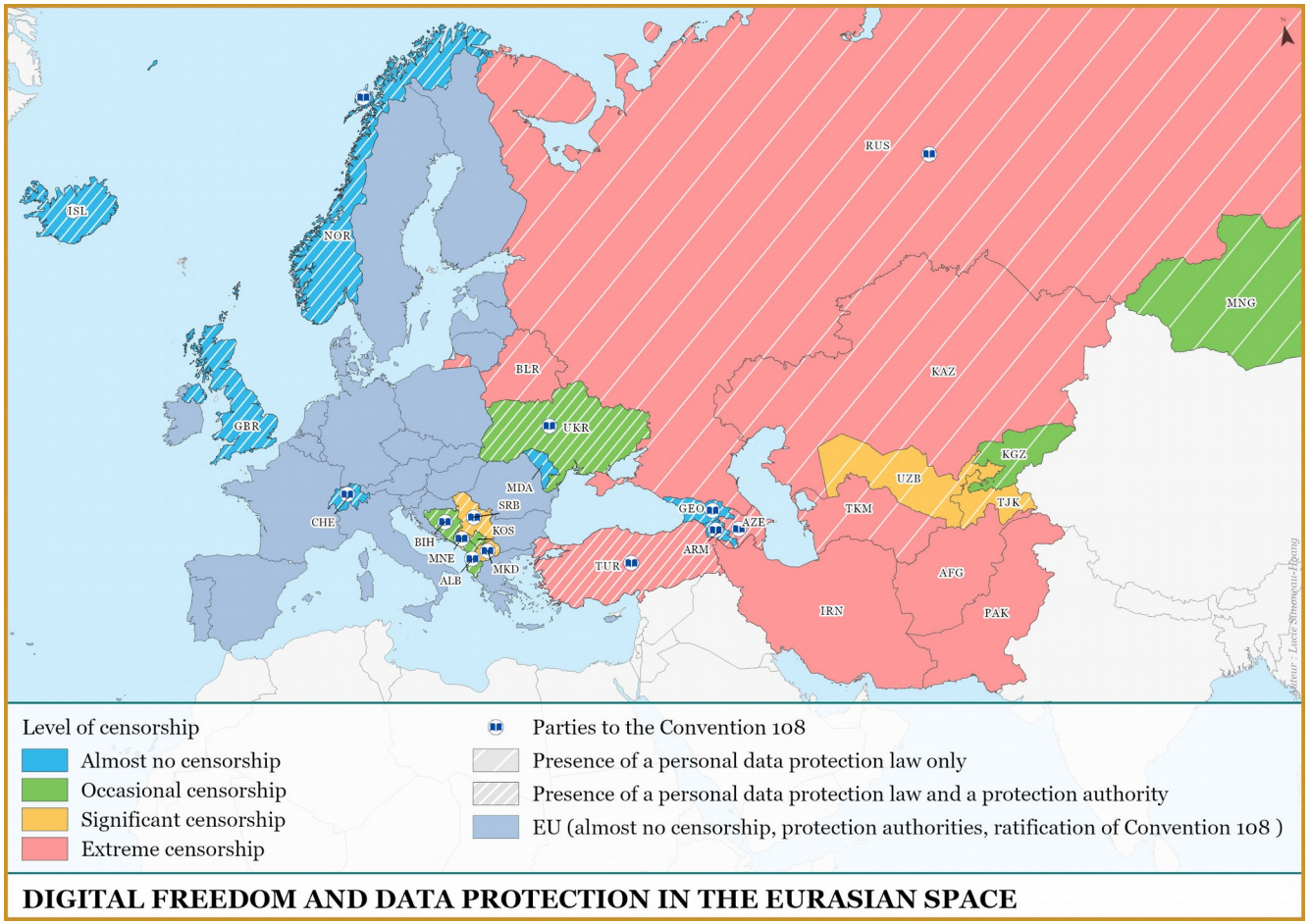
Так обстоит дело в Казахстане, где, начиная с 2020 года была разработана и введена концепция кибербезопасности «Киберщит», намеревающаяся стать одним из факторов, призванных повысить привлекательность страны. Как оказалось, в началу 2030-х Нур-Султан стремится войти в число тридцати наиболее развитых стран мира. Таким образом, правительство Казахстана выдвинуло генеральный план, направленные на распространение передового опыта в области кибербезопасности как среди граждан, так и среди государственных органов и учреждений. Монголия последовала примеру своего соседа, разработав в 2021 году собственный закон о кибербезопасности, который подготавливался одновременно с законом о защите персональных данных. В соответствии с новым законом для оценки существующих в Монголии рисков и координации мер реагирования в случае кризисных ситуаций и кибератак в стране был создан Совет по кибербезопасности под руководством премьер-министра. Важность развития методов кибербезопасности отразилась в правовых системах государств Центральной Азии, осознавших значимость новых технологий в развитии государств и повышении их привлекательности.

Однако эти достижения сопровождаются и другими правовыми актами, зачастую ограничивающими свободу информации и слова даже в государствах с менее репрессивным политическим режимом, чем, например, в Туркменистане. В 2021 году закон о защите от недостоверной (ложной) информации был опубликован в Кыргызстане. Данный правовой акт предлагает бороться с распространением клеветнических высказываний и недостоверной информации путем ограничения доступа к сайтам с подобным содержанием. К сожалению, как отмечают многие НПО, неточность терминов, фигурирующих в законе, увеличивает риски неправильного толкования и может привести к появлению цензуры в интернете или введению неправомерных ограничений.

Таким образом, действующие в странах Центральной Азии законы отражают особое видение интернет-пространства

и его использования. Прежде всего, Интернет выступает в качестве инструмента развития и технологии, призванной помочь государствам стать более конкурентоспособными и повысить собственную привлекательность, а также предоставить своим гражданам возможность узнать больше о цифровых технологиях. Однако интернет-пространство по-прежнему находится под контролем государственных властей, пусть и проявляющегося в разной степени. Новые законодательные акты, принятые в политических целях или ввиду неприязненного отношения к американским веб-гигантам GAFAM и западным социальным сетям, наглядно демонстрируют существующее в регионе недоверие к свободному интернету и возможные последствия его использования для соответствующих стран.

# Карта - цифровая свобода и защита данных на евразийском пространстве



# Борьбы за информацию и киберпространство в Иране и Пакистане

Киберпроблемы относятся не только к современным формам преступности или шпионажа, против которых право и межгосударственное сотрудничество должны развиваться на международном уровне. Они связаны с новыми так называемыми «информационными» рисками и в основном обозначают манипулирования общественным мнением, иногда с использованием сознательного использования и преднамеренное присвоение правды или даже лжи.

Показательный феномен фрагментации мира под влиянием взрыва социокультурных и политических репрезентаций или простое отрицание реальности на службе геополитической и геоэкономической власти? Мы решили сосредоточиться на структурировании двух малоизученных киберпространств, Ирана и Пакистана, взяв интервью у нескольких исследователей по этим вопросам.

Если речь едет о угрозе возникшой в последние годы представляющей серьезную международную озабоченность, то ее можно опредилить общим термином «информационная борьба». Беспокойство, отражающее растущее стирание границы между различиями в восприятии и представлениях мира и откравенной ложью в мире, где распространение информации опереться практически полностью на технологические средства связанные с интернетом.

За борьбой против постмодернистской стандартизации способов мышления и бытия в мире, а также против исчезновения великих нарративов в ответ на всплеск американской идеологии после падения советского блока тайно кроется опасным и миметическим способом все более значимое навязывание нарративов, где истина не имеет места быть, которое управляется манипулированием умами и желанием навязать свою власть, ценой восприятия реальности будущим

поколением и их адаптации к этим самым реалиям, прежде всего к экологическим уязвимостям.

## Интервью с Клеман Барнье и Ларой Айдиной об иранском киберпространстве

**предоставлен Мари Корсель и Морган Кайе**

Clément BARNIER окончил Гренобльский институт политических исследований, Международный университет Рабата, Школу экономической войны и Sciences Po Paris. **Он пришел в область цифровой геополитики после написания дипломной работы о подводных кабелях и работает аналитиком киберугроз в компании Sésame IT**.

Родилась в США, училась в Вашингтоне, получила образование в Париже, работала волонтером в Греции... Lara Aidi, свободно владеет более чем пятью языками, включая английский, французский, арабский, испанский и турецкий. **Она окончила магистратуру по международным отношениям и дипломатии в HEIP (Hautes Etudes Internationales et Politiques) и магистратуру по праву в области предотвращения, арбитража и разрешения конфликтов в Сорбонне.**

Они совместно написали доклад, который является темой данного интервью: ***"Digital Frontline: Examining Cyber Warfare in the 2022 Iranian uprising"***.

**EurasiaPeace (E.P) : Расскажите нам о своей работе в качестве аналитика киберугроз, в чем она заключается и что способствовало написанию вашего недавнего доклада об иранском киберпространстве? Какие выводы удалось сделать на основании этой работы?**

**Клеман Барнье и Лара Аиди (К.Б и Л.А) :** Мы работаем в подразделении CTI (cyber threat intelligence) в Sésame IT – французском стартапе, который разработал решение для обнаружения киберугроз, сертифицированное ANSSI.

Наша работа проходит в два этапа. Во-первых, наши команды собирают достаточно стандартную, скажем так, общую информацию о ситуации с угрозами и их эволюцией на мировой киберсцене. В этот мониторинг, осуществляемый отчасти при помощи OSINT (Open Source Intelligence), входит, например, как наблюдение за модификациями программ-вымогателей и методами, разработанными новыми хакерскими группировками, так и китайско-американская напряженность. Потом идет обработка этой информации, которая поступает в виде исследовательских статей, отчетов, комментариев на форумах, из «глубокой сети», что и является нашей основной деятельностью. Она заключается в изучении данных, собранных и хранящихся на нашей платформе анализа угроз, с целью разработки для наших клиентов возможных сценариев атак, а также соответствующих правил их обнаружения.

Кроме выявления путей доступа, используемых злоумышленниками, названий вредоносных файлов или IP-адресов, **для понимания природы угрозы, мотивов тех, от кого она исходит, и как ей противостоять, все большее значение приобретает геополитический контекст.** Это особенно актуально в тех областях, где много работоспособных специалистов в сфере высоких технологий, не обязательно обладающих стратегическим или тактическим опытом. Многогранный характер угроз требует комплексного подхода. Поэтому, если попытаться провести аналогию с экономикой, можно сказать, что мы также занимаемся вопросом «макрокибер»... В этом заключается дополнительная ценность аналитика.

Мы, изначально не связанные с кибербезопасностью (Лара - юриспруденция, Клеман - политические науки. – Прим. ред.), **быстро осознали масштабы угрозы со стороны Ирана в глобальном киберландшафте**, осуществляющего сложные операции по шпионажу, дестабилизации и созданию программ-вымогателей по российскому и китайскому образцу. Например, недавняя компьютерная атака на сайт Charlie Hebdo была

осуществлена иранской группой Neptunium. Мы внимательно следили за событиями после убийства Махсы Амини полицией нравов Тегерана и, ввиду отсутствия литературы на эту тему, сочли нужным подготовить соответствующий доклад. Ведь за каждым физическим восстанием граждан сейчас стоят международные кибернетические силы, организованные в альянсы. Эти силы сами по себе не могут привести к революции на улице, но они так или иначе влияют на ее ход.

В данном докладе (Digital Frontline: Examining Cyber Warfare in the 2022 Iranian uprising) рассматривается эволюция кибервозможностей режима мулл и гибридные стратегии, применяемые его противниками для обхода цифровой цензуры и репрессий. Подводя итоги текущей информационной войны, кибершпионажа и хакерства в Иране, мы хотели понять ключевую роль социальных сетей, а также сообщества хактивистов в происходящем восстании. С этой целью мы проанализировали поведение первых групп, участвующих в **операции #OpIran**, начатой сетью хакеров Anonymous, типы планируемых атак и мотивы участников. Наконец, мы рассмотрели случай Ирана в рамках более широкого явления – прогрессирующей нормализации цифрового авторитаризма.

**Е.Р : Как развивалась политика иранского государства по отношению к использованию интернета протестующими гражданами с начала 1990-х годов? В чем заключаются различные формы протеста за последние несколько десятилетий и как они изменились в своем понимании использования интернета для поддержки требований? Какими способами правительство использует интернет внутри страны для подавления несогласных?**

**К.Б и Л.А : Когда в 1993 году во время мандата президента Х. Рафсанджани в Иране произошло первое подключение к Интернету, Иран стал одним из первопроходцев в этой области на Ближнем Востоке** вслед за Израилем (1990). Тогда Интернет был положительно воспринят властями, как в экономическом, так и в культурном плане, как средство распространения

коранических предписаний. Однако, как и в случае с книгой и печатной революцией в XV веке, **доступ к информации, новым теориям и знаниям во всей их целостности в конечном итоге больше дестабилизировал авторитарный режим, чем служил ему.** Сама суть Интернета – пространства, которое постоянно расширяется,– делает его трудным, если не сказать невозможным для полного освоения. Это особенно верно с учетом влияния социальных сетей. В 2009 году после обвинений в фальсификации президентских выборов в пользу консервативного М. Ахмадинежада, народное восстание получило в СМИ название **"Твиттер-революция"** из-за ведущей роли приложения в координации демонстрантов и распространении изображений насилия со стороны правительства. В целом в период с 1990 по 2010 год произошла радикальная смена парадигмы восприятия Интернета иранскими властями, которые разработают свою стратегию по отношению к Интернету, ставшим для них настоящей угрозой.

По данным опроса, проведенного Iranian Students Polling Agency (ISPA), в 2021 году 73,6% населения Ирана пользуются социальными сетями или приложениями для обмена сообщениями, при этом лидируют Whatsapp (64,1%), Instagram (45,3%) и Telegram (36,3%). Гражданам удается обходить все новые вводимые запреты, используя VPN ('virtual private networks') или прокси-серверы. Киберарсенал режима, с другой стороны, был структурирован и усилен в ходе протестов. Создание иранской киберполиции (FATA) в 2009 году... Создание иранской киберармии в 2010 году... Усиление надзора за интернетом и социальными сетями... Цензура интернета в зонах напряженности... Одна шпионская программа – EyeSpy, вызывает особое беспокойство, поскольку она тайно устанавливается во внутреннюю систему некоторых VPN правительственными службами, которые затем получают доступ к данным пользователей (местоположение, посещеемые сайты, контакты, личные сообщения и т.д.).

**Е.Р : Иранская киберармия официально не входит в ведение правительства. Как это можно объяснить?**

**К.Б и Л.А : Электронная армия Ирана или Iranian Cyber Army – это группа хакеров, известная компьютерными атаками на правительственные сайты западные IT-компании западных стран**, которая действует с 2009 года. Хотя она официально не связана с режимом, ее члены, тем не менее, обязуются хранить верность Верховному лидеру, что делает ее действенным нетрадиционным оружием для КСИР (Корпуса стражей исламской революции). Коллективное сознание часто ассоциирует хакерские группы с кем-то вроде современных пиратов. Однако в данном случае они больше похожи на каперов, которым государство поручило грабить ресурсы другого государства.

**Е.Р : Способен ли Иран на сегодняшний день противостоять внешним киберугрозам? Вспомним случай использования компьютерного червя "Stuxnet" США и Израилем для того, чтобы замедлить реализацию ядерной программы Ирана в 2010-х годах. В чем заключается его уязвимость? И, наоборот, можно ли считать Иран уже вполне сформировавшимся игроком на международной киберарене или ему еще предстоит развить собственный потенциал?**

**К.Б и Л.А :** Прежде чем рассматривать этот вопрос, необходимо понять одну вещь: если перефразировать Клаузевица, **кибернетика в некотором смысле стала продолжением политики или войны, но уже другими средствами...** Цифровой мир – новое поле битвы международного уровня, где страны защищают свои нематериальные активы, а также нападают на активы противника или конкурента, является отражением геополитического баланса. Однако есть и существенные отличия, такие как **отсутствие регулирования киберпространства, сложная координация действий международных организаций в этой области и трудность определения лица, ответственного за вторжение в систему, – все это факторы, поощряющие наступательные стратегии государственных субъектов**. Ирану также угрожает то, что он называет сионистско-западной коалицией (США, Израиль,

Великобритания, Франция и т.д.), а его союзники (Китай, Россия), тем не менее будут проводить операции по краже данных или кибершпионажу против самого Ирана, исходя из личных интересов. Это дикое состояние без каких-либо физических границ, если говорить словами Гоббса, усиливает сложившийся конфронтационный режим, в котором союзы непрочны, а вражда вполне допустима.

**Хотя Иран сегодня является важным участником международного киберпространства, способным взломать так называемые сложные структуры на иностранной территории с помощью опыта социальной инженерии, его изоляция на международной арене и, следовательно, его незащищенность, подчеркивают его цифровые уязвимости.** Особенно от этого недостатка международного сотрудничества страдает образовательная экосистема страны, что вынуждает государственные группировки нападать на академические учреждения для получения данных и продвижения в исследованиях. **Например, в 2009 году АНБ, ЦРУ и израильские спецслужбы разработали компьютерного червя "Stuxnet", чтобы остановить ядерную программу Ирана.** В результате теоретически лучше всего защищенные объекты мулл были сильно повреждены. Эта успешная операция, получившая широкую огласку, заставила правительство проводить более жесткую политику в области киберзащиты, в частности, путем создания организаций, занимающихся защитой жизненно важных инфраструктур. Однако оборонительный потенциал страны все еще значительно ниже его наступательных возможностей, и это вполне логично, учитывая агрессивную стратегию Тегерана.

***«отсутствие регулирования киберпространства, сложная координация действий международных организаций в этой области и трудность определения лица, ответственного за вторжение в систему, – все это факторы, поощряющие наступательные стратегии государственных субъектов».***

**<u>E.P</u> : Как охарактеризовать кибервойну между Тель-Авивом и Тегераном? Украину иногда называют**

**"киберлабораторией" России; был ли Иран такой лабораторией для США и их союзников, в частности Израиля?**

**К.Б и Л.А: Особенность киберконфликта между Тель-Авивом и Тегераном, как говорится, "заклятыми врагами", заключается в том, что он происходит в основном в военной и разведывательной сферах.** В этом заключается его существенная разница, например, с китайско-американским киберконфликтом, который также в значительной степени протекает в производственной сфере. Ирано-израильская напряженность находит отражение в кибервойне, скрытой и тайной, которую в настоящее время предпочитают вооруженному противостоянию. **Каждая из сторон стремится нарушить работу критической инфраструктуры другой** (гидроэлектростанции, телекоммуникационные операторы, буровые станции и т.д.) или провести дезинформационные кампании среди населения.

Во многих отношениях Иран можно назвать "киберлабораторией" США так же, как Украина была и остается таковой для России с 2014 года. Враждебный характер отношений между Тегераном и Вашингтоном, географическая удаленность этих двух государств, дисбаланс в военных арсеналах и демократические тенденции режима мулл создают благоприятную почву для открытой, фактически признанной войны в киберпространстве. Однако, если иранская ударная сила в этой области уже была продемонстрирована, американская сверхдержава продолжает опираться на свою политику глобальной гегемонии, сравнимую лишь с Китаем. **Многочисленные кампании, проводимые против иранских инфраструктур США и их точкой опоры в регионе – Израилем, подтверждают теорию масштабной киберлаборатории**.

***«Хотя Иран сегодня является важным участником международного киберпространства, способным взломать так называемые сложные структуры на иностранной территории с помощью опыта социальной инженерии, его изоляция на международной арене и, следовательно, его незащищенность, подчеркивают его цифровые уязвимости».***

**<u>Е.Р</u> : Могут ли группы киберактивистов в Иране оказать значимую поддержку текущему протестному движению? Можно вспомнить группировку Edalat-e Ali, которой удалось прервать выступление президента Эбрахима Раисси в начале февраля (чтобы призвать иранцев забрать свои деньги из "коррумпированных" банков режима и выйти на улицы) или в середине октября (прервав выступление аятоллы Али Хаменеи фотомонтажом последнего с его телом, окруженным пламенем, и прицелом на лице).**

**<u>К.Б и Л.А :</u> В Иране существует большое сообщество так называемых хактивистов (групп или отдельных лиц, движимых идеологическими причинами, такими как защита основных свобод, демократической прозрачности или, наоборот, авторитаризма и т.д.). Движение протеста также может рассчитывать на диаспору, прочно обосновавшуюся на международном уровне (Париж, Лондон, Лос-Анджелес и т.д.)**, которая сыграла решающую роль в распространении информации после ареста и смерти Махсы Амини и ее освещения в СМИ. Однако репрессии против многих хактивистов на иранской земле ограничили их влияние в последнее время. Многочисленные сообщения с призывом о помощи были отправлены международному сообществу в группах Telegram и Signal из иранских тюрем. Западные хактивисты в ответ начали операцию **#OpIran 20 сентября 2022 года под руководством группы Anonymous**. Группы SpiderChat и YourAnonSpider первыми атаковали правительственные сайты, за ними последовали DDOSEmpire, Ghostec, Atlas Intelligence Group и Black Reward, которая прославилась тем, что раскрыла секретную информацию об иранской армии.

**Возможно, самым значительным событием в ведущейся Ираном кибервойне является взлом телеканала Islamic Republic of Iran Broadcasting (IRIB) группой Edalat-e Ali.** Подобные действия, конечно, направлены на то, чтобы повлиять на общественное мнение, и являются частью информационной войны. Неизвестно, как был осуществлен этот взлом, но предполагается, что имела место значительная материально-техническая поддержка какой-либо третьей стороны (США, Израиль и т.д.), поскольку компрометация подобных инфраструктур обычно является делом прерогативы государственных групп, обладающих значительными техническими и человеческими ресурсами.

***«Особенность киберконфликта между Тель-Авивом и Тегераном, как говорится, "заклятыми врагами", заключается в том, что он происходит в основном в военной и разведывательной сферах».***

**<u>Е.Р</u> : Нынешний протест проходит под лозунгом "Женщины, жизнь, свобода!", но к нему также присоединяются многочисленные требования со стороны этнических групп. Есть ли среди них активные хакерские группировки? И существуют ли между ними какие-либо формы сотрудничества?**

**<u>К.Б и Л.А</u> :** Как сообщается, лозунг "Женщина, жизнь, свобода" был впервые скандирован вблизи тегеранской больницы, куда была помещена в реанимацию Махса Амини. Снятый на мобильные телефоны, он сразу же широко распространился через независимые СМИ (1500tasvir, Iran Wire и т.д.) и личные переписки пользователей Интернета и стал самым популярным гимном протеста наряду с лозунгом "Смерть диктатору".

Если в восстании против мулл участвовали все провинции, то наиболее жестокие столкновения наблюдались на северо-западе в курдских районах, откуда была родом Махса Амини. Таким образом, ее смерть послужила катализатором протестов в изначально враждебном иранскому режиму сообществе. **Эти**

**геополитические данные также нашли отражение в киберпространстве, хоть и в меньшем масштабе. Мы действительно обнаружили существование по крайней мере одной группы хактивистов, утверждающих, что они являются частью курдского движения "Аль-Тахреа"**, которая в августе 2022 года участвовала в компьютерной атаке на украинские инфраструктуры от имени России. В этой связи следует обратить внимание на одно явление. Усиление репрессий в отношении иранских курдов привело к отъезду многих молодых людей в провинцию Эрбиль в Ираке. Установление прямого контакта между этими общинами в конечном итоге может привести к появлению новых независимых или связанных с РПК (Рабочая партия Курдистана) кибергрупп.

***«В Иране существует большое сообщество так называемых хактивистов (групп или отдельных лиц, движимых идеологическими причинами, такими как защита основных свобод, демократической прозрачности или, наоборот, авторитаризма и т.д.). Движение протеста также может рассчитывать на диаспору, прочно обосновавшуюся на международном уровне (Париж, Лондон, Лос-Анджелес и т.д.)».***

**Е.Р : Были ли в Иране предприняты попытки отгородиться от мирового Интернета, как это было в случае с Россией и ее Рунетом? В 2019 году правительство приказало провести полную блокировку Интернета, в результате чего Иран был на неделю отрезан от остального мира, в стране работали только государственные цифровые сервисы, создав тем самым национальный Интранет... Если да, то каковы его шансы на успех?**

**К.Б и Л.А :** Желание иранского режима отключить страну от мирового Интернета не является несбыточной мечтой.

У этой программы даже есть название: NIN (National Internet Network), и государство финансирует ее с 2011 года. **Бывший президент Х. Рохани (2013 - 2021) издал фетву о создании "халяльного Интернета", считая, что "3G противоречит предписаниям шариата"**. Не имея возможности осуществить этот проект по получению почти неограниченного контроля над внутренней сетью, режим пока прибегает к хорошо известным методам цензуры. Так, в начале протестов 2019 и 2022 годов иранская интернет-связь зафиксировала снижение трафика в стране более чем на 90% в течение нескольких дней в 2019 году и нескольких часов в 2022 году (Netblocks).

**Теоретически возможность создания Интранета под контролем режима вполне реальна, учитывая власть правительства над телекоммуникационным сектором. На практике степень технологического развития инфраструктуры для поддержки всех требований вызывает сомнения.** С одной стороны, реализация такой программы неизбежно приведет к появлению сети антенн, кабелей и подпольных операторов, мотивированных идеологическими или финансовыми соображениями. **С другой стороны, трудно представить, как правительство сможет решить проблему VPN и Proxies, которые уже широко используются пользователями Интернета для обхода цензуры**, спрос на которые в 2022 году вырос более чем на 3000%. В конечном итоге, интерес других держав может заключаться в обеспечении такого доступа к глобальному Интернету, а значит, и к определенной информации. Это был один из вопросов, стоящих на кону в сентябре 2022 года. Тогда Белый дом дал добро компании Starlinks на развертывание своей спутниковой сети, как это было сделано в Украине. Связь хоть и остается очень медленной, поскольку в Иране менее 100 активных спутников, но все же сохраняется.

**E.P : Считаете ли вы, что недавнее сближение Ирана и Саудовской Аравией под эгидой Китая предвещает новое сотрудничество между этими странами в киберсфере?**

**К.Б и Л.А: Разрядка между Саудовской Аравией и Ираном, отмеченная восстановлением дипломатических отношений, в значительной степени структурирует геополитический ландшафт региона, но, похоже, не имеет серьезных последствий в киберсфере**. Подписанное в Пекине соглашение о сотрудничестве носит в основном экономический характер. Можно, конечно, ожидать ослабления иранской поддержки йеменских хути, "Хезболлы" или иракских шиитских ополченцев в качестве дипломатического жеста доброй воли со стороны Тегерана. Тем не менее разногласия после такого длительного периода взаимной вражды кажутся слишком глубокими, чтобы предполагать тесное сотрудничество в среднесрочной перспективе, особенно в области военной разведки и кибернетики. Среди многочисленных случаев предполагаемого кибершпионажа, в 2012 году саудовский нефтяной гигант Aramco был взломан группировкой «Рассекающий меч правосудия» (The Cutting Sword of Justice), подозреваемой в связях с иранскими стражами революции.

Эти новые балансы в сочетании с изоляцией Израиля, в свою очередь, способствуют увеличению числа кибератак в этом регионе, которые, с одной стороны, проводит Тель-Авив при поддержке Вашингтона, а с другой – блок Тегеран-Пекин против западного врага.

***«Теоретически возможность создания Интранета под контролем режима вполне реальна, учитывая власть правительства над телекоммуникационным сектором. На практике степень технологического развития инфраструктуры для поддержки всех требований вызывает сомнения».***

**Е.Р : Хотите ли Вы что-нибудь добавить?**

**К.Б и Л.А :Мы хотим предупредить исследовательское сообщество. В последнее время было опубликовано несколько докладов, в которых подробно описываются фишинговые операции, направленные на журналистов, активистов, преподавателей университетов и аспирантов, изучающих иранскую проблематику. Любой, кто имеет хоть какую-то**

**узнаваемость, даже в очень узких кругах, является потенциальной мишенью (взлом учебных и личных данных, манипуляции и т.д.)**. Речь идет не о том, чтобы становиться параноиком, а о том, чтобы осознавать реальный риск. Сообщается, что группировка Charming Kitten, также известная как APT 42, получила заказ от Тегерана на проведение подобных операций. В декабре 2022 года были официально идентифицированы три жертвы. Хакеры получили доступ к их электронной почте, облачным хранилищам, календарям и контактам. Они также провели "Google Takeout", используя инструмент, который экспортирует данные из основных и дополнительных сервисов аккаунта Google.

Что касается способа действия, то злоумышленники отправляют вредоносную ссылку (PDF, URL и т.д.) через Whatsapp или Gmail, которая после открытия запускает загрузку вредоносного программного обеспечения. Поскольку первой уязвимостью в кибербезопасности является человек, всегда будьте бдительны, регулярно меняйте свои пароли и проверяйте, чтобы они имели достаточный уровень защиты, прежде чем применять двойную аутентификацию.

## Интервью с Намвайом Опалинским о пакистанском киберпространстве

**предоставлен Энцо Падован при содействии Мари Корсель и Морган Кайе**

Навмай Опалински - **аспирант, специалист по географии во Французском институте геополитики (IFG), (Университет Париж 8)**. Он готовит свою докторскую диссертацию под руководством Фредерика Дузе и Изабель Сен-Мезар. **Он также член исследовательского проекта GEODE - Геополитика датасферы (Geopolitics of the Datasphere). Его исследования посвящены « китайскому цифровому шелковому пути » и влиянию китайских инвестиций в инфраструктуру ИКТ на интернет-связь в Азиатском регионе - его особо интересует пример Пакистана.** Он китаист и учился в Пекинском университете языков и культур ( 北京语言大学 ). Он также член Лахорского университета наук управления – University of Management Sciences (LUMS), где он принимает участие в исследовательском проекте по изучению интернета-связи

в Пакистане - EPIC (Exploring Pakistan's Internet Connectivity).

**<u>EurasiaPeace (E.P):</u> Не могли бы вы познакомить нас с вашей исследовательской работой по киберпространству Пакистана ? В чем заключается общая проблематика работы, посвященной теме, о которой у нас мало информации ?**

**<u>Навмай Опалински (Н.О)</u>:** На данный момент, я учусь в аспирантуре во французском институте геополитики - IFG, мои работы посвящены роли различных геополитических конфликтов и борьбы за сферы влияния в организации работы Интернета в Пакистане. В моей диссертации впервые предпринята попытка составить пространственную визуализацию интернета в Пакистане на нескольких уровнях –сетевой инфраструктуры – физическом, логичеком и информационном, и понять, как на них влияют политические, экономические или стратегические решения различных субъектов. Меня также интересует вопрос устойчивости пакистанской сети и то, как различные соображения политического и экономического характера сказываются на географии интернета. Моя работа проводится в рамках исследовательского проекта GEODE (Геополитика Датасферы), который сосредотачивается, в частности, на маршрутизации и который недавно получил европейское финансирование.

Пакистан представляет собой интересный пример для исследования, так как он расположен на стыке Ближнего Востока и Южной Азии, его касаются непосредственно риски разделения в технологической сфере, связанные с китайско-американским конфликтом, и поскольку он страдает от многочисленных кризисов, которые разворачиваются в киберпространстве. Пакистан также является страной, где подключение к Интернету все еще находится на стадии расширения, и где структурирование национальной сети все еще продолжается - это дает повод задуматься о политике цифрового планирования. В конце концов нужно сказать, что цифровая связь Пакистана сильно зависит от геополитического контекста, в котором находится страна, и с географией маршрутов передачи данных, которая следует скорее политическим, чем техническим решениям.

**Меня также интересует Пакистан в контексте « цифрового шелкового пути » - стратегии установления телекоммуникативных связей между Китаем и его соседями. Пакистан – часть маршрутов этого пути, последнее подключение к цифровому шелковому пути действует с 2019 года. Цель моей диссертации - понять стратегию Китая касательно цифровой инфраструктуры по отношению к своим соседям на примере Пакистана.**

**<u>E.P</u> : Каковы главные киберугрозы, с которыми сталкивается Пакистан? Министр информационных технологий в конце прошлого года говорил о 900 000 хакерских инцидентах в день в стране. Также недавно поступили сообщения об атаке на электросеть 23 января, в которой подозревается индийская группировка "Сайдуайндер", спонсируемая индийским государством. Израильское программное обеспечение « Pegasus », по сообщениям, также было использовано Индией против своего соседа. Напомню, что Пакистан является 6-й ядерной державой в мире. В чем заключается сопротивление между Индией и Пакистаном ? Есть ли желание перенести ядерное сдерживание на киберпространство? Какая из этих двух стран более успешна в этой области?**

**<u>H.O</u> :** Прежде всего, отключение электроэнергии 23 января не было вызвано кибер-атакой. Это было явно необоснованное заявление, которое позволило правительству снять вопрос, обвинив Индию. Между двумя соседями действительно идет кибервойна, но последние сообщения объясняют отключение электроэнергиглубоким экономическим кризисом в Пакистане, в том числе из-за нехватки иностранной валюты и , как следствие, нехватка снабжения нефтью и газом –необходимых для должного функционирования пакистанских электростанций. В этом деле интересно отметить, как сильно власти Пакистана одержимы индийскими кибератаками на их сеть. Однако осознание, хоть и очень позднее, вопросов кибербезопасности в Пакистане есть, и оно реальное. С начала 2000-х годов Пакистан пережил многочисленные кибернападения (вероятно, со стороны Индии), и масштаб этих нападений набирал обороты. Раньше атаки ограничивались часто атаками **воспрещения доступа – теперь же выявляется**

**все больше и больше программ- вымогателей. К тому же власти Пакистана выразили серьезную озабоченность по поводу скандалов, связанных с программным обеспечением « Pegasus » или другими операциями по кибершпионажу под руководством Индии.** В этой стране власти сталкиваются с ростом числа случаев использования программ вымогателей, которые также могут исходить от местных групп, преследующих финансовую выгоду. Из-за волны кибератак, нахлынувших на Пакистан, власти страны чувствуют себя обезоруженными.

Индия и Пакистан постоянно нападают друг на друга, особенно во время сильной дипломатической напряженности. Недавняя отмена в августе 2019 года специального статуса штата Джамму и Кашмир привела к росту числа нападений. В важные для истории этих государств даты государственные здания в Пакистане регулярно подвергаются нападениям, в частности во время Дня независимости Пакистана и Индии. В частном секторе подвергаются нападениям, в основном, банки и федеральный комитет по налогам и сборам (Federal Board of Revenue). В 2017 году единственный провайдер электроэнергии в Карачи, компания K-Electric , не смог выплатить выкуп в размере 7 млн долларов, после атаки одной программы-вымогателя, что привело к крупной утечке данных. В месяц федеральный комитет по налогам и сборам подвергается около 71 000 атак, что свидетельствует о неотложном характере ситуации. Шпионское ПО « Pegasus » использовалось даже для слежки за Имраном Ханом, Бывшим премьер-министром. Наступательные возможности обоих государств, как правило, направлены друг против друга.

**Тем не менее дело Pegasus для Пакистана было серьезным поводом для беспокойства по поводу усиления влияния Индии в киберапространстве, поддерживаемой такими государствами, как США или Израиль. Успех Индии в установлении партнерских отношений в киберпространстве с главными державами вызывает беспокойство у пакистанцев, особенно, если учесть их восприятие Израиля как главную угрозу.** Пакистанское правительство всегда считало необходимым полагаться на крупные державы для обеспечения своей безопасности, исторически оно

сначала полагалось на Великобританию, затем на США, а теперь и на Китай. **Руководство Пакистана, и в частности пакистанская армия, воспринимают наращивание военного потенциала Индии, в том числе в киберсфере, которое в Нью-Дели считают необходимым на фоне растущего конфликта с Китаем, как экзистенциальную угрозу для благополучия Пакистана.** Помимо нападений на объекты критически важной инфраструктуры и операций по кибершпионажу власти Пакистана уделяют большое внимание информационной войне с соседней Индией. Исламабад пытается выйти из дипломатической изоляции, привлечь иностранных инвесторов и представить себя в лучшем свете на международной арене. Однако пакистанские лидеры считают себя жертвами кампании по дезинформации в интернете, которую ведет Индия. Бывший генерал-лейтенант Пакистана в отставке Раза Мухаммад Хан в 2020 году описал информационный фронт как "*самый уязвимый асимметричный фланг*" обороны Пакистана. В Стратегии национальной безопасности, опубликованной в 2021 году, психологическая война и противодействие дезинформации многократно упоминаются как главные угрозы, представляющие ещё большую опасность, чем шпионаж.

Европейская общественная организация "EU Desinfo Lab" составила досье под названием "Индийские хроники". В досье общественная организация проливает свет на крупнейшую в истории операцию по дезинформации на первый взгляд организованную Индией. Целью была в первую очередь дискредитация политики Пакистана в Кашмире. Поэтому передали эту информацию в Исламабад, чтобы доказать, что против них ведется информационная борьба.

Все же пакистанцы не отстают от них. Проводятся информационные кампании в поддержку мятежных движений в Кашмире, осуждающих репрессии Нью-Дели в регионе, особенно против мусульманского населения. Однако важно понимать, что эта вспышка напряженности в информационном пространстве не ограничивается противостоянием между Нью-Дели и Исламабадом. **На самом деле, власти Пакистана сталкиваются с еще более опасной**

**внутригосударственной проблемой с тех пор, как бывший премьер-министр Имран Хан перешел в оппозицию. Имран Хан поддерживал с армией теплые отношения, пока не был отстранен от власти вотумом недоверия весной 2022 года.** С тех пор он призывает народ, в частности через социальные сети, требовать проведения новых выборов, осуждает коррупцию, в пакистанской армии, что в результате привело к демонстрациям широкого размаха. В прошлом пакистанская армия никогда не подвергалась такой резкой критике, теперь же, можно наблюдать вспышки недоволстьва, с которыми правительство не в силах справиться. В марте 2023 года армия потребовала создания оперативной группы, в которую вошли представители Федерального агентства расследований, управления по Телекоммуникациям Пакистана, национального управления хранения персональных данных и регистрации (NADRA) – Целью создания этой группы было противостояние распространению враждебных высказываний против армии в социальных сетях. Критика в сторону армии воспринимается ее представителями серьезно, несмотря на то, что у них нет инструментов ей противодействовать.

***«Тем не менее дело Pegasus для Пакистана было серьезным поводом для беспокойства по поводу усиления влияния Индии в киберапространстве, поддерживаемой такими государствами, как США или Израиль. Успех Индии в установлении партнерских отношений в киберпространстве с главными державами вызывает беспокойство у пакистанцев, особенно, если учесть их восприятие Израиля как главную угрозу»***

**<u>Е. Р</u> : Имели ли какие-то особые последствия с точки зрения международного сотрудничества страны откровения Эдварда Сноудена о шпионаже АНБ за Пакистаном? С кем сотрудничает правительство Пакистана на региональном и международном уровне в области кибербезопасности? Пакистанское правительство, по всей видимости, считает, что западные страны развернули против Пакистана**

**кампанию по дезинформации - власть подчеркивает свою мусульманскую идентичность и занимает позицию жертвы, насколько можно в это верить ?**

**Н.О:** Действительно, Пакистан был одной из стран, наиболее пострадавших от широкомасштабного шпионажа АНБ. Наблюдатели ссылаются на отчеты западных компаний или заявления Эдварда Сноудена, никаких официальных заявлений правительства по этому поводу не было сделано. Нет ничего необычного в том, что Пакистан находится под наблюдением АНБ- США нуждались в этой стране, так как американские войска присуствовали в Афганистане и они превратили страну в свое тыловое обеспечение.

По словам Эдварда Сноудена, АНБ использовало вредоносную программу под названием "Secondate" для шпионажа за линиямм связи военных и гражданского населения в Исламабаде. Стоит также отметить, что в 2015 году в пакистанской прессе появилась информация о том, что британская спецслужба Центр правительственной связи (GCHQ) получила доступ к маршрутизаторам Cisco основной точки обмена трафиком в стране, что позволило ей отслеживать значительную часть IP-трафика.

Напомню еще раз, что эти откровения не вызвали у правительства сильной реакции . В любом случае, власти Пакистана поддерживали тесное сотрудничество с западными агентствами (включая АНБ) в сфере борьбы с терроризмом, даже на национальной территории. Это партнерство означало доступ к финансированию и технологиям перехвата. **Пакистан не следует относить к той же категории, что Иран или Россию- связи с США со времен холодной войны всегда были сильными и, что самое главное - органы безопасности обеих стран имеют общие каналы связи. Исламабад в гораздо большей степени обращен к Западу, чем к своим ближайшим соседям.**

Подтвердить факт наличия партнерских отношений в киберпространстве довольно сложно. Пакистанские наблюдатели сожалеют об отсутствии партнерских отношений с союзными странами, что является результатом недостаточного инвестирования в эту область. Существует тесное сотрудничество с Китаем и Турцией, включающее обмен ноу-хау, тренинги и доступ к

технологиям. **Но в том, что касается киберсферы как таковой и обмена сведениями о кибератаках**, **никакой информации о потенциальном партнерстве или обмене сведениями между Пакистаном и другой страной не была опубликована. Сложно опрделить даже**, **есть ли у правительства Пакистана какие-то соглашения на региональном уровне в этой области. В любом случае, официально никакого двухстороного партнерства не существует. Нью-Дели, в свою очередь, с 2018 года установил партнерские отношения с США, Японией, Россией, Малайзией, Сингапуром и Израилем**. Это вызывает у властей Пакистана опасения по поводу возможного усиления изоляции в киберпространстве. Тем не менее наблюдается сближение Пакистана с Россией, которое, однако, не рассчитано на долгосрочную перспективу. Осуждение слежки за Пакистаном со стороны запада - скорее политическая позиция бывшего правительства, так как современные власти не осуждают Запад. На самом деле кампания по дезинформации, направленная против Пакистана, в основном, приписывается Индии и затрагивает Кашмирский вопрос, внутрение политические проблемы Пакистана и плохую репутацию китайско-пакистанского партнерства, в частности Китайско-пакистанский экономический коридор (КПЭК).

***«Пакистан не следует относить к той же категории, что Иран или Россию- связи с США со времен холодной войны всегда были сильными и, что самое главное - органы безопасности обеих стран имеют общие каналы связи. Исламабад в гораздо большей степени обращен к Западу, чем к своим ближайшим соседям»***

**<u>E. P :</u>Не могли бы вы рассказать о политике государства Пакистана, о его организации в отношении киберпространства? Следует ли расценивать закон от 2016 года о предотвращении киберпреступлений (Prevention of Electronic Cybercrimes Act of 2016) как желание властей Пакистана усилить контроль над интернетом? Является ли, по крайней мере, орган управления телекоммуникациями, независимым или оно находится под непосредственным контролем**

**правительства? Как вы могли бы охарактеризовать состояние цифровой свободы в Пакистане?**

**Н.О :** Во-первых, вопрос интернета в Пакистане следует рассматривать в историческом контексте. Организация системы телекоммуникация в Пакистане похожа на ту, что существует во многих странах Азии.С конца 1990-х годов в стране проводились реформы в этой отрасли и усиливалась либерализация, сопровождавшаяся появлением конкуренции на рынке телекоммуникаций и прекращением государственной монополии в этом секторе. В то время международная политика настаивала на либерализации области телекоммуникаций, как это было в Европе. Государственный сотовый оператор был приватизирован и частично перешел под контроль компании - Коммуникации Etisalat Group, а все остальные крупные мобильные операторы - принадлежать иностранным компаниям, работающим в Пакистане. Таким образом, основные игроки на рынке телекоммуникаций в стране принадлежат или находятся под контролем иностранных компаний, что не типично для этого региона.

Государство не управляет сетями, но сохраняет определенный контроль в сфере посредством агентств, находящихся в ведении министерства информации и телекоммуникаций. **Управление Телекоммуникациями Пакистана (Pakistan Telecommunication Authority PTA) занимается именно выдачей лицензий и мониторингом сетей. Закон от 2016 года о предотвращении киберпреступлений (PECA) наделяет правительство Пакистана, среди прочего, полномочием подвергать цензуре контент, который они считают противозаконным.** Цензура онлайн-контента существовала и раньше, но этот закон создал для нее правовую основу. **Закон подвергся критике со стороны многих общественных групп за произвольный характер его применения** ( в частности, из- за слабого независимого судебного за решениями управления Телекоммуникациями Пакистана -PTA), а также за отсутствие четкого понимания, что является поводом для блокировки - позволяя интерпретировать понимание закона от случая к случаю.

Интернет-цензура в Пакистане – существует, но она ограничена отсутствием контроля над контентом.

Действительно, в отличие от Китая или России, где существуют отечественные платформы и где государство может оказывать давление, в Пакистане доминируют американские платформы. Поэтому государству Пакистана приходится договариваться с этими платформами об удалении контента, который оно считает нежелательным. Но за последние десять лет стало невозможным заблокировать только один раздел сайта - это автоматически блокирует весь сайт. Для некоторых сайтов (особенно для порнографических сайтов) проще фильтровать их, но для других государство часто вынуждено либо договариваться с ними, либо польностью блокировать сайт. Так как у американских компаний нет офисов в Пакистане, невозможно обратиться к кому-то с претензиями что вызывает недовольство у пакистанцев, тем более что в Индии есть официальное представительство этих компаний. Таким образом, цензура работает скорее на криминализацию опубликованного контента. Закон о предотвращении киберпреступлений (PECA) позволяет, таким образом, подвергать цензуре кощунственные или непристойные высказывания в интернете, наказывая за это пользователей. Власти Пакистана находятся в затруднительном положении, о чем свидетельствуют постоянные колебания между запретом или разрешением на использование платформ. На протяжении трех лет в стране был запрещен YouTube. Тик Ток периодически запрещался. А потом вновь разрешался. Последнее дело о блокировке Википедии, весьма показательно : По данным хорошо информированного источника, Управление Телекоммуникациями Пакистана не смогло договориться с Википедией об ограничении доступа к проблемному для Пакистана контенту. Из-за отсутствия свободы действия и каналов связи Управлению Телекоммуникациями Пакистана пришлось польностью заблокировать доменное имя Википедии в стране, вызвав гнев гражданского общества, поэтому спустя некоторое время сайт вновь был разблокирован. Правительство Имрана Хана предложило ввести более строгие правила ( Правила защиты граждан от вреда в интернете – « Protection of Citizen Against Online Harm Rules »), которые обязывали бы платформы с более 500 000 пользователей в Пакистане, иметь офисы в стране. Американские платформы, объединились в группу интересов -

Азиатскую интернет-коалицию и дали согласованный ответ на решение о принятии этого законопроекта, написав письмо прьемер-министру, в котором они выразили свою озабоченность и подчеркнули намерение уйти с пакистанского рынка , если этот закон вступит в силу.

**<u>E. P :</u> Представляет ли Афганистан под контролем талибов киберугрозу для Пакистана, учитывая неоднозначность их отношений, особенно в плане информационной борьбы?**

**<u>H.O :</u>** На мой взгляд, режим в Афганистане никакой киберугрозы для власти Пакистана не представляет. Конфликты между афганскими группировками и Исламабадом, в основном, связаны с отказом Пакистана вывести сторонников террористической организации (Терих-е Талибан Пакистан) из их святилища на территории Афганистана и с обеспечением безопасности на границе. Талибы не могут использовать киберпространство в своих интересах - у них недостаточно средства для этого. Зато пропаганда террористических групп в социальных сетях, как средство вербовки, уже представляет из себя более серьезную угрозу. Так что власти Пактистана уже давно начали относиться к вербовкам террористов в интернете, как к угрозе.

**<u>E. P :</u> Делает ли Пакистан какие-то выводы из влияния войны на Украине на киберпространство? Какое последствие этого сильного аспекта конфликта для этой страны?**

**<u>H.O:</u>** Довольно сложно сказать, так как Пакистан практически не озвучил свою позицию по этому вопросу. Возвращаясь к украинскому вопросу и этому конфликту высокой интенсивности, мне кажется, что не стоит переоценивать роль киберпространства в различного рода конфронтациях : согласно специалистам по этому вопросу - и я здесь ссылаюсь на работы и наблюдения моего коллеги Луи Петиньо, ученого-исследователя в - GEODE (Геополитика Детасферы), киберпространство, выступающее инструментом, позволяющим проводить кибератаки в дополнение к обычным военным операциям, занимает довольно второстепенную роль в текущем конфликте. Однако мы можем заметить, что систематически наносятся удары по критически важным телекоммуникационным объектам, необходимым для поддержания подключения к интернету. Сам факт, что

государственный орган может нанести удары по этим объектам вызывает некоторое беспокойство, ведь это может привести к проблемам с координацией. **Интересно также то, как украинцы воспользовались новыми средствами коммуникации, особенно спутниковыми системами - Starlink, для децентрализации контроля над операциями.**

Вероятно, Пакистан вынесет из этой ситуации ценный урок. Также, пакистанские власти начали - правда, с опозданием — модернизацию **системы киберзащиты критически важных инфраструктур, создав Компьютерную группу реагирования на чрезвычайные ситуации – CETR (Cyber Emergency Response Team)** для работы на национальном уровне, а также отраслевые группы - CERT, отвечающие за обеспечение безопасности телекоммуникационных и энергетических инфраструктур ы и банковской системы.

После того, как увеличилось число кибератак, взломов или и случаев использования програм-вымогателей против правительственных информационных систем, власти Пакистана, похоже, решили все-таки начать проводить последовательную политику в области кибербезопасности. **Однако до сих пор в стране нет государственного органа, отвечающего за кибербезопасность гражданских учреждений или за повышение осведомленности в области кибербезопасности.** Существуют механизмы обмена информацией о последних атаках, но они все еще находятся в зачаточном состоянии (Национальный совет по телекоммуникациям и информационной безопасности – NTISB, входящий в состав секретариата премьер-министра, в его полномочия входит предоставление консультаций правительству по вопросам кибербезопасности и по оценке качества ИТ-продуктов, используемых государственными учрежденями). **Целью данного подхода является создание Компьютерной группы реагирования на чрезвычайные ситуации-CERT на** национальном уровне, но помимо этого, можно сказать, что меры по развитию кибербезопасности носят фрагментированный и некоординированный характер. Одним из факторов, который необходимо учитывать в отношении уязвимости общественных деятелей в Пакистане - отсутствие равновесия между гражданской и военной сферами в стране, где армия играет важную роль,

как в плане внешней, так и внутренней обороны. Так как армия Пакистана способна защитить свои сети, учреждения и объекты, которые, по ее мнению, представляют собой насущный интерес для страны, только она в состоянии определять , что является жизненно важным интересом для нации , а значит со стороны государственных учреждений нет прозрачностипо поводу реального состояния кибербезопасности в стране. В целом, все остается очень непрозрачным и на усмотрение армии.

В 2019 году в ежегодной публикации пакистанской армии - *Pak Army Green Book*, констатировался низкий уровень инвестиций в сферу кибербезопасности. В той же публикации ссылаются на отчет Microsoft за 2015 год, в котором отмечается, что Пакистан - это страна, которая подвергается наибольшей опасности от вредоносных программ (с показателем встречаемости вредоносных программ 45,1%, по сравнению со средним мировым показателем 15%). С тех пор вопрос о кибербезопасности начал учитывался при разработке политики национальной безопасности-National Security Policy (2022-2026). Это первый документ такого рода со стороны канцелярии премьер-министра, направленный на определение основных направлений в области национальной безопасности в широком понимании, включая политику по экономическому развитию, внешнюю политику и более традиционные вопросы, связанные с обороной в том числе кибербезопасность. Одним словом, вопросы кибербезопасности были приняты во внимание с опозданием, но сейчас над ними идет активная работа.

Одна из главных задач - обучить достаточное количество квалифицированных специалистов по вопросам кибербезопасности. **Для этого в апреле 2021 года была запущена национальная образовательная программа под названием « Национальный центр кибербезопасности » - National Center for Cyber Security (NCCS), целью которой является подготовка высококвалифицированных специалистов в области кибербезопасности.** Одним из вызовов также является удержание лучших специалистов, в том время, как их часто привлекают более выгодные предложения за рубежом.

Хотя с недавнего времени некоторые сферы находятся под особым контролем, в частности, телекоммуникационные и банковский системы, частные компании теперь подвергаются регулярным проверкам со стороны властей, позволяющим гарантировать определенный уровень безопасности своим клиентам. Это является частью политики кибербезопасности - Cyber Security Policy, документом, опубликованным министерством информационных технологий и телекоммуникаций в 2021 году. (Этот документ вышел вскоре после разоблачения об использовании программного обеспечения – Pegasus для слежки за премьер-министром Имраном Ханом).

***«Интересно также то, как украинцы воспользовались новыми средствами коммуникации, особенно спутниковыми системами - Starlink, для децентрализации контроля над операциями».***

**<u>E. P</u> : Есть ли в Пакистане, как это происходит в России попытки или стремлнения отключиться от мирового интернета? Кроме того, каковы нынешние взаимодействия России и Пакистана и как они влияют на киберсферу ?**

**<u>H.O :</u>** На данном этапе Пакистан не планирует отключаться от глобального интернета. В отличие от соседнего Ирана, в стране доминирует использование международных платформ, в основном американских, и национальный трафик сети по большей части сосредоточивается вокруг них. **Пока власти Пакистана еще не выразили** желания подвергнуть контент тотальному контролю. Тем не менее понятно, что проблемы во взаимодействии с международными платформами из-за **трудностей, возникающих при соблюдении местного законодательства власти воспринимают отрицательно.**

Благодаря DNS-фильтрации у властей Пакистана теперь есть средства для блокировки сайтов, считающихся ими богохульственными, аморальными или антигосударственными. По тем же причинам в стране на протяжении многих лет были заблокированы некоторые

интернет-платформы, например, Youtube. Поэтому пакистанское правительство хотело бы, чтобы платформы открыли свои офисы в Пакистане и подчинялись требованиям управления Телекомуникациями Пакистана - PTA, но пока этого не произошло. Таким образом, отключение от мирового интернета для Пакистана, на данный момент, не является приоритетом, однако контроль за контентом остается целью правительства. Поэтому роль государства, по сути, является регулирующей, но у него нет возможности призвать интернет-провайдеров (ISP), полностью поменять сетевую структуру в Пакистане, чтобы установить над ней контроль. **Однако власти Пакистана так не считают – они пытаются привлечь больше иностранных инвестиций и партнеров и выйти из изоляции.** Вот почему они постепенно налаживают партнерские отношения с Россией. Пакистан хочет иметь разные возможности, так как партнерские отношения в регионе меняются. Учитывая, что США неожидано сблизились с Нью-Дели, у Исламбада больше нет препятствий сблизиться с Москвой. **Более того, пакистанские власти хотят извлечь выгоду из возможной стабилизации ситуации в Афганистане, превратив свою территорию в особый транзитный пункт для стран центральной Азии в направлении индийского океана. Пакистан считает поддержку России необходимой для реализации подобного проекта и для стабилизации ситуации в Афганистане. Для России этот проект представляет интерес с точки зрения поставок углеводородов,, которых стране очень не хватает, а также возможности найти новых партнеров в области технологий и науки**. С другой стороны, на данном этапе эти отношения все еще находятся в самом начале развития и никак не могут сравниться с тесными партнерскими отношениями, которые Исламабад уже давно установил с Китаем, Турцией, Саудовской Аравией и Объединенными Арабскими Эмиратами**.**

**<u>E.P</u> : Каковые могут быть последствия строительства новых дорог на китайском шелковом пути для организации киберпространства в Пакистане? Вы, в частности, совместно с Фредериком Дузе написали главу под названием "Освоение датасферы: цифровые**

**шелковые пути Китая" в недавнем коллективном исследовании. Какие у Вас есть идеи на эту тему?**

**H.O** : Действительно, Китай оказывает значительное влияние на интернет-связь Пакистана. Во-первых, китайские телекоммуникационные компании сделали из Пакистана своей опытной площадкой, начиная с момента, когда их продвижение на международный рынок стало возможным в конце 1990-х - начале 2000-х годов. Телекоммуникационные гиганты, такие как- Huawei и ZTE впервые выбрали пакистанский рынок в качестве своей опытной площадкой, так как страны поддерживают дружеские отношения а затем уже расширять свой бизнес в других странах. Поэтому в Пакистане очень много китайских цифровых компаний, а китайское оборудование активно используется в обеспечении работы системы цифровых сетей, несмотря на присуствие на рынке . Передача навыков и оборудования, необходимого для цифровизации государственных учреждений, также является частью этого процесса , и в Пакистане, как и во многих других странах, сотрудничающих с Китаем, китайские компании способствуют развитию цифровизации. В последней главе нашего исследования мы рассказываем о том, что **Китай, преследуя собственные интересы, хочет создать новую Интернет-систему в Азии, для того чтобы стать региональным центром подключения для передачи данных. По этой же причине они хотять создать точки подключения на границах Китая**. Последняя точка подключения была установлена в Пакистане, возле знаменитого Каракорумского шоссе, создав новый альтернативный маршрут для непосредственного подключения к цифровым сетям между Китаем и его соседями. Таким образом, системы подключения к цифровым сетям в регионе действительно представляется возможной.

# Вопрос киберпространства в Арктике

## Интервью с Селестиной Рабуам об арктическом киберпространстве

**предоставлен Мари Корсель и Морган Кайе**

Селестина Рабуам –– **аспирант Французского института геополитики (IFG Lab) университета Париж 8, также прикрепленная к научно-исследовательскому центру «Геополитика датасферы» (GEODE).** Ее работа посвящена геополитическим вопросам, возникающим в связи с распространением и объединением телекоммуникационных систем в Североамериканской Арктике.

**EurasiaPeace (E.P)**: **Ваше исследование посвящено геополитическим вопросам, возникающим в связи с разрастанием и объединением телекоммуникационных систем в Североамериканской Арктике. Вы работаете над физической сетью в этом регионе мира (наряду с двумя другими слоями интернета, называемыми "логическим" и "контентным") и, в частности, над спутниками LEO. Не могли бы вы рассказать нам немного об этой теме, что заставило вас заинтересоваться ею и уточнить для наших читателей проблематику и ставки такой темы в геополитической области, о которой все чаще говорят? Какова ситуация и что поставлено на карту для Нунавута в этом отношении?**

**Célestine Rabouam (C.P) :** Я начала интересоваться проектами широкополосных созвездий, включив проблемы, связанные с монополизацией низкоорбитальных частотных ресурсов, в свою диссертацию М2, которая была посвящена проекту микропусковой базы на севере Шотландии. Затем **эта исследовательская работа позволила мне поставить**

**вопрос об эволюции отношений власти между субъектами, традиционно участвующими в цифровом развитии слабо связанных территорий, таких как канадская Арктика (т.е. федеральным государством, правительствами территорий и действующими операторами), в контексте прогрессирующей приватизации космической деятельности**.

В то время как технологические достижения позволяют большей части населения планеты полностью интегрироваться в цифровой мир, многие арктические сообщества по-прежнему полагаются на дорогостоящую и часто прерываемую спутниковую связь. В Североамериканской Арктике (Канадская Арктика - Юкон, Северо-Западные территории (СЗТ), Нунавут - и Аляска) территории не имеют одинакового уровня подключения, а внутри территорий наименее населенные и наиболее изолированные общины, как правило, находятся в наиболее неблагоприятном положении с точки зрения доступа к Интернету. **Юг Аляски и Юкон особенно хорошо связаны между собой оптоволоконными кабелями, в то время как многие населенные пункты на северо-востоке СЗТ и все 25 населенных пунктов Нунавута полагаются на спутники для предоставления всех телекоммуникационных услуг**. Отчасти это объясняется характером территорий и характерными для них геофизическими экологическими и климатическими ограничениями (таяние вечной мерзлоты, полярный климат), которые делают сложной установку традиционной цифровой инфраструктуры, такой как кабели. Одним из решений, которого с нетерпением ждали для облегчения этой проблемы, является развертывание низкоорбитальных спутниковых группировок, предназначенных для широкополосного Интернета, таких как Starlink и OneWeb, которые уже несколько месяцев доступны в канадской Арктике и на Аляске.

В своей диссертации я сосредаточилась на североамериканской Арктике, так как это пространство уже несколько лет находится в центре внимания государственных стратегий развития, управления и адаптации, в которых телекоммуникации играют ключевую роль. Эти инициативы в целом направлены на понимание изменения климата - вопроса, который

привлекает внимание как ученых, так и амбиции некоторых государств и частных игроков, которые видят в таянии льдов новые экономические возможности и новые потенциально выгодные морские маршруты.

**Я также решила провести исследование на примере Нунавута, поскольку это единственная канадская территория, связь которой полностью зависит от спутников. Такая ситуация в значительной степени способствует изоляции населения (85% инуитов) и препятствует экономическому развитию и децентрализованному управлению территорией.** Появление созвездия Starlink (SpaceX) на телекоммуникационном рынке Арктики в ноябре 2022 года было долгожданным, поскольку этот новый игрок позволит населению больше не зависеть от традиционных операторов и интернет-провайдеров, но для региональных ассоциаций инуитов Нунавута, которые все больше вовлекаются и берут на себя ответственность за телекоммуникации, монополизация Starlink части рынка также усиливает географическую концентрацию принятия решений и организационной власти на Юге, в то время как они стремятся перенести эти навыки на местный уровень.

**<u>E.P</u> : Арктический регион становится главным предметом конкуренции для крупных держав, таких как США, Россия и Китай, в особенности потому, что таяние льдов разжигает их аппетиты в отношении природных ресурсов, которые можно эксплуатировать, и из-за новых транспортных маршрутов, которые становятся доступными. Но это также связано с растущим военным соперничеством. Это враждебная территория площадью 21 млн км2 с очень низкой плотностью населения (4 млн жителей, включая 500 000 коренных жителей), использование которой потребует применения все более совершенных технологий. Какая инфраструктура уже создана, и какая еще планируются? Каковы основные маршруты межконтинентальных подводных кабелей или оптического волокна? Как используются эти сети и каковы основные киберуязвимости в этой области?**

**C.P :** Действительно, в ряде российских и американских дипломатических и политических выступлений осуждалось возобновление военной активности в Арктике. Однако такое заявление неоднозначное, поскольку **даже если Россия восстановила старые базы и военную технику на своем арктическом побережье, маловероятно, что в этом районе разразится конфликт, учитывая, что китайско-российские амбиции направлены в основном на поиск эксплуатационных ресурсов и адаптации судоходства по Северо-Восточному проходу.**

В североамериканской Арктике Канада приняла план модернизации средств наблюдения, воздушного оружия, инфраструктуры и вспомогательных возможностей на канадских арктических территориях.

Что касается телекоммуникационной инфраструктуры, то международные трансарктические кабельные проекты направлены на обеспечение связи между Европой и Азией путем прокладки волоконно-оптических кабелей вдоль российского арктического побережья на востоке и вдоль побережья Аляски и Канады в Северо-Западном морском проходе.

**Самым передовым проектом кабельной системы является российский проект "Полярный экспресс", который позволит развивать портовую инфраструктуру вдоль Северного морского пути и укрепить арктическую цифровую инфраструктуру России. Прокладка кабеля началась в августе 2021 года, его протяженность составит 12 650 км от Мурманска до Владивостока.**

**На Аляске наиболее передовой кабельный проект ведет компания Квинтиллион (Quintillion), который основан на планах канадского проекта Arctic Fiber, приобретенного американской компанией в 2016 году.** Первоначально проект предполагал прокладку кабеля в нескольких населенных пунктах канадской Арктики, но в 2018 году компания изменила свою стратегию, изменив маршрут кабеля, чтобы соединить его с американской базой в Туле. Компания уже проложила первую часть кабеля на Аляске, но все еще ищет финансирование для завершения следующих этапов разработки кабеля (2. Канадская Арктика - Европа и 3. Аляска - Япония).

Как и Квинтиллион, проект Far North Fiber предполагает использование одного из морских путей Северо-Западного прохода для прокладки трансарктического кабеля, который соединит Японию через Канаду с Финляндией и Норвегией. Кабель будет обслуживать изолированные населенные пункты вдоль Северо-Западного прохода, связь с которыми обычно зависит от спутников, а также позволит в три раза сократить время задержки между финансовыми рынками Японии и Великобритании. Проект осуществляется консорциумом в составе финской компании Cinia, японской компании Arteria, компании Far North Digital из Аляски и компании Alcatel, основного поставщика проекта.

Целью планируемых трансарктических кабелей в Северо-Западного прохода также является повышение устойчивости сетей на территориях, которые иногда полагаются исключительно на спутники для обеспечения надежности и безопасности эксплуатируемых систем. В отличие от кабелей, которые в настоящее время связывают Северную Европу и Азию через Суэцкий канал, морское и подводное сообщение в Северо-Западным проходом гораздо менее оживленное, что потенциально может снизить риск саботажа.

***« даже если Россия восстановила старые базы и военную технику на своем арктическом побережье, маловероятно, что в этом районе разразится конфликт, учитывая, что китайско-российские амбиции направлены в основном на поиск эксплуатационных ресурсов и адаптации судоходства по Северо-Восточному проходу. »***

**E.P : Не могли бы вы описать стратегии, принятые геополитическими державами в Арктике для борьбы с этими различными угрозами? Дания недавно осудила значительный рост кибератак на Гренландию. Россия считает себя ведущей державой в Арктике, а Китай жаждет новых транспортных маршрутов для продолжения своего проекта "Новый шелковый путь". Каковы цели и стратегии этих двух международных держав в регионе и их сильные стороны в киберпространстве?**

**С.Р** : Действительно отмечается рост угроз в арктических стратегиях государств-членов Арктического совета (пяти прибрежных государств - Дании, Норвегии, России, США, Канады - и трех государств, характеризуемых как циркумполярные - Финляндии, Швеции, Исландии), но эти угрозы неоднозначные. **Даже если влияние и присутствие Китая в определенных горнодобывающих и инфраструктурных проектах в канадской Арктике, Гренландии и Исландии регулярно отмечается Соединенными Штатами, в настоящее время они являются предметом почти систематического вмешательства со стороны государств (аэропорты городов Нуук и Илулиссат в 2019 году, золотой рудник Хоуп-Бей, Нунавут, в 2020 году).** В рамках проекта "Новый шелковый путь" полярные направления в стратегии Китая базируются на сотрудничестве с Россией для освоения и дальнейшей эксплуатации минеральных и углеводородных ресурсов, а также связанных с ними коммерческих морских перевозок.

В области кибербезопасности компании и крупные государственные структуры в канадской Арктике, на Аляске и в Гренландии действительно все чаще становятся мишенью кибератак, но эта тенденция не ограничивается арктическими территориями и подтверждается в других странах мира. Насколько мне известно, атаки на медицинские службы в Гренландии и на Аляске не привели к обвинениям, направленным непосредственно против государства, хотя в случае с Аляской в 2021 году администрация утверждала, что злоумышленников спонсировало иностранное правительство.

**Е.Р : Каковы стратегии, активы и международное сотрудничество Канады в киберсфере? И каковы ее уязвимые места? Мы слышали о политике влияния Китая на Канаду... или о его политике развития спутниковой сети на севере своей территории, оставляя в стороне крупные трансарктические проекты... Канада, похоже, оказалась между амбициями США (как показывает стратегия "Северная звезда"), а также Китая и России в этом регионе. Как она справляется с этим положением?**

**С.Р** : **Канада является членом альянса "Пять глаз" (FVEY) и поэтому пользуется преимуществами**

**сотрудничества между различными разведывательными службами и службами США, Австралии, Новой Зеландии и Великобритании. Такое партнерство имеет огромное стратегическое значение для этих государств, поскольку позволяет им принимать совместные решения и действовать сообща, будь то применение кибератак или решение о запрете определенных иностранных игроков на своих национальных рынках, как это было в случае с компанией Huawei.** В 2018 году Австралия, а далее США и Новая Зеландия приняли решение о запрете оборудования Huawei и ZTE в своих национальных сетях, а в 2020 году к ним присоединилась Великобритания. Эти государства утверждают, что существует риск шпионажа со стороны китайских компаний, которые с 2017 года, руководствуясь статьями 7 и 10 Закона о национальной разведке, потенциально обязывают китайские компании передавать информацию национальным спецслужбам даже при работе за рубежом. **Решение Канады о запрете оборудования ZTE и Huawei было принято позже, в мае 2022 года, после нескольких предупреждений со стороны США и союзников по альянсу "Пять глаза" о последствиях, которые партнерство с Huawei может создать для Канады**. Одна из причин, по которой либеральному правительству премьер-министра Джастина Трюдо понадобилось время, чтобы изучить этот вопрос и заблокировать ZTE и Huawei в канадских сетях, связанна с тем, что телекоммуникационный рынок Канады в сельской местности и Арктике очень неконкурентоспособен, в то время как недорогое оборудование 3G/4G компании Huawei используется во многих мобильных сетях.

Канада всегда полагалась на спутники и своего национального оператора Telesat для связи с изолированным населением Арктики. Компания все еще пытается получить инвестиции для своей группировки Lightspeed, но рассчитывает на 1,44 миллиарда долларов от федерального правительства, чтобы продолжить свой проект, несмотря на неопределенность, которая отягощает ее финансы, и значительные задержки, которые испытывает проект (запуск перенесен на 2026 год). В отличие от Starlink, который продает свои услуги непосредственно потребителям, группировки Lightspeed и

OneWeb позиционируются как традиционные спутниковые операторы, продавая свою пропускную способность уже существующим на рынке интернет-провайдерам. Однако группировки OneWeb и Starlink работают в канадской Арктике уже несколько месяцев, и многие пользователи на Крайнем Севере теперь сомневаются в реальной пользе этого проекта, основной целью которого было подключение сельского и арктического населения Канады к услугам широкополосного Интернета.

***« Канада является членом альянса "Пять глаз" (FVEY) и поэтому пользуется преимуществами сотрудничества между различными разведывательными службами и службами США, Австралии, Новой Зеландии и Великобритании. Такое партнерство имеет огромное стратегическое значение для этих государств, поскольку позволяет им принимать совместные решения и действовать сообща, будь то применение кибератак или решение о запрете определенных иностранных игроков на своих национальных рынках, как это было в случае с компанией Huawei. »***

**<u>E.P</u> : С начала войны на Украине и напряженности в Балтийском море переговоры и сотрудничество между прибрежными странами, граничащими с Арктическим советом (основанным в 1996 году) были приостановлены, так как носили в основном экологический характер. Какая правовая система действует в этой области в настоящее время (использование проливов, территориальный суверенитет на море, эксплуатация ресурсов и т.д.) и в чем заключаются ее недостатки? Какие территориальные конфликты существуют между прибрежными странами? Есть ли необходимость в новом форуме для обсуждения и законодательных дебатов?**

**<u>C.P:</u> Арктический совет - это международная организация, не имеющая обязательной юридической силы, которая в первую очередь занимается экологическими, экономическими и социальными**

**аспектами устойчивого развития в регионе. Военные вопросы оставались за пределами их компетенций, хоть и вторжение России в Украину в значительной степени поставило под сомнение "миф об арктической исключительности", согласно которому сотрудничество между арктическими государствами никогда не будет нарушено внешними конфликтами.** Публикация в марте 2022 года совместного заявления, осуждающего вторжение и подписанного всеми странами-членами Арктического совета (кроме России), отмечает этот переломный момент в Арктике, поскольку деятельность совета была приостановлена до июня 2022 года. С тех пор Совет возобновил некоторые мероприятия, не затрагивающие Россию, но в "ограниченном" режиме, что парализует сотрудничество между арктическими государствами по многим вопросам.

**Конвенция ООН по морскому праву (1982) заложила основу международной правовой базы в Арктике, выделив каждой стране исключительной экономической зоны (ИЭЗ) в 200 морских миль (360 км) от ее береговой линии и установив процедуры для государств по утверждению экономического суверенитета над континентальными шельфами.** В частности, конвенция позволяет арктическим государствам сохранять суверенитет над экономической деятельностью в пределах своих ИЭЗ, разрешая свободное движение судов и предусматривая возможность для государств подать заявку на расширение своих ИЭЗ до 350 мм, доказав расширение национальной территории под водой. Таким образом, большая часть Северного Ледовитого океана находится под исключительным экономическим контролем прибрежных стран, поскольку никто не оспаривает принцип ИЭЗ.

Между арктическими государствами все еще существуют разногласия по поводу точного разграничения их ИЭЗ (например, между Канадой и Гренландией по поводу острова Ханс) или правового статуса некоторых морских проходов**. Например, вопрос о правовом статусе Северо-Западного прохода по-прежнему вызывает противостояние Канады и США, и прокладка американскими компаниями (Quintillion или Far North Fiber) кабеля по дну этого прохода может возродить этот скрытый конфликт 1970-х годов.** С точки зрения юридической интерпретации Канада считает Северо-

Западный проход частью своих внутренних вод, в то время как США рассматривают его как международный пролив, соединяющий Атлантический и Тихий океаны, где действуют принципы свободы судоходства. Хотя в 1988 году между двумя соседними государствами было заключено Соглашение об арктическом сотрудничестве, оно не является постоянным решением, а лишь инструментом для ограничения напряженности в этой области.

**Конвенция по морскому праву 1982 года, которая не была ратифицирована США, признает свободу прокладки кабелей в открытом море, но подчеркивает, что она должна уважать законы прибрежных государств, а также меры по защите окружающей среды, которые применяются к прокладке подводных кабелей. В этой Конвенции правовой статус подводных кабелей в ледовитом океане рассматривается как "lex specialis", в статье 234, которая дает прибрежным государствам право принимать (без какой либо дискриминации) законы для предотвращения и снижения риска загрязнения в пределах своей исключительной экономической зоны (ИЭЗ).** Данная статья позволяет прибрежным государствам устанавливать более высокие стандарты по предотвращению, сокращению и контролю загрязнения морской среды, чем те, которые приняты во всем мире. Эти стандарты применяются к загрязнению моря "с судов" и относятся к кабелеукладочным судам во время их операций по прокладке, ремонту и отслеживания кабеля.

**При поддержке Канады и России во время переговоров по Конвенции Монтего-Бей, статья 234 придает юридическую силу принятию национальных норм, касающихся морских перевозок в Арктике, и в то же время оправдывает канадскую интерпретацию Северо-Западного прохода.** В действительности, статья оставляет большой простор для интерпретации и дает повод для одностороннего применения национальных законов прибрежных государств в отношении судов, работающих в Арктике. В 1970 году Канада приняла Закон о предотвращении загрязнения арктических вод, который определяет, что арктические воды являются частью 100-мильной зоны предотвращения загрязнения, и устанавливает строгие требования к строительству или

навигационному оборудованию. В 2010 году Канада также ввела обязательное судовое сообщение в соответствии с Положением о зоне обслуживания движения судов в Северной Канаде. Эти правила распространяются на ИЭЗ Канады, а также на Арктический архипелаг и 7 маршрутов PNO. Перед проходом судна необходимо получить разрешение на движение, а отчеты должны подаваться в Центр морской связи и обслуживания движения Канадской береговой охраны до и после прохода судна. Несмотря на эти усилия, заявленная Канадой функциональная юрисдикция над ПНО не признается Соединенными Штатами, и сохраняется правовая неопределенность в отношении применения статьи 234 Конвенции 1982 года. **Отказ Соединенных Штатов и Европейского Союза объявить Канаду суверенной страной над Северо-Западным проходом основан, прежде всего, на опасении создания юридического прецедента для других государств, претендующих на юрисдикцию над международными проливами**.

В то время как этот интерпретационный спор между Канадой и США был предметом статус-кво, изменение климата, вероятное увеличение морских перевозок через проход и проекты по прокладке волоконно-оптического кабеля, скорее всего, возобновят дискуссии между двумя государствами относительно статуса Северо-Западного прохода. Судя по информации, которую мне удалось собрать во время моей исследовательской работы в Канаде прошлым летом, эти дискуссии, скорее всего, приведут к сотрудничеству между двумя государствами, а не к конфронтации.

***« Например, вопрос о правовом статусе Северо-Западного прохода по-прежнему вызывает противостояние Канады и США, и прокладка американскими компаниями (Quintillion или Far North Fiber) кабеля по дну этого прохода может возродить этот скрытый конфликт 1970-х годов. »***

**<u>E.P</u> : Существуют ли планы по ограничению размещения оружия в данном регионе, который является контактным пунктом между США и Россией, в рамках международного права? Можно ли представить**

**сотрудничество между различными государствами, граничащими с Арктикой, в этой области?**

**С.Р** : Насколько мне известно, международно-правовые рамки не накладывают ограничений и не направлены ограничивать размещение оружия в этом пространстве. На самом деле существуют другие формы военного сотрудничества между некоторыми прибрежными и приполярными государствами вне Арктического совета, но такое сотрудничество не касается всех арктических государств и следует традиционной логике альянсов (например, США/Канада).

**Е.Р : Позволил ли доступ к Интернету различным коренным народам региона выработать гражданскую и политическую позицию в этих вопросах? Является ли эти народы объектом иных форм дезинформации?**

**С.Р**: В Канаде в ряде исследований подчеркивается, что уровень доступа и участия в цифровом мире для коренных народов ниже среднего, и этот разрыв еще больше для этнической группы инуитов в канадской Арктики. Поэтому в выступлениях и программах, связанных с цифровым равенством в Канаде, вопросы, касающиеся коренного населения, регулярно освещаются государством или компаниями, которые обеспечивают связь с коренным населением. Доступ к цифровым ресурсам рассматривается не только как всеобщая потребность, но и как политический инструмент для удовлетворения конкретных потребностей коренных общин. Это привело к росту инициатив, направленных на устранение этого разрыва, таких как создание программ и техническое обучение для коренных народов и для частного сектора, как например NorthwesTel (крупнейший интернет-провайдер на севере).

**Тем не менее, необходимо отметить, что инуитские общины были вовлечены в цифровое развитие территории на очень ранней стадии, во время переговоров с федеральными властями, что привело к официальному учреждению территории в 1999 году.** В канадской Арктике также есть немало деятелей, таких как Адами Иторчеак в Нунавуте, которые сыграли важную роль в реализации первых местных инициатив по подключению общин к Интернету.

В настоящее время два интернет-провайдера - SSi Micro и NorthwesTel - делят телекоммуникационный рынок в Нунавуте, а NorthwesTel также является ведущим интернет-провайдером в Юконе и Северо-Западных территориях. В последние годы в Канаде значительно возросло количество инициатив, направленных на удовлетворение цифровых потребностей коренных общин. Эти инициативы включают в себя предоставление общинам возможности владеть собственной телекоммуникационной инфраструктурой, чтобы по-настоящему участвовать в принятии решений и организации цифровых технологий. Например, **этим летом компания NorthwesTel продала часть своей инфраструктуры в Юконе концерну из 13 «Первых наций», что было расценено как первый и очень важный шаг частной компании по удовлетворению цифровых потребностей коренных народов Крайнего Севера Канады.**

## Заключение

Если раньше часть человечества еще могла ориентироваться в биполярном устройстве мира, между, грубо говоря, коммунистическими икапиталистическими державами, то теперь появились опасные проблемы, такие, как новые киберуязвимости. Все больше и больше встает вопрос о статусе правдивой информации, и о возможности рассуждать логически в нынешнем мире, который стал легко управляем различными интересами и эмоциями.

Предположим, что строго правовой и защитной реакции Европейского Союза будет недостаточно, чтобы выявить и спроецировать альтернативу в формирующемся многополярном мире. Пространство для диалога, взаимопоимания и международных переговоров еще должно развиваться...

Цель EurasiaPeace в этом досье -

дать ключи к общему пониманию кибервопросов в и предоставить слово профессионалам и исследователям, чтобы осветить различные актуальные вопросы, а также

определить долгосрочные направления для размышлений над этими вопросами, позволив при этом каждому читателю прийти к своему собственному мнению и использовать это досье как почву для размышлений.

Мы надеемся что эта работа частично увенчится успехом, и будем рады прислушаться к вашей критике...