ICANN81 | AGM – Совместное заседание: GAC и SSAC
Воскресенье, 10 ноября 2024 года - 16:30 - 17:30 TRT

JULIA CHARVOLEN: Здравствуйте и добро пожаловать на заседание GAC и SSAC. Меня зовут Джулия Чарволен (Julia Charvolen) из группы поддержки ICANN в GAC. Пожалуйста, обратите внимание, что эта сессия записывается и регулируется Ожидаемыми стандартами поведения ICANN и Политикой сообщества ICANN по борьбе с домогательствами.

Во время сессии вопросы и комментарии будут зачитываться вслух, если они будут представлены в чате. Устный перевод на этом заседании будет осуществляться на шесть языков ООН и португальский язык. Если вы хотите выступить на этой сессии, пожалуйста, поднимите руку в комнате Zoom. Пожалуйста, назовите свое имя или язык, на котором вы будете говорить, если это не английский, и не забывайте говорить в разумном темпе. Сейчас я передам слово Найджелу Хиксону (Nigel Hickson). Найджел, пожалуйста, передаю вам слово.

NIGEL HICKSON: Здравствуйте, добрый день. Сегодня вы уже достаточно наслушались моего голоса, не так ли? Так что на этой сессии вы его больше не услышите. И я обещаю, что завтра буду вести себя тише. Итак, Нико приносит свои извинения. Ему пришлось

присутствовать на заседании Правления ICANN. Но мне, на самом деле, нечего больше сказать. Как вы можете видеть, соотношение GAC и SSAC такое, каким оно должно быть. И нет, эта сессия – сессия SSAC.

Мы очень рады возможности провести брифинг с их участием. За эти годы они проделали огромную работу, способствующую эффективному управлению ICANN. И я уверен, что вам будет очень интересно узнать, что они скажут. Итак, все, что я собираюсь сделать на данный момент, я имею в виду, что я буду модерировать вопросы и аргументы позже. Но сейчас мне остается только передать слово Раму.

RAM MOHAN: Большое спасибо. И спасибо за приглашение SSAC встретиться с вами здесь, в GAC. Мне всегда приятно быть с вами. Меня зовут Рам Мохан (Ram Mohan). Я являюсь председателем SSAC. Прежде чем приступить к повестке дня, позвольте мне также обратиться к моим коллегам, которые собрались здесь, и попросить их уделить минутку, чтобы представиться. Все они являются членами SSAC. И вы сможете убедиться в разнообразии знаний, опыта и квалификации присутствующих. Давайте начнем справа от меня.

ROD RASMUSSEN: Род Расмуссен (Rod Rasmussen).

MERIKE KAEO: Мерике Каео (Merike Kaeo).

GREG AARON: Грег Аарон (Greg Aaron).

ROBERT GUERRA: Роберт Гэрра (Robert Guerra).

WARREN KUMARI: Уоррен Кумари (Warren Kumari).

JOHN LEVINE: Джон Левин (John Levine).

STEVE CROCKER: Стив Крокер (Steve Crocker).

TARA WHALEN: Тара Уолен (Tara Whalen), заместитель председателя SSAC.

BARRY LEIBA: Барри Лейба (Barry Leiba). И я стараюсь, но у Уоррена шляпа лучше.

SUZANNE WOOLF: Сюзанн Вульф (Suzanne Woolf), которая иногда носит слишком много шляп, SSAC.

RAM MOHAN: Спасибо, Сюзанн. И еще несколько членов, которых я вижу сзади. Вы увидите их поднятые руки. Они также присутствуют в зале, чтобы быть с нами на этой сессии. Наджман, спасибо, что пригласили нас сюда. Гейб, вы не подняли рук. Вы должны поднять руку. Давайте . Спасибо, что пригласили нас сюда. Мы решили, что сначала, учитывая, что не все из вас видели нас раньше, мы потратим пару минут на то, чтобы представиться, кто мы и чем занимаемся, а затем перейдем к остальным темам.

Если посмотреть на миссию самой ICANN, то она достаточно ясна. SSAC учрежден непосредственно в соответствии с миссией ICANN. Таким образом, мы являемся Консультативным комитетом, так же как и вы являетесь Консультативным комитетом. И у нас нет формальной власти, если хотите, внутри структуры ICANN. Нам это нам нравится, потому что тогда наши рекомендации должны жить и умирать по собственным достоинствам, а не по наличию или отсутствию права голоса, верно? Так что мы такие.

В наш состав входят представители всех стран мира или, по крайней мере, большинства стран мира. Мы идем по пути увеличения разнообразия членов во всех отношениях, которые вы измеряете разнообразием. Только в этом году мы добавили девять новых членов. И из этих девяти новых членов нам очень приятно видеть, что двое из них приехали из Африки, а также из других частей света. Но основная причина, по которой люди попадают в SSAC, отбираются в SSAC, заключается в том, что они обладают конкретным и, как правило, глубоким опытом в той

области, в которой они специализируются. Большинство людей в SSAC являются техническими экспертами.

У них самый разный опыт. У нас есть люди, которые занимаются различными областями системы идентификации Интернета. В основном мы опираемся именно на них. Но большая часть знаний и опыта остается внутри SSAC. И причина этого в том, что мы в первую очередь занимаемся предоставлением технических консультаций сообществу, которое мы обслуживаем, верно? Поэтому мы стараемся, чтобы на борту было много технических специалистов. Спасибо.

Это руководящая группа SSAC. Слева от меня и справа от вас вы увидите членов, которые были выбраны в руководящую группу. Вы также видите сотрудников службы поддержки политики. И я хочу воспользоваться моментом, чтобы упомянуть об этом. В отличие от многих других подразделений ICANN, где персонал поддержки в конечном итоге играет вспомогательную роль, в SSAC вы посмотрите на людей, которые здесь перечислены, например, Стив Ченг (Steve Cheng), другие люди, которые здесь присутствуют, являются высококвалифицированными экспертами в своем собственном праве.

В итоге они участвуют в наших дискуссиях, вносят свой вклад и делают больше, чем просто пишут. Они часто дают очень полезные указания и вносят полезный вклад, когда мы работаем над различными темами, которые нас интересуют. Если вы посмотрите на навыки только этой группы руководителей, то

увидите, как много их собрано. Но если вы посмотрите на это по всем SSAC, то увидите еще большее разнообразие.

У нас есть люди, пришедшие из академических кругов. У нас есть люди из гражданского общества, из бизнеса, из правительства, из правоохранительных органов. Как правило, люди попадают в SSAC в результате открытого процесса подачи заявок. Они подают свои заявки. Внутри SSAC существует комитет по членству, который рассматривает заявки и проводит собеседования. После собеседования они рекомендуют людей для вступления в SSAC.

SSAC высказывает свое мнение по поводу этих людей. И когда мы пройдем весь этот процесс, мы предоставим список рекомендованных членов Правлению. Каждый член SSAC назначается Правлением ICANN. Итак, я попрошу Тару выступить по этой теме, потому что это основа нашей работы.

TARA WHALEN: Спасибо, Рэм. Итак, для тех, кто не знаком с SSAC, я полагаю, мы выпускаем большое количество технических материалов и делаем это уже несколько лет. Темы могут быть разными. Они касаются безопасности и стабильности интернет-идентификаторов по целому ряду вопросов. Но есть некоторые темы, к которым мы возвращаемся снова и снова, и это практически наши вечнозеленые темы. Поэтому мы ищем способы сосредоточиться на них и сделать эти материалы доступными для сообщества.

Поэтому по мере развития этих постоянно возникающих важных тем вы сможете приходить к нам и получать ответы на свои вопросы. Итак, темы, которые мы здесь обозначили, одна из них - злоупотребление DNS. Конечно, DNS - это важная система, и это делает ее местом, где также происходит значительное количество злоупотреблений в Интернете. Это полезный инструмент для людей, которые хотят нанести большой ущерб. Так, если люди совершают фишинговые атаки, распространяют вредоносное ПО, мы изучаем, как DNS влияет на это, и что мы можем сделать для смягчения последствий. Таким образом, это та область, в которой мы довольно часто выпускаем рекомендации и работаем с комитетами, чтобы попытаться смягчить этот вред.

Вторая область, о которой, возможно, думают многие, кто с нетерпением ждет следующего раунда, - это новые gTLD. Каждый раз, когда вы собираетесь добавить в систему новые имена, возникают вопросы безопасности и стабильности. Люди, возможно, следят за проектом анализа столкновения имен, например, изучая, что произойдет при расширении. Поэтому мы не хотим, чтобы возникали проблемы с путаницей строк. Таким образом, много работы направлено на то, чтобы предусмотреть эти проблемы. И это очень своевременный вопрос, к нам обращаются за советом по этой теме.

Существует также DNSSEC. Это одна из основных технологий безопасности в пространстве DNS. Мы, вместе с другими специалистами, работаем в этой области, давая советы в течение некоторого времени, продвигая эту технологию, пытаясь

убедиться, что она хорошо внедряется, что она хорошо реализована. Мы признаем, что она сложна, и людям часто требуется помощь, чтобы заставить ее работать так, как было задумано. Поэтому мы хотим, чтобы люди получали хорошие советы. Могут быть такие вещи, как, например, более эффективная автоматизация, чтобы облегчить людям внедрение этой функциональности безопасности и сделать ее, опять же, легкодоступной.

Существует также проблема альтернативных пространств имен. Люди могли видеть это в последние годы, когда блокчейн был в центре внимания. Это, конечно, никуда не делось. Но существовало множество других систем именования, которые не были идентичны тем, что предоставляются в DNS. Люди создавали криптовалюты и позволяли покупать различные виды доменов, что, конечно, вызывало вопросы: как это взаимодействует или интегрируется с DNS? Как нам предусмотреть различные вопросы сосуществования этих систем? Так что мы продолжаем изучать этот вопрос, потому что это очень развивающееся пространство.

И наконец, одна из тем, которая, возможно, волнует многих людей в этой аудитории, - это вопросы управления Интернетом, но особенно вопросы безопасности и стабильности, на которых сфокусирована наша группа, потому что в Интернете существует множество вопросов, которые пересекаются в техническом и политическом пространстве с множеством очень сложных вопросов с обеих сторон. И если вы собираетесь принимать решения в этом пространстве, очень полезно иметь четкое и

полезное руководство от технических специалистов, чтобы помочь вам в разработке политики.

И мы хотели бы быть в состоянии предоставить эту информацию с нашей технической точки зрения. Но мы также отмечаем, что наша работа становится более эффективной, когда мы получаем информацию от людей, которым нужна эта консультация, чтобы попытаться направить ее в нужное русло, убедиться, что мы отвечаем на правильные вопросы, убедиться, что мы доносим информацию на нужном уровне и с нужными подробностями.

Поэтому мы очень ценим, когда у нас есть возможность взаимодействовать с приглашенными экспертами или, например, беседовать с ними, консультироваться с ними, когда мы разрабатываем некоторые из наших советов, чтобы в случаях, когда они должны быть полезными для аудитории в политическом пространстве, мы в значительной степени сотрудничали друг с другом, чтобы подготовить правильный совет, который будет полезен для аудитории.

Итак, прямо сейчас у нас есть несколько рабочих групп, которые занимаются разработкой. Кстати, наша работа часто может охватывать более чем одну из этих областей. Но две из инициатив, реализуемых прямо сейчас, - это группа по свободному и открытому программному обеспечению в инфраструктуре DNS. Некоторые из вас, возможно, знают, что многие компоненты, которые внедряются в инфраструктуру DNS, например, резолверы, являются частью инициатив с открытым исходным кодом. Это могут быть большие или малые группы с разным

объемом финансирования, которые могут иметь различные виды обязательств, контрактных соглашений и отношений с различными сторонами. И это часть критической инфраструктуры для работы DNS.

Поэтому мы решили, что будет полезно показать, где находятся некоторые из этих зависимостей, чтобы люди могли понять, где находятся эти части программного обеспечения с открытым исходным кодом, где вы зависите от них, а также поставить под сомнение некоторые предположения людей об этих частях программного обеспечения, о том, что они могут и не могут делать, и что вы можете думать о надежности и прочности этих частей программного обеспечения.

По крайней мере, один из председателей группы здесь. Мартина здесь нет. У нас есть один. Ладно, просто проверяю, правильно ли я... Да, председатель дал мне большой палец вверх, что я правильно подытожила рабочие группы. Итак, работа только начинается. И мы надеемся, что некоторые из вас будут следить за результатами, когда они появятся, если вас интересует программное обеспечение с открытым исходным кодом. Еще одно направление, над которым мы работаем, - это блокировка и фильтрация DNS. Итак, одним из механизмов блокировки контента в Интернете является использование DNS в качестве одного из подходов к управлению блокировкой контента между конечными пользователями и ресурсом.

Технология уже давно существует, и SSAC обращал на нее внимание, но последним рекомендациям, которые мы выпустили,

уже более десяти лет. С тех пор как мы в последний раз писали об этом, технологический ландшафт изменился, изменился и нормативный ландшафт. Поэтому мы решили, что настало время взглянуть на эти вещи еще раз.

Так, например, многие технологические аспекты: многие DNS-запросы теперь выполняются по транспорту, что делает их менее очевидными. Люди не могут смотреть на запросы так, как раньше. Это, возможно, изменило ответы и информацию, которую люди получают, когда выясняют, как блокировать контент.

Так что это определенно та область, в которой нам необходимо внести свой вклад, мы общаемся с людьми, работающими в сфере политики. Нам повезло, что совсем недавно мы обсуждали с политиками из ICANN то, что они слышали и за чем следили, поскольку они следят за политическим пространством. И мы очень благодарны за то, что такой вклад помогает нам определить направление, в котором мы можем продвигать документы, чтобы они снова отвечали на самые актуальные вопросы. И поэтому мы еще раз повторяем, что нам нравится этот процесс сотрудничества.

Итак, это общий обзор наших тем. У нас есть и более глубокий уровень, которым, как я уже сказала, займется кто-то другой, на следующем слайде.

RAM MOHAN: Прежде чем мы перейдем к следующему слайду, Найджел, я хотел бы воспользоваться моментом и спросить, есть ли какие-либо вопросы или выступления, которые хотели бы сделать люди.

NIGEL HICKSON: Да, спасибо, Рэм. Я как раз собирался это сделать, потому что мы получили довольно много информации. Очень интересно, что у вас есть стабильные темы, к которым вы возвращаетесь, потому что все они очень актуальны. Итак, есть ли у вас вопросы или замечания, прежде чем мы углубимся в вопросы ИИ и блокчейна? Вы должны крикнуть, если они есть в сети. Дэниел? О, наши друзья. Да, Европейский Союз, пожалуйста.

GEMMA CAROLILLO: Спасибо, Найджел. Джемма Каролилло из Европейской комиссии. Просто краткий комментарий. Прежде всего, очень приятно видеть, что большая часть того, что у вас на тарелке, у нас на тарелке. Так что, возможно, мы должны видеться с вами очень часто, чаще, чем сегодня. И еще один небольшой вопрос, поскольку, как я понимаю, работа над безопасностью открытых источников только началась или недавно началась, и это тема, представляющая для нас большой интерес, можем ли мы получить точечную информацию, можем ли мы получить момент для повторной связи и получить больше информации об этой работе. Спасибо.

BARRY LEIBA: Хорошо, я возьму этот вариант. Это Барри Леба (Barry Leba). Я являюсь сопредседателем рабочей группы, которая будет готовить этот документ. Да, мы будем рады периодически представлять его вам по мере продвижения. Мы надеемся, что работа этой рабочей группы пройдет быстро, и мы должны закончить ее в течение следующих двух конференций ICANN. Так что, возможно, на следующем заседании в Сиэтле мы сможем представить вам обновленную информацию о том, на каком этапе мы находимся.

GEMMA CAROLILLO: Просто чтобы сказать, что это было бы здорово, спасибо.

RAM MOHAN: В дополнение к тому, что только что сказал Барри, я хотел бы добавить, что у рабочих групп есть возможность по усмотрению председателей приглашать экспертов или приглашать людей, обладающих информацией, чтобы они пришли и провели брифинг, который может быть информативным для рабочей группы. Так что есть возможность сделать это, возможно, и в межсессионный период, Барри.

NIGEL HICKSON: Еще что-нибудь? Ну, у нас будут возможности вернуться после следующей сессии. Итак, Рэм, возвращаемся к вам.

RAM MOHAN: Большое спасибо. Итак, давайте перейдем к следующему слайду. Джефф Бедсер (Jeff Bedser) планировал быть здесь, чтобы представить этот доклад, но, к сожалению, он чувствует себя не очень хорошо. Поэтому я возьму эту часть на себя. Мы подумали, что вам будет полезно услышать мнение некоторых наших членов по поводу ИИ и злоупотребления DNS. SSAC как комитет не поручал рабочей группе изучить эту тему и дать консенсусную рекомендацию от SSAC.

Итак, то, что вы увидите на следующих слайдах, в значительной степени основано на опыте некоторых наших членов. То есть это не голос SSAC, а технические знания и опыт некоторых наших членов в SSAC. Итак, в качестве начального уровня можно сказать, что есть машинное обучение, а есть искусственный интеллект. Машинное обучение - это подмножество. В этом подмножестве алгоритмы учатся на основе данных, чтобы делать прогнозы или принимать решения. В то время как искусственный интеллект охватывает более широкие технологии, которые позволяют машинам имитировать человеческий интеллект. Таким образом, машинное обучение является ключевым методом в рамках ИИ.

Злоупотребление DNS может стать отличным применением для ИИ. Это может быть именно то, что хотят использовать и использовать те, кто хочет стать преступниками или уже стал таковыми. Потому что ИИ, особенно генеративный ИИ, умеет создавать новые тексты, изображения, видео и другие артефакты. Например, очень точные логотипы банков или сайтов электронной коммерции. И это вместе с возможностями

генеративного ИИ и машинного обучения, распознавания образов, которое есть в машинном обучении, позволяет системам ИИ создавать электронные письма, текстовые сообщения, другие подсказки, которые выглядят почти так же, как если бы их написал или создал человек. И чем более аутентичными вы можете их сделать, тем больше вероятность того, что цели станут их жертвами.

И опять же, благодаря генеративному ИИ и его собственным возможностям, раньше, когда вы получали фишинговое письмо, вы могли почти полностью положиться на какие-то недостатки, что-то, что было составлено неправильно, грамматику, орфографию, неправильное написание заглавных букв. Но теперь все это не только хорошо сделано на базовом языке, но и может быть автоматически переведено на целый ряд других языков. А это значит, что масштаб и область применения проблемы значительно расширяются.

Итак, если взглянуть на злоупотребления DNS, то до сих пор в борьбе с злоупотреблениями DNS в масштабе использовались распознавание образов и сопоставление образов как основные механизмы борьбы с злоупотреблениями DNS в масштабе. Так, например, вы смотрите на информацию, лежащую в основе доменного имени или в основе конкретного уровня мошенничества, которое происходит. NS-записи, имена хостов, IP-адреса, связанные с ними, на кого зарегистрировано имя или ресурс, кто является регистратурой или регистратором. Вы находите закономерности или анализируете контент. Вы

смотрите на HTML-файл, на шаблоны, они используются повторно, или вы смотрите на хэш-значения файлов, потому что люди делали это в прошлом, были доступные и повторяющиеся шаблоны.

С помощью генеративного ИИ каждый конкретный домен или URL может быть полностью рандомизирован. Каждый фиш, который рассылается, а мы говорим о 100 000 фишей, которые генерируются в течение четырех часов, часто добавляет имя в файл зоны. В прошлом один фиш рассылался 100 000 целей. Теперь вы можете получить 100 000 отдельных сообщений, каждое из которых будет выглядеть подлинным, каждое из которых будет выглядеть так, будто оно пришло от человека и написано человеком. Итак, довольно эффективные способы заманивания целей.

Каковы другие способы использования ИИ для злоупотреблений? Итак, мы видим, что ИИ также используется для кукловодства, создания и использования фальшивых личностей, фальшивых аккаунтов, фальшивых отзывов. Сочетайте это с регистрацией доменных имен и хостинговых аккаунтов. Его также используют для создания интимных изображений без согласия, а также для CSAM. И довольно простое использование для фальсификации, фабрикации данных, фабрикации документов, фабрикации изображений. В некоторых юрисдикциях вы можете создавать такие удостоверения личности или другие документы. Например, есть коды стран, в которых говорится, что для получения доменного имени необходимо предоставить удостоверение личности.

Теперь эту личность можно создать без особых проблем. Таким образом, один из созданных способов защиты можно обойти довольно быстро. Вы также заметите, что, возможно, вы уже заметили, но вы заметите, что изображения, которые сопровождают все это, созданы искусственным интеллектом и связаны с контентом. Но вы увидите, что некоторые изображения выглядят реалистично, некоторые - нет, но все становится гораздо лучше. Тот же набор подсказок два года назад, тот же набор подсказок шесть месяцев назад привел бы к появлению изображений, которые не выглядели бы так, как будто их создал графический дизайнер.

На этом слайде трудновато все прочитать, но вот некоторые данные, полученные из исследовательского отчета, в котором говорится о частоте тактик злоупотреблений с использованием генеративного ИИ. Как вы можете видеть, чаще всего это самозванство, но также масштабирование и усиление существующих атак, фальсификация и так далее. Я уже говорил об этом на предыдущем слайде, но на этом слайде вы узнаете все до самого конца. Итак, он используется довольно широко.

И, как говорил предыдущий участник этой презентации, генеративный ИИ, похоже, создает все более темные изображения. По мере того как мы углубляемся в этот набор слайдов, мы не пытались сделать это. Это то, что получилось. Так что, возможно, здесь есть какой-то сигнал. Таким образом, даже если возможности не всегда приводят к более изощренным атакам, мы считаем, что генеративный ИИ способен увеличить их

масштаб и охват. И мы говорим, что киберпреступники будут постепенно интегрироваться. Мы ошиблись. Нам следовало бы сказать: уже интегрируют методы ИИ и уже используют системы ИИ в своих планах. Именно это мы и наблюдаем в реальности. Но это не все плохие новости. За исключением изображений, и вы увидите, что лица теперь сформированы. Это то, о чем мы просили, опять же, мы сказали движку, учитывая все, что вы видели до сих пор, сгенерировать это, и вот что вы получили.

Таким образом, как бы ни использовалось машинное обучение ИИ для увеличения масштабов и частоты этих атак, ИИ может быть весьма эффективным средством обнаружения фишинговых писем. И дело в том, что фишинговые письма, генерируемые ИИ, по крайней мере, в его нынешнем аватаре, в его нынешнем поколении, отличаются от обычных писем, которые генерирует человек. Они также отличаются от фишинговых писем, созданных вручную. А если объединить машинное обучение и обработку естественного языка, это поможет инструментам генеративного ИИ понять, обработать и создать тексты, которые будут звучать по-человечески и аутентично. Зная о существовании такой технологии, вы можете использовать ИИ для поимки ИИ. И это действительно то, к чему все идет.

Итак, векторы атак и стратегии, использующие ИИ в неправомерных целях, многим из вас, если не всем, уже знакомы. Политическая дезинформация - ее очень легко генерировать. Для этого уже не так часто нужны люди. Конечно, злоупотребления, ориентированные на получение прибыли, масштабирование и

ускорение преступных предприятий. Но в конечном итоге киберпреступность напрямую связана с деньгами, которые киберпреступники в итоге получают. И поэтому люди меняют стратегии, когда это необходимо, чтобы обеспечить прибыль.

Поэтому, даже если ИИ будет применяться для решения подобных проблем, мы увидим, что эволюция будет происходить. И сам ИИ развивается очень быстро. Но в целом мы считаем, что это продолжение той же угрозы, которая существовала до появления технологий. У вас есть субъекты, которые решили использовать технологии и задействовать их для получения какой-то выгоды, какого-то преимущества. И задача состоит в том, чтобы быть в курсе происходящего, а затем принять меры, которые позволят смягчить, если не противостоять, эти угрозы.

Итак, я только что говорил об искусственном интеллекте и DNS. Я не собираюсь тратить много времени на блокчейн и DNS. Мы уже говорили об этом на других форумах внутри ICANN. Есть отчет, который мы опубликовали, SSAC123, с которым можно ознакомиться. Мы также организовали дискуссию на семинаре SSAC 2024 в Вашингтоне, округ Колумбия, в сентябре этого года. Это тоже общедоступно. Она записана. Его можно найти в открытом доступе. Это была группа, в которую входили эксперты в области блокчейна. В ее состав входили представители офиса главного директора по технологиям ICANN.

Таким образом, между SSAC и OCTO ICANN ведется активное сотрудничество, чтобы убедиться, что мы согласовываем области

исследований. Мы не координируем свои действия в плане точных результатов работы, но стараемся не дублировать друг друга.

Итак, я перехожу к следующему слайду. И это, по крайней мере, с моей точки зрения, самый важный слайд, самая большая просьба к вам в GAC. Со временем мы пришли к выводу, что политические деятели, в частности, нуждаются в наращивании потенциала. Они хотели бы получать информацию по ключевым темам и получать ее от людей, которые действительно знают, о чем говорят, но могут рассказать об этом в доступной для них форме, а не просто посыпать вас жаргоном. У нас есть возможность. У нас есть возможность сделать это.

Мы также предоставляем отчеты. Мы создаем отчеты. Но эти отчеты часто занимают десятки страниц. В настоящее время мы работаем над тем, чтобы свести их к резюме объемом от 500 до 1000 слов, на страницу или две, и собрать все это вместе. Но что действительно помогло бы, так это если бы вы, как политики, сказали нам, какие темы для вас наиболее важны, потому что у нас есть 126 написанных нами документов, и мы не думаем, что будет эффективным просто пойти и собрать их воедино. Скажите нам, что было бы ценным для вас, и мы с удовольствием будем работать вместе с вами, чтобы помочь подготовить информационные документы для вас и вашей аудитории.

И наконец, мы хотели бы сотрудничать с вами и вашим правительством. Возможно, вы проводите важные встречи по темам, связанным с безопасностью, стабильностью и устойчивостью. Одна из вещей, которая, несомненно, происходит

с вами, - это то, что вы участвуете в некоторых из этих встреч, и к вам приходят другие коллеги или другие политики, которые недостаточно информированы о фактах, но без проблем дают советы о том, что следует сделать в этой конкретной области. И тогда возникает несоответствие между политическим решением и реальной технической осуществимостью. Мы считаем, что будет лучше, если при разработке политики вы будете опираться на достоверные факты, фактические данные, которые помогут вам и вашим правительствам в разработке этой политики.

Поэтому мы хотели бы открыть этот канал связи с вами и предложить широкий спектр и глубину технических знаний, которыми мы обладаем, помимо документов, которые мы предоставляем. Возвращаемся к вам, Найджел.

NIGEL HICKSON: Большое спасибо за такой подробный обзор. Подхватывая мысль в конце, я думаю, очевидно, что мы, как разработчики политики, в значительной степени обязаны советам, которые мы получаем от технического сообщества, советам, которые мы получаем от других подразделений ICANN. Я хорошо помню, как несколько лет назад, да и сейчас, когда мы обсуждали злоупотребление DNS в рамках раунда новых gTLD и другие вопросы, ваш отчет SSAC, номер которого я не помню, но помню, что читал его в деталях, и рекомендации, которые вы выработали по поводу злоупотребления DNS, оказали влияние на рекомендации, которые мы выработали на наших встречах.

Так что я действительно считаю, что у нас есть много возможностей для более эффективной совместной работы. Я также могу отметить большой интерес к блокчейну, в частности к DNS Abuse, и работу над этим. И это, несомненно, тема, к которой мы вернемся в свое время. Так что большое спасибо за то, что нашли нас по этим вопросам. Теперь я приму вопросы и комментарии от присутствующих. И я думаю, что наши друзья из Нидерландов.

ALISA HEAVER: Спасибо. И спасибо за презентацию о работе SSAC. Должно быть, я знаю, но на самом деле я не уверена, есть ли представитель GAC в SSAC или наоборот. Если нет, то я думаю, что это могло бы очень сильно помочь.

RAM MOHAN: Спасибо за это. Я не думаю, что у нас есть такая формальная роль. Мы, конечно, будем рады, если вы захотите это сделать. Единственное, что мы делаем в рамках SSAC, это то, что все, кто, даже представители, новые представители, проходят через тот же процесс проверки, чтобы они могли стать полноправными членами и участвовать. Но среди вас много специалистов. Так что, я думаю, это было бы полезно. У нас есть Гейб, который сидит прямо перед вами. Гейб - член SSAC. Так что в некоторых случаях он выступает в качестве неофициальной передачи информации, которая происходит, но, конечно, не формальным образом.

NIGEL HICKSON: Большое спасибо за то, что подняли этот актуальный вопрос. И я думаю, что ответ заключается в том, что на данный момент мы этим не занимаемся. Но мы, конечно, можем рассмотреть этот вопрос, потому что мне кажется, что это важно. Я имею в виду, что вы очень прозрачный консультативный комитет, и ваши документы хорошо опубликованы. Но даже в этом случае иметь некоторое представление о работе, которую вы делаете, вероятно, уместно. Я бесполезен в очках или без них. Но кто-нибудь еще? А, это были вы? Иэн, или нет? Да, продолжайте. А потом перед вами. Но сначала Иэн.

IAN SHELDON: Извините, Найджел, образовалась виртуальная очередь. Просто хотел обратить ваше внимание на это. Но я тоже был в начале этой очереди.

NIGEL HICKSON: Тогда действуйте.

IAN SHELDON: Спасибо, Рэм. GAC Австралия, Иэн Шелдон (Ian Sheldon) с вами. Спасибо за предложение помощи. Я вижу, что на сцене собрались люди с большим опытом и знаниями. Как вы, наверное, знаете, у членов GAC часто бывает довольно большое досье. Мы занимаемся многими вопросами, как в рамках ICANN, так и за ее

пределами. Поэтому мне было бы интересно услышать ваши мысли о предложении экспертизы и поддержки. Насколько широки эти полномочия? Мы говорим только о проблемах DNS или можем воспользоваться некоторыми экспертными знаниями, которые могут находиться немного за пределами этого форума?

RAM MOHAN: Спасибо, Иэн. Отличный вопрос. Итак, что касается самого SSAC, мы останемся в рамках наших полномочий и того, что у нас есть. Но у вас есть доступ к нашим членам. И если наши члены захотят помочь вам в вопросах, выходящих за рамки сферы деятельности ICANN, то это будет полезно для вас обоих.

NIGEL HICKSON: Спасибо, Иэн. Позвольте мне до вас предоставить слово США. А потом я перейду к списку онлайн.

LEONARD HAUSE: Да, Леонард Хауз (Leonard Hause), Государственный департамент США. Когда генеративный ИИ сочетается со злоупотреблемнием DNS, есть ли у них передовой опыт в том, как это можно сделать, либо через процесс регистрации, либо где-то по ходу дела, они могут копнуть немного глубже и добраться до корня того, с чего все это начинается, будь то какой-то тест Тьюринга или что-то подобное, что может пройти и прижать генеративный ИИ до того, как он будет выпущен на свободу, если хотите. Итак, просто

вопрос в рамках отчета о лучших практиках в этой области. Спасибо. Спасибо за отличную работу над этим.

RAM MOHAN: Спасибо. Я не знаю ответа на этот вопрос. Но я могу спросить экспертов в SSAC, которые изучают эту тему, и ответить на него. Одна вещь в пространстве ICANN, которая, по крайней мере, должна быть частью рассмотрения: если это правда, что с генеративным ИИ вы можете получить в течение нескольких часов после добавления домена в разрешение такое огромное количество оскорбительных сообщений. Можно ли что-то сделать в рамках ICANN, чтобы быстро уменьшить это количество? Если злоупотребления происходят в течение нескольких часов, возможно ли смягчить их последствия в течение нескольких минут после обнаружения? Я думаю, что это открытый вопрос, который мы должны рассмотреть здесь.

NIGEL HICKSON: Большое спасибо. И спасибо за ответ. Теперь у меня есть два или три человека онлайн. Сначала Джемма из Европейской комиссии.

GEMMA CAROLILLO: Большое спасибо, Найджел. Поскольку вы спросили о возможных темах, представляющих интерес, я подумала, что здесь, в GAC, при обсуждении злоупотреблений DNS среди прочего мы обсуждали использование инструментов прогнозирования. И в Европейском союзе у нас есть некоторый опыт в этом. Было бы очень хорошо,

если бы уже имелся материал или если бы существовало пространство для дальнейшей работы над потенциалом инструментов прогнозирования для предотвращения злоупотреблений DNS, прежде чем мы перейдем к смягчению последствий. И еще одно небольшое уточнение. Если я правильно понимаю, при использовании ИИ и генеративного ИИ мы не расширяем ландшафт угроз. Я бы сказал, что количество атак становится больше, но они не становятся более изощренными. У нас не стало больше угроз, по крайней мере, на данный момент.

RAM MOHAN: Спасибо. Что касается второго вопроса, то да, это так. Мы не считаем, что сфера угроз расширилась, но частота, масштабы резко возросли. Что касается первого вопроса, есть ли здесь члены SSAC, которые хотели бы ответить нашему коллеге?

GABRIEL ANDREWS: Я могу кратко рассказать о работе правоохранительных органов. Но мы видим очень похожие группы угроз, те же преступные группы, которые делали все вручную или просто использовали инструменты искусственного интеллекта, чтобы делать это более эффективно, как это делают хорошие парни. Поэтому нельзя сказать, что мы наблюдаем что-то особенно новое. Это все те же старые трюки, только с использованием новых инструментов для их выполнения, - таков общий вывод, который мы можем сделать из нашего обзора на данный момент.

RAM MOHAN: Спасибо, Гейб. Мне просто интересно, я думаю, что вам следует переформулировать первый вопрос, чтобы другие члены обратили на него внимание и, возможно, ответили.

GEMMA CAROLILLO: Это очень любезно. Спасибо вам большое. И я постараюсь сформулировать это как можно яснее. Итак, раз уж вы спросили о потенциальных темах для работы SSAC и брифингах, которые могли бы быть полезны GAC. В GAC при обсуждении злоупотреблений DNS мы иногда говорили о существовании инструментов прогнозирования для предотвращения злоупотреблений DNS до того, как мы перейдем к фазе смягчения последствий. Поэтому я хотела бы узнать, есть ли у вас под рукой материалы или дальнейшая работа, которую можно было бы провести в этой области. Спасибо.

RAM MOHAN: Спасибо. Кто-нибудь хочет прокомментировать это? Бенедикт, а затем Стив.

BENEDICT ADDIS: Здравствуйте. Бенедикт Аддис (Benedict Addis). Мне не удалось занять место на трибуне. Итак, в злоупотреблениях DNS есть некоторые элементы, которые очень хорошо поддаются прогнозированию. Так, в частности, ботнеты и вредоносные

программы используют очень предсказуемые алгоритмы для генерации доменов на недели, месяцы и годы вперед. Этих доменов не существует. Они называются доменами DGA. Мы можем предсказать их очень точно. Но я бы предостерег вас: к любым инструментам, которые утверждают, что предсказывают вредоносность в более общем смысле с помощью волшебной пыли ИИ, я бы относился с большой осторожностью. Итак, есть некоторые области, которые хорошо поддаются прогнозированию. Но не в целом.

RAM MOHAN: Стив?

STEVE CROCKER: Спасибо. Для того чтобы управлять процессом прогнозирования, необходимо иметь быстрый и оперативный доступ к регистрационным данным и самим регистрациям. Я бы сказал, что сейчас мы переживаем очень бурный период, когда большое внимание уделяется конфиденциальности, что вполне оправданно для защиты от различных форм преследования, спама и так далее, и так далее. Но в то же время это затрудняет, где-то между трудностью и невозможностью, получение доступа к данным для законных целей, особенно для некоторых из этих целей, таких как прогнозный анализ и корреляция между доменами.

Поэтому приходится решать сложные и непростые вопросы: как обеспечить доступ к информации, чтобы можно было проводить качественный прогнозный анализ, и в то же время не нарушать неприкосновенность конфиденциальности. Таким образом, между этими двумя идеями существует взаимосвязь.

NIGEL HICKSON: Большое спасибо. Спасибо за вопрос, который побудил несколько замечательных ответов. Думаю, следующим будет наш друг Сантош из Индии.

T. SANTOSH: Спасибо, Найджел. Спасибо, Рэм Мохан, за подробную презентацию об искусственном интеллекте и злоупотреблениях DNS. Итак, давайте начнем с основ. Может ли ИИ помочь в работе над точностью определения «кто есть кто», потому что это основная проблема, которую используют злоумышленники, поскольку в большинстве случаев «кто есть кто» не является точным. Итак, можем ли мы создать систему, в которой инструмент ИИ сможет сказать, что, окей, это не является точным WHOIS, поэтому домен не может быть делегирован? Спасибо.

RAM MOHAN: Спасибо. Итак, конкретный ответ на это: конечно, можно взять ИИ или другие алгоритмы машинного обучения, применить их к базе данных, сравнить с реальными адресами, людьми и т. д. и прийти к определенным выводам. Но, как только что сказал Стив, большая

часть этих данных сейчас замаскирована или недоступна. Поэтому, даже если бы эта технология существовала сегодня и была доступна, наборы данных, которые могли бы лечь в основу этих инструментов, просто недоступны.

BARRY LEIBA: И небольшое дополнение к этому, Рэм. Недоступны не только данные, необходимые для проверки, но и данные, необходимые для обучения двигателя. Таким образом, это двойная проблема.

GREG AARON: Я бы сказал по-другому. Контактные данные доменных имен недоступны большинству из нас, например, компаниям, занимающимся безопасностью, правоохранительным органам, если их нет, например, в WHOIS. Однако есть стороны, которые располагают этими данными, - это регистраторы и операторы регистратур. И сейчас операторы регистратур и регистраторы проводят проверку достоверности с помощью различных методов. Например, это делают .nl в Нидерландах, .uk. Таким образом, теперь у нас есть в основном регистраторы, особенно те, кто может проводить проверки достоверности и потенциальных киберпреступлений.

У них есть данные WHOIS, у них также есть данные о покупке, например, финансовые инструменты, использованные для регистрации доменных имен, исходные IP-адреса и другие вещи.

Таким образом, потенциал для использования ИИ есть, но теперь он находится в руках этих сторон.

NIGEL HICKSON: Большое спасибо за это. У нас есть еще два или три вопроса в чате, так что я продолжу с ними. У нас есть семь минут времени, или шесть, потому что нам нужно будет подвести итоги. Но я думаю, я не очень понимаю порядок этих вещей, но Марко, почему бы вам не высказаться?

MARCO HOGEWONING: Я буду очень краток и повторю слова моих коллег и очень благодарен SSAC за то, что вы здесь, а также за то, что вы протягиваете нам руку помощи. Вы задали простой, но в то же время сложный вопрос: что мы считаем важным? Все - это как выбрать любимого ребенка, мне кажется, на этот вопрос очень сложно ответить. Я очень ценю работу SSAC, особенно за то, что она помогает нам понять влияние новых и новейших технологий на стабильность системы DNS и Интернета в целом. Но если говорить о приоритетах и отвлечься, то, с одной стороны, мне хотелось бы услышать, смотрит ли SSAC в этом смысле на некоторые глобальные диалоги, которые мы ведем, и на некоторые глобальные процессы, например, на недавно опубликованный Глобальный цифровой договор.

И где, по вашему мнению, можно провести важную работу, чтобы помочь всем нам, а также видите ли вы возможность для SSAC

внести свой вклад в некоторые из этих текущих глобальных обсуждений, например, обзор WSIS или несколько направлений действий WSIS также касаются безопасности и стабильности системы. Спасибо.

RAM MOHAN: Большое спасибо. Управление Интернетом и связанные с ним аспекты безопасности, стабильности и отказоустойчивости - одна из пяти областей нашего постоянного внимания. Поэтому мы, безусловно, хотели бы принять участие в этой работе. У нас нет структуры, в рамках которой мы посылали бы представителя или направляли кого-то в эти области. Но у нас есть члены, которые обращают на это внимание, которые непосредственно занимаются этим в своей повседневной работе. И это определяет многое из того, что мы делаем. И на самом деле, именно это привело к созданию нашей рабочей группы по открытым источникам. Один из наших членов признал, что на правительственном уровне этому уделяется определенное внимание. И поэтому это может быть полезно.

BARRY LEIBA: Сейчас я отвечу. В основном, SSAC решает работать над чем-то тремя способами. Первый - один или несколько членов SSAC, которые заинтересованы в этом и предлагают это. Один – Правление просит нас рассмотреть что-то. Другой - сообщество просит нас рассмотреть что-то. И очевидно, что мы не можем сделать все. Но если к нам придут члены сообщества и скажут:

«Это очень важно для нас, не могли бы вы взглянуть на это?» Это вполне возможно.

NIGEL HICKSON: Спасибо. У нас есть еще пара вопросов. Оуэн из США.

OWEN FLETCHER: Привет, Найджел. Думаю, Ванг Ланг (Wang Lang) был раньше меня.

NIGEL HICKSON: Ах, да. Я приношу свои извинения. Мне очень жаль, Ван Ланг (Wang Lang). Это моя неспособность понять порядок этих вещей. Продолжайте, сэр.

WANG LANG: Спасибо, Найджел. Спасибо, Оуэн. Я хочу поблагодарить Рэма за фантастическую презентацию. Вы только упомянули блокчейн, DNS, но не стали углубляться в эту тему. А мы знаем, что ICANN принимает его безоговорочно как аккредитованный регистратор. Итак, мой вопрос: каково ваше мнение о будущем Web3 DNS? Спасибо.

RAM MOHAN: Спасибо. Итак, SSAC не готовил отчет конкретно о блокчейне, но мы подготовили отчет об эволюции DNS и новых технологий. В целом, наш подход заключается в том, что технологии будут

развиваться. Нам следует принять эти новые пространства имен, а не говорить, что мы должны защищать только свое и запрещать все остальные. Однако важно то, что если другие пространства имен захотят интегрироваться в пространство имен DNS, это должно быть сделано ответственно. Это должно быть сделано с учетом стабильности и безопасности. Итак, на высоком уровне мы смотрим на это именно так. Существуют и другие артефакты и другие проблемы. Если бы мы подготовили отчет только о блокчейне, я уверен, что были бы выявлены и другие проблемы. Мы еще не дошли до этого.

NIGEL HICKSON: Большое спасибо, Рэм. Переходим к Оуэну.

OWEN FLETCHER: Спасибо, Найджел. Это Оуэн Флетчер (Owen Fletcher) из Соединенных Штатов. Я думаю, что это была фантастическая сессия, а ИИ и злоупотребление DNS - прекрасный пример темы, где технический опыт SSAC может принести нам пользу в GAC, пытаясь разработать научно обоснованные, хорошо информированные позиции по типам вещей, которые GAC может захотеть прокомментировать.

Поэтому я думаю, что было бы здорово проводить больше подобных встреч, возможно, в том числе на сессиях по развитию потенциала, которые проводит GAC. И я увидел еще один комментарий на этот счет в чате. Рам, в презентации были

описаны некоторые виды злоупотреблений, которые, очевидно, не являются злоупотреблениями DNS, как они описаны или определены в ICANN, хотя многие из них могут быть использованы людьми, совершающими злоупотребления DNS. Но если говорить о злоупотреблениях DNS в соответствии с определением ICANN, ожидаете ли вы, что то, что я понял из презентации, как ускорение темпов создания плохих доменов, приведет к увеличению числа зарегистрированных случаев злоупотреблений? Например, следует ли нам иметь это в виду, когда мы будем изучать статистику и отчеты о злоупотреблениях DNS в ближайшие месяцы или годы? Спасибо.

RAM MOHAN: Я просто выскажусь лично, потому что у SSAC нет позиции по этому вопросу. Но лично я считаю, что это логичный следующий шаг. Когда технология позволит сделать сложность и масштабы этого настолько простыми, тогда можно будет ожидать, потому что на этом можно будет сделать очень много денег. Я имею в виду, что Джефф Бедсер (Jeff Bedser) в своем вчерашнем комментарии сказал, что стоимость хорошей рыбы составляет около 20 000 долларов. Так что, если регистрация доменного имени стоит 200, 100, даже 1000 долларов, это не всегда является достаточным сдерживающим фактором. Так что, думаю, если вы выстроите логическую цепочку, мы можем ожидать, что подобных злоупотреблений и сообщений о них станет гораздо больше. Это моя личная точка зрения. Есть ли другие, Мерике?

MERIKE KAEO: Да, с личной точки зрения, я имею в виду, что ежедневно занимаюсь безопасностью и практически ничему не доверяю. Но для меня это было очень интересно. Я не фильтрую спам, потому что хочу посмотреть на кампании и происходящие события. И что действительно интересно, причиной этого должен быть искусственный интеллект, но тип фишинговых писем становится чрезвычайно правдоподобным. И я полагаю, что они на самом деле смотрят на то, что вы публикуете на Facebook или LinkedIn, и потенциально нацеливаются на конкретные организации, конкретное руководство, чтобы у них были сведения о том, что является более правдоподобным. И я думаю, что это то, что действительно важно, когда мы можем действовать быстрее, чтобы обнаружить и предотвратить.

NIGEL HICKSON: Спасибо. Большое спасибо, Рэм. Боюсь, нам придется на этом закончить. У нас закончилось время, но это было очень, очень продуктивно. Это просто показывает, насколько высок интерес к той невероятной работе, которую вы ведете. И это здорово, что за столом собрались такие эксперты. Я всегда горжусь тем, что сижу за столом вместе с г-ном Стивом Крокером (Steve Crocker). Меня вдохновляет то, что многие из вас внесли свой вклад не только в работу ICANN, но и в работу Технического сообщества по многим вопросам.

Так что спасибо, что снова пришли. Это не последний раз. Спасибо за ваши любезные предложения продолжить работу над различными вопросами. И на этом, я думаю, нам лучше закрыть

заседание. Хотя мои уважаемые коллеги, сидящие сзади, не могли бы вы сказать нам, когда будет утренняя сессия? Не могли бы вы просто напомнить нам, когда?

JULIA CHARVOLEN: Одну минуту. Вы знаете?

НЕИЗВЕСТНЫЙ ОРАТОР: Да, в 1:15. До этого еще будет церемония приветствия, политический форум, но GAC начнется в 1:15 по местному времени с обсуждения вопросов регистрационных данных WHOIS.

NIGEL HICKSON: Потерял отсчет времени.

RAM MOHAN: Найджел, большое спасибо от имени SSAC за то, что пригласили нас сюда. Мы надеемся, что это не последний раз. Мы с нетерпением ждем дальнейшего взаимодействия.

[КОНЕЦ СТЕНОГРАММЫ]