

ВРАГИ ИНТЕРНЕТА - 2013

В честь Международного дня против цензуры в Интернете 12 марта “Репортеры без границ” публикуют “Специальный доклад о сетевом мониторинге”, с которым вы можете ознакомиться на сайте surveillance.rsf.org. Благодаря технологиям вмешательства в информационные системы и перехвата сообщений, государства продолжают арестовывать все больше журналистов, гражданских активистов и инакомыслящих. На 12 марта 2013 года уже около 180 кибер-активистов остаются за решеткой за их информационную деятельность в Интернете.

Для версии доклада 2013 года организация “Репортеры без границ” создала список из пяти стран-врагов Интернета, в который попали государства, систематически контролирующие Интернет и серьезно нарушающие права человека. Сирия, Китай, Иран, Бахрейн и Вьетнам оцениваются организацией как самые активные “шпионы”, все возрастающие усилия которых по контролю за Интернетом направлены против инакомыслящих. Кибер-атаки и вторжения принимают массовый характер, в частности отправка вредоносного программного обеспечения оппозиционерам и их коллегам. Так называемый “Великий китайский файрвол” - это, возможно, самая совершенная система в мире, которая усиливает войну против анонимных сетей и подключает частные веб-компании к слежке за пользователями. Иранский режим сделал еще один шаг к надзору за Интернетом: эта страна развернула собственную глобальную сеть “Интернет Halal”. Что касается Сирии, “Репортеры без границ” получили доступ к **секретному документу**, объявлению 1999 года о тендере Сирийского общества телекоммуникации (STE). Этот документ показывает, что сирийская Интернет-сеть была создана с учетом возможности фильтрации контента и слежки за пользователями.

Авторитарные страны не могли бы шпионить за своими гражданами без передовых технологий. Впервые организация публикует список из пяти компаний-врагов Интернета, “наемников цифровой эры”: Gamma, Trovicor, Hacking Team, Amesys и Blue Coat. Их продукция, инструменты “оптимизации сетей или борьбы с преступностью” использовались или все еще используются властями репрессивных стран для ограничения свободы информации, что нарушает права человека. Программы слежки и перехвата информации компании Trovicor позволили королевской семье Бахрейна шпионить за журналистами и интернет-активистами и задерживать их. В Сирии продукты DPI (углубленная проверка протоколов, технология проверки и фильтрации Интернета), разработанные Blue Coat, помогли режиму шпионить за инакомыслящими и интернет-активистами по всей стране, а после арестовывать и пытаться их. Программы Eagle компании Amesys обнаружили в штабе секретной полиции Муаммара Каддафи. Вредоносное программное обеспечение, созданное компаниями HackingTeam или Gamma, позволили властям заполучить пароли журналистов и интернет-активистов.

“Онлайн-слежка представляет собой все возрастающую опасность для журналистов, гражданских журналистов, блоггеров и правозащитников. Режимы, которые пытаются контролировать информацию, больше не прибегают к прямой блокировке информации, которую легко обойти, и которая неблагоприятно сказывается на имидже государства. Они все чаще предпочитают действовать незаметно, используя тонкую цензуру и слежку за пользователями помимо их воли”, - сожалеет Кристоф Делуар, генеральный секретарь “Репортеров без границ”.

*“Серьезные нарушения прав человека возможны лишь при использовании репрессивными режимами программ и технологий слежки, поставляемые предприятиями, которые базируются в демократических странах. Поэтому самое время лидерам этих стран, которые официально порицают покушения на свободу выражения в Интернете, принять действенные меры, в частности поставить под **серьезный контроль экспорт цифрового оружия** в страны, которые пренебрегают фундаментальными правами”, - советует он.*

Переговоры между странами уже имели место, например Вассенаарские соглашения, заключенные в 1996 году, которые поощряют “прозрачность и большую ответственность в распространении обычных вооружений и товаров и технологий двойного применения, чтобы предотвратить опасное скопление”. Этот договор объединяет 40 стран, в числе которых Франция, Германия, Великобритания и США.

События арабской весны в ряде стран, которые подтвердили огромную роль веб-информации, также убедили репрессивные государства в необходимости контроля данных и цифровых коммуникаций. Некоторые демократии тоже постепенно очаровываются идеями о том, что кибер-безопасность и слежка за интернет-пользователями необходимы любой ценой. В этом убеждают многочисленные законы и инициативы, которые теоретически смогут ограничивать свободу: FISAA и CISPA в США, *British Communications Data Bill* в Великобритании, *Wetgeving bestrijding cybercrime* в Нидерландах.

Чтобы помочь всем, кто работает с информацией, избавиться от все более активной и навязчивой слежки, “Репортеры без границ” предоставляют доступ к “набору для выживания в сети” на сайте WeFightCensorship.org.

REPORTERS WITHOUT BORDERS

<https://e.mail.ru/cgi-bin/msglist#readmsg?id=13630719180000000042&folder=0>