Информационный Бюллетень CSRC #1

Публикуем первый выпуск нерегулярного бюллетеня ресурсного центра. **csrc.link/ru**

Международная координация против целенаправленной слежки

Мы – анархисты. Мы верим в международную координацию неформальных анархистских групп для продолжения борьбы против всех форм господства. Мы считаем, что обмен знаниями о возможностях и тактике наших врагов должен быть важной частью этой координации. Эти знания – не самоцель, а средство для того, чтобы уменьшить наши шансы быть пойманными, чтобы мы могли продолжать атаковать.

Наши враги обладают большими возможностями и отточенной тактикой. На их стороне полиция и судебная система, ученые и технократы, а в некоторых случаях и поддержка населения. Они контролируют огромные инфраструктурные сети. У них бесконечная память, архивы и базы данных ДНК.

На нашей стороне неформальный и децентрализованный характер наших организаций, тень, в которой можно спрятаться, и солидарность, позволяющая помогать друг другу в трудные времена, продолжать борьбу товарищей, которые больше не могут этого делать.

“Несмотря ни на что, мы совершаем и будем совершать ошибки в борьбе с такими сильными репрессивными механизмами. Ошибки, которые всегда будут “стоить” дороже по сравнению с ошибками полицейских, которые “списываются”. Мы должны еще раз взвесить ситуацию и убедиться, что ошибки, которые произошли однажды, просто не могут повториться. Мы должны изучить и оценить накопленный за многие годы опыт и, принимая во внимание существующую тенденцию готовиться к битвам, которые уже были, а не к тем, которые будут, давайте будем готовы, и пусть удача будет на нашей стороне.”

—товарищи-анархисты из Греции, текст с подробным описанием слежки, которая привела к их арестам, 2013 год

Наши враги уже организованы на международном уровне; они обмениваются информацией, тактикой, технологическими и научными разработками. Это прискорбно, но это также означает, что сообщение товарищей в одной стране – скажем, о хорошем способе борьбы со следами ДНК, или о жучке, найденном в сквоте, или о дешевом средстве для уничтожения полицейских дронов – может помочь другим в любой другой точке мира.

Безусловно, не все следует выкладывать в открытый доступ. Иногда информация, до сих пор неизвестная нашим врагам, должна оставаться в тайне, исходя из определенной стратегии или плана. Но в остальном: давайте делиться знаниями и опытом и самоорганизовываться!

База, на которой можно стоять: различие между OpSec и культурой безопасности

Иногда родственные термины становятся синонимами, и иногда это вполне нормально. В английском языке их полно, например, “amazing” и “awesome” – оттенки значений здесь не важны.

Однако иногда, если разница между терминами теряется, мы теряем и полезную часть смысла. Оперативная безопасность (OpSec) и культура безопасности – два термина, которые

Объявляем: создана Библиотека угроз

Цель недавно выпущенной Библиотеки угроз Ресурсного центра против целенаправленной слежки проста: изучить набор репрессивных методов государства, чтобы лучше их обходить. Библиотека документирует два десятка различных полицейских методов, разделяя их на три тактики (сдерживание (deterrance), уличение(incrimination) и арест (arrest)) и предлагая потенциальные противоядия (mitigation), то есть способы уменьшения ущерба, для каждого из них. В книге также приводятся ссылки на конкретные репрессивные операции, проведенные государством против анархистов за последние несколько десятилетий.

Библиотека угроз призвана помочь вам в моделировании угроз – процессе, в ходе которого вы пытаетесь понять, какие меры государство может предпринять против вас, чтобы вы могли подготовиться к ним. Это упражнение лучше всего выполнять совместно с товарищами, с которыми вы работаете над конкретным проектом. Хорошее моделирование угроз может превратить страх или паранойю в мужество, поскольку дает нам конкретное представление о том, с чем мы сталкиваемся, чтобы мы могли принять меры предосторожности. Другими словами, это помогает нам принять решение о соответствующей оперативной безопасности (OpSec). CSRC предлагает использовать библиотеку угроз для составления “деревьев атак”. “Деревья атак – это инструмент для содействия коллективному мозговому штурму различных способов, которыми противник может успешно атаковать вас в данном контексте, путем представления атак в виде структуры в форме дерева”. Пошаговое руководство по их использованию см. в учебнике “Библиотека угроз”.

Библиотека угроз также может использоваться для навигации по ресурсам, не относящимся к моделированию угроз. Предположим, что анархисты в моем районе столкнулись с использованием агентов и информаторов для разрушения нашей организации. На вкладке “Incrimination” я выбираю “Infiltrators” (агенты). В записи, состоящей не более чем из 300 слов, перечислены пять основных типов агентов и предложены три возможных способа борьбы с ними (нападение, принцип “нужно знать” и упражнение с сетевой картой). Если я нажму на кнопку “Infiltrators topic”, мне откроется список из 27 текстов, написанных анархистами об агентах в их сетях. Мой страх перед агентами ослабляется благодаря знанию того, какие конкретные признаки следует искать, и некоторым практическим инструментам для укрепления моих сетей доверия.

Библиотека угроз, в которой представлены самые разные темы: от стука в дверь до обысков и судебной экспертизы, стремится быть исчерпывающей, но при этом оставаться краткой и понятной. У CSRC есть огромное количество информации о репрессиях и о том, как с ними бороться, и “Библиотека угроз” обобщает и сортирует ее для вас, чтобы она была практичной и в ней было легко разобраться. Библиотека угроз также доступна в формате zine для легкого чтения и распространения.

Может быть, вы считаете, что вам не хватает какого-то метода, противоядия или информации о репрессивной операции? Хотели бы вы отредактировать один из тех методов, которые уже перечислены? Чтобы добавить, улучшить, дать критику или отзыв на Библиотеку угроз, свяжитесь с нами по адресу csrc@riseup.net.

имеют схожие, но разные значения, и оба являются необходимыми частями анархистской практики безопасности против репрессий.

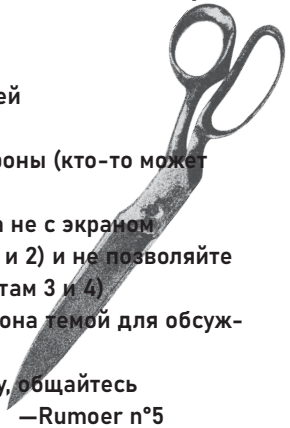
OpSec относится к конкретным практикам, используемым для того, чтобы не быть пойманным за определенное действие или проект. Некоторые практики OpSec включают в себя ношение перчаток и масок, использование другой обуви, меры по предотвращению оставления ДНК, одежду черного блока, использование Tails для анонимного доступа в Интернет и так далее. OpSec находится на уровне акции или проекта. Этим практикам можно обучить, но в конечном итоге только люди, выполняющие конкретный проект вместе, должны договориться о том, какие практики OpSec использовать.
Цитата из текста "Confidence Courage Connection Trust"[1] (Уверенность. Храбрость. Связь. Доверие): "Культура безопасности относится к набору практик, разработанных для оценки рисков, контроля потока информации через ваши сети и построения прочных организационных связей". Культура безопасности возникает на уровне отношений или сети. Чтобы эти практики были эффективными, их необходимо распространять как можно шире.

На первый взгляд, OpSec может показаться более важной. Если у нас есть практики, необходимые для обеспечения безопасности, то какая разница, что делают другие люди в нашей среде? Многие анархисты (вполне обоснованно) скептически относятся к окружению и не считают себя связанными или зависимыми от людей, с которыми они не имеют близкой связи. Много энергии в анархистском пространстве уходит на совершенствование OpSec, что кажется уместным, поскольку, если вы хотите предпринять наступательные действия, предпочтительнее не попасться. Однако культура безопасности также важна, и хороший OpSec не заменит ее. Она обеспечивает социальный контекст – основу, на которой строится вся наша деятельность. Потому что, нравится нам это или нет, мы все встроены в сети, и цена полной изоляции от них высока. Без стабильной базы гораздо труднее предпринимать безопасные действия.

Авторы статьи "Уверенность. Храбрость.Связь. Доверие" пишут, что культура безопасности – это не закрытость, а поиск способов безопасно оставаться открытым для связей с другими людьми. Она предполагает честные разговоры о рисках и установление некоторых базовых норм с более широким кругом людей, чем те, с кем мы собираемся действовать. Культура безопасности не статична – это не просто набор правил, которые должны знать люди из "радикальных" субкультур. Она должна быть динамичной, основанной на постоянных разговорах и нашем лучшем анализе текущих моделей репрессий.

Такие методы, как поручительство, проверка связей в социальных сетях и проверка биографии, могут показаться OpSec и могут быть важной частью планирования определенных действий, но они являются результатом культуры безопасности. Культура безопасности подразумевает вопрос: "Что нужно сделать, чтобы я вам доверял?". Это не означает, что вы должны поручиться за каждого, кого вы знаете, или что вы не проводите время с людьми, за которых вы не поручились, просто вы должны четко знать, кому вы доверяете, что и почему, и что у вас есть механизмы для обучения безопасному доверию новым людям. Никакое количество хороших привычек о том, как говорить о действиях, происходящих в вашем городе (культура безопасности), не защитит вас, если вы оставите ДНК на месте преступления (OpSec), и никакое количество обнаружения физического наблюдения (OpSec) не защитит вас от полицейского под прикрытием, который подружился с вашим соседом, чтобы подобраться к вам (культура безопасности). Практика OpSec и культура безопасности отличаются друг от друга, и одно не заменяет другое. Развивая более глубокое понимание обеих структур, мы можем попытаться уберечь себя и друг друга от тюрьмы, продолжая строить связи и расширять неформальные дружеские связи.

Десять советов по уничтожению телефонов



1. сожгите свой телефон
2. бросьте телефон в канал
3. соожгите телефоны своих друзей
4. бросьте все телефоны в канал
5. не всегда берите с собой телефоны (кто-то может бросить его в огонь)
6. разговаривайте друг с другом, а не с экраном
7. уничтожайте улики (к советам 1 и 2) и не позволяйте другим создавать улики (к советам 3 и 4)
8. сделайте использование телефона темой для обсуждения
9. будьте недоступны по телефону, общайтесь
10. к черту технологии

—Rumoer n°5

1. csrc.link/#confidence-courage-connection-trust

Коротко против слежки

В этом разделе мы хотели бы поделиться короткими заметками, которые относятся к сфере деятельности CSRC, но не заслуживают отдельной записи на сайте. Вы можете присылать нам такие заметки, если хотите, чтобы они были опубликованы в следующем выпуске.

- В 2021 году несколько человек были арестованы во Франции после поджога автомобилей, принадлежащих компании Enedis (ответственной за управление сетью распределения электроэнергии во Франции), и важной ретрансляционной антенны. В тексте на французском языке подробно описывается интересный спектр методов слежки, которые предшествовали их арестам: слежка, взятие ДНК с ручки автомобиля, пока его владелец ходил по магазинам, проникновение ночью в дом, чтобы установить кейлоггер на компьютер, просьба к Enedis предоставить список людей, отказавшихся от установки нового "умного" счетчика электроэнергии, который они устанавливают повсеместно, и просьба к местному журналу предоставить IP-адреса, которые получили доступ к их статье о поджоге.
- В 2022 году два анархиста были арестованы в Италии и обвинены в изготовлении и хранении взрывчатых веществ. В тексте объясняется, что расследование, приведшее к арестам, началось с того, что в июне 2021 года "неизвестный человек" нашел в лесу взрывчатые вещества, электроматериалы и другие устройства. После этого полицейские установили фото- и видеоловушки, чтобы "поймать" любого, кто приблизится к этому месту. Впоследствии один человек был сфотографирован со спины неподалеку от этого места, и полиция впоследствии якобы узнала и опознала его.
- В заключение этого раздела приведем обнадеживающую цитату из коммюнике, взявшего на себя ответственность за поджог офиса по строительству тюрем в Германии: "Чтобы не создавать хороших снимков на камерах наблюдения, мы носили дождевые пончо, чтобы замаскировать форму тела и походку. Чтобы сделать форму головы неузнаваемой, мы использовали шляпы". ейчас многих товарищей беспокоит дальнейшее развитие возможностей видеоанализа. Мы же хотим показать возможности противостояния этой технике слежки."

Внесите свой вклад в CSRC !

Мы предлагаем использовать сайт CSRC для обмена между товарищами знаниями и опытом по теме целенаправленного наблюдения. Просмотрите наши 180+ ресурсов на сайте csrc.link, который также доступен в браузере Tor через адрес .onion. Распечатайте наши новые наклейки и распространите их. Внесите свой вклад, отправив нам письмо по адресу csrc@riseup.net – если вы хотите шифроваться, наш ключ PGP находится здесь.