



**ВООРУЖЕНИЕ ПСЕВДОЭКСПЕРТОВ И БЮРОКРАТОВ "ДЕЗИНФОРМАЦИЕЙ":
КАК ФЕДЕРАЛЬНОЕ ПРАВИТЕЛЬСТВО В ПАРТНЕРСТВЕ С УНИВЕРСИТЕТАМИ
ПОДВЕРГАЕТ ЦЕНЗУРЕ ПОЛИТИЧЕСКИЕ ВЫСКАЗЫВАНИЯ АМЕРИКАНЦЕВ**

Промежуточный отчет

Подготовлен комитетом по
судебной власти и
Специальным подкомитетом по вооружению федерального правительства

Палата представителей США



6 ноября 2023 года

Примечания редактора:

- 1) Для корректности перевода были убраны ссылки на оригинальные источники, которые смешивались с основным текстом. Значительные примечания были встроены в основной текст. При необходимости, в будущем возможно добавить библиографию и ссылки в следующей редакции;
- 2) В тексте сохранены англоязычные аббревиатуры органов власти США;
- 3) Несмотря на попытку сохранить максимально точный перевод, в некоторые предложения добавлены, не искажающие смысл, но позволяющие понять смысл на русском языке.

Оглавление

Кто подвергался цензуре?.....	8
Что подвергалось цензуре?.....	9
ГЛОССАРИЙ КЛЮЧЕВЫХ ТЕРМИНОВ И НАЗВАНИЙ.....	11
A. Попытки цензуры предшественников CISA.....	16
1. Коммутация, отказ от ответственности и угроза репрессий со стороны правительства.....	16
2. EI- ISAC.....	26
3. Портал для сообщений о дезинформации.	28
4. CISA не делала различий между иностранными и внутренними акторами в социальных сетях.....	36
B. Создание EIP	35
C. Цель EIP: использование доверенностей для обхода первой поправки.....	41
II. ПОЛНОЕ ПЕРЕПЛЕТЕНИЕ CISA С EIP	44
A. CISA в сговоре с EIP.....	44
B. “Тикеты” Jira: Главное оружие в арсенале цензуры EIP	54
C. Сговор на практике: Координированное отметание постов.....	55
D. Непосредственное участие Государственного департамента в операции EIP «Цензура»	61
E. Участие других федеральных агентств в EIP: FBI и NHS.....	63
III. «ТИКЕТЫ» JIRA ОТ EIP: ЭНЦИКЛОПЕДИЯ КОНСЕРВАТИВНОЙ ЦЕНЗУРЫ	66
A. Отказ от претензий на «дезинформацию»: Абсурдный подход EIP	67
B. Усилия по цензурированию правды.....	68
C. Усилия по цензуре президента Трампа и его семьи.....	69
D. Усилия по цензуре политических кандидатов и законодателей	72
E. Усилия по цензуре юмора и сатиры	75
F. Усилия по цензуре других влиятельных консервативных аккаунтов	78

IV.	ТАКТИКА ПРИНУЖДЕНИЯ EIP	79
V.	УСИЛИЯ СТЭНФОРДА ПО ПРЕПЯТСТВОВАНИЮ РАССЛЕДОВАНИЮ КОМИТЕТА.....	82
A.	Обманчивые публичные заявления Стэнфорда о том, что EIP отмечал сообщения на сайте.....	82
B.	Первоначальные усилия Стэнфорда по незаконному искажению и сокрытию данных Jiga.....	85
C.	Многочисленные документы опровергают показания свидетелей о непричастности CISA к EIP.	87
D.	Стэнфорд продолжает вводить в заблуждение относительно CISA, EIP и Jiga.....	88
ЭПИЛОГ	93
ПРИЛОЖЕНИЕ I	97

ИСПОЛНИТЕЛЬНОЕ РЕЗЮМЕ

После президентских выборов 2016 года появился сенсационный нарратив, будто бы иностранная "дезинформация" повлияла на честность выборов. Эти утверждения, подпитанные левым отрицанием легитимности [победы президента Трампа](#), вызвали новое внимание к роли социальных медиаплатформ в распространении такой информации.

Были созданы "дезинформационные" аналитические центры и "эксперты", правительственные целевые группы и университетские центры. Все это для изучения и борьбы с предполагаемым ростом дезинформации. Как показал ранее Комитет Палаты представителей по судебной системе и Специальный подкомитет по вооружению федерального правительства, эти усилия по борьбе с так называемым иностранным влиянием и дезинформацией быстро трансформировались в борьбу с внутренней, то есть американской, свободой слова.

Первая поправка к Конституции справедливо ограничивает роль правительства в контроле и цензуре речи американцев, но исследователи дезинформации (часто финансируемые, по крайней мере частично, за счет средств налогоплательщиков) не были строго связаны этими конституционными рамками. То, что федеральное правительство не могло делать напрямую, оно фактически передавало на аутсорсинг только что возникшему цензурно-промышленному комплексу.

Election Integrity Partnership (EIP) - консорциум "дезинформационных" ученых во главе со Стэнфордской интернет-обсерваторией (SIO) Стэнфордского университета, который напрямую сотрудничал с Министерством внутренней безопасности и Центром глобального взаимодействия, многоведомственной структурой, входящей в состав Госдепартамента, для мониторинга и цензуры высказываний американцев в Интернете в преддверии президентских выборов 2020 года. Созданная летом 2020 года "по просьбе" Агентства кибербезопасности и безопасности инфраструктуры (CISA), EIP дала федеральному правительству возможность отменить свои цензурные действия в надежде обойти как Первую поправку, так и общественный контроль.

В преддверии выборов 2020 года, на фоне пандемии [COVID-19](#), американская общественность и законодатели обсуждали достоинства беспрецедентных изменений избирательных процедур в середине избирательного цикла. Эти вопросы, как и все современные дискуссии по вопросам политической важности, активно обсуждались на крупнейших в мире социальных медиаплатформах — будто бы современной версии городской площади. Но когда американские граждане, включая кандидатов на этих выборах, пытались реализовать свои права по Первой поправке на этих платформах, их речь, защищенная Конституцией, была намеренно подавлена вследствие прямой координации федерального правительства со сторонними организациями, в частности университетами, и платформами социальных сетей. Речь, касающаяся выборов - процесса, посредством которого американцы выбирают своих представителей, - конечно же, имеет право на надежную защиту в соответствии с Первой поправкой. Этот основополагающий принцип еще более важен, когда речь идет о политических кандидатах. Но, как признают "эксперты" по дезинформации, навешивание ярлыков на любой вид речи "по своей сути является политическим" и само по себе представляет собой форму "цензуры".

В этом промежуточном отчете сотрудников подробно рассказывается об активном

участии федерального правительства в создании и работе EIP, которая способствовала цензуре политических высказываний американцев в течение недель и месяцев, предшествовавших выборам 2020 года. В этом отчете также впервые публично раскрываются секретные отчеты о "дезинформации" из централизованной системы отчетности EIP, которые ранее были доступны только избранным лицам, включая федеральные агентства, университеты и Big Tech компании. Комитет и специальный подкомитет получили эти непубличные отчеты из Стэнфордского университета только под угрозой наказания за неуважение к Конгрессу. Эти отчеты о предполагаемой дезинформации были использованы для цензуры американцев, занимающихся основной политической речью в преддверии выборов 2020 года.

Как следует из этой новой информации, а также из данного отчета, федеральное правительство и университеты оказывали давление на представителей социальных сетей, заставляя их цензурировать правдивую информацию, шутки и политические мнения. Это давление было направлено в основном в пользу одной стороны политического прохода: правдивая информация, размещенная республиканцами и консерваторами, была помечена как "дезинформация", в то время как ложная информация, размещенная демократами и либералами, оставалась практически незамеченной и не тронутой цензорами. Псевдонаука дезинформации сейчас - и всегда была - не более чем политической уловкой, чаще всего направленной против сообществ и отдельных людей, придерживающихся взглядов, противоречащих господствующим представлениям.

Принцип работы EIP был прост: "внешние заинтересованные стороны", включая федеральные агентства и организации, финансируемые федеральным правительством, представляли отчеты о дезинформации непосредственно в EIP. Далее "аналитики" EIP по дезинформации просматривали интернет в поисках дополнительных примеров цензуры. Если в представленном отчете отмечался, например, пост в Facebook, аналитики EIP искали аналогичный контент в Twitter, YouTube, TikTok, Reddit и других крупных социальных сетях. После того как все оскорбительные ссылки были собраны, EIP отправляла наиболее значимые из них непосредственно в Big Tech с конкретными рекомендациями о том, как социальные медиа-платформы должны цензурировать эти посты, например, уменьшить их "обнаруживаемость", "приостановить возможность аккаунта продолжать твиты в течение 12 часов", "отслеживать, если какой-либо из отмеченных аккаунтов влияния ретвитнет" конкретного пользователя, и, конечно же, удалять тысячи постов американцев.



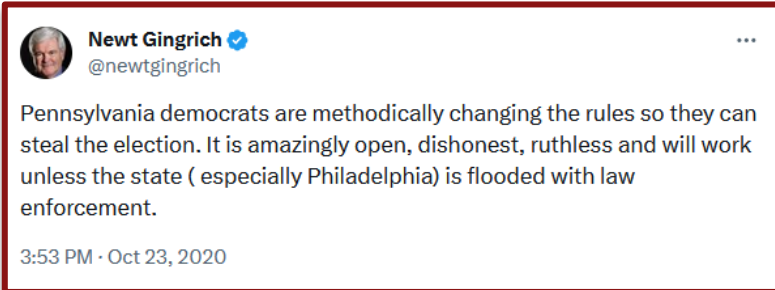
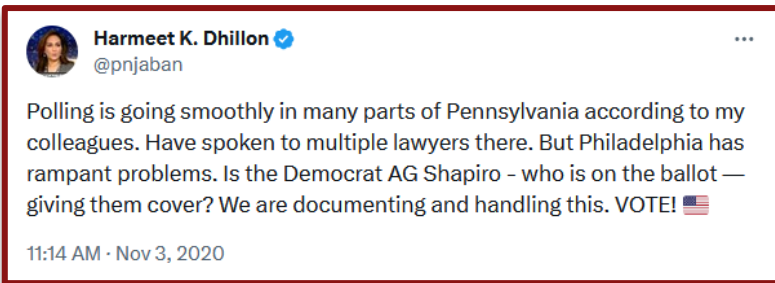
Правительственные агентства и "эксперты" по дезинформации быстро ссылаются на необходимость борьбы с иностранными субъектами, пытающимися подорвать

американские выборы, в качестве оправдания этого режима цензуры. Хотя иностранные государства действительно пытаются проводить операции по оказанию влияния, расследование Комитета и Специального подкомитета показало, что истинным фокусом и целью работы цензоров по обеспечению "честности выборов" были те самые американцы, которых они, как они утверждают, защищают. Вместо того чтобы бороться с иностранными или неаутентичными (*прим. фейковыми, ненастоящими*) аккаунтами, EIP нацелилась на американцев, в основном на кандидатов и комментаторов с консервативными взглядами. И несмотря на заявленную цель борьбы с "дезинформацией", EIP сотрудничала с представителями социальных сетей для цензуры правдивой информации, шуток и сатиры, а также политических мнений.

Кто подвергался цензуре?

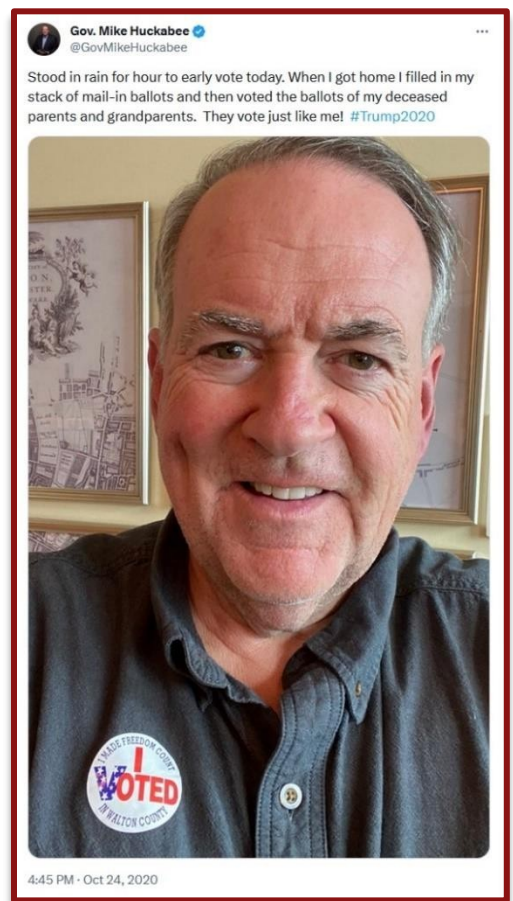
- Президент Дональд Трамп
- Сенатор Том Тиллис
- Спикер Ньют Гингрич
- Губернатор Майк Хакаби
- Конгрессмен Томас Масси
- Конгрессвумен Марджори Тейлор Грин
- Newsmax
- Вавилонская пчела (блогер)
- Шон Хэннити
- Молли Хемингуэй
- Хармит Дхиллон
- Чарли Кирк
- Кэндис Оуэнс
- Джек Пособиец
- Том Фиттон
- Джеймс О'Киф
- Бенни Джонсон
- Мишель Малкин
- Шон Дэвис
- Дэйв Рубин
- Пол Сперри
- Трейси Бинз
- Шанель Рион
- Неисчислимо количество обычных американцев всех политических взглядов





Что подвергалось цензуре?

- Правдивая информация
- Шутки и сатира
- Политические взгляды



В рамках этого отчета Комитет и специальный подкомитет публикуют все ранее секретные архивные данные, полученные Комитетом в соответствии с повесткой, выданной Стэнфордскому университету, которую Стэнфорд предоставил только после угрозы презрения. В преддверии выборов 2020 года Министерство внутренней безопасности (DHS) имело возможность видеть, какие высказывания американцев подвергаются цензуре. Сегодня, в результате расследования, проведенного Комитетом и Специальным подкомитетом, политические кандидаты, журналисты и все американцы имеют возможность узнать, были ли они объектом преследования со стороны правительства и какие точки зрения DHS, Стэнфорда и других лиц подвергались цензуре. Хотя EIP в непропорционально большой степени была направлена на консерваторов, жертвами цензуры стали американцы всех политических убеждений.

Первая поправка запрещает правительству "ущемлять свободу слова" и защищает "право народа... обращаться к правительству с петициями". Возможность американцев критиковать правительство и его политику является фундаментальным и священным принципом американской конституционной республики. Верховный суд давно признал, что для "основных политических высказываний" "важность защиты Первой поправки находится в зените".

Более того, как объясняют ученые-конституционалисты: "Поскольку Первая поправка запрещает "ущемлять" свободу слова, любой закон или правительственная политика, которые ограничивают эту свободу на платформах [социальных сетей] ... нарушают Первую поправку".

Правительство не может диктовать тип или условия критики, которой оно подвергается, особенно когда правительство не согласно с достоинствами этой критики. В целях подготовки потенциального законодательства Комитет и специальный подкомитет расследуют сговор исполнительной власти с третьими сторонами-посредниками, включая университеты, с целью цензуры защищенной речи в социальных сетях.

Комитет и специальный подкомитет отвечают за расследование "нарушений гражданских свобод граждан Соединенных Штатов". В соответствии с этим мандатом данный промежуточный отчет сотрудников о нарушениях Первой поправки и других неконституционных действиях CISA выполняет обязанность выявлять и сообщать об использовании оружия федерального правительства против американских граждан. Расследование Комитета и специального подкомитета продолжается.

CISA до сих пор не выполнила должным образом повестку о предоставлении соответствующих документов, и необходимо провести дополнительную работу по установлению фактов. Чтобы лучше информировать Комитет о законодательной деятельности, Комитет и Подкомитет продолжат расследование того, как исполнительная власть работала с платформами социальных сетей и другими посредниками для цензуры неугодных точек зрения в нарушение Конституции США.

ГЛОССАРИЙ КЛЮЧЕВЫХ ТЕРМИНОВ И НАЗВАНИЙ

Срок/название	Организация	Описание/определение
CFITF	Целевая группа CISA по противодействию иностранному влиянию (CFITF)	Целевая группа Министерства внутренней безопасности (DHS) при Агентстве по кибербезопасности и защите инфраструктуры (CISA), объединившая компоненты DHS, включая разведку и анализ DHS, и другие организации для рассмотрения более широкой проблемы иностранного влияния и дезинформации на основе оценки иностранного влияния, проведенной разведывательным сообществом США в 2017 году. В 2021 году название CFITF было изменено на Mis-, Dis- и Команда по сбору вредоносной информации ("Команда MDM").
CIP	Центр информированной общественности	Миссия Центра информированной общественности Вашингтонского университета - противостоять стратегической дезинформации, способствовать развитию информированного общества и укрепление демократического дискурса. Один из четырех членов-основателей EIP.
CIS	Центр интернет-безопасности (CIS)	CIS - некоммерческая организация, финансируемая CISA, которая направляет сообщения о дезинформации, поступающие от представителей государственных и местных органов власти, в социальные сети.
CISA	Агентство по кибербезопасности и защите инфраструктуры Министерства внутренней безопасности	Агентство по кибербезопасности и защите инфраструктуры (CISA), входящее в состав Министерства внутренней безопасности, заявило, что одной из его целей является создание "устойчивости к иностранным операциям влия и дезинформации... в тесном взаимодействии с межведомственными организациями, частным сектором, научными кругами и международными заинтересованными сторонами".

DFRLab	Исследовательская лаборатория Атлантического совета по цифровой криминалистике	Лаборатория DFRLab Атлантического совета занимается оперативным изучением дезинформации, отслеживанием информационных кампаний, разоблачением попыток загрязнения информационного пространства и созданием цифровой устойчивости. Один из четырех членос-основателей EIP.
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ И АДМИНИСТРАЦИИ	Разведка и анализ DHS	DHS I&A специализируется на обмене уникальными разведывательными и аналитическими данными с операторами и лицами, принимающими решения, с целью выявления и смягчения угроз для родины.
Дезинформация		CISA определяет дезинформацию как "преднамеренно созданную с целью ввести в заблуждение, навредить или манипулировать человеком, социальной группой, организацией или страной".
EI-ISAC	Центр обмена и анализа информации об инфраструктуревыборов	EI-ISAC выступал в качестве посредника между государственными и местными избирательными органами и платформами социальных сетей, предлагая централизованный механизм отчетности.
FITF	Целевая группа FBI по борьбе синостранным влиянием (FITF)	В 2017 году Федеральное бюро расследований (FBI) создало Целевую группу иностранного влияния (FITF) для выявления и противодействия злонамеренным операциям иностранного влияния, направленным против Соединенных Штатов.
GEC	Государственный департамент, Центр глобального взаимодействия	GEC — это многоведомственная организация, расположенная в Государственном департаменте, в задачи которой входит выявление и борьба с иностранной пропагандой и дезинформацией.

Graphika	Graphika, компания, занимающаяся цифровым интеллектом	Graphika — это аналитическая платформа для социальных сетей, которая специализируется на мониторинге онлайн-сетей и контента, чтобы получить представление о распространении информации.
Хейл, Джефф	Старший сотрудник CISA	
Jira	Программная система Jira	Jira — это программная система, используемая для создания тикетов, помогающих управлять проектами. EIP использовала «тикеты» JIRA для отслеживания и обмена отчетами о дезинформации с крупными компаниями, работающими в социальных сетях, а также с правительством и другими сторонами.
Кребс, Крис	Бывший директор CISA	
MDM		Дезинформация, дезинформация и дезинформация (прим. Использованы 3 разных слова Misinformation, Disinformation и Malinformation означающие одно и то же)
MDM Подкомитет	Консультативный комитет по кибербезопасности CISA (CSAC) Подкомитет по "Защите критической инфраструктуры от дезинформации и дезинформации"	Подкомитет MDM, который впоследствии был распущен, играл консультативную роль и состоял из руководителей компаний Big Tech, бывших чиновников федерального правительства и академических "экспертов" по дезинформации. На заседаниях подкомитета MDM присутствовали участники CISA.

<p>EIP</p>	<p>Партнерство за честность выборов ("EIP")</p>	<p>Первоначально названный "Партнерство по дезинформации на выборах", EIP представлял собой совместный проект по разработке возможностей реагирования на дезинформацию в режиме реального времени. EIP сотрудничала с рядом "внешних заинтересованных сторон", включая федеральное правительство. В EIP изначально входили четыре человека:</p> <ul style="list-style-type: none"> • Стэнфордская интернет-обсерватория; • Университет Вашингтона, Центр информированной общественности; <p>Graphika и Лаборатория исследований цифровой криминалистики Атлантического совета (DFRLab).</p>
<p>Команда MDM (CISA)</p>	<p>Группа CISA по борьбе с ошибками, дезинформацией и вредоносным влиянием (бывшая Целевая группа CISA по противодействию иностранному влиянию (CFITF))</p>	<p>В январе 2021 года CISA перевела свою целевую группу по противодействию иностранному влиянию в более гибкий режим, чтобы сосредоточиться на общем MDM, или так называемой "дезинформации, дезинформации и дезинформации". Согласно сайту CISA в феврале 2023 года, группе по MDM было поручено "повысить национальную устойчивость к MDM и деятельности по оказанию иностранного влияния". CISA публично заявила, что "иностраные и внутренние субъекты угроз использовать MDM-кампании для создания хаоса, путаницы и раскола".</p>
<p>MS-ISAC</p>	<p>Многоштатный центр обмена информацией и анализа</p>	<p>MS-ISAC — это совместное сотрудничество с Центром интернет-безопасности (CIS), поддерживаемое CISA, призванное служить центральным ресурсом по кибербезопасности для национальных штатов, местных, территориальных и племенные правительства (SLTT).</p>
<p>Скалли, Брайан</p>	<p>Бывший руководитель группы CFITF CISA (позднее – группы MDM)</p>	
<p>SIO</p>	<p>Стэнфордская интернет-обсерватория</p>	<p>SIO - междисциплинарная лаборатория в рамках Центра киберполитики Стэнфордского университета, занимающаяся изучением злоупотреблений в сфере информационных технологий с акцентом на неправомерное использование социальных сетей.</p>

<p>Стамос, Алекс</p>	<p>Директор по связям с общественностью; бывший. Главный специалист по безопасности в Facebook</p>	
-----------------------------	--	--

I. РОЛЬ CISA В СОЗДАНИИ EIP

Партнерство за честность выборов (EIP) было создано в июле 2020 года и включало в себя "ведущие национальные институты, занимающиеся изучением дезинформации и дезинформации в социальных сетях: Стэнфордскую интернет-обсерваторию, Центр информированной общественности (CIP) Вашингтонского университета, Graphika и Лабораторию цифровых криминалистических исследований Атлантического совета". Согласно посмертному отчету о цензурной деятельности EIP во время избирательного цикла 2020 года, в задачи EIP входило "выявление дезинформации до того, как она станет вирусной", а также "фиксация нарушений политики на платформах [социальных сетей]".

Возглавляемый Стэнфордом, EIP был разработан и основан в тесной координации с CISA, малоизвестным агентством в составе Министерства внутренней безопасности (DHS), созданным менее чем двумя годами ранее. Стэнфорд и другие, сотрудничая с федеральным правительством, создали EIP с явной целью нарушения гражданских свобод американцев: поскольку ни одно федеральное агентство "не занимается дезинформацией о выборах, поступающей из внутренних источников на территории США, и не имеет соответствующих полномочий", существует "критический пробел, который должны заполнить неправительственные организации". CISA и Стэнфорд создали EIP, чтобы заполнить этот "критический пробел" - неконституционный обходной путь для неконституционной цензуры.

A. Попытки цензуры предшественников CISA

Создание EIP происходило не в вакууме. До создания EIP летом 2020 года CISA прямо или косвенно участвовала в работе или рассмотрении как минимум трех других каналов передачи информации о дезинформации:

- (1) Коммутатор;
- (2) Центр обмена информацией и анализа инфраструктуры выборов (EI-ISAC);
- (3) "Портал передачи информации о дезинформации", которым будет управлять Центр безопасности Интернета (CIS), некоммерческая организация, частично финансируемая CISA.

Несмотря на конституционные недостатки этих каналов отчетности, эксперты CISA и "дезинформации" признали, что им нужен еще один способ отслеживать и удалять речь американцев в преддверии выборов 2020 года. EIP выполняла эту роль, функционируя, по словам главы EIP (и бывшего начальника службы безопасности Facebook) Алекса Стамоса, как "единое окно для местных избирательных органов, *Министерства здравоохранения* и организаций по защите избирателей", чтобы работать напрямую с платформами социальных сетей для цензуры речи американских политических кандидатов и комментаторов.

1. Коммутация, отказ от ответственности и угроза репрессий со стороны правительства.

Под "переключением" понимается практика федерального правительства по передаче запросов на удаление контента в социальных сетях от государственных и местных

избирательных органов на соответствующие платформы. Сотрудники CISA, участвующие в работе агентства по переключению, описывают этот процесс как "ресурсоемкий".

Документы и информация, полученные Комитетом и Специальным подкомитетом, свидетельствуют о том, что CISA знало о серьезных правовых и конституционных проблемах, связанных с "переключением» (в этом процессе, по свидетельству секретаря DHS Майоркаса, CISA больше не участвует). Включение в CISA длинного и постоянно меняющегося юридического отказа свидетельствует о том, что внутри агентства понимали, что участие федерального правительства в подобном (прямом) общении с платформами социальных сетей по поводу сообщений и контента рядовых американцев вызывает серьезные юридические вопросы. Хотя "отказ от ответственности» якобы служил письменным обязательством по предотвращению репрессий со стороны правительства, по иронии судьбы, в нем CISA на самом деле описывал, как многоведомственный подход федерального правительства к цензуре предоставляет ряд возможностей для репрессий со стороны правительства, если компании не подчиняются.

Усилия DHS по оказанию помощи в информировании о "дезинформации" на платформах социальных сетей предпринимались еще до создания такой структуры как CISA. Бывший директор CISA Кристофер Кребс в расшифрованном интервью Комитету и Отдельному подкомитету сообщил, что предшественник CISA - Управление национальной защиты и программ (NPPD), занималось подменой информации до создания CISA. После создания CISA "переключение» продолжалось в течение всего избирательного цикла 2020 года, но было прекращено к выборам 2022 года.

Министерство здравоохранения в ходе судебных разбирательств и в Комитете настаивало на том, что роль CISA в "переключении" заключалась лишь в том, что посредник способствовал обмену сообщениями, но не играл существенной роли в процессе оповещения о "дезинформации". Например, в июле 2023 года министр DHS Майоркас заявил Комитету: *"все это сводилось к тому, что мы выступали в качестве посредника между избирательными органами и представителями социальных сетей; мы не выносили суждений"*.

Глава целевой группы CISA по противодействию иностранному влиянию Брайан Скалли дал показания в ходе рассмотрения дела *"Миссури против Байдена"*, заявив, что *"роль CISA заключалась в передаче отчетности, полученной от избирательных органов, ... платформам социальных сетей"*. Однако документы, полученные Комитетом и отдельным подкомитетом, показывают, что "переключение" может включать в себя и более предметное взаимодействие.

Например, в одной цепочке электронных писем старший сотрудник CISA объяснил офису госсекретаря штата Колорадо, как Twitter ранее обрабатывал отмеченные пародийные аккаунты и как Twitter, вероятно, будет обрабатывать отмеченные в этой

From: Scully, Brian [REDACTED]@cisa.dhs.gov
Sent: 11/3/2020 4:22:20 PM
To: [REDACTED]@fb.com
CC: Masterson, Matthew [REDACTED]@cisa.dhs.gov; [REDACTED]@fb.com
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Both a and b are correct. Not a poll worker and no ballots destroyed.

Brian

Brian Scully
DHS Countering Foreign Interference Task Force
National Risk Management Center
[REDACTED]
[REDACTED]@cisa.dhs.gov

From: [REDACTED]@fb.com
Sent: Tuesday, November 3, 2020 4:18:42 PM
To: Scully, Brian [REDACTED]@cisa.dhs.gov
Cc: Masterson, Matthew [REDACTED]@cisa.dhs.gov; [REDACTED]@fb.com
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hello again, wanted to follow up on a few points just to be crystal clear -- could you please confirm that (a) the worker in question is not a pollworker; or (b) that he did not, in fact, destroy ballots (or at least that there is no evidence that he destroyed ballots).

Would appreciate this clarity tremendously, thank you so much.

From: [REDACTED]@fb.com
Sent: Tuesday, November 3, 2020 3:57:18 PM
To: Scully, Brian [REDACTED]@cisa.dhs.gov
Cc: Masterson, Matthew [REDACTED]@cisa.dhs.gov; [REDACTED]@fb.com
Subject: Re: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Appreciate the swift response!!

From: Scully, Brian [REDACTED]@cisa.dhs.gov
Sent: Tuesday, November 3, 2020 3:52:45 PM
To: [REDACTED]@fb.com
Cc: Masterson, Matthew [REDACTED]@cisa.dhs.gov
Subject: Fwd: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

Statement from PA. Confirms person was not poll worker.

Brian

Tranche 2

CISA to HJC 3/22/23 Letter & 4/28/23 Subpoena
Page 000470

Brian Scully
DHS Countering Foreign Interference Task Force
National Risk Management Center
[REDACTED]
[REDACTED]@cisa.dhs.gov

From: CFITF [REDACTED]@hq.dhs.gov
Sent: Tuesday, November 3, 2020 3:43:52 PM
To: CFITF All [REDACTED]@hq.dhs.gov
Subject: FW: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

From: [REDACTED]@cisecurity.org
Sent: Tuesday, November 3, 2020 8:43:42 PM (UTC+00:00) Monrovia, Reykjavik
To: CFITF
Subject: EIP-664 Poll worker in Erie PA says announces on Instagram they will throw away Pro-Trump votes

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Reply above this line.

[REDACTED]@cisecurity.org commented:
The county has issued an official statement on the matter:

Помимо того, что CISA, по существу, высказывается или комментирует сообщения о дезинформации, передаваемые компаниям социальных сетей, CISA также может попытаться повлиять на решения компаний социальных сетей, принимая решения о том, следует ли и сколько раз следует предпринимать последующие действия. Согласно документам, полученным Комитетом в соответствии с повесткой в суд, начиная примерно с марта 2020 года CISA использовало отказ от ответственности, в котором говорилось, что DHS и CISA не являются "источником" дезинформации, но что отчет *"может быть также передан правоохранительным или разведывательным органам"*.

Отказ от ответственности указывал: *"В случае если CISA обратится за дополнительной информацией, такой запрос не является требованием или запросом. Ответ на этот запрос является добровольным, и CISA не будет предпринимать никаких действий, благоприятных или неблагоприятных, на основании решения о том, отвечать или не отвечать на этот повторный запрос информации"*.

From: [REDACTED]@twitter.com>
Sent: Tuesday, March 17, 2020 3:42 PM
To: Scully, Brian [REDACTED]@cisa.dhs.gov>
Subject: Re: FW: Potential Twitter Account

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Well, thanks for being patient on that call. One day at a time!

I just heard back regarding the additional investigation. The account is not in violation of any policies.

Let me know if you have any questions!

On Tue, Mar 17, 2020 at 12:05 PM Scully, Brian [REDACTED]@cisa.dhs.gov> wrote:

Hi [REDACTED]

Received the below reporting on a potential bad Twitter account.

Thanks,
Brian

The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source - this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

In the event that CISA follows up to request further information, such as a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

К сентябрю 2020 года электронные письма CISA стали включать дополнительный абзац, в котором говорилось, что *"Министерство здравоохранения подтверждает, что оно не имеет и не стремится удалять информацию, размещенную на платформах социальных сетей"*, но при этом открытой оставлялась возможность того, что *"информация также может быть передана правоохранительным органам или разведке"*.

From: Scully, Brian <[REDACTED]@cisa.dhs.gov>
To: [REDACTED]
Sent: 9/15/2020 6:13:02 AM
Subject: FW: Fwd:
Attachments: Screensho.jpg

Email 2.

Thanks,
Brian

Neither the U.S. Department of Homeland Security (DHS) nor the Department's Countering Foreign Interference (CFI) Task Force is the originator of this information. The CFI Task Force is forwarding this information, unedited, from its originating source – this information has not been originated or generated by DHS or the CFI Task Force. This information may also be shared with law enforcement or intelligence agencies.

DHS affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. DHS makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, DHS will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that the CFI Task Force follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and DHS will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

Проще говоря, юрист одной из компаний, работающих в социальных сетях, может понять, что DHS и правоохранительные органы (например, FBI) могут знать, что компания получила сообщение о дезинформации, но только DHS обязуется не предпринимать никаких неблагоприятных действий против компании на основании ее "решений о том, как или иначе использовать эту информацию" - то есть FBI или другие правоохранительные органы (например DHS) могут предпринимать действия, если компания, работающая в социальных сетях, не провела цензуру должным образом.

В следующем месяце CISA, как оказалось, сузила формулировку отказа от ответственности, заявив, что CISA не будет "предпринимать никаких действий, благоприятных или неблагоприятных, на основании решений о том, как или иначе использовать эту информацию". Более ограниченный отказ от ответственности теперь гласил только следующее: "*CISA подтверждает, что не имеет и не стремится к тому, чтобы удалять или редактировать информацию, размещенную на платформах социальных сетей. CISA не дает никаких рекомендаций относительно того, как информация, которой она делится, должна обрабатываться или использоваться представителями социальных сетей*". CISA также удалила целый абзац из своего заявления об отказе от ответственности, в котором говорится о последующих сообщениях. В текущем федеральном судебном процессе "*Миссури против Байдена*" администрация Байдена ссылалась на включение этого отказа в качестве доказательства того, что CIS и EIP не являются "партнерами CISA по цензуре" и что отказ от ответственности поддерживает компании в применении их политики "независимо". Но, как было описано выше вместо того, чтобы гарантировать, что компании не почувствуют давления, в пересмотренном

On Tue, Oct 27, 2020 at 4:09 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Please see below report from Washington.

Thanks,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

отказе от ответственности подчеркивалось, что CISA будет привлекать правоохранительные органы и что CISA не может гарантировать, что правоохранительные органы не предпримут неблагоприятных действий на основании того, как платформы социальных сетей решили отреагировать на сообщение о дезинформации.

Примерно 28 октября 2020 года CISA восстановила в своем отказе от ответственности пункт, касающийся последующих сообщений. На сегодняшний день CISA предоставила Комитету и Отдельному подкомитету более двадцати электронных писем, датированных периодом с 1 октября по 27 октября, в которых отказ от ответственности не содержит пункта о последующих контактах.

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7F0C5C3963484338B25437EAAE765D72 [REDACTED]]
Sent: 10/19/2020 6:34:53 PM
To: [REDACTED]@twitter.com]
CC: [REDACTED]@twitter.com]; [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]@hq.dhs.gov]
Subject: RE: FW: Case #CIS-MIS000041: Twitter misinformation regarding ballots dumped on highway in CT

Checking in to see if there is anything that can be shared in regards to this reported incident.

From: [REDACTED]@twitter.com>
Sent: Thursday, October 15, 2020 11:42 AM
To: [REDACTED]@cisa.dhs.gov>
Cc: [REDACTED]@twitter.com>; [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]@hq.dhs.gov>
Subject: Re: FW: Case #CIS-MIS000041: Twitter misinformation regarding ballots dumped on highway in CT

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi [REDACTED]
We will ask the team to review.

Best,
[REDACTED]

On Wed, Oct 28, 2020 at 6:29 PM Scully, Brian <[REDACTED]@cisa.dhs.gov> wrote:

Please see below report from Washington.

Regards,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

Неудивительно, что примерно в это же время CISA начала переписываться с социальными сетями по поводу сообщений, отмеченных агентством, как показано в примере ниже.

Во время интервью с Комитетом Мэтт Мастерсон, бывший старший советник по кибербезопасности в CISA, показал, что юристы CISA проводили внутренние обсуждения по поводу отказа от ответственности и того, затрагиваются ли конституционные права и гражданские свободы:

Вопрос: припоминаете ли вы какие-либо обсуждения во время вашей работы в CISA относительно того, существуют ли какие-либо конституционные последствия, если работа CISA будет связана с, скажем так, дезинформацией, исходящей от внутренних субъектов?

Ответ: Я не помню конкретного разговора на эту тему. Я помню, что, очевидно, юристы CISA были вовлечены, как я уже указывал ранее, например, в разговор об отказе от ответственности, включая юристов по конституционным и гражданским свободам. Но я не знаю и не помню конкретного разговора на эту тему.

Включение CISA в письмо оговорки о том, следует ли трактовать частые электронные письма CISA как просьбу или отказ отвечать на них может привести к "неблагоприятным" действиям, свидетельствует о том, что юристы DHS, как минимум, сочли необходимым рассмотреть вопрос о том, является ли практика подмены юридически и конституционно обоснованной. Но вместо того, чтобы прекратить эту практику (как CISA, очевидно, сделала к выборам 2022 года), осенью 2020 года CISA решила продолжить свои усилия по цензуре, добавив бессмысленный отказ от электронной почты в качестве слабой и прозрачной попытки удовлетворить вопиющие опасения по поводу Первой поправки.

Крайне важно, что отказ от ответственности в CISA включает в себя зловещую строку: "Эта информация также может быть передана правоохранительным или разведывательным органам". В то время как отказ от ответственности гласил, что "CISA не будет предпринимать никаких действий, благоприятных или неблагоприятных, по отношению к компаниям социальных сетей на основании решений о том, как или иначе использовать эту информацию", отказ от ответственности не дает никаких гарантий относительно возмездия со стороны "правоохранительных или разведывательных органов", с которыми CISA может поделиться соответствующим контентом социальных сетей.

Угроза расправы со стороны правоохранительных органов усиливается тем фактом, что FBI информировало представители социальных сетей, когда CISA предоставляла FBI отчет о "дезинформации". Комитет и специальный подкомитет получили множество документов, которые показывают, что представители социальных сетей знали, что CISA обменивается информацией с федеральными разведывательными и правоохранительными органами, включая FBI.

From: Elvis Chan
Date: Sunday, October 4, 2020 at 2:31 PM
To: [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED]
Subject: Tipper & Next FITF Meeting
Facebook folks,
First, I got a tip from CISA that there is a Facebook page that is misleading voters about time, place, and manner of voting, as well as trying to elicit Facebook user information. Please review and take whatever steps you deem appropriate. We would appreciate it if you let us know whether you take any actions based on this referral.

Другими словами, CISA сообщила компаниям социальных сетей, что CISA, правоохранительные и разведывательные органы могут получить отчет о дезинформации, но в заявлении говорилось лишь о том, что CISA не будет принимать ответных мер в отношении компаний социальных сетей, если они не смогут подвергнуть цензуре отмеченный контент. CISA не давала никаких обещаний относительно того, что может сделать FBI или одна из спецслужб. И представители социальных сетей прекрасно знали, что CISA направляет некоторую часть сообщений в FBI (если не в другие федеральные правоохранительные или разведывательные органы).

В своем интервью перед Комитетом и Специальным подкомитетом бывший руководитель Facebook Алекс Стамос заявил, что взаимодействие с правоохранительными органами, такими как FBI, вызывает у компаний больше опасений, чем CISA, объяснив, что *"вы не можете случайно пообщаться с агентом FBI, если вы являетесь руководителем компании. Это небезопасно. Рядом с вами сидят люди, которые получают \$3 000 в час"*. Мистер Стамос продолжил:

Вопрос: Что вы имеете в виду, говоря, что вы не можете вести непринужденный разговор с FBI? Почему?

Ответ: Я думаю, адвокаты защиты скажут вам, что агенты FBI всегда начеку - вам может показаться, что вы ведете с ними дружескую беседу, но вы никогда не знаете, являетесь ли вы на самом деле целью. И я думаю, что было много ситуаций, когда компании пытались привлечь FBI, потому что они стали жертвами, скажем, киберпреступления, но по итогу их или их руководителей наказывали. Сотрудничать с правоохранительными органами, обладающими полномочиями по принуждению, просто рискованно, если вы являетесь частью какой-то крупной организации, а в отношении нее может вестись какое-то расследование, о котором вы даже не знаете.

Вопрос: Как вы думаете, та точка зрения, которой вы только что поделились в отношении FBI, была широко распространена среди руководителей Facebook, когда вы работали в компании?

Ответ: Конечно, политика компании заключалась в том, что руководитель не мог разговаривать с FBI без присутствия адвокатов.

Вопрос: Даже если правительство считает, что интересы совпадают, может случиться так, что впоследствии правительство передумает. Вы считаете так?

Ответ: Да.

Вопрос: Хорошо. И этот факт хорошо известен руководителям технологических компаний?

Ответ: Да. И я думаю, что все руководители публичных компаний понимают, что есть много частей правительства, которые могут наказать вас за деятельность, которую вы считали правильной.

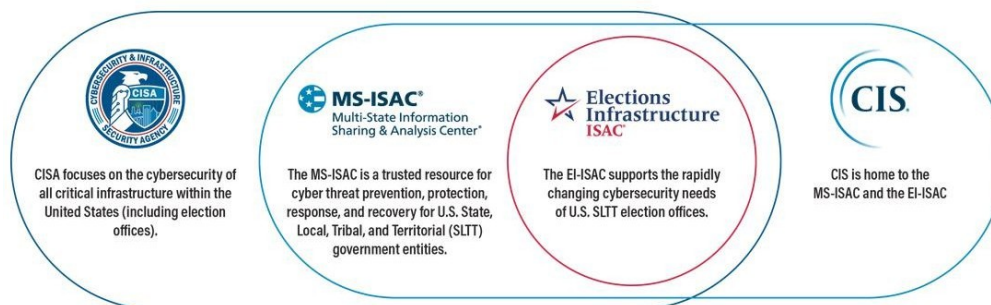
Почему же CISA, которая задействовала этот "ресурсоемкий" процесс "переключения», пошла на то, чтобы переписать отказ от ответственности в надежде обойти серьезные конституционные проблемы, и напрямую привлекла федеральные правоохранительные и разведывательные органы? Потому что CISA хотела удалить помеченный контент, а "переключение" обеспечивало эффективное средство для этого. Во время дачи показаний по делу "Миссури против Байдена" старший сотрудник CISA Брайан Скалли признал, что CISA действительно понимала, что ее сообщения приведут к удалению контента платформами.

2. EI- ISAC

Центр интернет-безопасности (CIS) — это некоммерческая организация, базирующаяся в Нью-Йорке, которая была создана «в партнерстве с Агентством кибербезопасности и защиты инфраструктуры США (CISA)».

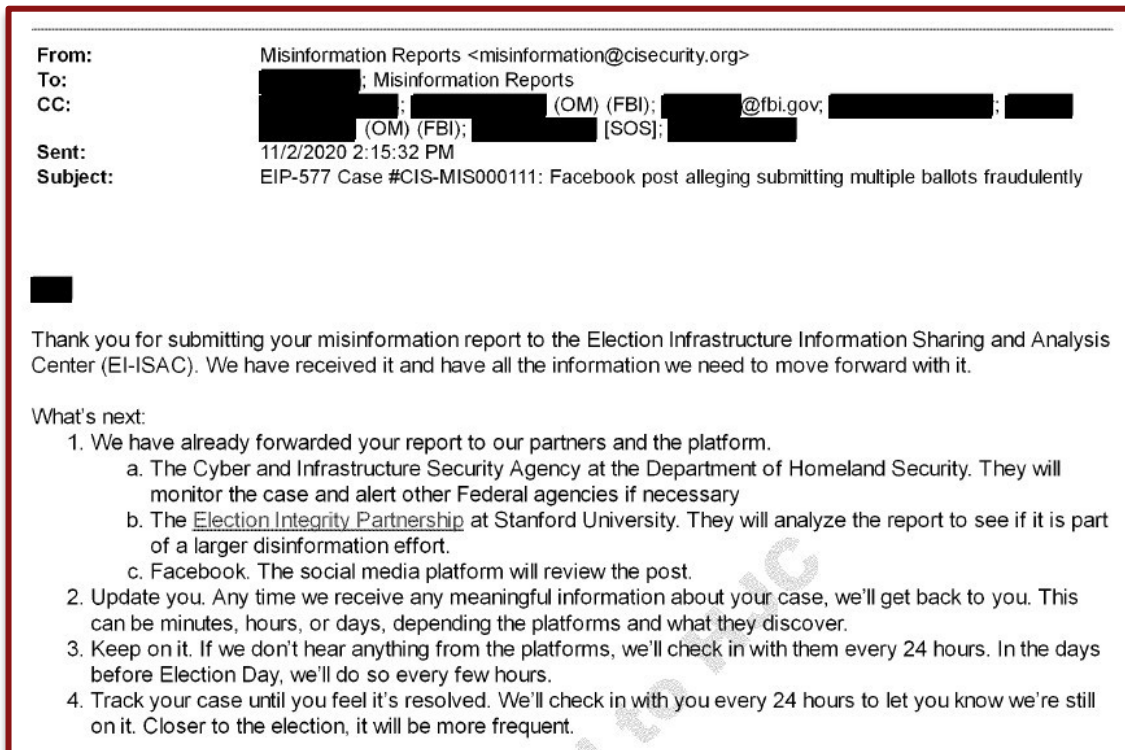
CIS управляет Центром обмена информацией и анализа инфраструктуры выборов (EI-ISAC), который финансируется вместе с Многоштатным центром обмена информацией и анализа (MS-ISAC). Оба структуры ISAC получили финансирование в размере 27 миллионов долларов на 2024 год.

EI-ISAC — это канал обмена информацией, используемый государственными и местными избирательными органами для передачи сообщений о предполагаемой «дезинформации» на платформы социальных сетей. Во время промежуточных выборов 2018 года все пятьдесят штатов участвовали в EI-ISAC. Более того, согласно свидетельским показаниям, данным Комитету и Специальному подкомитету, сотрудники EI-ISAC считаются сотрудниками CIS.



Согласно отчету EIP, в избирательном цикле 2020 года «EI-ISAC служил единственным каналом, по которому сотрудники избирательных комиссий могли сообщать платформам ложную или недостоверную информацию». В отчете также объясняется

функция EI-ISAC по отношению к CIS: «Служа в качестве единого центра. благодаря интерфейсу отчетности, EI-ISAC позволил сотрудникам избирательных комиссий сосредоточиться на выявлении и противодействии дезинформации о выборах, в то время как CIS и его партнеры передавали информацию на соответствующие платформы социальных сетей». В отчете также описывается роль CISA, отмечается, что «Целевая группа по противодействию иностранному влиянию (CFITF), подкомпонент CISA, помогла в процессе отчетности и в реализации усилий по противодействию дезинформации на выборах». Отчеты о дезинформации, поданные в EI-ISAC в преддверии выборов 2020 года, «также направлялись в систему тикетов EIP».



Подобно коммутаторам, EI-ISAC выступал в качестве посредника между государственными и местными избирательными органами и платформами социальных сетей, предлагая централизованный механизм отчетности в попытке удалить контент из социальных сетей. Например, 2 ноября 2020 года должностное лицо избирательного штата направило сообщение о предполагаемой дезинформации в EI-ISAC, который, в свою очередь, переслал сообщение на соответствующую платформу. Согласно ответу EI-ISAC чиновнику штата, EI-ISAC также передал сообщение в CISA и EIP.

From: Aaron Wilson [/O=EXCHANGE/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=]
Sent: 1/3/2020 11:09:01 AM
To: Matt Masterson []@hq.dhs.gov]; []@associates.cisa.dhs.gov'
CC: HALLGREN, JILL (CTR) []@associates.cisa.dhs.gov]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=]; []@cisa.dhs.gov
Subject: Misinformation Reporting Portal
Attachments: Election Infrastructure Misinformation Reporting Portal Proposal v1.docx

Matt, Brian,

I have spoken to both of you separately about a concept we are developing to help election officials report mis/disinformation during the 2020 elections. You both, along with NASS and NASED, indicated our proposal may be helpful. I am attaching a brief write-up I made that describes it. Your feedback is welcome.

We are beginning the development of the misinformation reporting portal with the hope that it could be piloted in the Presidential Preference Primaries. I am planning on setting up a call between you all, NASS, NASED, and us as soon as I have something to show you. My goal is to demonstrate the basic capabilities by the end of this month. Please stay tuned and let me know if you have any feedback on the write up.

Thanks,

Aaron

3. Портал для сообщений о дезинформации.

Даже после создания коммутатора и EI-ISAC CISA, и CIS в течение первой половины 2020 года вели внутренние обсуждения и дискуссии с представителями социальных сетей о том, стоит ли создавать «портал для сообщений о дезинформации». В соответствии с многочисленными повестками Комитет и Подкомитет получили документы, раскрывающие усилия CISA и CIS по созданию третьего направления «сообщения о дезинформации».

Уже в январе 2020 года чиновники CISA вели переговоры с CIS о создании «портала сообщений о дезинформации». 3 января Аарон Уилсон, старший директор по безопасности выборов в CIS, отправил электронное письмо старшим должностным лицам CISA Мэтту Мастерсону и Брайану Скалли, написав: *«Я говорил с вами обоими по отдельности о концепции, которую мы разрабатываем, чтобы помочь сотрудникам избирательных комиссий сообщать о дезинформации во время выборов 2020 года. Вы оба... отметили, что наше предложение может быть полезным»*. Мистер Уилсон указал, что его цель - *«продемонстрировать основные возможности [портала для сообщений о дезинформации] к концу этого месяца»*.

From: Aaron Wilson [/O=EXCHANGE/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=]
Sent: 1/20/2020 2:09:04 PM
To: @fbi.gov
CC: Wedekind, Kirby @hq.dhs.gov; HALLGREN, JILL (CTR) @associates.cisa.dhs.gov; Scully, Brian @cisa.dhs.gov; Josiah, Chad @cisa.dhs.gov; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=]
Subject: Misinformation Reporting Portal FBI Briefing

JC,

It was great to meet you last week. As I mentioned, CIS is working with DHS on a misinformation reporting portal. The intent is to build a web portal to manage the reporting of election infrastructure misinformation from local and state election officials to the social media platforms. We are working with our partners at the National Association of Secretaries of States (NASS), National Association of State Election Directors (NASED), and DHS to vet this idea. We are currently building a prototype and will have something to show by the first week of February.

Given the FBI's role, I'd like to bring you up to speed on our efforts and get your feedback on this effort, and hopefully your engagement. Our primary goals are to:

- Provide election officials a single place/POC to report misinformation
- Ease the burden on election officials when they go to report the misinformation
- Collect the information necessary for the FBI, DHS, and social media platforms to do their jobs
- Expedite and enhance the process by which social media companies are made aware of the misinformation
- Provide visibility about what election officials are reporting to: other election officials, DHS, NASS, NASED, FBI, etc.
- Facilitate information sharing between election officials about what they are seeing, what to look out for, etc.
- Provide meaningful feedback to election officials on the status of their misinformation reports

Are you available for a call this week to discuss more?

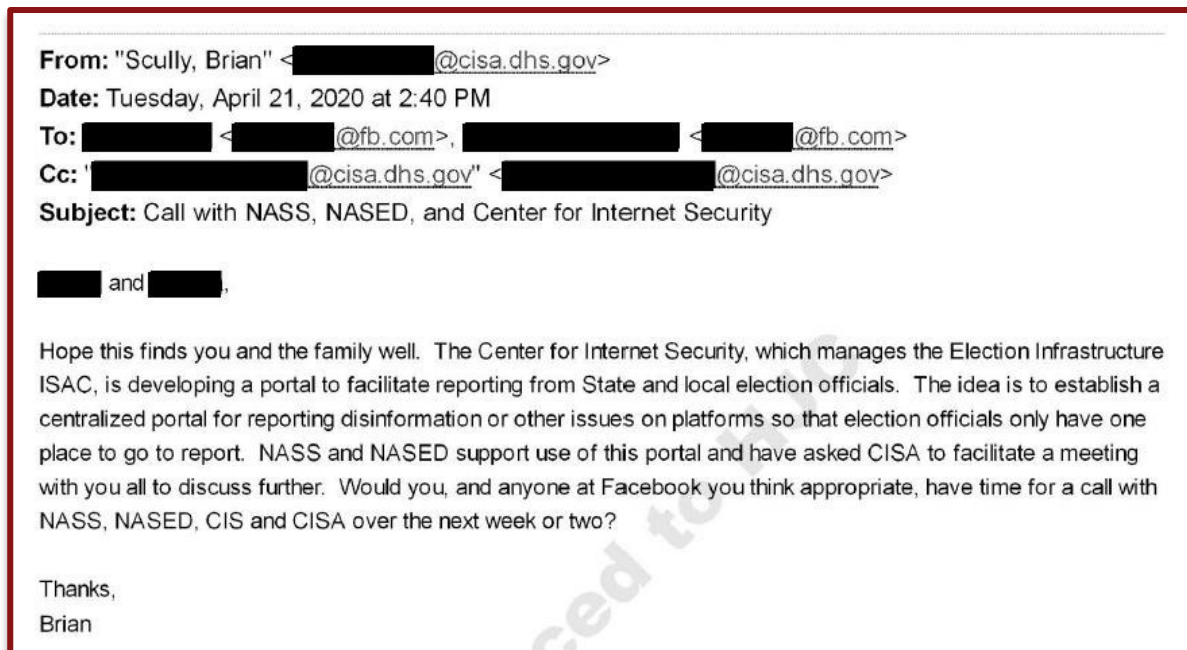
Thanks,

Aaron

В январе 2020 года о совместных усилиях CIS и CISA даже проинформировали правоохранительные органы: CIS обратился к FBI, заявив, что «CIS работает с DHS над порталом для сообщений о дезинформации. Цель состоит в создании веб-портала для управления сообщениями о дезинформации избирательной инфраструктуры от местных и государственных избирательных органов к платформам социальных сетей. Мы работаем с нашими партнерами из Национальной ассоциации секретарей штатов (NASS), Национальной ассоциации директоров по выборам штатов (NASED) и DHS, чтобы проверить эту идею. В настоящее время мы создаем прототип, и к первой неделе февраля нам будет что показать».

CISA приняла на себя активную роль в продвижении предложения CIS о создании портала для сообщений о дезинформации, способствуя проведению встреч между соответствующими сторонними некоммерческими организациями и платформами социальных сетей. Например, 21 апреля 2020 года Брайан Скалли отправил электронное письмо двум сотрудникам Facebook, в котором Скалли написал: «Идея состоит в том, чтобы создать централизованный портал для сообщения о дезинформации, чтобы у

сотрудников избирательных комиссий было только одно (прим. централизованное) место, куда можно обратиться с отчетом».



Однако к маю 2020 года планирование портала для сообщений о дезинформации CIS-CISA зашло в тупик. Согласно внутренним записям телефонного разговора между сотрудниками Facebook и DHS по поводу «Портала сообщений о дезинформации», «DHS не может открыто одобрить портал, но в кулуарах сообщило, что [Национальная ассоциация государственных секретарей]/[Национальная ассоциация государственных директоров по выборам] сказала им, что многим штатам было бы проще иметь «один канал отчетности», а CISA и ее ISAC хотели бы иметь входящий портал в то же время, что и платформы». Менее чем через два месяца был создан EIP, который должен был служить именно этой цели.

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Sunday, May 31, 2020 10:44 AM
To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>
Subject: CIS & NASS/NASED & DHS Call

Team,

Wanted to share a read-out from our call late Friday with DHS, NASS & NASED. Great job by [REDACTED] & [REDACTED]

No action for us now; however, we will reconvene after a Beta test of their proposed reporting portal in the next few weeks.

Best,
[REDACTED]

TL;DR: On May 29, U.S. Public Policy ([REDACTED]), P&G Outreach ([REDACTED]), and Security Policy ([REDACTED]) met with DHS, the Center for Internet Security, and NASS/NASED about a **"Misinformation Reporting Portal"** that CIS is developing for state and local-level elections officials to report mis/disinformation and IO-type activity concerning election interference to the platforms, with a focus on Facebook, Twitter, and Google. Following a beta test CIS will do in Florida, Colorado, North Carolina, and Rhode Island in early June, they would like to do a demo for Facebook. Internally, Facebook would prefer our independent reporting channel which makes us an industry leader, and was reported as successful by all parties on this call and is monitored 24/7, but we are aware that if the majority group moves towards a centralized channel, there are PR challenges for not participating.

o **Highlights:**

- **DHS cannot openly endorse the portal** but has behind-the-scenes signaled that NASS/NASED has told them it would be easier for many states to have "one reporting channel" and CISA and its ISAC would like to have incoming the same time that the platforms do.
- CIS is in discussions with **Twitter** to gauge their interest, and it was unclear what engagement has been with **Google**.
- CIS is talking with **Graphika**, which has said it is interested in nationwide trends that the reporting portal may reveal.
- CIS is talking with the **Belfer Center**, which is developing an "IO Playbook & Training" that may be released in the coming months before November 2020.
- NASS/NASED is supportive, but **not all the states are onboard** – CIS said they would like to launch with platforms supportive and engaged and bring states incrementally along.
- **CIS would like some sort of API with Facebook** – such a set up may be impossible, and CrowdAngle, if this progresses, may be the way to go.

From: [REDACTED] <[REDACTED]@fb.com>
Sent: Thursday, July 16, 2020 7:41 AM
To: Aaron Wilson <[REDACTED]@cisecurity.org>; [REDACTED] <[REDACTED]@cisecurity.org>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; Scully, Brian <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@sso.org>; [REDACTED] <[REDACTED]@sso.org>; [REDACTED] <[REDACTED]@nased.org>
Cc: [REDACTED] <[REDACTED]@fb.com>; Matt Masterson <[REDACTED]@hq.dhs.gov>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; John Gilligan <[REDACTED]@cisecurity.org>; Mike Garcia <[REDACTED]@cisecurity.org>; Ben Spear <[REDACTED]@cisecurity.org>
Subject: RE: Call with CIS/NASS/NA SED and Facebook, RE: Social Media Misinformation Reporting Portal

Thank you so much, Aaron – very much appreciate the time for meeting earlier this week.

- Below are the questions from our various teams (there is a wee bit of duplication on some of them, but we are erring on the side of inclusiveness for maximum understanding and insight).
- For next meeting time, should we plan on doing that after getting a sense of responses and feasibility on the below questions? From our end, early August window would be good, if you would like to suggest some time blocks (outside of Mondays and Fridays, if possible). [REDACTED] could reach out to [REDACTED] from our team who graciously help coordinate on the previous meeting).

Questions:

1. What steps will CIS take to ensure that only mis/disinformation type leads will be surfaced via the portal related to voter suppression/interference to ensure that scope is narrowly defined, and how will CIS ensure quality control?
2. What access controls will be in place to ensure that only vetted state-level and platform-level onboarded partners will have access to view and analyze the information and how will these access controls be maintained?

Представители социальных сетей, включая Facebook и Twitter, в течение нескольких месяцев обсуждали с CIS предложение о создании портала дезинформации. После первоначального ознакомления с предложением в мае сотрудники Facebook направили в CIS список вопросов о портале 16 июля 2020 года.

3. To what extent can the U.S. government, other platforms, and others view back and forth with platforms and also cross-platform content or escalations, and how will this be controlled? Are you open to a version of the portal that forwards intake to a platform email, with further back and forth being handled just between the platform and the reporter (but the initial report is available to other states/platforms/portal users).
4. How will portal access be determined?
5. What is the limit on the number of people and organizations who will have access to the portal?
6. What is the data retention period for the portal?
7. Is it the expectation that the portal will be a short-term or long-term project?
8. How will the portal sort information so that it is of importance and properly sorted by various terms of service depending on the platform, so that recipients of the information will be able to triage it quickly and deconflict?
9. What quality control measures will be in place to ensure that the escalations sent to the portal are not "noise" and will be properly described and not duplicative, and also not repeats of the same already-escalated content, to avoid burdening resource, operational, and engineering bandwidth during a very high-stakes election cycle where timely response and action will be critical?
10. Is the expectation that the portal will replace the dedicated 1:1 reporting channels maintained by the platforms, either in the short or long terms?
11. How will the portal advise whether or not a particular escalation has already been reported to the platforms and avoid sending an alert when such an escalation has already been made?
12. To what extent can the portal be used to surface trends and patterns across platforms that can be shared, if of value, while maintaining direct platform-level communication from the states?
13. Which states are not yet onboarded to the portal and what is the plan for those states?
14. How will the portal be made user-friendly for the wide range of users?
15. Who will train users on the portal, trouble shoot, and provide tech support for the portal?
16. What will turn around time, both before the election, and on election day, for portal support and login issues?
17. How long does it take to approve access to the portal? Will there be expedited review closer to the election?
18. How will the portal enable platform-specific back and forth?
19. Will the portal provide links and not just screenshots to enable swift actioning of context?
20. How does the portal plan to surface behavior-type or pattern-type signals, as opposed to discrete pieces of content?
21. How will the portal prevent the same escalation being reported multiple times by multiple sources?
22. Aside from receiving "intake," and evaluating that, if possible, pursuant to platform-specific terms of service, what are other expectations of engagement from the platforms?

Misinformation Reporting Portal Discussion with Twitter

May 11, 2020, 2pm to 3pm ET

VTC Dial in information: TBD

Agenda and Candidate Discussion Points

Welcome – Brian Scully, CISA or Matt Masterson, CISA

- DHS appreciates the efforts of Twitter to help improve the ability of elections officials to submit mis/disinformation (e.g., the recent addition of an electronic submission capability). Also, we appreciate the opportunity to have a discussion with Twitter about the use of a Portal to improve the ability of elections officials to report mis/disinformation and to provide elections officials with visibility of similar reports and across platforms. Hopefully, this effort will streamline and make more efficient the process that has been improving over the past several years, but is still far from efficient and effective from the perspective of the elections community and Federal government.

Twitter был первоначально проинформирован о портале в мае 2020 года, согласно повестке дня заседания, предоставленной Комитету. Согласно повестке дня, «DHS высоко оценивает усилия Twitter по улучшению возможностей сотрудников избирательных комиссий по подаче дезинформации». Повестка дня также свидетельствует о том, что CISA и федеральное правительство в целом стремятся улучшить работу цензуры через портал: «Надеюсь, эти усилия позволят упорядочить и сделать более эффективным процесс, который совершенствовался в течение последних нескольких лет, но все еще далек от полной эффективности и результативности с точки зрения избирательного сообщества и федерального правительства». Как указано в приведенной ниже выдержке, первые лица CISA должны были открыть дискуссию о потенциальном портале CIS для сообщений о дезинформации.

Как и Facebook, Twitter также представил CIS список вопросов, касающихся портала.

From: [REDACTED] [REDACTED]@twitter.com]
Sent: 6/16/2020 3:59:09 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Aaron Wilsonb0d]
CC: [REDACTED] [REDACTED]@twitter.com]; Scully, Brian [REDACTED]@cisa.dhs.gov]; Masterson, Matthew [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey [REDACTED]@cisa.dhs.gov]; Snell, Allison [REDACTED]@cisa.dhs.gov]; John Gilligan [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdl)/cn=recipients/[REDACTED]]; [REDACTED] [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Amanda Burkart66d]; Amy Cohen [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Maria Benson [REDACTED]@sso.org]; Leslie Reynolds [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; [REDACTED] [REDACTED]@twitter.com]; [REDACTED] [REDACTED]@twitter.com]; [REDACTED] [REDACTED]@twitter.com]; [REDACTED] [REDACTED]@twitter.com]
Subject: Re: Reporting Portal with CIS, NAASS, NASED and Twitter

All,

Below are some of the questions we hope to discuss during our next call. Looking forward to it!

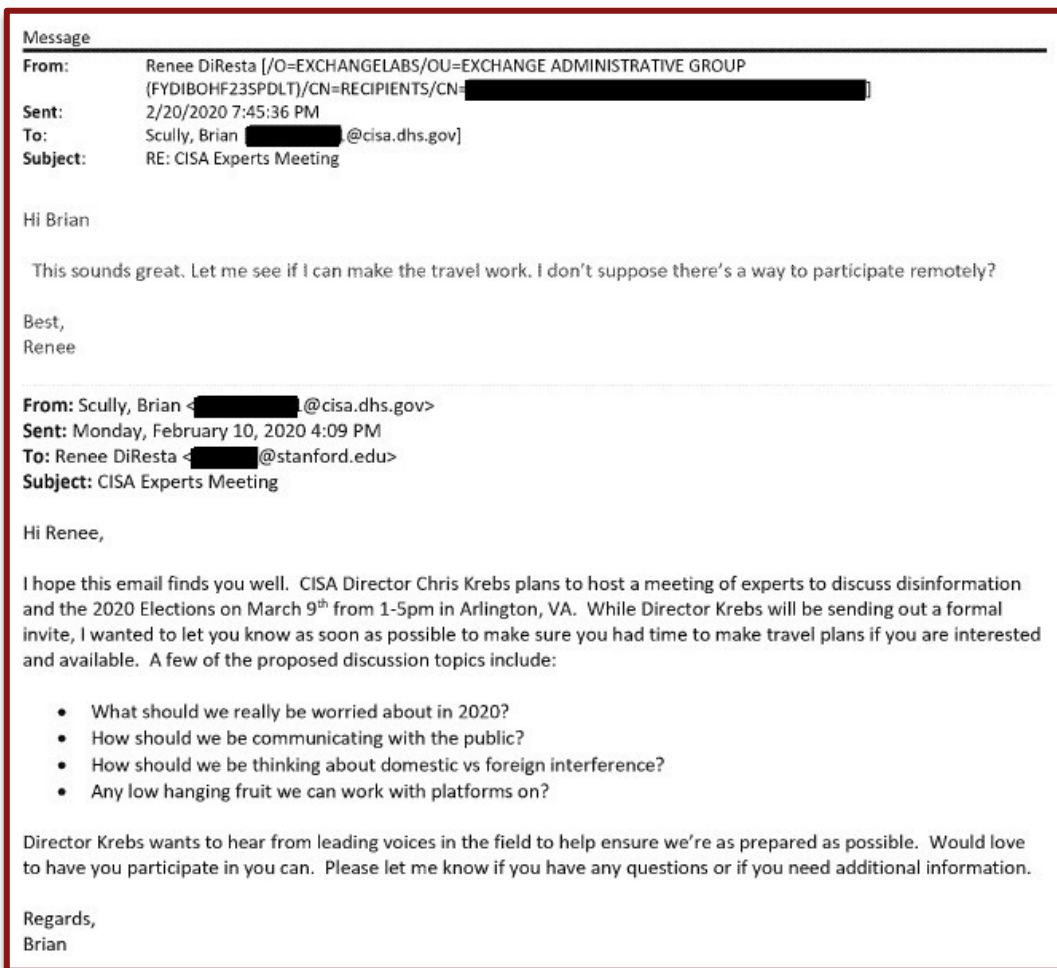
[REDACTED]

Эти документы свидетельствуют о том, что CISA и CIS заставили представители социальных сетей серьезно задуматься и рассмотреть предложение о создании портала для сообщений о дезинформации, хотя в конечном итоге такой портал создан не был.

- 1.
2. Will there be some sort of agreement or terms of reference that will align all participants (reporters, government entities, companies) on objectives and usage of the portal?
- 3.
- 4.
5. Who will have access to view/analyze reported information? Will there be any restrictions in place to dictate what can be done with this information?
- 6.
- 7.
8. Would other companies have access to see reports for other platforms? What if the report has content from multiple companies?
- 9.
- 10.
11. What is the criteria used to determine who has access to the portal? How many individuals do you anticipate having access?
- 12.
- 13.
14. How long will reported information be retained?
- 15.
- 16.
17. How long will the portal be in operation? Just through the 2020 presidential election?
- 18.
- 19.

CONFIDENTIAL-NON-PUBLIC INFORMATION-PROVIDED TO CONGRESS IN RESPONSE TO SUBPOENA CIS-JUDCOM0000070_Confidential

20. Companies' terms of service vary. How will individuals know what to report?
- 21.
- 22.
23. Will there be any quality checks in place? Will there be a review of reports before they are submitted to companies? Will all reports be treated with equal priority?
- 24.
- 25.
26. Will partners continue to use Partner Support Portal (PSP) or will everyone migrate to this reporting tool?



4. CISA не делала различий между иностранными и внутренними акторами в социальных сетях.

Наконец, в разгар работы или рассмотрения до трех различных способов «сообщения о дезинформации» (коммутатор, EI-ISAC и «портал сообщений о дезинформации»), к началу 2020 года CISA отбросила всякую претензию на то, чтобы сосредоточиться только на иностранной дезинформации, и открыто обсуждала, как лучше контролировать и цензурировать речь американцев.

20 февраля 2020 года Брайан Скалли, глава Целевой группы CISA по противодействию иностранному влиянию (CFITF), отправил электронное письмо Рене Ди Реста из SIO, пригласив ее на встречу, организованную директором CISA Кребсом, «для обсуждения дезинформации и выборов 2020 года». Скалли предоставил в электронном письме список пунктов повестки дня, в том числе: «Как мы должны думать о внутреннем и внешнем вмешательстве?» и «Есть ли у нас какие-нибудь «висячие плоды» (прим. актуальная работа), над которыми мы могли бы поработать с платформами?».

MICROSOFT CONFIDENTIAL

MSFT_HJC_00008049

- *Monitoring disinformation:* how quickly can we work with social media organizations, as well as state and local governments to clarify and combat misinformation
- The best source of information is always your state and local officials. Always go there to make sure what you're seeing is accurate

Message

From: [REDACTED] [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=5F516F6204EA4FDABEE4078904481238-[REDACTED]]
Sent: 3/13/2020 11:00:33 PM
To: [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=7c7868c34ad94e839b4c3de4e4fbd43b-[REDACTED] [REDACTED]]
[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=microsoft.onmicrosoft.com-55760-[REDACTED]; [REDACTED]]
[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a2e269f304f64b6490d27cafc1adefc7-[REDACTED] [REDACTED]]
[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=microsoft.onmicrosoft.com-56975-[REDACTED]; [REDACTED]]
[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=microsoft.onmicrosoft.com-55760-[REDACTED] [REDACTED]]
[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2caff8c994504311b32dda723f0bf28c-[REDACTED]; [REDACTED]]
[REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=4213854aba984c929c246fda0c4b9c55-[REDACTED]]
Subject: Fwd: CISA call readout

Below is a more complete set of notes from one of the USGA consultants on today's call.
[Get Outlook for iOS](#)

Пандемия COVID-19 усилила желание CISA играть более активную роль в наблюдении и цензуре в социальных сетях. 13 марта 2020 года директор Кребс принял участие в «конференции с широким кругом заинтересованных сторон, чтобы предоставить обновленную информацию о текущей деятельности, связанной с COVID-19».

Согласно внутренним записям Microsoft, полученным Комитетом в соответствии с повесткой, направленной в Microsoft, Кребс назвал «Мониторинг дезинформации» одним из четырех «основных направлений деятельности» и спросил, *«как быстро мы можем работать с организациями социальных сетей, а также государственными и местными органами власти для разъяснения и борьбы с дезинформацией»*.

В своих показаниях перед Комитетом Кребс неоднократно недвусмысленно заявлял, что CISA не рассматривает контент в социальных сетях по-разному в зависимости от его внутреннего или иностранного происхождения. В какой-то момент Кребс даже назвал название Целевой группы CISA по противодействию иностранному влиянию «неправильным термином». Кребс далее дал показания:

Вопрос: Предпринимались ли в это время попытки определить, был ли источник отечественным или иностранным?

Ответ: Мы, конечно, обращались к разведывательному сообществу, если они указывали на угрозу со стороны иностранных агентов. Но, опять же, когда появляются такие вещи, как «молоток и оценочная карта», не обязательно важно, иностранные они или внутренние. Опять же, наши полномочия основаны на Законе о национальной безопасности, который позволяет нам действовать в отношении внутренних или иностранных угроз. И, опять же, они не приходят, размахивая перед нами флагом

Директор Кребс подтвердил подход CISA, согласно которому иностранная и внутренняя деятельность в социальных сетях рассматривается одинаково в контексте инициативы CISA «Контроль за слухами». Например, он сказал:

Вопрос: Когда впервые начались эти дискуссии о внутреннем влиянии?

Ответ: Я не помню.

Вопрос: Хорошо. Продолжались ли они к началу 2020 года?

Ответ: Опять же, я не помню момента или периода времени, в течение которого мы думали о различии между внутренним и внешним вмешательством. Опять же, я думаю, это относится к тому, как мы, увидели ситуацию с контролем “слухов”: нарративы есть нарративы, и мы даем объяснение тому, как все это на самом деле работает. Так что, опять же, для контекста - не имеет значения, иностранное это вмешательство или внутреннее.

Appointment

From: [REDACTED]@cisa.dhs.gov
Sent: 7/8/2020 11:32:38 PM
To: [REDACTED]@cisa.dhs.gov; Snell, Allison [REDACTED]@cisa.dhs.gov; Scully, Brian [REDACTED]@cisa.dhs.gov; Masterson, Matthew [REDACTED]@cisa.dhs.gov; Hale, Geoffrey [REDACTED]@cisa.dhs.gov; Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Elena Cryst [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/[REDACTED]]
Subject: CISA <> Stanford Internet Observatory, Election Misinformation Project Introduction
Location: Microsoft Teams Meeting
Start: 7/9/2020 4:00:00 PM
End: 7/9/2020 5:00:00 PM
Show Time As: Tentative

Recurrence: (none)

Good Afternoon All,

Thank you for taking the time to meet tomorrow for an introductory conversation on the Election Misinformation Project: a potential collaboration between ESI/CFI and the Stanford Internet Observatory. As we have discussed, this project aims to increase CFI's real-time misinformation response capabilities by connecting SLTT and other CFI stakeholders to the third party misinformation research community.

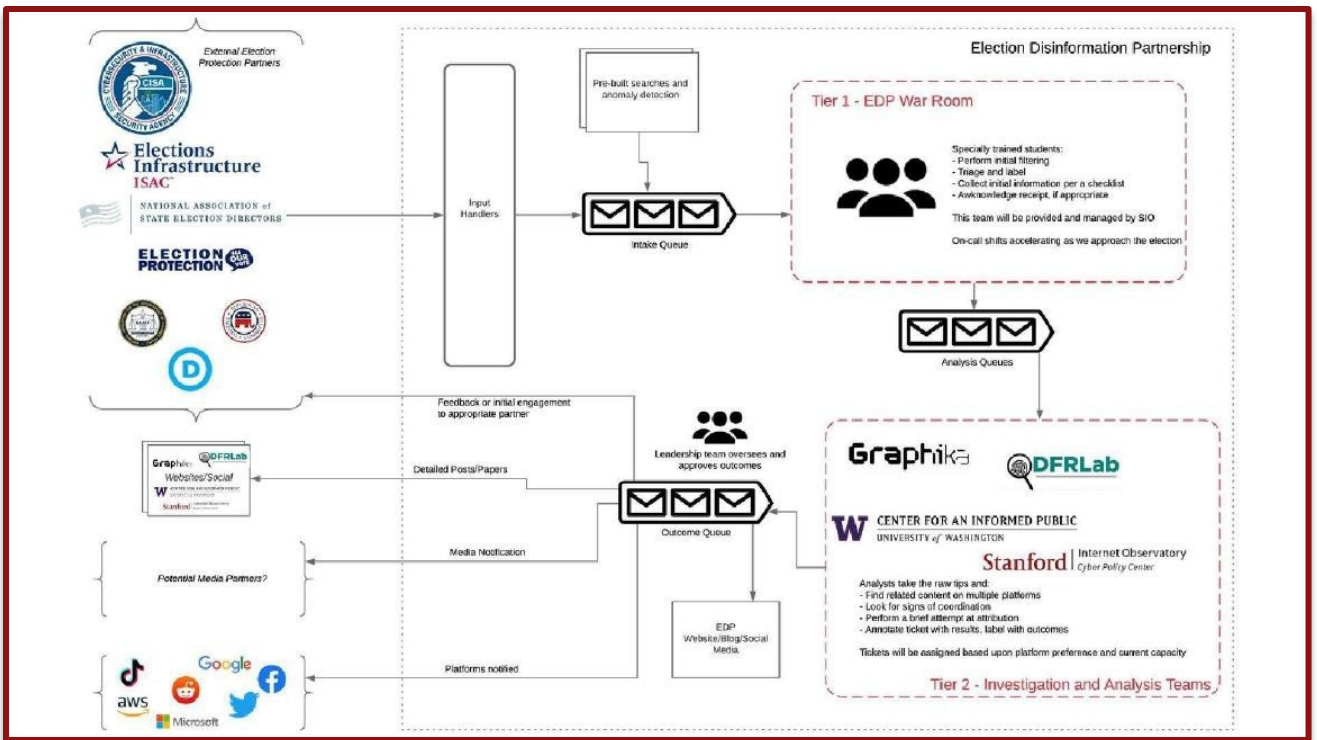
The main topics we hope to cover this meeting are as follows:

- Overview of the Election Misinformation Project ([SLIDES](#))
- What are SIO's core capabilities in this space?
- How would CISA and SIO's misinformation response capabilities be augmented from such a partnership?
- Overview of open questions, concrete next steps.

В. Создание EIP

Не имея возможности реализовать свой первоначальный план, CISA привлек Стэнфорд для цензуры. 8 июля 2020 года директор Стэнфордской интернет-обсерватории (SIO) Алекс Стамос отправил электронное письмо доктору Кейт Старберд из Центра информированной общественности (CIP) при Университете Вашингтона, написав: *«Мы работаем над некоторыми идеями мониторинга выборов вместе с CISA, и я хотел бы получить вашу неофициальную обратную связь, прежде чем мы зайдем слишком далеко по этому пути... Те вещи, которые должны были быть собраны год назад, на этой неделе появляются значительно быстрее»*.

На следующий день, 9 июля 2020 года, представители SIO провели «встречу с CISA, чтобы представить концепцию EIP». На встрече присутствовали Брайан Скалли, будущий руководитель группы CISA по дезинформации (MDM), Джефф Хейл, директор Инициативы CISA по безопасности выборов, и Мэтт Мастерсон, в то время старший советник по кибербезопасности CISA.



Согласно электронному приглашению на встречу, «Проект по дезинформации на выборах», который позже будет переименован в более эвфемистическое «Партнерство по обеспечению честности выборов», «направлен на расширение возможностей реагирования на дезинформацию в режиме реального времени». Одним из пунктов повестки дня было обсуждение того, как «возможности CISA и SIO по реагированию на дезинформацию будут расширены благодаря такому партнерству».

Ранняя схема работы «Партнерства по дезинформации на выборах» показывает, что с самого начала Стэнфорд и CISA предполагали, что партнерство будет связывать федеральные агентства с платформами социальных сетей.

Action Items

CISA (@ who I will be reaching out to)

- EI-ISAC connection: introduction to Aaron Wilson heading social media reporting (@Masterson, Matthew)
- CFI plug-in: discussions how to best integrate reporting into CISA/CFI's ops center and send tips back to SIO (@Scully, Brian)
- Legal: get an initial proposal for OCC (@Snell, Allison)

SIO

- Finalize operational details
 - Full deliverables calendar to be created and shared
 - Define workflow management system which will be the surface presented to Legal
- General development will now ramp up
 - Toolset + OSINT training (to invite CISA)
 - Partnership building within research community
- Publicly announcing the partnership in 2-3 weeks (webinar)

From: '[REDACTED]' <[REDACTED]@cisa.dhs.gov>
Date: Thursday, July 9, 2020 at 5:21 PM
To: '[REDACTED]' <[REDACTED]@cisa.dhs.gov>, "Snell, Allison" <[REDACTED]@cisa.dhs.gov>, "Scully, Brian" <[REDACTED]@cisa.dhs.gov>, "Masterson, Matthew" <[REDACTED]@cisa.dhs.gov>, "Hale, Geoffrey" <[REDACTED]@cisa.dhs.gov>, Alex Stamos <[REDACTED]@stanford.edu>, Elena Cryst <[REDACTED]@stanford.edu>, Renee DiResta <[REDACTED]@stanford.edu>, '[REDACTED]' <[REDACTED]@cisa.dhs.gov>, "Masterson, Matthew" <[REDACTED]@cisa.dhs.gov>
Cc: '[REDACTED]' <[REDACTED]@cisa.dhs.gov>
Subject: CISA <> Stanford Internet Observatory, Election Misinformation Project Introduction

Good Afternoon All,

Thank you very much for taking the time to meet this morning. Overall, I think we got good buy-in from both SIO and CISA on the proposal and its potential to improve the impact of both organizations this upcoming November. I have attached notes which @ [REDACTED] graciously took during the meeting, as well as some action items below.

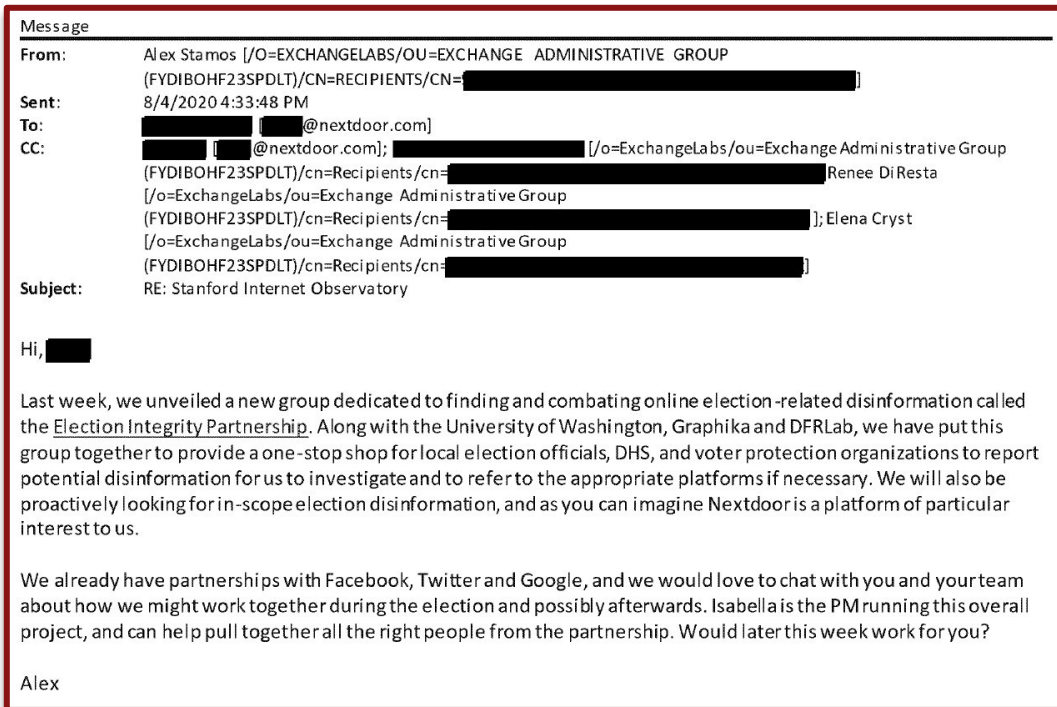
July will be big to get things going on both the CISA and SIO front, so we will be sure to keep open lines of communication. Thank you again for everyone's help in getting this going, looking forward to getting to work here!

Respectfully,

[REDACTED]

В последующем резюме стартового совещания 9 июля от сотрудника CISA говорилось: «Я думаю, что мы получили хорошую поддержку со стороны SIO и CISA в отношении предложения и его потенциала для улучшения влияния обеих организаций в предстоящем ноябре... Июль будет очень значительным, чтобы получить информацию от CISA и с SIO, а потому мы удостоверимся, что наши каналы коммуникации остаются открытыми».

В резюме также перечислялся ряд пунктов действий для CISA и SIO, включая «обсуждение того, как лучше интегрировать отчетность в оперативный центр CISA/CFA (Countering Foreign Influence) и отправлять подсказки обратно в SIO». В числе обязательных мероприятий была консультация с отделом главного юрисконсульта CISA (ОСС – Офис Исполнительного Консула), как видно из пункта «Юридический отдел: подготовить первоначальное предложение для ОСС».



Сотрудники EIP, включая Алекса Стамоса, в своих обращениях к платформам социальных сетей ясно давали понять, что истинная цель EIP - действовать в качестве канала цензуры для федерального правительства. Например, 4 августа 2020 года Стамос написал в электронном письме сотруднику Nextdoor, что EIP была создана «для того, чтобы обеспечить единое окно для местных избирательных органов, Министерства здравоохранения и организаций по защите избирателей, чтобы сообщать о потенциальной дезинформации для расследования [EIP] и передачи соответствующим платформам».

В своем отчете после выборов EIP утверждает, что «первоначальная идея создания партнерства исходила от четырех студентов, которых Стэнфордская интернет-обсерватория (SIO) финансировала для прохождения волонтерской стажировки в [CISA]». Эта ревизионистская версия событий, по всей видимости, призванная дистанцировать CISA и высшее руководство SIO от создания EIP, опровергается доказательствами, полученными Комитетом.

В июне 2023 года Комитет провел расшифрованное интервью с Алексом Стамосом, директором SIO. Отвечая на вопрос о происхождении EIP, Стамос заявил, что он, а не четыре стажера, «первым придумал идею EIP». Он сказал:

Вопрос: помните ли вы, кому первому пришла в голову идея создания EIP?

А. Это был я.

From: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>
Sent: Friday, July 31, 2020 17:54
To: [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.ORG>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>
Cc: [REDACTED] <[REDACTED]@atlanticcouncil.org>; [REDACTED] <[REDACTED]@atlanticcouncil.org>; [REDACTED] <[REDACTED]@ATLANTICCOUNCIL.org>
Subject: Re: Quick question -- Park Advisors

Thanks, [REDACTED]

And understood. Given the work DFRLab does on geopolitics, technology, and election interference with GEC, we were just caught off guard because they asked us about it.

I am not as concerned on the money or the project, but rather consolidating our approach to GEC as we go into the season for expanded renewals on two separate, multi-year agreements in the six figure range that cover a significant amount of our work on elections and all of our work in South Africa and Latin America.

On the DHS app, fake news, and any other US election-related work, it would be great to sync-up, as well. I know the Council has a number of efforts on broad policy issues around the elections, but we just set up an election integrity partnership at the request of DHS/CISA and are in weekly comms to debrief on disinfo, IO, etc..

Best,
Graham

Стамос также признал в ходе допроса, что летом 2020 года он, вероятно, консультировался с тогдашним директором CISA Кристофером Кребсом по поводу EIP. Он показал:

Вопрос: *Вы консультировались с Крисом Кребсом летом 2020 года?*

Ответ: *Скорее всего, да.*

Документы, предоставленные Комитету и Специальному подкомитету, также ставят под сомнение идею о том, что за создание EIP отвечала горстка студентов. Независимо от того, какую роль в «идее» EIP сыграли студенты, эти документы свидетельствуют о непосредственной роли высокопоставленных сотрудников CISA, CIS и SIO в создании операции, в которой непосредственно участвовали около 100 человек и которая работала с более чем десятком партнеров, отмечая тысячи сообщений и нарративов в сотнях отчетов о «дезинформации».

Наконец, даже четыре партнера-основателя EIP, такие как Лаборатория DFRLab Атлантического совета, летом 2020 года понимали, что EIP была создана по просьбе CISA. Как следует из внутренней электронной почты Атлантического совета, полученной Комитетом в соответствии с повесткой, Грэм Бруки, одна из центральных фигур, участвовавших в EIP, в июле 2020 года понимал, что EIP была «создана... по просьбе DHS/CIS».

From: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>
Sent: Wednesday, September 30, 2020 5:05 PM
To: Andy Carvin <[REDACTED]@ATLANTICCOUNCIL.org>; Emerson Brooking <[REDACTED]@ATLANTICCOUNCIL.org>
Subject: ANDY / EMERSON -- Coordination

COORDINATION ON US DOMESTIC PRIORITIES

Hi to both –

The struggle here is that Emerson is managing efforts and Andy is managing staff and outputs. The only way to be successful is to make sure that the three of us are explicitly on the same page about how we are allocating staff to efforts.

The below is intended to do that – and I will be adding Emerson to the DCHQ WhatsApp chain, where we will coordinate in general, as soon as we're on the same page as below. Our first obligation is always to our staff and not setting them up for failure. Our second obligation is to our core work, which every single one of us is managing key elements of. Thus the burden falls on the three of us to coordinate both.

Please reply in red or blue to the below. I also didn't have explicit names in the "staffing" section of each, so please fill out.

Thanks,
Graham

Election Integrity Partnership

Key questions: What is the schedule of shifts, noting that we just need to assign people to them? EIP, the voluntary shift system is a potential challenge because it requires a person to spend X amount of hours monitoring things, which either results in no outputs being produced, or a sudden need to complete an output that the person may or may not be suited to complete, especially if it's an international member of the team with limited knowledge of US politics, geography, culture, etc.

In scenarios where something potentially important surfaces within EIP, how do we go about prioritizing it? For example, when is it simply a matter of "this is a good story so please get me a draft in 72 hours" vs "all hands on deck, this is like a major takedown?" In either case, the three of us need to be locked up in order to not undermine our whole business operation through editorial capacity, who gets assigned, scheduling, etc.

One not ideal scenario is a situation where Jean or Ayush volunteer for a few hours, end up finding something important, and then having not having all three of our awareness and approval, which could lead to significant members of staff being taken away from their core responsibilities for extended periods of days/week. In other words, a shift is just the tip of the iceberg, commitment-wise.

Another question is what constitutes a contribution to EIP. While the focus has been on the partnership and the process (which makes sense) we're part of a team reviewing leads and deciding when to act on them. But we also continue to cover election-related stories that will originate from our original research, rather than the college students volunteering at EIP, especially now that Jared is coming on board and while looking into more conspiracy related content. Can we consider those contributions? I imagine for some researchers there's more incentive to contribute when they're able to generate research leads themselves rather than being responsive to tips, though I understand responding to tips is still core to the partnership.

Important to note: not college kids surfacing EIP leads. Krebs CISA is texting Stamos with some regularity. A few tickets have been flagged by the platforms. Starbird's UW team is surfacing a lot of stuff using advanced soc media listening methods. College kids (T-1) just doing the first round of analysis.

The job of DFRLab is to be T-2, doing a deep dive into tickets, attaching more contextual information, and writing up a twitter thread/blog post if that's the recommendation of the researcher (and the T-3 shift manager approves).

Analysts can step away and write a blog post on-shift. That's what Alyssa did [last week](#).

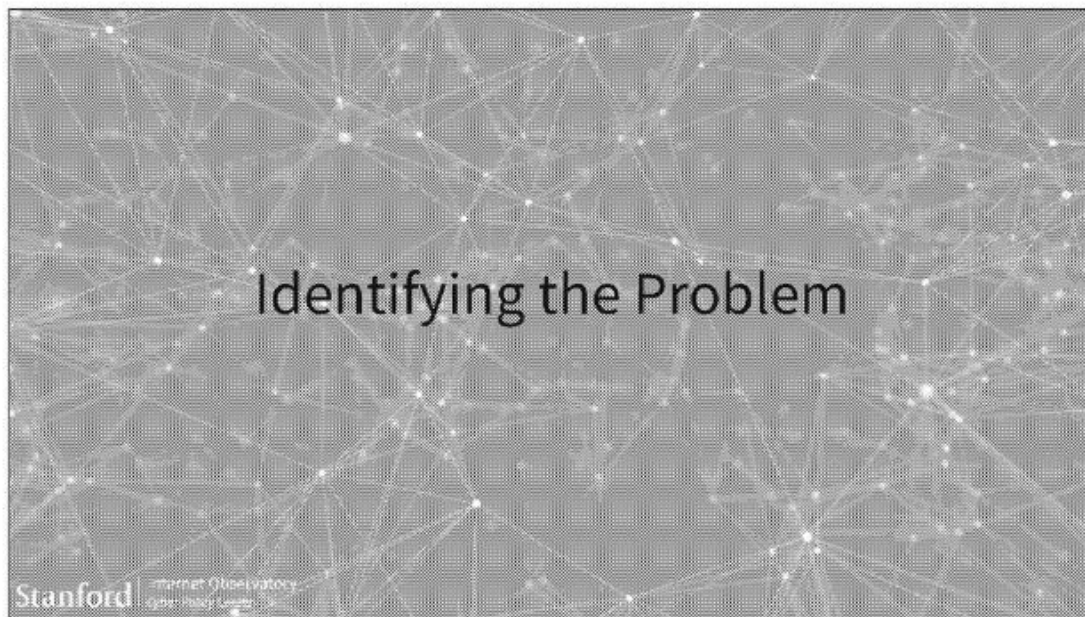
Внутренние документы Атлантического совета, полученные Комитетом и Специальным подкомитетом в соответствии с повесткой, направленной Атлантическому совету, также показывают, что, хотя студенты участвовали в EIP, критическая работа, включая «добавление более контекстуальной информации», подготовку постов в блогах и составление рекомендаций для социальных медиаплатформ, выполнялась профессионалами по дезинформации.

С. Цель EIP: использование доверенностей для обхода первой поправки.

По собственному признанию, EIP была создана «по согласованию с CISA» для достижения неконституционной цели - как механизм для обхода законных ограничений на незаконную деятельность правительства. Как говорится в отчете EIP, подготовленном после выборов:

Ни одно государственное учреждение в Соединенных Штатах не имеет четкого мандата на мониторинг и исправление дезинформации о выборах. Это особенно верно в отношении дезинформации, исходящей из Соединенных Штатов, которая, скорее всего, будет исключена из сферы действия правоохранительных органов в соответствии с Первой поправкой и не подходит для изучения спецслужбами, которым запрещено действовать внутри США. В результате, во время выборов 2020 года местные и государственные избирательные органы, которые имели сильного партнера по избирательным системам и общим усилиям по кибербезопасности в CISA, остались без информационного центра для оценки дезинформации, направленной на их операции по голосованию. В результате консультаций с CISA и другими заинтересованными сторонами была создана коалиция, в которую вошли учреждения-партнеры, придерживающиеся аналогичных взглядов.

В своих заметках для презентации на ежегодном саммите CISA осенью 2021 года Рене Ди Реста, менеджер по исследованиям в SIO, написала в рамках сценария своей презентации, что «пробел», который должен был заполнить EIP, «состоит из нескольких компонентов», один из которых – “*неясные правовые основания, включая реальные вопросы, связанные с Первой поправкой*”.



Our team and CISA's team have done some pioneering work in partnership thinking about how to respond to mis- and disinformation in areas in which it can have significant harm. One of those areas is elections, and I'm going to talk about some learnings from that work today.

In August 2020, students from the Stanford Internet Observatory (SIO) who were doing an internship with CISA identified a massive gap in the capability of federal, state and local governments to become aware of, analyze and rapidly respond to mis- and disinformation — both foreign and domestic — targeting the 2020 election.

That gap had several components:

- Federal gov't not prepared to identify and analyze election mis/disinfo:
 - There was no clear federal lead to coordinate this work. The IC, of course, is rightly limited to a foreign-focus. The FBI also has very specific designations and limitations, and CISA had created support but had no real capability.
 - Unclear legal authorities including very real 1st amendment questions
 - No expertise resident within federal gov't to analyze public content across platforms to identify trends & risks
- Lack of reporting mechanisms for state and local partners to surface activity that they saw building in their communities, to help them understand it.

The federal government was building relationships with platforms but there is a healthy distrust both ways for good reason

A trusted, nonpartisan partner(s) with expertise in the way that misinformation moved on public platforms, with analysts capable of understanding public conversations, and broad ability to explore publicly available data, was needed.

Чтобы обойти эти «очень важные вопросы, связанные с Первой поправкой», организации, занимающиеся распространением псевдонауки «дезинформации», такие как SIO и CIP Университета Вашингтона, были выбраны в качестве части «центральной организации для поддержки должностных лиц, ответственных за выборы, или CISA в выявлении и реагировании на дезинформацию». Согласно одной из первых публикаций EIP, в их представлении «Академические/исследовательские институты» были выбраны в качестве инициаторов этих усилий именно потому, что они считались «самыми простыми в политическом плане».

Current Landscape

Who could potentially solve this problem? Why aren't they?

	CISA	Platforms	Academic/Research Institutions
Currently Offers	E-ISAC collaboration to provide real-time monitoring tools such as the SOC as well as the classified and unclassified Situation Rooms	Direct contact with secretaries of state as well as some cross-platform communication on this front	Institutions have created their own independent groups, little coordination
Strengths	Direct communication with every election official, central node in the election infra ecosystem	Highest monitoring capacity into what is happening in the social landscape, lots of \$\$\$ and resources	'Easiest' politically, transparent, existing institutions (SIO). Agile, lightweight teams.
Weaknesses	All efforts focused on hardware, no misinformation workstream, govt entity, can't be seen as 'monitoring' the electorate, highly political.	Political, easily seen as partisan, don't have the direct communication/rapport with all election officials.	Don't have the direct communication or rapport with all election officials, need to raise \$\$\$

Как пояснил Верховный суд, «аксиома» заключается в том, что правительство «не может побуждать, поощрять или стимулировать частных лиц к выполнению того, что ему запрещено конституцией». Участие CISA в создании и сотрудничестве с EIP — это тот тип неконституционного аутсорсинга, против которого Верховный суд уже давно вынес решение. Цензура по доверенности — это особенно гнусная форма действий государства, поскольку она предназначена для уклонения от обнаружения, надзора и запросов публичных документов.

II. ПОЛНОЕ ПЕРЕПЛЕТЕНИЕ CISA С EIP

«CISA и EIP были полностью переплетены».

*-Миссури против Байдена, дело № 3:22-cv-1213,
ECF № 293 (судебный приказ и заключение) на 113 (4 июля 2023 г.).*

A. CISA в сговоре с EIP

После того как CISA помогло создать EIP, федеральное агентство оставалось тесно связанным с деятельностью EIP в месяцы, предшествующие выборам 2020 года. На протяжении всей осени 2020 года сотрудники CISA активно координировали свои действия с EIP и CIS. Электронные письма, полученные Комитетом и Специальным подкомитетом в соответствии с повесткой, ясно показывают, что система EIP была разработана для работы как единое целое, а не как отдельная структура от DHS. Более того, хотя в EIP (на которую работало около 100 человек, не считая внешних заинтересованных сторон, таких как GEC и CISA) было вовлечено множество студентов, ее возглавляли известные деятели цензурно-промышленного комплекса, такие как директор Стэнфордской интернет-обсерватории (SIO) (и бывший директор по безопасности Facebook) Алекс Стамос, руководитель исследований SIO Рене ДиРеста и вице-президент и старший директор исследовательской лаборатории цифровой криминалистики Атлантического совета (DFRLab) Грэм Бруки. EIP также тесно сотрудничала со старшими должностными лицами CISA, включая Брайана Скалли, главу целевой группы CISA по противодействию иностранному влиянию (CFITF).

Мало того, что в EIP участвовало несколько студентов университета, по крайней мере четверо из них работали в CISA во время работы EIP, используя свои государственные электронные почтовые ящики для общения с должностными лицами CISA и другими «внешними заинтересованными сторонами», участвующими в EIP. Например, к 3 сентября 2020 года CISA назначила одного из этих стажеров DHS-SIO контактным лицом, ответственным «за многие вопросы взаимодействия EIP и CISA».

From: [REDACTED] [REDACTED]@cisa.dhs.gov]
Sent: 9/3/2020 1:51:40 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlT)/cn=recipients/cn=[REDACTED]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; [REDACTED] [REDACTED]@cisa.dhs.gov]
CC: Masterson, Matthew [REDACTED]@cisa.dhs.gov]; Snell, Allison [REDACTED]@cisa.dhs.gov]; Scully, Brian [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey [REDACTED]@cisa.dhs.gov]
Subject: RE: CISA <> CSI Disinfo Reporting follow up

Hello Aaron:

Sorry for the delay here – for some reason, the @cisecurity alias keeps getting routed to my 'Other' folder, so I was about to follow up on this myself. I'll try and chat with our techdesk today about this.

On the EIP side, if you could please add tips@eipartnership.net, this alias will auto create Jira tickets for any incoming reports for visibility to the whole EIP team. I've also added [REDACTED] to this thread, [REDACTED]@cisa.dhs.gov, who will be taking point on a lot of the EIP <> CISA interface here, so he should also be added. I will let Brian and Matt note whether they also would like to be on the backend of this alias.

One note on the EIP side: we just finished getting our Jira system online to be ready for intake. For security purposes, the tips@eipartnership.net alias has a strict whitelist of emails which will be allowed through: any email not specifically designated into an organization will be silently dropped. I've created a new CIS organization on our system and added misinformation@cisecurity.org to it, as well as [REDACTED]'s CISA email. Any reports forwarded from these email addresses will make it into our system. However, if misinformation@cisecurity.org auto forwards anything in such a way that it is sent from a different alias (ex: bob@washington.gov), this will be dropped in our system.

There are ways around this, but I just wanted to flag this upfront and get a sense from you how this might be working on your end? I have a free calendar all day tomorrow basically, and could hop on a call with our tech lead to figure out the best way of doing this.

Best,

[REDACTED]

Этот студент из Стэнфорда, работающий в качестве стажера DHS, будет находиться «внутри сети EIP» и отвечать за «пересылку отчетов с псевдонимов cissecurity.org в EIP», а также «следить за внутренней системой тикетов EIP, чтобы убедиться, что отчеты рассмотрены и что все соответствующие записи EIP направлены соответствующим SLTT [государственным, местным, племенным и территориальным] органам».

From: David Thiel <[REDACTED]@stanford.edu>
Sent: Tuesday, September 8, 2020 11:02 AM
To: [REDACTED] <[REDACTED]@fb.com>
Cc: [REDACTED] [REDACTED] Renee DiResta <[REDACTED]@stanford.edu>; Elena Cryst <[REDACTED]@stanford.edu>
Subject: Re: Checking in re: fact-checking flags

Hi [REDACTED]

We've mostly just been going through exercises so far, mostly with claims that our CISA folks already know the answer to. We're ramping up our new RAs this week though, and I expect we'll start getting more of a pipeline of stuff that needs fact-checked soon.

Thanks!
David

From: [REDACTED] <[REDACTED]@cisa.dhs.gov>
Sent: Tuesday, September 8, 2020 9:28 AM
To: Aaron Wilson <[REDACTED]@cisaecurity.org>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; Ben Spear <[REDACTED]@cisaecurity.org>; Mike Garcia <[REDACTED]@cisaecurity.org>; Scully, Brian <[REDACTED]@cisa.dhs.gov>
Cc: Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; Snell, Allison <[REDACTED]@cisa.dhs.gov>; Hale, Geoffrey <[REDACTED]@cisa.dhs.gov>
Subject: Re: CISA <> CSI Disinfo Reporting follow up

Hi Aaron,

I'll be taking point on the CIS/CISA<>EIP reporting interface, so we can sync about this if you'd like. The way [REDACTED] and I are envisioning it right now, essentially I would be forwarding reports from the cisaecurity.org aliases to EIP, and I would be watching EIP's internal ticketing system to make sure reports are addressed and that any EIP write-ups that are relevant are forwarded to the proper SLTT folks. The reports outbound from EIP would follow a similar flow.

Happy to hop on a call to discuss.

Best,
[REDACTED]

Другими словами, у DHS было контактное лицо с прямым доступом к внутренней системе регистрации заявок EIP, которое могло (и делилось) этой информацией с агентством.

Готовясь к выборам 2020 года, EIP, судя по всему, координировала с CISA проведение цензурных «учений». В электронном письме от 8 сентября 2020 года, направленном сотруднику Facebook Дэвидом Тейлом, главным технологом SIO, говорится следующее: «Пока что мы просто проводим учения, в основном с претензиями, на которые наши сотрудники CISA уже знают ответ».

From: Aaron Wilson <[REDACTED]@cisecurity.org>
Sent: Friday, September 11, 2020 2:05 PM
To: Amy Cohen <[REDACTED]@nased.org>; Maria Benson <[REDACTED]@sso.org>
Cc: [REDACTED] <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>; Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; Ben Spear <[REDACTED]@cisecurity.org>; Mike Garcia <[REDACTED]@cisecurity.org>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@sso.org>
Subject: Misinformation@cisecurity.org

Amy, Maria,

I hope you both are doing well. I want to let you know we have misinformation@cisecurity.org setup and the EIP, CISA, and CIS went through a detailed discussion of the workflow this afternoon. We feel ready to start promoting this to election officials as a way to report misinformation. What do you think is the best way to approach election officials with this new option?

Thanks,

Aaron

11 сентября Аарон Уилсон сообщил по электронной почте, что «сегодня днем EIP, CISA и CIS провели детальное обсуждение рабочего процесса. Мы считаем, что готовы начать продвигать это среди сотрудников избирательных комиссий как способ сообщить о дезинформации».

Предложенный рабочий процесс ясно показывает, что ни EIP, ни CIS не действовали полностью независимо от CISA, а вместо этого сотрудничали и систематически работали в рамках того же самого органа цензуры, который CISA помог создать. Как описано ниже в том же потоке электронной почты в середине сентября 2020 года, должностные лица, ответственные за проведение выборов, отправляли отчеты о дезинформации в CIS.

Затем CIS

- (1) пересылали электронное письмо в CISA, а агентство направляло отчет на платформы социальных сетей;
- (2) Пересылали электронное письмо в EIP, который занимался другими подобными материалами, необходимые к поставке отметок прежде чем они были отправлены на платформы социальных сетей. Как следствие, CISA имела возможность видеть, что отправляется в EIP. И что очень важно, платформы социальных сетей знали, что CISA знает о том, что поступает в EIP.

From: Aaron Wilson <[REDACTED]@cisecurity.org>
Date: Friday, September 11, 2020 at 2:59 PM
To: Maria Benson <[REDACTED]@sso.org>, Amy Cohen <[REDACTED]@nased.org>
Cc: [REDACTED] <[REDACTED]@cisa.dhs.gov>, "Scully, Brian" <[REDACTED]@cisa.dhs.gov>, "Masterson, Matthew" <[REDACTED]@cisa.dhs.gov>, Ben Spear <[REDACTED]@cisecurity.org>, Mike Garcia <[REDACTED]@cisecurity.org>, "[REDACTED]" <[REDACTED]@cisa.dhs.gov>, [REDACTED] <[REDACTED]@sso.org>
Subject: RE: Misinformation@cisecurity.org

Maria,

I think I can describe it succinctly here in an email (or at least I'll try ☺).

Election officials will email misinformation@cisecurity.org when they want to report misinformation on any platform. CIS will receive the email and forward to CISA and EIP. We will do some basic validation before forwarding (i.e. if they say 'see attached' but forgot the attachment, we will get back with them).

CISA will forward to the appropriate platform(s) and cc misinformation@cisecurity.org. The EIP will intake the report into their internal tracking system which will assign it to researchers, etc.

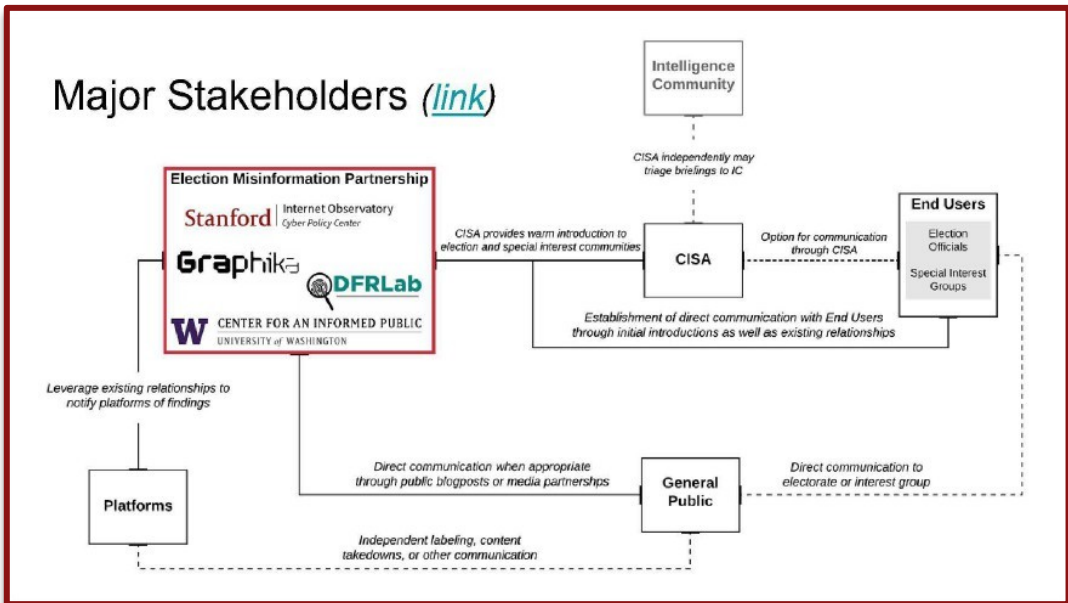
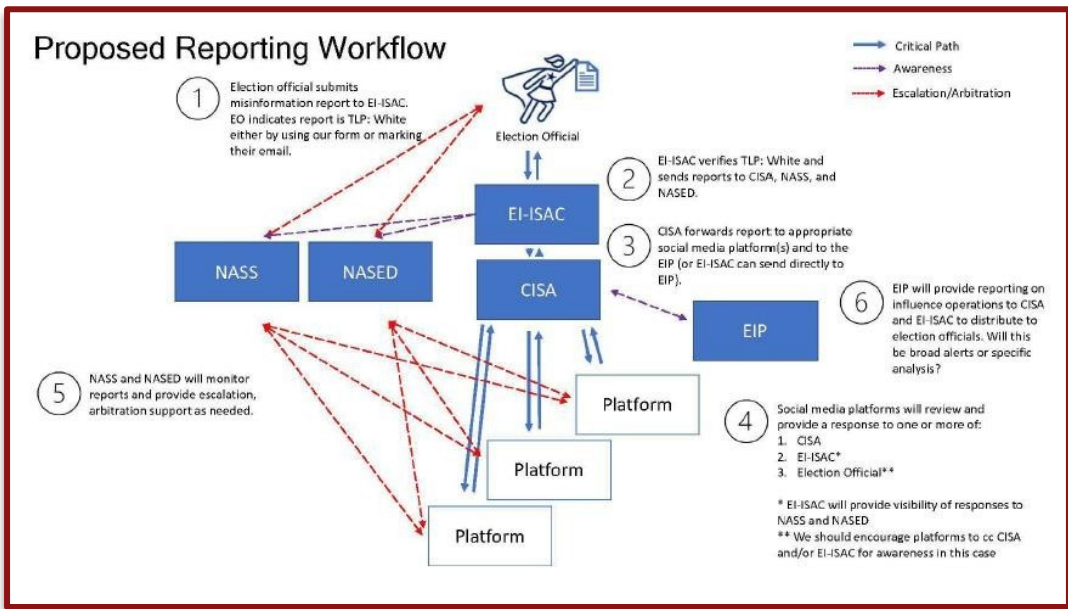
CISA will respond to misinformation@cisecurity.org when they have an update from the platform. EIP will send automated notifications of updates to misinformation@cisecurity.org as the case it tracked and updated in their system.

CIS will synthesize (as necessary) the information and provide regular, succinct, and relevant updates to the election officials.

Please let me know if any of this creates questions or concerns.

Thanks,

Aaron



Тесная координация между CISA и EIP предусматривалась с самого начала, как видно из приведенных ниже диаграмм, содержащихся, по-видимому, в ранних информационных материалах EIP. Несколько шагов в «Предлагаемом рабочем процессе отчетности» прямо связывают CISA и EIP.

Например, один из этапов гласил: «CISA направляет отчет на соответствующую платформу социальных сетей и в EIP (или EI-ISAC может отправить его непосредственно в EIP)». Другая диаграмма, озаглавленная «Основные заинтересованные стороны», устанавливала связь между EIP, CISA и разведывательным сообществом.

From: [REDACTED] [REDACTED]@cisa.dhs.gov]
Sent: 9/17/2020 9:50:59 AM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdlt)/cn=recipients/cn=[REDACTED]]
CC: Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; [REDACTED] [REDACTED]@cisa.dhs.gov]
Subject: Fwd: EIP-167 Tweet says Newsom changed voting preference

Hi Aaron and Ben,

Thanks for the clarification email yesterday regarding the reporting workflow, we are glad these flows are getting finalized. Just in time, too! I'm forwarding you here one of the first substantive regional election misinfo tickets that EIP has actioned that led to platform intervention. After EIP found this with their own monitoring and flagged the content to Twitter, Twitter took action almost immediately. EIP is producing a blogpost about this very soon.

This ticket has the misinformation@cisecurity.org box tagged — are you monitoring for these tickets yet and are they being received? EIP is now in a place where this sort of event will occur regularly, so starting up the information flow identified in the one-pager might be prudent at this stage.

Let us know if you have questions or concerns as well.

Best,

[REDACTED]

Эта договоренность быстро принесла плоды для операции федерального правительства по отмыванию цензуры. 17 сентября сотрудник CISA отправил письмо сотрудникам CIS Аарону Уилсону и Бену Спиру, написав: «Я направляю вам один из первых существенных заявлений о дезинформации на региональных выборах, которые EIP приняла к рассмотрению и которые привели к вмешательству платформы». После того как EIP обнаружила это с помощью своего собственного мониторинга и пометила контент в Twitter, Twitter почти сразу же принял меры». Проще говоря, EIP отчиталась перед федеральным правительством о том, что она успешно побудила BigTech («крупнейшие IT компании» прим. автора) цензурировать политическую речь американцев от имени CISA.

CISA понимала, что для достижения цели полноценной цензуры нежелательных точек зрения, в первую очередь консервативной политической речи, недостаточно отмечать отдельные сообщения для удаления. Вместо этого цензуре должны подвергаться целые «нарративы». В соответствии с многочисленными повестками Комитет и Подкомитет получили сообщения между CISA, EIP и CIS, демонстрирующие, что истинной целью отметки контента на платформах социальных сетей была цензура целых нарративов (тем, повесток), а не только конкретных сообщений. Однако это не помешало EIP выявить огромное количество сообщений в социальных сетях, якобы распространяющих «дезинформацию», причем некоторые сообщения о дезинформации содержали более 500 отдельных ссылок.

From: [REDACTED]@cisa.dhs.gov
Sent: 9/24/2020 5:21:14 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; [REDACTED]@cisa.dhs.gov; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]
CC: Scully, Brian [REDACTED]@cisa.dhs.gov; Snell, Allison [REDACTED]@cisa.dhs.gov; Tipton, James [REDACTED]@cisa.dhs.gov; Dragseth, John [REDACTED]@cisa.dhs.gov; Masterson, Matthew [REDACTED]@cisa.dhs.gov; Hale, Geoffrey [REDACTED]@cisa.dhs.gov
Subject: RE: EIP-167 Tweet says Newsom changed voting preference

Hello Aaron:

Jumping in to answer a couple of the technical questions! We just had an issue with Facebook's reporting box which was configured oddly as a 'bulk' email inbox. Is your mail receiver for misinfo@cisecurity.org automatically dropping emails tagged as 'bulk'? Because if so, the Jira alias where these tips are coming from (which I think is a bulk inbox) won't work with it. I am relaying this from our technical team so can ask for more information as helpful.

Regarding your second question on whether the ticket is closed: we closed the ticket as we had given the organizations tagged a reasonable amount of time to respond (~1 week in this case) and received no further commentary. We also wrote up our findings publicly. I don't think the status of the ticket as Open or Closed means much for the election officials – we are sending this to you early in hopes of having it go straight to the impacted stakeholders as close to instantly as possible, so that if its of interest, they can ask further questions and we can be responsive to find more information. We just don't know what is helpful to them yet.

As to the action on certain links: there is no way we found every piece of misinfo related to this incident, so we don't give a ton of weight to how many of the links that we sent over got actioned (though we hope all would) because we know we didn't find all the links anyways, and that the platforms are not going to communicate to us how many further leads they found and actioned as well (it could be none, it could be a network of 1000 users. Though they'd likely tell us about the latter). Because of this, we see the narrative itself as the most important thing to communicate, and the links as supplementary examples. We are always available to re-open a case to give further information on a narrative as helpful.

24 сентября один из стажеров CISA-SIO написал: «Мы никак не можем найти все дезинформационные материалы, связанные с этим инцидентом, поэтому мы не придаем большого значения тому, сколько ссылок, которые мы отправили, были приняты к цензурированию (хотя надеемся, что все). С этим мы видим, что нарративы (прим. Консервативные позиции) само по себе - самое важное, что нужно передать (к цензуре)».

В другом электронном письме, отправленном 24 сентября, один из стажеров CISA-SIO, который позже был принят в штат CISA на полную ставку, высказался в поддержку совместного предприятия по цензуре, написав: *«EIP ожидает увеличения частоты инцидентов с дезинформацией, связанных с конкретными регионами, так что скорейшая реализация этих планов была бы идеальным вариантом... Я буду рад предоставить дополнительные ресурсы на стороне CISA, чтобы направлять запросы, если это поможет».*

From: Mike Garcia <[REDACTED]@cisecurity.org>
Sent: Wednesday, October 21, 2020 10:24 AM
To: Amy Cohen <[REDACTED]@nased.org>; Misinformation Reports <misinformation@cisecurity.org>; Aaron Wilson <[REDACTED]@cisecurity.org>; Maria Benson <[REDACTED]@sso.org>
Cc: Scully, Brian <[REDACTED]@cisa.dhs.gov>
Subject: Re: Misinformation regarding online replacement ballot portal

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian may know otherwise but I don't believe we heard back from the platforms on the "CISA track" just on the EIP track.

From: [REDACTED] <[REDACTED]@cisa.dhs.gov>
Sent: 9/24/2020 12:48:12 PM
To: Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]
CC: Scully, Brian <[REDACTED]@cisa.dhs.gov>; Snell, Allison <[REDACTED]@cisa.dhs.gov>; Tipton, James <[REDACTED]@cisa.dhs.gov>; Dragseth, John <[REDACTED]@cisa.dhs.gov>; [REDACTED] <[REDACTED]@cisa.dhs.gov>; Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; Hale, Geoffrey <[REDACTED]@cisa.dhs.gov>
Subject: Re: EIP-167 Tweet says Newsom changed voting preference

Good afternoon Mike and Aaron,

I just wanted to follow up on this forwarded ticket. Since we last talked, it has been turned into a short blog post [here](#). While blog posts are nice, most misinformation events will not be discussed publicly and are best remediated through the ticketing flow we have worked out. Could we further discuss the criteria that the managers of the misinformation@cisecurity.org have for forwarding EIP tickets like the below to SLTT folks? For example, this ticket would be most directly relevant to the California Secretary of State Elections Division. Also, some states, such as Colorado and Washington, have dedicated social media monitoring/misinformation response teams, so if this ticket had been about those states, would it also get a forward there? If it had been about a particular county, how would that have been handled? We may have discussed this in a preliminary discussion, but I would like to concretize it now that there are live reports coming through EIP.

I think it would help both sides here if the person manning the misinformation@cisecurity.org box were to update the ticket when information has been forwarded, also to allow for cross-communication between EIP and the SLTT officials. EIP anticipates increased cadence of regionally-specific misinformation incidents, so nailing down these processes soon would be ideal. As [REDACTED] and I said last week, I am more than happy to provide additional resources on the CISA side to route requests if that would help.

Более того, хотя SIO утверждает, что «целью EIP было и остается исследование и анализ попыток помешать или удерживать людей от голосования», связанный с SIO человек написал в том же письме, что «хотя сообщения в блогах - это хорошо, большинство событий, связанных с дезинформацией, не будут обсуждаться публично, и их лучше всего устранять с помощью разработанного нами механизма создания отдельных «тикотов» (прим. Запросов в службы поддержки)».

Свидетельства, полученные Комитетом и Специальным подкомитетом, также ясно показывают, что высшее руководство CISA, включая тогдашнего директора Кребса, было осведомлено о цензурной кампании CISA-EIP-CIS. 2

5 сентября 2020 года в электронном письме CISA в CIS сообщается, что Twitter принял «меры в отношении одного из твитов в “тикете» [EIP]. Очевидно, директор Кребс лично связался с [главой SIO] Стамосом, спрашивая, что произошло вокруг этого события, примерно в то время, когда контент был удален». Во внутренней электронной переписке Атлантического совета примерно в это время члены EIP заявили, что «Кребс из CISA переписывается со Стамосом с некоторой регулярностью».

From: [REDACTED] [REDACTED]@cisa.dhs.gov]
Sent: 9/25/2020 7:45:38 PM
To: Aaron Wilson [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Mike Garcia [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Misinformation Reports [/o=EXCHANGE/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=093d02c79b0f4dba805c5322cd750647-misinformation]
CC: Ben Spear [/o=exchange/ou=exchange administrative group (fydibohf23spdl)/cn=recipients/cn=[REDACTED]]; [REDACTED] [REDACTED]@cisa.dhs.gov]
Subject: Re: EIP-243 Claim the thousands of ballots found in dumpster in Sonoma

Hi all,

Just bumping this. Twitter has now taken action on one of the tweets in this ticket. Evidently Director Krebs personally reached out to Stamos asking what had happened around this event around the time the content was taken down, which was only an hour after this ticket was created. If this system is to work, we will need the turnaround time to be much faster for sending these tickets out to states.

Can anyone advise on next steps for actioning this event?

Thank you,
[REDACTED]

Открытая координация между CISA, EIP и CIS продолжалась вплоть до избирательного цикла 2020 года. 5 октября 2020 года Мастерсон, Скалли, Стамос и Гарсия, среди прочих, были приглашены на встречу под названием «EIP-CIS Sync». Согласно приглашению по электронной почте: «Система отчетности misinformation@cisecurity.org уже запущена, как и система входящих и исходящих сообщений EIP. Цель этого призыва - обсудить, как прошел этот процесс, и определить взаимодействие SLA EIP и ISAC на будущее».

Электронное письмо от CIS, отправленное 21 октября 2020 года, показывает, что CIS отслеживала как «трек CISA», так и «трек EIP» (прим. набор сообщений по категориям) для отметки сообщений на платформах социальных сетей.

EIP и CISA провели еще одну встречу для координации своей цензурной операции 29 октября 2020 года, о чем свидетельствует приглашение на встречу с темой «EIP-EIS Elections — Security Initiative Call Disinfo Pre-Brief».

EIS, по-видимому, является ссылкой на Инициативу CISA по безопасности выборов, в которую в то время входили Джефф Хейл и Мэтт Мастерсон.

Appointment

From: [REDACTED] [REDACTED]@cisa.dhs.gov]
Sent: 10/28/2020 7:12:36 PM
To: [REDACTED]@cisa.dhs.gov; Snell, Allison [REDACTED]@cisa.dhs.gov]; Hale, Geoffrey [REDACTED]@cisa.dhs.gov]; Masterson, Matthew [REDACTED]@cisa.dhs.gov]; [REDACTED]@stanford.edu; [REDACTED]@stanford.edu; Graham Brookie [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; [REDACTED]@wu.edu; Emerson Brooking [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; [REDACTED]@uw.edu; Scully, Brian [REDACTED]@cisa.dhs.gov]; Dragseth, John [REDACTED]@cisa.dhs.gov]
Subject: EIP EIS Call Disinfo Pre-Brief
Start: 10/29/2020 10:30:00 AM
End: 10/29/2020 10:45:00 AM
Show Time As: Busy
Recurrence: (none)

V. “Тикеты” Jira: Главное оружие в арсенале цензуры EIP

From: [REDACTED]
Sent: Monday, October 5, 2020 12:52 PM
To: Masterson, Matthew <[REDACTED]@cisa.dhs.gov>; Scully, Brian <[REDACTED]@cisa.dhs.gov>; [REDACTED]@ciscureity.org <[REDACTED]@ciscureity.org>; [REDACTED]@stanford.edu <[REDACTED]@stanford.edu>; [REDACTED]@stanford.edu <[REDACTED]@stanford.edu>; Snell, Allison <[REDACTED]@cisa.dhs.gov>; [REDACTED]@ciscureity.org <[REDACTED]@ciscureity.org>; Tipton, James <[REDACTED]@cisa.dhs.gov>
Subject: EIP-CIS Sync
When: Wednesday, October 7, 2020 1:00 PM-1:45 PM.
Where:

Hi all,

The misinformation@ciscureity.org reporting system is now up and running, as is EIP's inbound and outbound tip system. This call is to discuss how this process has gone so far, and to nail down the EIP ↔ ISAC SLA moving forward.

Best,
[REDACTED]

EIP member 04/Nov/20 11:00 AM
Hello platform partners - we have added you on several different cases of sharpie or felt tip claims which are going viral right now. We will be consolidating the overall arc and all the content we have gathered on this ticket, it is affecting all of Youtube, FB, Twitter, TikTok... Please Standby for the comprehensive content links

ISAC partners are added as we believe a general counter narrative is needed.

Government partner 04/Nov/20 11:00 AM
Do we have a running accounting of which states this is affecting?

Platform partner 04/Nov/20 11:07 AM
Received, thank you.

Government partner 04/Nov/20 11:27 AM
One detail missing in these claims is if there were Overvotes created by the use of sharpies in the polling locations, the machines (by Federal law) are required to kick that ballot back to the voter for confirmation or correction. So, this would have never happened without the voter's knowledge.

Government partner 04/Nov/20 11:32 AM
the claim that sharpies aren't read at all is absolutely false, which is why I focused on the idea of overvotes (caused by a bleed through) which would invalidate the voters (but not without the warning I mentioned). If the claim was about yellow highlighter or red pens, I would buy it. Some scanners red or white light scanners have a hard time with those colors

Platform partner 04/Nov/20 11:43 AM
Thank you. Reviewing this content on [REDACTED] side.

Figure 2.2: Discussion on the #Sharpiegate ticket. The commenters include members of the EIP, government partners, and platform partners.

После того как 26 июля 2020 года EIP была официально создана, она быстро приступила к разработке метода массовой маркировки контента, который она считала нежелательным, на соответствующих платформах социальных сетей. В качестве «линии связи» EIP выбрала Jira: программное обеспечение для отслеживания, разработанное австралийской компанией Atlassian.

Согласно отчету EIP, подготовленному после выборов, EIP «выбрала Jira, потому что она поддерживала большую команду и позволяла добавлять рабочие процессы, требующие как надежных возможностей управления клиентами, так и организационных функций, чтобы отразить многочисленные роли, необходимые для ответа на любой входящий запрос».

Отчет EIP включает в себя пример изображения того, что такое Jira и как наглядно выглядит демонстрация того, как система Jira позволяет в режиме реального времени

сотрудничать «членам EIP, правительственным партнерам и партнерам платформы».

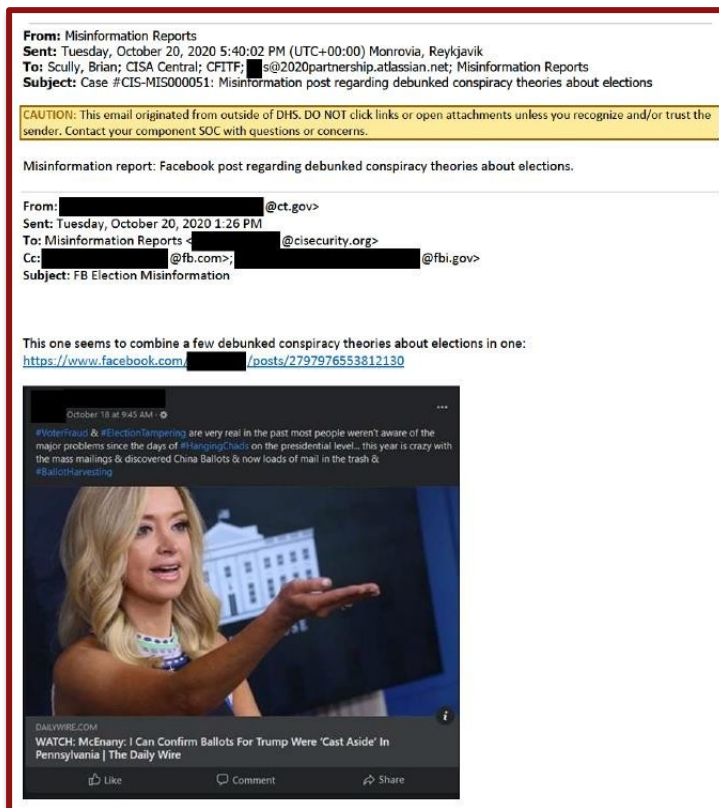
С. Сговор на практике: Координированное отметание постов

В соответствии с повесткой в суд CISA предоставила Комитету и Специальному подкомитету десятки электронных писем, в которых CIS отправляла сообщения о дезинформации от государственных и местных избирательных органов как в EIP, так и в CISA. Затем CISA пересылала эти сообщения на соответствующие платформы социальных сетей. CIS часто включала CISA и EIP в одни и те же цепочки электронной почты, в том числе Брайана Скалли из CISA, CFITF из CISA и EIP (на что указывает электронный домен EIP «@2020partnership.atlassian.net»).

Проще говоря, федеральное правительство, CIS и EIP были в одних и тех же цепочках электронной почты, обсуждая цензуру политической речи американцев. Один из многочисленных примеров приведен ниже. Хотя Стэнфорд и директор SIO (и фактически глава EIP) Алекс Стамос делали тщательно продуманные заявления и давали показания Комитету и Специальному подкомитету о том, что CISA не может *напрямую* сообщать EIP о содержании дезинформации, эта и другие цепочки электронных писем показывают, что CISA регулярно копировала электронные письма от CIS в EIP, в которых сообщалось о дезинформации. Другими словами, хотя CISA не сообщало напрямую о содержании дезинформации *в EIP*, CISA имело полную информацию о том, что сообщалось в EIP, и в то же время сообщало об аналогичном содержании непосредственно на платформы социальных сетей. Хотя CISA «не играла никакой официальной роли», она знала, какие отчеты поступают в EIP, получала отчеты и уведомления по электронной почте, имела персонал с прямым доступом к системе «тикетов» EIP и напрямую контактировала с платформами социальных сетей.

From: Misinformation Reports <[REDACTED]@cisecurity.org>
Date: November 11, 2020 at 4:49:18 PM EST
To: Brian Scully <[REDACTED]@cisa.dhs.gov>, CISA Central [REDACTED]@cisa.dhs.gov>, CISA CFITF [REDACTED]@hq.dhs.gov>, EIP <[REDACTED]@2020partnership.atlassian.net>, Misinformation Reports <[REDACTED]@cisecurity.org>
Subject: Case #CIS-MIS000196: allegations of election fraud

Twitter account alleging election fraud: [https://twitter.com/\[REDACTED\]](https://twitter.com/[REDACTED])



В другом характерном примере, приведенном ниже, почтовый ящик CIS «Misinformation Reports» отправил Брайану Скалли, CISA Central, CFITF CISA и EIP письмо следующего содержания:

«Отчет о дезинформации: Сообщение в Facebook о развенчанных теориях заговора о выборах». Пост в Facebook, о котором идет речь, ссылался на статью из Daily Wire, известного консервативного издания.

Электронные письма от CIS в CISA и EIP продолжали поступать на протяжении всего избирательного цикла 2020 года, включая октябрь и ноябрь 2020 года, когда многие американцы полагались на информацию, размещенную в социальных сетях, при голосовании. Более того, значительное количество электронных писем из CIS было адресовано непосредственно руководителю группы CISA CFITF «Брайану [Скалли] и EIP» и включало сотрудников социальных медиаплатформ, на которых размещался интересующий их контент.

Например, 5 ноября с электронного адреса CIS «Отчеты о дезинформации» было отправлено письмо в CISA, EIP и Facebook, в котором говорилось: «Брайан и EIP - мы включили Facebook в этот отчет». В электронном письме двум сотрудникам Facebook было прямо указано на сообщение о «дезинформации». Таким образом, сотрудники Facebook, получившие это письмо, должны были понять, что CISA и EIP получили одинаковые уведомления в одно и то же время. Письма, подобные этому, показывают, что федеральное

From: Misinformation Reports [REDACTED]@cisecurity.org
Sent: 11/11/2020 8:51:20 PM
To: Scully, Brian [REDACTED]@cisa.dhs.gov; CISA Central [REDACTED]@cisa.dhs.gov; CFITF [REDACTED]@hq.dhs.gov; [REDACTED]@2020partnership.atlassian.net; Misinformation Reports [REDACTED]@cisecurity.org
CC: [REDACTED]@twitter.com
Subject: Case#CIS-MIS000197: allegations of election fraud in Kentucky
Attachments: 197.PNG

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian and EIP, we have included Twitter in this report.

From: Misinformation Reports [REDACTED]@cisecurity.org
Sent: 11/5/2020 5:18:37 PM
To: Scully, Brian [REDACTED]@cisa.dhs.gov; CISA Central [REDACTED]@cisa.dhs.gov; CFITF [REDACTED]@hq.dhs.gov; [REDACTED]@2020partnership.atlassian.net; Misinformation Reports [REDACTED]@cisecurity.org
CC: [REDACTED]@fb.com; [REDACTED]@fb.com
Subject: Case#CIS-MIS000177: Facebook post alleging election fraud
Attachments: 177.PNG

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian and EIP – we have included Facebook in this report.

Misinformation Report: Facebook post alleging election fraud

правительство было напрямую осведомлено о том, что сообщалось в EIP.

11 ноября CIS отправила электронное письмо сотруднику Twitter, нескольким аккаунтам CISA и EIP, написав: «Брайан и EIP, мы включили Twitter в этот отчет». В электронном письме сотрудник Twitter предупреждал о «дезинформации».

В одном особенно тревожном случае CIS передала отчет из офиса госсекретаря штата Аризона, который в то время возглавляла демократ Кэти Хоббс, в CISA, EIP и Facebook: «Брайан и EIP, я включил Facebook в этот отчет». В первоначальном отчете о «дезинформации», направленном в CIS, сотрудник отдела информационной безопасности офиса госсекретаря штата Аризона отметил URL-адрес Facebook, написав: «Это сообщение было размещено на *частной* странице [Facebook]».

From: Misinformation Reports [REDACTED]@cisecurity.org]
Sent: 11/6/2020 10:08:42 AM
To: Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [REDACTED]@cisa.dhs.gov]; CRITF [REDACTED]@hq.dhs.gov]; [REDACTED]2020partnership.atlassian.net; Misinformation Reports [REDACTED]@cisecurity.org]
CC: [REDACTED]@fb.com; [REDACTED]@fb.com]
Subject: Case#CIS-MIS000182: Misinformation post that Trump already won AZ
Attachments: misinformation.jpg

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Brian and EIP, I included Facebook in this report.

Misinformation report: (private) Facebook post that Trump already won AZ

From: [REDACTED]@azsos.gov>
Sent: Friday, November 6, 2020 9:54 AM
To: Misinformation Reports <[REDACTED]@cisecurity.org>
Subject: Fake statement by Arizona Election Worker about fraud

Hi There.

[https://www.facebook.com/photo.php?fbid=\[REDACTED\]](https://www.facebook.com/photo.php?fbid=[REDACTED])

This post was on a private FB page, above. I've included a screenshot.

Thank you!



KATIE HOBBS
SECRETARY OF STATE
State of Arizona

[REDACTED]
Information Security Officer
Arizona Secretary of State's Office

Email: [REDACTED]@azsos.gov
Office: [REDACTED]
Cell: [REDACTED]

From: "[REDACTED]" <[REDACTED]@cisa.dhs.gov> on behalf of CFITF <[REDACTED]@hq.dhs.gov>
Date: Monday, November 2, 2020 at 2:34 PM
To: "[REDACTED]@twitter.com" <[REDACTED]@twitter.com>, "[REDACTED]@twitter.com" <[REDACTED]@twitter.com>, "[REDACTED]@twitter.com" <[REDACTED]@twitter.com>, "[REDACTED]@twitter.com" <[REDACTED]@twitter.com>
Subject: FW: Case #CIS-MIS000107: twitter post alleging CT will be reverting back to phase 1 (of pandemic) on or before election day

Twitter Gov Team, [REDACTED]

Please see below reporting from Connecticut election officials. The ticket is also tagged EIP-572.

Regards,

[REDACTED]
Cybersecurity and Infrastructure Security Agency
[REDACTED]

Хотя Первая поправка, безусловно, распространяется на штаты и государственных служащих, вызывает беспокойство тот факт, что секретарь Хоббс тратила ограниченные ресурсы своего офиса на то, чтобы отмечать в социальных сетях контент, касающийся выступления кандидата-республиканца. Но еще большее беспокойство вызывает тот факт, что сотрудники Хоббс, очевидно, просматривали *частные* страницы Facebook, чтобы выявить несогласных и «дезинформацию» для удаления. Согласно публичным отчетам, офис Хоббса продолжал отмечать посты в социальных сетях и после выборов, вплоть до января 2021 года. В некоторых случаях сотрудники Хоббс отправляли электронные письма непосредственно на платформы социальных сетей с просьбой подвергнуть цензуре критикующие ее сообщения.

Еще более разрушительным для аргумента о независимости CISA и EIP является тот факт, что сотрудники CISA, которые якобы не имели доступа к системе Jira EIP, при обсуждении сообщений о «дезинформации» ссылались на коды «тикетов», характерные для EIP. Приведенное ниже электронное письмо, отправленное 2 ноября - за день до выборов 2020 года, - является одним из таких примеров, в котором сотрудник CISA сообщает в Twitter: *«Пожалуйста, ознакомьтесь с приведенным ниже сообщением от сотрудников избирательных органов штата Коннектикут. «Тикет» также помечен как EIP-572».*

В какой-то момент Кристофер Кребс, тогдашний директор CISA, поручил Роберту Шолу, руководителю отдела анализа и политики устойчивости CISA, связаться с Грэмом Бруки, старшим директором Лаборатории цифровых криминалистических исследований Атлантического совета (DFRLab), чтобы узнать о конкретной информации, связанной с выборами, распространяемой в социальных сетях. В электронном письме Шол написал: *«Мы тоже получаем информацию от EIP, но хотели бы уточнить у вас [директор Кребс], что мы особенно заинтересованы в любой аналитике, которую мы можем собрать вместе по этой информации, а также в том, откуда она исходит и кто ее усиливает».* Внутренние документы Атлантического совета показывают, что

From: Graham Brookie <[REDACTED]@ATLANTICCOUNCIL.ORG>
Sent: Wednesday, September 30, 2020 5:05 PM
To: Andy Carvin <[REDACTED]@ATLANTICCOUNCIL.org>; Emerson Brooking <[REDACTED]@ATLANTICCOUNCIL.org>
Subject: ANDY / EMERSON -- Coordination

COORDINATION ON US DOMESTIC PRIORITIES

Hi to both –

The struggle here is that Emerson is managing efforts and Andy is managing staff and outputs. The only way to be successful is to make sure that the three of us are explicitly on the same page about how we are allocating staff to efforts.

The below is intended to do that – and I will be adding Emerson to the DCHQ WhatsApp chain, where we will coordinate in general, as soon as we're on the same page as below. Our first obligation is always to our staff and not setting them up for failure. Our second obligation is to our core work, which every single one of us is managing key elements of. Thus the burden falls on the three of us to coordinate both.

Please reply in red or blue to the below. I also didn't have explicit names in the "staffing" section of each, so please fill out.

Thanks,
Graham

Election Integrity Partnership

Key questions: What is the schedule of shifts, noting that we just need to assign people to them? EIP, the voluntary shift system is a potential challenge because it requires a person to spend X amount of hours monitoring things, which either results in no outputs being produced, or a sudden need to complete an output that the person may or may not be suited to complete, especially if it's an international member of the team with limited knowledge of US politics, geography, culture, etc.

In scenarios where something potentially important surfaces within EIP, how do we go about prioritizing it? For example, when is it simply a matter of "this is a good story so please get me a draft in 72 hours" vs "all hands on deck, this is like a major takedown?" In either case, the three of us need to be locked up in order to not undermine our whole business operation through editorial capacity, who gets assigned, scheduling, etc.

One not ideal scenario is a situation where Jean or Ayush volunteer for a few hours, end up finding something important, and then having not having all three of our awareness and approval, which could lead to significant members of staff being taken away from their core responsibilities for extended periods of days/week. In other words, a shift is just the tip of the iceberg, commitment-wise.

Another question is what constitutes a contribution to EIP. While the focus has been on the partnership and the process (which makes sense) we're part of a team reviewing leads and deciding when to act on them. But we also continue to cover election-related stories that will originate from our original research, rather than the college students volunteering at EIP, especially now that Jared is coming on board and while looking into more conspiracy related content. Can we consider those contributions? I imagine for some researchers there's more incentive to contribute when they're able to generate research leads themselves rather than being responsive to tips, though I understand responding to tips is still core to the partnership.

Important to note: not college kids surfacing EIP leads. Krebs CISA is texting Stamos with some regularity. A few tickets have been flagged by the platforms. Starbird's UW team is surfacing a lot of stuff using advanced soc media listening methods. College kids (T-1) just doing the first round of analysis.

The job of DFRLab is to be T-2, doing a deep dive into tickets, attaching more contextual information, and writing up a twitter thread/blog post if that's the recommendation of the researcher (and the T-3 shift manager approves).

Analysts can step away and write a blog post on-shift. That's what Alyssa did [last week](#).

Бруки и другие поняли, что директор Krebs и директор SIO Алекс Стамос переписывались «с некоторой регулярностью».

Сотрудники CISA также запрашивали информацию о политических высказываниях

From: Scully, Brian <[REDACTED]@cisa.dhs.gov>

Sent: Tuesday, November 10, 2020 9:24:57 AM

To: [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>; [REDACTED] <[REDACTED]@fb.com>

Subject: Hammer and scorecard narrative

Good morning,

Director Krebs is particularly concerned about the hammer and scorecard narrative that is making the rounds. Wanted to see if you all have been tracking this narrative and if there's anything you can share around amplification?

Thanks,
Brian

в социальных сетях у сотрудников платформ. В тот же день, 10 ноября, Скалли отправил электронное письмо трем сотрудникам Facebook, написав: *«Директор Krebs особенно обеспокоен нарративом о «молотке» и «оценочной карте», который муссируется. Хотел узнать, отслеживали ли вы эту информацию и можете ли вы чем-нибудь поделиться по поводу ее усиления?»*

Эти электронные письма прямо опровергают утверждения о том, что CISA играла «очень незначительную роль, если вообще играла» в EIP. Напротив, CISA в режиме реального времени была в курсе того, что подается в EIP, какие шаги предпринимает EIP и какие действия предпринимают платформы социальных сетей - и EIP, и платформы социальных сетей были осведомлены о значительной роли CISA.

D. Непосредственное участие Государственного департамента в операции EIP «Цензура»

Центр глобального взаимодействия (ГЕС) — это многоведомственная организация, входящая в состав Государственного департамента, которую Илон Маск назвал «злейшим преступником в цензуре правительства США и манипулировании СМИ со стороны правительства США».

ГЕС и организации, финансируемые ГЕС, неоднократно «отмечали» на платформах социальных сетей контент, в котором фигурировали американцы, занимающиеся защищаемой Конституцией речью.

Appointment

From: Levis, Adela [REDACTED]@state.gov]
Sent: 10/15/2020 3:35:38 PM
To: Levis, Adela [REDACTED]@state.gov]; Kate Starbird [REDACTED]@uw.edu]; Shelby Grossman [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e995f09f3b364dde8a93beed3a5f55db-shelbybg]; Ruppe, Adele E [REDACTED]@state.gov]; Jevin West [REDACTED]@uw.edu]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; info@eipartnership.net; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Beebe, William [REDACTED]@state.gov]; Stewart, Samaruddin K [REDACTED]@state.gov]; Dempsey, Alex L [REDACTED]@state.gov]
CC: Elena Cryst [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=2a59e34f3cbe4c78a497962dc7161e3f-ecryst]
Subject: [eip-info] RE: GEC/Election Integrity Partnership
Start: 10/16/2020 7:30:00 PM
End: 10/16/2020 8:30:00 PM
Show Time As: Busy
Recurrence: (none)

Dear All,
please join us today Friday, Oct. 16th, at 3:30pm EST/12:30 PT to discuss a concrete idea we have for possible support of the EIP effort.

Please let me know if you have any questions ahead of time.

Join Microsoft Teams Meeting

+1 509-824-1908 United States, Spokane (Toll)
Conference ID: [REDACTED]

Warm regards,
Adela

В отличие от предлога CISA о непричастности, EIP открыто признала, что GEC сообщала о «тикетах» в EIP в своем заключительном отчете по итогам избирательного цикла 2020 года. Более того, согласно этому отчету, GEC была одной из наиболее часто отмечаемых организаций в системе Jira EIP.

15 октября 2020 года Адела Левис, «связной с академическими и аналитическими центрами» при GEC, отправила по электронной почте приглашение на встречу с названием «Партнерство GEC и честных выборов». В тексте письма Левис написала, что встреча состоится «для обсуждения конкретной идеи, которую мы имеем для возможной поддержки усилий EIP».

Message

From: Beebe, William [REDACTED]@state.gov]
Sent: 12/4/2020 11:12:27 PM
To: Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; [REDACTED] [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED] Kate Starbird [REDACTED]@uw.edu]; Shelby Grossman [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e995f09f3b364dde8a93beed3a5f55db-shelbybg]; Jevin West [REDACTED]@uw.edu]
CC: Levis, Adela [REDACTED]@state.gov]; Ruppe, Adele E [REDACTED]@state.gov]; Dempsey, Alex L [REDACTED]@state.gov]; Stewart, Samaruddin K [REDACTED]@state.gov]
Subject: Thank You from the GEC

EIP Team,

I want to send my sincerest thanks for allowing me to participate in the Election Integrity Partnership as an analyst with the GEC. My colleagues and I appreciated your taking the time to meet with us before the election and accommodating my involvement on short notice. I am proud to have worked on such an impactful initiative with so dedicated a team and look forward to reading the products you continue to produce.

We'd like to stay in touch and look for ways to collaborate further. When you have time, we'd welcome a follow-up meeting to exchange ideas and lessons learned on the disinformation challenge. Adela Levis (cc'd here) would also like to know how her Academic Liaison Unit can support your research efforts.

Have a great weekend!

Best Regards,

Will

После выборов 2020 года «аналитик по борьбе с дезинформацией» из GEC отправил директору SIO Алексу Стамосу, менеджеру по исследованиям SIO Рене Диресте и директору UW по СІР Кейт Старберд, а также всем остальным, восторженное письмо с темой «Спасибо от GEC». Аналитик воскликнул: «Я хочу выразить свою искреннюю благодарность за то, что вы позволили мне принять участие в партнерстве по обеспечению честности выборов с GEC. Я и мои коллеги высоко оценили то, что вы нашли время встретиться с нами до выборов и приняли мое участие в короткие сроки». Аналитик продолжил: «Я горжусь тем, что работал над такой важной инициативой с такой преданной командой».

Е. Участие других федеральных агентств в EIP: FBI и NHS.

CISA была не единственной правительственной организацией, осведомленной о деятельности EIP. 23 июня 2023 года Комитет и Отдельный подкомитет провели расшифрованное интервью с Алексом Стамосом, изучая его и CISA участие в EIP. В ходе интервью Стамос показал, что SIO информировал о EIP ряд других правительственных учреждений, включая Агентство национальной безопасности (NSA) и Киберкомандование.

Стамос также показал, что специальный агент Федерального бюро расследований (FBI) Элвис Чан, который был главным связным между FBI и Кремниевой долиной и участвовал в подавлении новостей о вредной для семьи Байденов информации, найденной на ноутбуке, принадлежащем Хантеру Байдену, организовал брифинг между SIO и NSA.

Стамос дал показания:

Вопрос: *С какими другими федеральными агентствами EIP проводила консультации?*

Ответ: *Я проводил брифинг для генерала Накасоне, тогдашнего директора NSA и Киберкомандования...*

Вопрос: *FBI также получало информацию о выборах?*

Ответ: *FBI было частью этого брифинга, поэтому я проводил его из офиса FBI в Сан-Франциско, потому что я просто не могу зайти в NSA.*

Вопрос: *Вы помните, кто организовал встречу между вами и NSA?*

Ответ: *Элвис Чан организовал встречу, потому что Накасоне приехал в университетский городок. Элвис был фасилитатором, который предоставил помещение и участвовал, слушал брифинг в Сан-Франциско.*

Вопрос: *Да. Знали ли вы мистера Чана до этой встречи?*

Ответ: *Я.*

SIO продолжал предоставлять FBI обновленную информацию о EIP на протяжении всего избирательного цикла 2020 года. Например, 5 октября 2020 года Алекс Стамос отправил электронное письмо Элвису Чану, написав: *«Сейчас Партнерство по обеспечению честности выборов работает в три смены каждый будний день... У нас нет никаких веских признаков иностранного вмешательства, и большинство замеченных нами фактов можно связать с известными внутренними акторами»,* то есть американцами.

Message

From: Chan, Elvis M. (SF) (FBI) [REDACTED]@fbi.gov
Sent: 10/6/2020 4:25:46 PM
To: Alex Stamos [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]; Renee DiResta [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=[REDACTED]]
Subject: RE: [EXTERNAL EMAIL] - RE: Status Update

Hi Alex,

It seems like you have a good system in place and are plugged in with the relevant entities. The FBI SF mandate is to be the conduit to/from the social media companies for all election-related threats, whether foreign or domestic. We've been receiving mostly domestic voter suppression-related accounts to flag for social media companies as each state had its primaries.

At our command post, we'll have a NCRIC-embed who will have access to HISSN, EI-ISAC, and MS-ISAC feeds as well. We are hoping USIC partners will be able to declassify information fast enough for us to push out to the companies for awareness.

Since you are also flagging things and sending them to the social media companies, I know they'll be able to relay any coordinated campaigns they see to us for examination and possible case opening. Let's plan to stay in touch as things start to heat up. Thanks!

Regards,
Elvis

From: Alex Stamos <[REDACTED]@stanford.edu>
Sent: Monday, October 5, 2020 7:44 PM
To: Chan, Elvis M. (SF) (FBI) <[REDACTED]@fbi.gov>; Renee DiResta <[REDACTED]@stanford.edu>
Subject: Re: [EXTERNAL EMAIL] - RE: Status Update

Elvis-

Right now, the Election Integrity Partnership is running three shifts each weekday (and one on Sunday) looking for election related disinformation. We are handling about a dozen "incidents" per day, which can correspond to multiple pieces of disinformation or just one (this is varying widely). We are intaking reports from locals via EI-ISAC, working with NGOs like Common Cause, and routing issues to platforms to get handled.

It's working pretty well. You can see a handful of incidents we wrote up at eipartnership.net. We will be adding shifts in a couple of weeks and will be staffing a war room at my house (post COVID-testing) on election day.

CONFIDENTIAL

SIO-HJC014624

What's your mandate look like? We don't have any good indications of foreign interference from our work, and most of the things we have spotted can be tied to known domestic actors. Probably some foreign amplifiers, but figuring that out is generally outside of our scope and the data we have access to. Check out our "Rapid Reaction" posts and see if any of those kinds of topics are in scope for your work.

Alex

Отвечая на вопрос Стамоса о мандате FBI, Чан написал: «Мандат FBI [Сан-Франциско] заключается в том, чтобы быть каналом связи с представителями социальных сетей по всем угрозам, связанным с выборами, как иностранным, так и внутренним. Мы получали в основном внутренние специальные аккаунты, связанные с наблюдением за избирателями, чтобы отметить их для представителей социальных сетей, поскольку в каждом штате прошли праймериз».

III. «ТИКЕТЫ» JIRA ОТ EIP: ЭНЦИКЛОПЕДИЯ КОНСЕРВАТИВНОЙ ЦЕНЗУРЫ

Изучение самих «тикето» Jira позволяет выявить настоящий список известных консервативных деятелей, ставших мишенью для цензуры со стороны CISA и EIP. 17 марта 2023 года, в ответ на повышенное внимание СМИ к деятельности SIO, в том числе на слушаниях в Подкомитете 9 марта, посвященных файлам Twitter, SIO опубликовала в своем блоге сообщение, изобилующее ложными заявлениями о EIP. Например, в блоге говорилось, что EIP не «преследует» и не дискриминирует консервативные аккаунты или контент в социальных сетях». Хотя EIP действительно отмечает неконсервативный контент, чтобы сохранить фасад нейтралитета, отчеты EIP демонстрируют явную попытку подавить консервативную речь в частности.

Согласно отчету, подготовленному EIP после выборов, существует четыре категории связанной с выборами «дезинформации», которые, по мнению EIP, «входят в сферу действия» типа «дезинформации», которую EIP будет анализировать. Некоторые из категорий, такие как «процедурное вмешательство», относительно однообразны, хотя часто выходят за пределы своих границ, и включают такие вещи, как «материалы, которые вводят избирателей в заблуждение относительно того, как правильно подписать бюллетень, отправленный по почте» и «материалы, которые призывают избирателей голосовать в другой день».

EIP неоднократно использовала четвертую категорию, в частности, для оправдания цензуры консервативной политической речи: «Делегитимация результатов выборов», определяемая как «материал, делегитимизирующий результаты выборов на основе ложных или вводящих в заблуждение утверждений». Этот произвольный и непоследовательный стандарт был определен политическими деятелями, маскирующимися под «экспертов» и ученых. Но что еще более тревожно, федеральное правительство было тесно связано с университетами при вынесении этих, казалось бы, произвольных решений, которые были направлены против одной из сторон политической оси.

EIP регулярно отмечала консервативный контент в социальных сетях под предлогом того, что он неправомерно «делегитимизирует» результаты выборов, даже в тех случаях, когда контент был фактически точным. Критика избирательной системы - это защищенная Конституцией речь. Политическая система, позволяющая небольшому меньшинству одобренных правительством «экспертов» оказывать влияние на способность других граждан выражать свое мнение правительству, представляет собой глубокую угрозу американской конституционной республике. Огульное или неправомерное подавление обвинений в мошенничестве на выборах неизбежно подавляет речь о реальных случаях мошенничества на выборах, тем самым позволяя правительству свободно проводить выборы таким образом, что оно не несет ответственности перед американским народом.

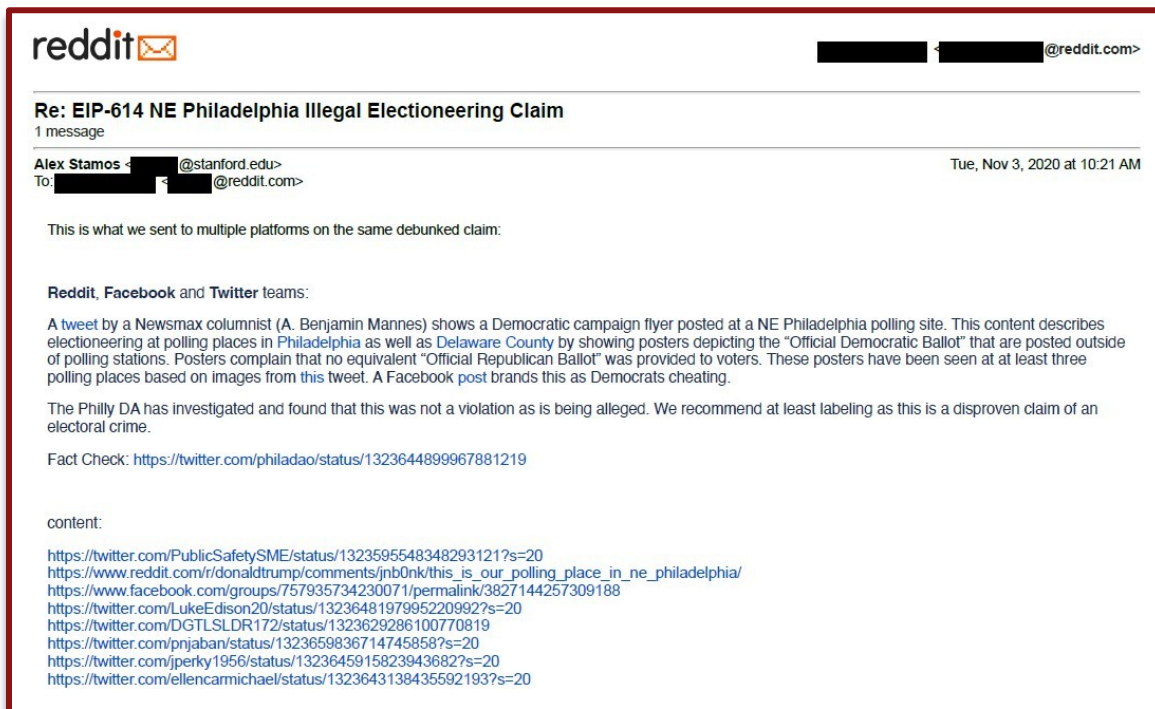
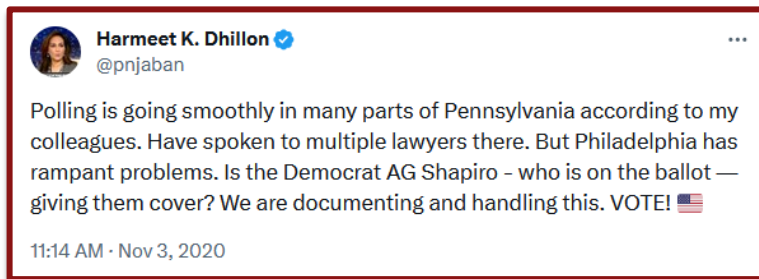
А. Отказ от претензий на «дезинформацию»: Абсурдный подход EIP к классификации

В своем отчете EIP признала, что «не является организацией по проверке фактов» и что «в некоторых случаях невозможно было найти внешнюю проверку фактов, потому что ни один специалист по проверке фактов еще не занимался этим вопросом, или потому что информация не поддавалась простой проверке». Невероятно, но EIP также признала, что ее аналитики «выявили по крайней мере один внешний источник проверки фактов примерно для 42 % “тикетов», попавших в поле зрения». Другими словами, аналитики EIP не смогли найти ни одного внешнего источника, подтверждающего, что в *большинстве сообщений*, отмеченных ими, конкретное сообщение или рассказ были названы «дезинформацией» или «ложью».

Общая зависимость цензоров социальных сетей от специалистов по проверке фактов, многие из которых имеют явно либеральные политические пристрастия, создает среду, враждебную свободе слова, особенно консервативным точкам зрения, и сама по себе вызывает беспокойство. Однако тот факт, что EIP не смогла найти ни одного проверяющего факты, предвзятого или нет, прежде чем пометать контент в социальных сетях в большинстве случаев, и готова публично признать этот факт, свидетельствует о наглости и манией величия подходе к цензуре, не заботясь о правде или сохранении даже видимости политического нейтралитета.

В случаях, когда EIP не могла проверить фактами выявленное утверждение или рассказ, она могла не отмечать контент на платформах социальных сетей, учитывая, что была неуверенность в правдивости данного контента. Вместо этого EIP агрессивно помечала такие посты на платформах, отмечая в тикетах, что у нее не было никаких оснований для сообщения об этом контенте, кроме политической повестки CISA и самой EIP.

Например, запись в EIP-713, тикете Jira, касающаяся статьи Gateway Pundit, написанной во второй половине дня выборов 3 ноября, гласила: «Мы отправляем это вам быстро, поскольку, скорее всего, не сможем провести здесь проверку фактов». В EIP-418, касающемся твита от One America News Network, один из авторов написал: «*Мы не видели фактчека по этой прямой истории, но эта история направлена на дискредитацию действительности голосования по почте*». В своем отчете EIP заявила, что ее целью было «выявление и анализ дезинформации», которую даже CISA публично определяет как *ложную* информацию. Однако подход, продемонстрированный в этих и других “тикетах”, ясно показывает, что в центре внимания EIP была не истина, а продвижение дискриминации по признаку альтернативной точки зрения.



В. Усилия по цензурированию правды

Даже в тех редких случаях, когда ЕИР удавалось найти внешнюю проверку фактов, специалисты по проверке фактов часто сами не были уверены в себе, признавали, что соответствующие утверждения не являются ложными, или были подвержены несомненной политической предвзятости. 3 ноября 2020 года Алекс Стамос отправил электронное письмо сотруднику Reddit с содержанием тикета Jira, касающегося нарушений на избирательных участках в Филадельфии, поскольку Reddit отказался напрямую участвовать в системе Jira.

Хотя «тикет» якобы касался конкретного утверждения о знаках, вывешенных у избирательных участков, в нем был отмечен более общий контент, включая приведенный ниже твит представителя Республиканской партии Хармита Дхиллона. Проверка фактов, на которую ссылается «тикет», — это твит офиса демократического окружного прокурора Филадельфии, который не оспаривает ни одно из утверждений в сообщении Дхиллона.

С. Усилия по цензуре президента Трампа и его семьи

Самым известным консерватором, ставшим мишенью CISA и EIP, был не кто иной, как действующий президент Соединенных Штатов Дональд Трамп. 27 октября 2020 года местный чиновник сообщил о твите президента Трампа на «дезинформационную» линию CIS, которая, согласно своему обычному протоколу, переслала сообщение в EIP и CISA. Затем CISA пометила содержание твита в Twitter. В данном случае речь идет о том, что неизбираемый чиновник исполнительной власти пометил заявление избранного лидера исполнительной власти для удаления с одного из крупнейших и наиболее активных публичных форумов в мире. CISA не предоставил Комитету никаких доказательств того, что он связался с Белым домом до передачи сообщения, чтобы высказать свое мнение о правдивости утверждения в твите.

[mailto:]

Sent: Tuesday, October 27, 2020 12:52 PM

To: Elections - Public <[REDACTED]@sos.wa.gov>

Subject: Disinformation

I'm reporting this disinformation about the elections. Please take steps to stop it, and correct it publicly. Thanks.

Federal Way, WA



From: Misinformation Reports <[REDACTED]@cisecurity.org>

Sent: Tuesday, October 27, 2020 4:07 PM

To: [REDACTED]@2020partnership.atlassian.net; Misinformation Reports <[REDACTED]@cisecurity.org>; Scully, Brian <[REDACTED]@cisa.dhs.gov>; CFITF <[REDACTED]@hq.dhs.gov>; CISA Central <[REDACTED]@cisa.dhs.gov>

Subject: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation tweet regarding re-voting

From: Scully, Brian

Sent: Tuesday, October 27, 2020 4:09 PM

To: [REDACTED]@twitter.com; [REDACTED]@twitter.com; [REDACTED]@twitter.com

Cc: CFITF <[REDACTED]@hq.dhs.gov>; Misinformation Reports <[REDACTED]@cisecurity.org>

Subject: FW: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

Please see below report from Washington.

Thanks,
Brian

Участие CISA в попытке цензуры президента Трампа не закончилось после того, как отчет был отправлен в Twitter. Вместо этого, как отмечается в записи в «тикете» Jira, обозначенном как EIP-482: «Мы [EIP] получили ответ от Twitter через CISA» относительно того, как Twitter решил обработать сообщенный твит.

Это был не единственный случай, когда CISA и EIP пытались помешать законно избранному президенту общаться с американской общественностью. 4 ноября 2020 года сотрудник избирательной комиссии штата Мичиган направил в CIS сообщение о «дезинформации», написав: «Сегодня мы узнали о явной ошибке в сообщении неофициальных результатов выборов в Антриме. Сообщенные неофициальные результаты были необычными. Округ рассмотрел этот вопрос и после разговора со своим поставщиком выборов определил, что, возможно, в программе, используемой для объединения результатов, произошла ошибка, которая привела к отображению неточных цифр». По словам представителя избирательной комиссии, это вызвало беспокойство, поскольку «отдельные лица используют этот инцидент для распространения дезинформации или теорий заговора, согласно которым результатам выборов нельзя доверять».

From: Misinformation Reports

Sent: Wednesday, November 4, 2020 7:42:36 PM (UTC+00:00) Monrovia, Reykjavik

To: Scully, Brian; CISA Central; CFITF; [REDACTED]@2020partnership.atlassian.net; Misinformation Reports

Subject: Case #CIS-MIS000159: Antrim County, MI election results error in reporting

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

From: [REDACTED]@michigan.gov>

Sent: Wednesday, November 4, 2020 2:35 PM

To: MS-ISAC SOC <[REDACTED]@msisac.org>; Misinformation Reports <[REDACTED]@cisecurity.org>

Subject: Antrim County Michigan Election Results Error in reporting

Importance: High

Good Afternoon,

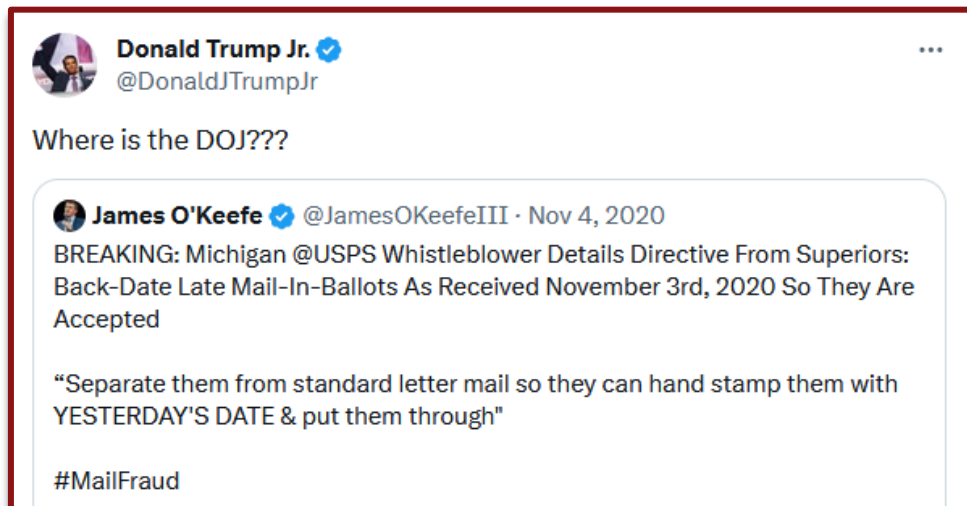
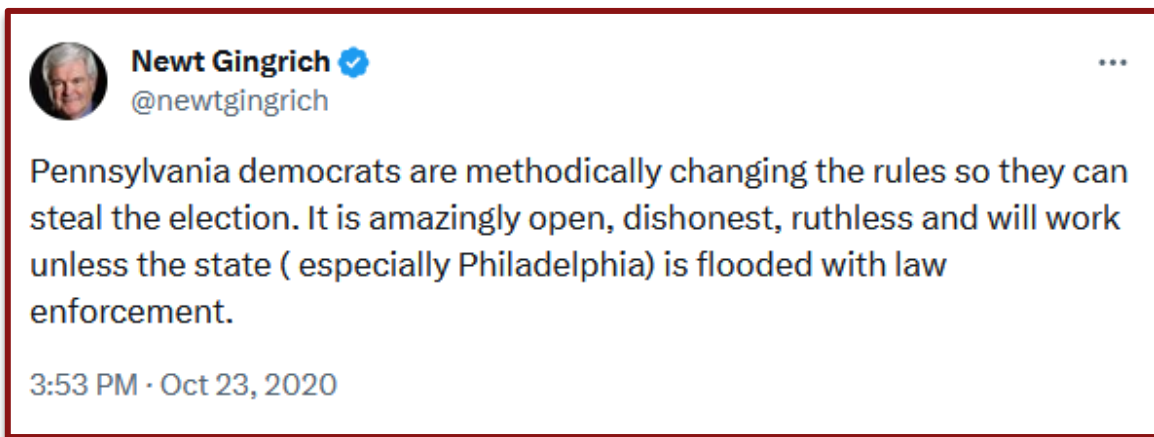
Today we learned of an apparent error in reporting unofficial election results from Antrim. The unofficial results reported were unusual. The County reviewed the issue and after speaking with their election vendor, determined that there may have been an error in the program used to combine the results that caused inaccurate numbers to display.

At this time, there is no reason to think that this was the result of malicious activity. We believe that all ballots and tabulators functioned properly. Voters are recorded on hand-marked paper ballots. The County is reviewing the issue further with its election vendor and will then determine when it will be able to report its unofficial results. Again, all results reported at this time are unofficial; the official results are determined after a County canvass of election results and certification by the Board of State Canvassers.

Individuals are using this incident to spread misinformation or conspiracy theories that the election results cannot be trusted. They may be combining this story with apparently doctored images of election results in other areas to suggest a widespread conspiracy to change election results. They may also combine this with efforts to undermine the ongoing counting of absent voter ballots. There is no basis to this whatsoever and as far as we know this was an isolated incident caused by an error that was quickly caught.

Как обычно, отчет был одновременно направлен в EIP и CISA для принятия дальнейших мер. В ответ на это EIP послушно включила свои антенны наблюдения, проверяя социальные сети на наличие сообщений и активности, связанных с нарушениями в отчетности, которые, как подтвердил представитель штата, действительно имели место. Затем EIP передала в Twitter и Facebook ряд URL-адресов, касающихся инцидента в округе Антрим. Facebook ответила, что «наложила соответствующие метки на ссылки, которыми вы поделились». Одной из ссылок, включенных в «тикет», был твит от президента Трампа поделился статьей из Breitbart с дополнительным комментарием: «Какой же полный бардак творится на этих «выборах!» CISA не предоставило Комитету никаких доказательств того, что агентство напрямую связывалось с Белым домом, чтобы выразить свою обеспокоенность твитом, вместо этого полагаясь на EIP для осуществления цензуры по доверенности.

Члены семьи президента Трампа также подвергались цензуре со стороны CISA и EIP. В ходе своей работы в период выборов 2020 года EIP отметила множество сообщений Дональда Трампа-младшего и Эрика Трампа, некоторые из которых, судя по всему, были удалены или помечены. В одном из документов, обозначенном как EIP-867, EIP отметила аккаунт Дональда Трампа-младшего в Twitter за то, что он просто перепостил твит консервативного журналиста Джеймса О'Кифа и спросил: «Где Минюст (DOJ)???».



D. Усилия по цензуре политических кандидатов и законодателей

Цензура CISA и EIP нацелена не только на президента Трампа, но и на бывших, действующих и будущих законодателей. В EIP-450 EIP отметила твит (на фото ниже) бывшего спикера Палаты представителей Ньюта Гингрича об изменениях в избирательном законодательстве Пенсильвании.

В деле EIP-904 EIP попытался подвергнуть цензуре представителя Джоди Хайса, действующего конгрессмена-республиканца от штата Джорджия, за то, что он выступил с основной политической речью, критикующей организацию выборов в его родном штате.



Thom Tillis
@ThomTillis



Thank you for this historic victory, North Carolina!

Looking forward to SIX MORE YEARS of fighting for you and your family in the U.S. Senate. #ncsen #ncpol



12:05 AM · Nov 4, 2020



Rep. Jody Hice ✓
@CongressmanHice



GA's handling of this election is embarrassing!

Two days are gone and we still don't know results...are you kidding?

Worse yet, partisan ballots keep appearing.

A fair vote & Trump wins, end of story!

Stop the fraud!

7:04 PM · Nov 5, 2020

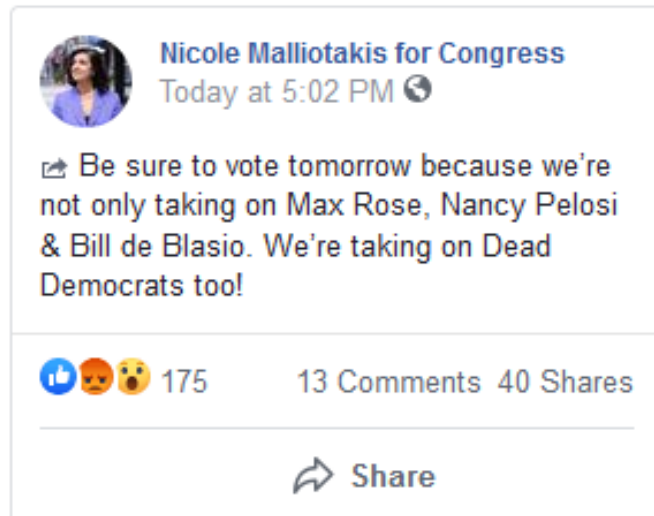
Аналитики EIP также отметили совершенно безобидный твит сенатора Тома Тиллиса из Северной Каролины в EIP-936, поскольку группа посчитала его заявление о победе преждевременным. Сенатор Тиллис действительно выиграл переизбрание в Сенат.

Кроме того, EIP нацелилась на кандидатов-республиканцев на политические должности, в том числе тех, кто впоследствии станет членом Конгресса. Например, в EIP-596 EIP отметила это сообщение в Facebook со страницы предвыборной кампании ректора Николь Маллиотакис. Судя по всему, сообщение было удалено Facebook.

В деле EIP-780 «аналитики» EIP отметили сообщение с аккаунта предвыборной кампании ректора Марджори Тейлор Грин, в котором конгрессвумен призывала своих подписчиков поделиться ее сообщением. Это скользкая дорожка, если политические кандидаты и их сторонники не могут выразить законное беспокойство по поводу избирательного процесса.

В то время как многие эксперты по дезинформации быстро критикуют кандидатов-республиканцев за подрыв «веры в выборы», эти эксперты, похоже, хранят молчание всякий раз, когда демократы возражают против результатов выборов или безосновательно обвиняют в поражении на выборах используя необоснованные заявления о мошенничестве или обмане, дезинформации.

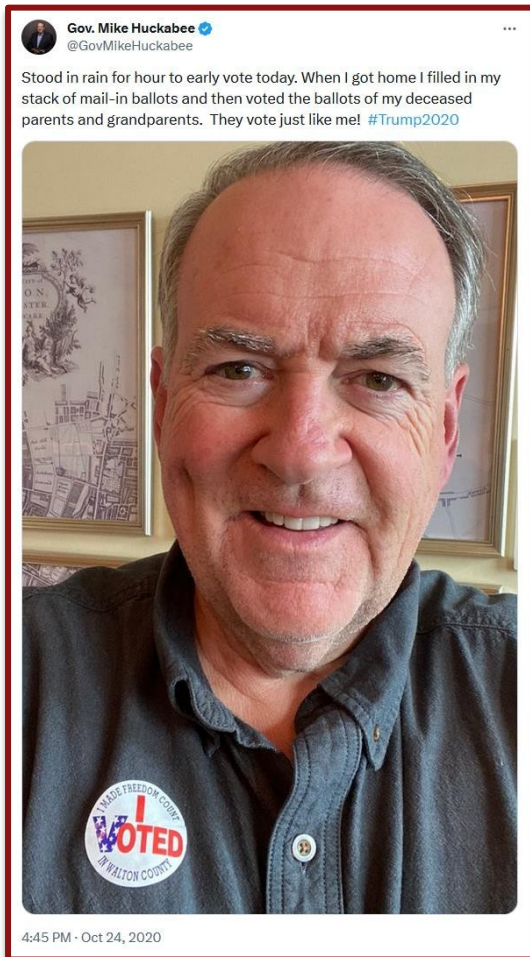
Возможно, наиболее примечательно то, что многие демократы повторяли необоснованное утверждение о том, что президент Трамп вступил в сговор с Россией, вместо того чтобы признать законность его победы над Хиллари Клинтон. Но, как признают сами эксперты по дезинформации, изучение «дезинформации», конечно же, «по своей сути дело чисто политическое».



Е. Усилия по цензуре юмора и сатиры

Документы, полученные Комитетом и Специальным подкомитетом, также показывают, что EIP отмечала контент, который был явно юмористическим и сатирическим.

Например, аналитики EIP внутренне идентифицировали твит бывшего губернатора Арканзаса Майка Хакаби, в котором Хакаби пошутил о голосовании умерших родственников. Согласно «тикету», помеченному EIP-460, человек, связанный с EIP, написал: *«ISAC Partners, добавляю вас в эту тему для наглядности. Мы рекомендуем Twitter пометить это, особенно в опции (b) поскольку оно было размещено общественным деятелем».*





Carol Ricks
@BVMgroupie



Some or all of the content shared in this Post is disputed and might be misleading about an election or other civic process. [Learn more](#)

Wow. They found boxes of “Emergency” Democrat Votes this morning.
How convenient???



1:33 PM · Nov 4, 2020

ЕІР даже возражала и пыталась подвергнуть цензуре юмористические изображения, которые не могли быть обоснованно восприняты как подлинные. Оба изображения, воспроизведенные ниже и отмеченные в ЕІР-811, являются очевидной фальсификацией и изображают транспортировку коробок с надписью «Чрезвычайное голосование демократов». ЕІР написала в “тикете»: «Пользователи в Twitter и Facebook делятся манипулированными изображениями людей, перевозящих коробки в грузовиках с надписью «Emergency Democrat Votes». Мы предлагаем пометить или удалить твиты, в которых используется эта фотография, поскольку она может подорвать веру людей в легитимность избирательного процесса». Хотя изображение может показаться нелепым, некоторые пользователи могут поверить в его реальность».

 Paula Priesse
November 4, 2020 · 🌐

November 4th – The Dems and their corrupt media comrades insist it's over. We say NOT EVEN CLOSE. Let the lawsuits begin! P



 Election officials follow strict rules when it comes to ballot counting, handling and reporting.
Source: Bipartisan Policy Center
[Get Accurate Election Info](#) 

В обоих случаях EIP успешно побудила платформы добавить ярлыки к постам. Подобные примеры иллюстрируют полное презрение, с которым CISA, CIS и EIP относились к американской общественности и ее способности оценивать информацию в социальных сетях.



Г. Усилия по цензуре других влиятельных консервативных аккаунтов

Помимо упомянутых ранее аккаунтов, EIP выбрала для подавления аккаунты в социальных сетях консервативных журналистов, комментаторов и деятелей с большим количеством подписчиков и высокой вовлеченностью. В “тикете» Jira под номером EIP-805 EIP отметила оба поста на скриншоте ниже - один от Кэндис Оуэнс, а другой от Чарли Кирка.

EIP также помечала посты известных и популярных консервативных аккаунтов, включая аккаунты Пола Сперри, Шанель Рион, Шона Дэвиса, Дэйва Рубина, Мишель Малкин, Джеймса О'Кифа, Бенни Джонсона, Джека Пособица, Трейси Бинза, Майка Романа, Шона Хэннити, Babylon Bee, Newsmax, Молли Хемингуэй, Тома Фиттона и других.

Подавление консервативных политиков и СМИ в результате этой “цензурной операции” лишило бесчисленное множество американских избирателей возможности ознакомиться с различными точками зрения на важнейшие политические вопросы в дни и недели, предшествующие всеобщим выборам. Очень важно, что EIP проводила свою цензурную операцию по указанию и в сотрудничестве с CISA, федеральным правительственным агентством, активно стремящимся подорвать свободу слова и действующего президента. Значение этих фактов невозможно переоценить.

IV. ТАКТИКА ПРИНУЖДЕНИЯ EIP

В преддверии выборов 2020 года социальные медиа-платформы были наводнены запросами о цензуре от ряда федеральных агентств, включая FBI и CISA. Как указано в разделе I этого промежуточного отчета, CISA и ее доверенные лица уже имели два канала для подачи отчетов - Switchboarding и EI-ISAC - и до создания EIP активно лоббировали третий канал, «портал для подачи отчетов о дезинформации», управляемый CIS. Затем, после создания EIP, данные тикетов Jira и электронные письма ясно показывают, что платформы социальных сетей понимают, что федеральное правительство работает напрямую с EIP.

Помимо явной и скрытой поддержки со стороны федерального правительства, в распоряжении EIP был еще один инструмент давления на представители социальных сетей, чтобы заставить их выполнить требования о цензуре: средства массовой информации. В своих показаниях перед Комитетом Алекс Стамос, директор SIO и бывший директор по безопасности Facebook, объяснил, как представители социальных сетей ощущают давление со стороны общественности, критикующей их за неспособность удалять контент, который эксперты квалифицировали как дезинформацию. Он сказал:

Вопрос: А что касается записей в блогах, кто-нибудь из EIP сообщал платформам, что вы собираетесь сделать эти записи публичными?

Ответ: Вполне возможно, что мы предупредили их, когда писали об этом.

Вопрос: И почему вы это сделали?

Ответ: Я думаю, что это вежливый поступок, чтобы они знали, что мы выходим на публику. Мы не хотели, чтобы у них возникло ощущение, что мы не замечаем их.

Вопрос: И что вы имеете в виду, говоря «предупредить» их?

Ответ: Мы хотели, чтобы они знали, что возможно обсуждение того, что происходило на их платформе, и они должны знать об этом. Я думаю... знаете, мы... я с пониманием отношусь к тому, как трудно быть в одной из этих компаний и пытаться сбалансировать все различные функции. И если кто-то пишет что-то, что может создать коммуникационный момент в период выборов, то это то, о чем я хотел бы знать наверняка.

Вопрос: *Что вы имеете в виду под “коммуникационным моментом”?*

Ответ: *Если мы пишем в блоге пост со словами: «Это вирусное явление, которое происходит, не является правдой», то вполне возможно, что представители СМИ выйдут на улицу, найдут этот контент на пяти разных платформах, а затем напишут о том, что это правда или нет.*

Вопрос: *И если бы он все еще работал, некоторые из этих медиа-изданий критиковали бы платформы?*

Ответ: *Это возможно.*

Доктор Кейт Старберд из Университета Вашингтона, одна из главных фигур, участвовавших в работе EIP, также дала показания об использовании своей платформы (независимо от EIP) для публичного давления на социальные медиаплатформы с целью изменения их политики. Она заявила:

Вопрос: *Была ли цель публичного сообщения в том, чтобы заставить Twitter изменить свою политику?*

Ответ: *Для меня это было... Опять же, это не относится к бренду EIP. Это что-то вроде того, что мы просто делали, чтобы в конечном итоге начать работать всем вместе. Но это просто то, что я часто делаю, а именно - провожу анализ и в конце этого анализа даю рекомендации для платформ.*

Иногда это делается в официальных документах. В данном случае я бы иногда выкладывала аналитические материалы в Twitter, чтобы сказать, что это происходит, что это проблема, привлечь к ней внимание, и чтобы они подумали, что им следует сделать, чтобы измениться. Да.

И я не всегда рекомендую... Я редко рекомендую конкретные действия. Я бы хотела... я не успела это сказать... Я бы хотела сказать что-то лучшее. Но чаще всего я просто указываю на проблемы и не говорю, как их решить. Я понимаю, что решение проблем очень сложное и трудное, поэтому я отдаю им должное. Но я много писала, как бы указывая: Это проблема.

Осенью 2020 года EIP также работала над подготовкой рабочего продукта, обобщающего политику модерации контента основных социальных медиаплатформ и различия между ними. Изначально EIP предоставила Alphabet (материнской компании Google и YouTube) возможность прокомментировать политику YouTube в отношении модерации контента. Как видно из приведенной ниже цепочки электронных писем, Alphabet прекрасно понимала, что EIP может «привлечь прессу». В частности, компания хотела убедиться, что EIP не будет публиковать «неточности» или «неправильные характеристики», которые, можно предположить, утверждали, что внутренние регламенты компании были недостаточны для удаления связанного с выборами контента, помеченного EIP как дезинформация.

From: [REDACTED] <[REDACTED]@google.com>
Date: Tuesday, August 11, 2020 at 4:30 PM
To: [REDACTED] <[REDACTED]@stanford.edu>
Cc: [REDACTED] <[REDACTED]@google.com>, Elena Cryst <[REDACTED]@stanford.edu>, [REDACTED] <[REDACTED]@google.com>, Alex Stamos <[REDACTED]@stanford.edu>, [REDACTED] <[REDACTED]@google.com>, Renee DiResta <[REDACTED]@stanford.edu>, [REDACTED] <[REDACTED]@google.com>, [REDACTED] <[REDACTED]@stanford.edu>
Subject: Re: Stanford Internet Observatory – Election Integrity Partnership

Hi [REDACTED]

In line with my previous comments related to inaccuracies in the draft post and our pending help center update, we'd like to send further information off the record. Are you amenable to receiving some of the new language slotted to go live Thursday (6 am est) on that basis?

Thanks
[REDACTED]

On Tue, Aug 11, 2020 at 12:23 PM [REDACTED] <[REDACTED]@google.com> wrote:

Hi [REDACTED]

We've socialized your draft blog internally and have some feedback and questions to share with you:

- We've identified some gaps and mischaracterizations of our policy. For example, Youtube/Google is listed as having no policy for Participation Interference (and fraud in the original draft), but we have explicit policies on both that have been in place since February. See [current policies](#).
- As mentioned last week (confidentially) we are publishing a help center update on our elections related policies this Thursday. Given that will describe our policies in a user-friendly format, we'd like to consider publishing this piece subsequent to reviewing the updated help center - else this blog will be outdated relative to what's public on our end
- Finally, are you planning to engage the press around this posting? My comms folks have asked whether you could share on your press strategy, if possible

Thanks very much
[REDACTED]

Is it true that the EIP censored 22 million tweets and labeled them as “misinformation”?

No, the EIP did not censor any tweets or label any tweets as “misinformation.” EIP has no ability to remove or label tweets or other posts, and content moderation decisions are independently made by social media platforms. As part of its non-partisan research relating to the 2020 U.S. presidential election, EIP analyzed 22 million tweets that contained keywords or URLs relevant to EIP’s scope of work. EIP identified 2,890 unique tweet URLs in potential violation of Twitter’s stated policies. EIP provided its factual analysis to the relevant platforms, which were then responsible for each platform’s own content moderation decisions. The EIP informed Twitter and other social media platforms when certain social media posts violated each platform’s own policies; **EIP did not make recommendations to the platforms about what actions they should take.**

V. УСИЛИЯ СТЭНФОРДА ПО ПРЕПЯТСТВОВАНИЮ РАССЛЕДОВАНИЮ КОМИТЕТА

A. Обманчивые публичные заявления Стэнфорда о том, что EIP отмечал сообщения на сайте.

17 марта 2023 года, после слушаний в Подкомитете 9 марта по делу «Файлы Твиттера», SIO опубликовала в блоге пост под названием «Справочная информация о проекте SIO по социальным медиа», в котором SIO пыталась преуменьшить масштабы цензуры и слежки в EIP, утверждая, что и EIP, и его преемник, проект Virality, «являются беспартийными исследовательскими коалициями, которые работают открыто, прозрачно и публично». 20 марта юрисконсульт SIO отправил ссылку на запись в блоге сотрудникам комитета, написав: «Вот заявление, которое Стэнфорд опубликовал в пятницу, пытаясь исправить некоторые мифы, распространяемые в прессе».

Помимо лживого изложения деятельности EIP и участия в ней CISA, в посте содержатся заявления, которые категорически не соответствуют действительности. В частности, SIO ложно утверждает, что «EIP информирует Twitter и другие платформы социальных сетей о том, что определенные сообщения в социальных сетях нарушают политику каждой платформы; *EIP не дает платформам рекомендаций о том, какие действия они должны предпринять*».

Документы, предоставленные Комитету и Отдельному подкомитету как SIO, так и другими организациями, содержат многочисленные примеры того, как аналитики и сотрудники EIP давали платформам четкие рекомендации по конкретным мерам принуждения. В Приложении I собраны рекомендации из 75 созданных Стэнфордом тикетов Jira, в которых EIP давала платформам прямые рекомендации о том, какие действия следует предпринять.

Ниже приведено несколько примеров, иллюстрирующих, насколько четко EIP предписывает компаниям, работающим в социальных сетях, действовать:

“Тикет » #	В х о д
EIP-345	«Статьей делятся на Facebook, и хотя она была помечена, когда ею поделились в группе, официальные акции на странице не получили такой пометки... Мы рекомендуем маркировать все случаи распространения статьи на Facebook».
EIP-378	«Это распространилось в протрамповских консервативных группах и под-сообществах... Мы рекомендуем вам отметить как ложные или удалить приведенные ниже сообщения.»
EIP-396	«Привет Facebook, Reddit и Twitter... мы рекомендуем удалить его с ваших платформ».
EIP-407	«Привет команда Twitter - пожалуйста, посмотрите тикет выше, который мы рекомендуем поместить в информацию, относящуюся к голосованию по почте».
EIP-421	«Мы рекомендуем помечать подобные сообщения, если они содержат утверждения о мошенничестве, и принимать дальнейшие меры, если это сообщение действительно свидетельствует о мошенничестве».
EIP-460	«Хакаби не сказал, был ли этот твит шуткой или нет... Мы рекомендуем Twitter пометить сообщение (а) надлежащей информацией о голосовании».
EIP-461	«Учитывая большую аудиторию и статус штата Пенсильвания как поворотного, мы бы рекомендовали принять меры в отношении этого контента».
EIP-581	«Мы рекомендуем вам пометить или уменьшить обнаруживаемость сообщения».

EIP-638	«Мы рекомендуем помечать его [sic] твиты и следить за тем, не ретвититли его какой-нибудь из отмеченных аккаунтов влиятельных лиц».
EIP-656	«@SeanHannity публикует частичное заявление представителя Ильхана Омара... мы рекомендуем Twitter добавить метку к твитам, содержащимссылку на статью».

EIP-668	«Мы повторяем нашу рекомендацию приостановить действие этого аккаунта на время дня выборов, чтобы он не размещал дополнительную вводящую в заблуждение информацию о голосовании».
EIP-673	«Мы рекомендуем удалить этот твит и другие твиты, содержащие эту ложную информацию»; «Мы рекомендуем принять конкретные меры в отношении этого аккаунта, например, приостановить его возможность продолжать твиты в течение 12 часов».
EIP-680	«Мы рекомендуем удалить этот твит, а также твиты с оригинальным видео или пометить их как вводящие в заблуждение».
EIP-1020	«[Мы] рекомендуем пометить или удалять ссылки на его содержание».

В EIP-421 ответственный аналитик EIP, похоже, сделал замечательное признание об истинных намерениях EIP, написав: *«Мы рекомендуем пометить подобные сообщения, если они содержат обвинения в мошенничестве, и что дальнейшие действия могут быть уместны, если это сообщение действительно подтверждает мошенничество».*

В. Первоначальные усилия Стэнфорда по незаконному искажению и сокрытию данных Jira

Несмотря на то, что EIP в своем собственном отчете признала, что система Jira способствовала общению между EIP и федеральным правительством, Стэнфорд изначально отказался предоставить Комитету и Специальному подкомитету архивные данные Jira. Основываясь на заявлениях Стэнфорда и других организаций, осведомленных о практике хранения данных в EIP, Комитет понял, что Стэнфорд был единственной организацией, имеющей доступ к данным «тикетам» Jira. После того как 24 марта 2023 года компания не смогла должным образом выполнить запросы Комитета о предоставлении данных Jira, 12 апреля Комитет выписал повестку в суд. 28 апреля, в день истечения срока, указанного в повестке, Стэнфорд представил набор сообщений с незначительными ответами, но снова не представил «тикеты» Jira.

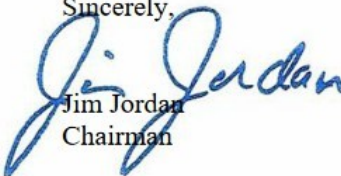
4 мая сотрудники Комитета вновь подняли вопрос о «тикетах» Jira во время телефонного разговора с адвокатом Стэнфорда, который согласился проконсультироваться со своим клиентом относительно характера и хранения «тикетов» Jira. Примечательно, что 15 мая адвокат Стэнфорда подтвердил сотрудникам Комитета в другом телефонном разговоре, что содержание «тикетов» Jira отвечает требованиям повестки Комитета, но Стэнфорд, тем не менее, отказывается их предоставить. По словам адвоката Стэнфорда,

“тикеты» Jira якобы «касаются только исследовательского проекта, проводимого студентами Стэнфорда». В свете очевидного нежелания Стэнфорда полностью выполнить повестку в суд, 1 июня 2023 года Комитет направил в Стэнфорд письмо, в котором говорилось о перспективе принудительного исполнения повестки в суд, срок которой давно истек.

Только после письма председателя SIO в конце концов смирилась и начала предоставлять данные Jira. В общей сложности Комитет получил от SIO пятнадцать документов, в том числе шесть, содержащих данные почти 400 “тикетов» EIP Jira в каждом.

The Committee’s subpoena imposes legal obligations on SIO to comply and produce responsive materials. Thus, your client’s refusal to produce documents responsive to the Committee’s subpoena—four weeks after the subpoena return date—is highly concerning. Accordingly, the Committee expects the SIO will complete its production of responsive documents, in full, by no later than Wednesday, June 14, 2023, at 5:00 p.m. If Stanford fails to comply in full with the subpoena’s demands, the Committee may be forced to consider the use of one or more enforcement mechanisms. Thank you for your client’s attention to this matter.

Sincerely,



Jim Jordan
Chairman

С. Многочисленные документы опровергают показания свидетелей о непричастности CISA к EIP.

Комитет и специальный подкомитет провели расшифрованные интервью с несколькими свидетелями, участвовавшими в EIP, которые утверждали, что CISA практически не участвовала в EIP. Эти показания опровергаются огромным количеством доказательств, полученных Комитетом и Подкомитетом в соответствии с несколькими повестками, выданными организациям, участвовавшим в EIP. Например, Алекс Стамос, глава EIP, утверждал, что роль CISA в EIP ограничивалась представлением EIP в EI-ISAC:

Вопрос: Итак, вы связались с CISA, CISA познакомила вас с EI-ISAC. И мы все еще находимся летом 2020 года, насколько вы помните?

Ответ: Хорошо.

Вопрос: Какую роль играла CISA, если вообще играла?

Ответ: В EIP у них не было официальной роли. У них не было возможности сообщать нам о происходящем напрямую. Мы получали информацию от EI-ISAC. Я не верю, что все, что EI-ISAC присылал нам, исходило от самих сотрудников CISA. Они не участвовали в нашей повседневной работе и анализе. Таким образом, их роль в EIP была очень мала, если вообще была.

Но доктор Кейт Старберд из SIP - и один из основателей EIP - заявила о болееактивном участии CISA. Она заявила:

Вопрос: Насколько вы понимаете, некоторые из внешних партнеров были государственными учреждениями?

Ответ: Насколько я понимаю, есть одно федеральное агентство, а есть и другие организации, которые собирают представителей местных и государственных избирательных органов, которые, как я понимаю, могли бы помочь им, а они могли бы помочь нам выяснить, какова истинная правда о процессах и процедурах выборов. И это было бы важной частью сотрудничества, когда вы пытаетесь бороться с такого рода дезинформацией.

Вопрос: И на какое федеральное агентство вы ссылались?

Ответ: Федеральное агентство, которое... которое вроде как было... является агентством CISA, да. Что касается создания EIP, бывший директор CISA Кребс дал показания, что "EIP" было независимым от CISA, что прямо противоречит документам от лета 2020 года, согласно которым один из членов EIP, писал, что EIP был создан «по просьбе DHS/CISA».

Показания Стамоса и Кребса о степени участия CISA в создании и работе EIP опровергаются огромным количеством доказательств, полученных Комитетом и

Специальным подкомитетом, из которых становится ясно, что CISA не только непосредственно участвовала в создании EIP, но и принимала активное участие в повседневной работе EIP, получая постоянный поток советов и другой информации как от CISA, так и от EIP, финансируемого CISA.

D. Стэнфорд продолжает вводить в заблуждение относительно CISA, EIP и Jira.

Не в силах скрыться, адвокат Стэнфорда в письме Комитету от 14 июня 2023 года сначала признал, что GEC подавала заявки через систему Jira. Однако затем адвокат Стэнфорда заявил, что «кроме этого небольшого количества “тикетов», инициированных GEC, SIO не использовала Jira для получения информации от федеральных правительственных агентств или официальных лиц о [проекте Virality] или проектах EIP, а также для обмена информацией с ними». Адвокат Стэнфорда также утверждал, что «для EIP SIO не предоставляла ни одному правительственному агентству или сотруднику правительственного агентства (федерального, государственного или местного) доступ к базе данных Jira и SIO общалась с помощью Jira только с одним федеральным агентством (Государственным департаментом) по поводу нескольких заявок, инициированных GEC».

The Honorable Jim Jordan
June 14, 2023
Page 4

that Jira data. However, the statement in the Committee's letter that the "government and large social media platforms initiated and received information" from Jira is not accurate.¹¹ Social media companies did not initiate any EIP or VP Jira tickets. Federal government agencies did not initiate any Jira tickets relating to the VP project. The State Department's Global Engagement Center (GEC), which was established by Congress to counter foreign state disinformation and propaganda, initiated a very small number of tickets (fewer than 20) during the EIP 2020 project. These tickets concerned foreign propaganda and disinformation, primarily instigated by Russia. Aside from this small number of GEC-initiated EIP tickets, SIO did not use Jira to receive information from, or share information with, any federal government agencies or officials about the VP or EIP projects. Information from a small number of Jira tickets relating to the EIP project, and from an even smaller number of tickets relating to the VP project, was shared with social media companies. (As stated above, Stanford is producing Jira ticket data that was received from the GEC or exchanged with social media companies.) As Stanford's counsel has explained in several telephone conversations with your staff, the vast majority of Jira tickets were generated by students and supervising researchers, and it is Stanford's understanding that the tickets were never accessed or viewed by individuals or entities other than the researchers and non-governmental institutions participating in EIP and VP.

More specifically, for EIP, SIO did not provide any government agency or employee of a government agency (whether federal, state, or local) access to the Jira database, and SIO only communicated using Jira with a single federal agency (the State Department) regarding the handful of tickets that GEC initiated. As noted above, social media companies did not initiate any Jira tickets. The non-governmental, non-profit Center

From: Elena Cryst <jira@2020partnership.atlassian.net>
Sent: Wednesday, November 4, 2020 5:41 PM
To: ██████████ <██████████@fb.com>
Subject: EIP-833 Case #CIS-MIS000164: inaccurate number of rejected absentee ballots in DeKalb County, GA

Reply above this line.

Elena Cryst shared this with your organization.

View the request and select Get notifications to follow along.

View request<<https://2020partnership.atlassian.net/.../c.../portal/5/EIP-833...>> · Turn off this request's notifications<<https://2020partnership.atlassian.net/.../EIP-833/unsubscribe...>>

This is shared with TikTok, Facebook, EHSAC, Twitter, CIS Misinformation Reporting, and CISA CFITF.

Powered by Jira Service Desk<<https://www.atlassian.com/software.../.../service-desk/powered-by...>>

Эти утверждения неточны. Помимо того, что сотрудники CISA ссылались на коды «EIP-» при переключении, Комитет получил записи переписки, доказывающие, что сотрудники CISA получали информацию из системы Jira или генерировали ее. Например, в приведенном ниже уведомлении по электронной почте, которое было сгенерировано системой Jira, указано, что «тикет» «EIP-833» был «передан... CFITF CISA».



██████████ <██████████@reddit.com>

Re: EIP-651 Livestream of "riots" between Trump and Biden supporters

1 message

Tue, Nov 3, 2020 at 12:36 PM

██████████ <██████████@reddit.com>
to: Alex Stamos <██████████@stanford.edu>

Thanks. Unfortunately as we mentioned at the beginning of this project we are unable to participate in external jiras, but we are happy to receive info over email.

On Tue, Nov 3, 2020 at 12:35 PM Alex Stamos <██████████@stanford.edu> wrote:

There is a widely watched YouTube livestream replaying old videos and claiming they are of live violence in the streets between Biden and Trump supporters. YouTube is looking into it, but here are the Reddit links we found:

https://www.reddit.com/r/Bad_Cop_No_Donut/comments/jfnlw/live_us_election_protests_riots_trump_vs_biden/
https://www.reddit.com/r/ThatsInsane/comments/jfo0a/live_us_election_protests_riots_trump_vs_biden/

It would be great if we could get somebody from Reddit on the JIRA, just like Facebook, Google, Twitter, TikTok, Instagram, CISA, EI-ISAC...

Обмен электронными письмами от 3 ноября 2023 года между Алексом Стамосом и Reddit еще больше указывает на то, что CISA имела определенный доступ к системе Jira. В этом письме Стамос пытался оказать давление на Reddit, чтобы они присоединилась к системе Jira EIP, написав: *«Было бы здорово, если бы мы могли подключить кого-нибудь из Reddit к JIRA, так же как Facebook, Google, Twitter, TikTok, Instagram, CISA, EI-ISAC...»*. Сотрудник Reddit ответил: *«Спасибо. К сожалению, как мы уже говорили в начале проекта, мы не можем участвовать во внешних проектах, связанных с системой JIRA, но мы рады получать информацию по электронной почте»*.

Когда Стамос столкнулся с этим расхождением во время своего интервью, он заявил, что *«вероятно, допустил ошибку, говоря о CISA, потому что EI-ISAC были людьми, имевшими доступ к Jira»* несмотря на то, что он независимо указали CISA, и EI-ISAC в электронном письме.

Данные Jira, предоставленные Комитету и Отдельному подкомитету, содержат ряд тикетов, в которых упоминается «CISA», в том числе в контексте, доказывающем тесную координацию между CISA и EIP. Например, EIP-315 содержит запись следующего содержания: *«EIP - эта информация была размещена в приложении, которое не является основной платформой социальных сетей. CISA изучает, как обрабатывать подобные сообщения»*.

27 июля 2023 года, более чем через месяц после интервью Стамоса, адвокат Стэнфорда в письме Комитету наконец признал, что CISA действительно работала с системой Jira в EIP и что CISA была непосредственно «отмечена» в ряде тикетов. Адвокат Стэнфорда утверждал в письме, что «на момент интервью, г-н Стамос не знал, что CISA или CFITF были «помечены» в каких-либо «тикетах» Jira».

Это особенно сомнительное утверждение, учитывая, что EIP-664, EIP-686, EIP-695 - «тикеты», которые, по признанию SIO, были переданы CISA - были закреплены за Стамосом, согласно данным Jira, предоставленным Комитету и Специальному подкомитету.

¹ Following Alex Stamos's June 23 interview with Committee Staff and the Committee's questions with respect to Stamos Ex. 16, Stanford has reviewed whether any federal government entity other than the Department of State's Global Engagement Center (GEC) initiated or was "tagged" in any Jira tickets. Stanford has since determined that the Cybersecurity and Infrastructure Security Agency (CISA) Countering Foreign Influence Task Force (CFITF) was "tagged" in a small number of Jira tickets. Based on the information currently available to Stanford, it appears that for a short period of time, some EIP researchers utilized this "tag," rather than or in addition to the "EI-ISAC" tag, to flag the Jira tickets potentially needing input or review by the relevant state and local election officials. Stanford has identified 14 Jira tickets with a CISA CFITF "tag," specifically: EIP-236, EIP -239, EIP-243, EIP-563, EIP-570, EIP-616, EIP-664, EIP-686, EIP-695, EIP-713, EIP-743, EIP-810, EIP-833, and EIP-1009. At the time of Mr. Stamos's interview, Mr. Stamos was not aware that CISA or CFITF had been "tagged" in any Jira tickets.

Arnold & Porter Kaye Scholer LLP

601 Massachusetts Ave, NW | Washington, DC 20001-3743 | www.arnoldporter.com

Message

From: [REDACTED] [REDACTED]@google.com]
Sent: 6/3/2021 12:36:17 AM
To: YT Policy Emergency Response Team (yt-pert) [yt-pert@google.com]
CC: [REDACTED] [REDACTED]@google.com]
Subject: Flag from Stanford Virality project – Utah teenager hospitalized for blood clots after vaccine
Attachments: unnamed.png

Hi PERT,

I'm reaching out to share this video that the Stanford Virality Project sent our way: <https://www.youtube.com/watch?v=a9uijTL-Xuw>

It pertains to allegations that a Utah teenager was hospitalized for blood clots after receiving a vaccine injection. While this, in and of itself, does not strike me as likely violating policy, the following quote in the video might:

2:12: "(...) he will never be the same, he'll be on blood thinners for life at best, because of this spike protein carried by a simple coronavirus, it's the spike protein that's the problem, and they put the spike protein in all of these jabs, okay, and they will do damage for a very long time – and I'm not quoting myself, I have 2000 hours of research in this; [hard-to-parse-name] has documented 20 mechanisms of action by which this spike protein will damage and kill humans. Millions of them. This will make Joseph Mengele, of the Hitler administration, roll in his grave wishing he had access to the bioweapon that we're dealing with."

Best,

[REDACTED]

For Public Release

Эпилог

Неудивительно, что Стэнфордский университет попытался отказаться предоставить документы, отвечающие на повестку Комитета: они показывают, что EIP не был беспартийным «школьным проектом», состоящим из студентов и исследователей, заинтересованных в борьбе с дезинформацией в Интернете. Вместо этого, от начала и до конца, операция EIP работала напрямую с федеральным правительством и была непропорционально нацелена на дискурс, ориентированный на консерваторов.

После выборов 2020 года то, что другие называют «промышленным комплексом цензуры», развивалось так, как и ожидалось. После того как президент Трамп уволил директора CISA Криса Кребса в ноябре 2020 года, г-н Кребс создал Krebs Stamos Group вместе с Алексом Стамосом, главой EIP и SIO, в январе 2021 года. Мэтт Мастерсон покинул CISA в конце 2020 года и занял должность научного сотрудника в Стэнфорде, работая с SIO и его проектом Virality Project.

После того как выборы закончились, а американский народ усомнился в целесообразности блокировки и безопасности вакцин COVID-19, EIP воссоздал себя как проект «Virality». Снова сотрудничая с федеральным правительством, SIO запустила проект «Virality» как *«глобальное исследование, направленное на понимание динамики дезинформации, характерной для кризиса COVID-19»*. В проекте «Virality» снова использовались «тикеты» Jira. Хотя Стэнфорд был менее конкретным в своих рекомендациях по цензуре, как это было в модели EIP, платформы социальных сетей все равно послушно удаляли контент, отмеченный Стэнфордом:



Thomas Massie ✓
@RepThomasMassie



Here's a comprehensive study that tracked re-infections and COVID complications for 187,549 people with prior SARS-CoV2 infection.

Conclusion: Effectiveness of immunity due to prior infection is the same as for the Pfizer vaccine.

medrxiv.org/content/10.110...

5:35 PM · May 19, 2021

453 Reposts 35 Quotes 1,373 Likes 64 Bookmarks

Message

From: [REDACTED] [REDACTED]@google.com]
Sent: 6/3/2021 1:43:48 AM
To: [REDACTED] [REDACTED]@google.com]
CC: [REDACTED] [REDACTED]@google.com; YT Policy Emergency Response Team (yt-pert) [yt-pert@google.com]; [REDACTED] [REDACTED]@google.com]
Subject: Re: Flag from Stanford Virality project – Utah teenager hospitalized for blood clots after vaccine

Hi [REDACTED]

Upon review and calibration, we have struck the video for violating our medical misinformation - claims that covid vaccines will kill people who receive them. Please let us know if you have any further questions. Thank you!

Best,
[REDACTED]

Как и EIP, Стэнфордский проект «Virality» продолжал отмечать контент непосредственно на платформах социальных сетей, включая *подлинный* контент выборных должностных лиц, как, например, приведенный ниже твит конгрессмена Томаса Масси. Ссылаясь на этот твит, тикет проекта «Virality» гласил: «Уважаемые команды Facebook и Twitter, обратите внимание на израильскую статью, утверждающую, что иммунитет от Covid-19 эквивалентен иммунитету от прививок, со следующими URL-адресами:», прежде чем отметить твит конгрессмена Масси среди других ссылок Facebook и Twitter.



Thomas Massie 
@RepThomasMassie



If the data show the vaccine is likely to harm young children more than the virus is likely to harm young children, giving children the vaccine as a sacrifice to save older adults is immoral and reprehensible.



Albert Bourla  @AlbertBourla · Jun 8, 2021

Although data shows that severe #COVID19 is rare in children, widespread vaccination is a critical tool to help stop transmission. That's why I'm excited we have begun dosing participants aged 5 to 11 in a global Phase 2/3 study of the Pfizer-BioNTech #COVID19 vaccine.

12:05 PM · Jun 12, 2021

Проект «Virality» позже отметил и этот твит конгрессмена Масси.

После инаугурации президента Байдена в январе 2021 года режим цензуры со стороны правительства усилился. В CISA команда CFITF отказалась от претензий на «иностранную» направленность и переименовала себя в «команду MDM», которая будет заниматься иностранными и отечественными высказываниями, которые правительство сочтет дезинформацией или вредоносной информацией. В течение 2021 года Белый дом Байдена проводил кампанию давления на Facebook и другие представители социальных сетей с целью заставить их цензурировать антивакцинальный контент, даже если он был правдивым. В 2022 году CISA пригласило доктора Старберда, тогдашнего руководителя Twitter Виджая Гадде и других создать консультативный подкомитет по MDM, чтобы проконсультироваться с CISA о том, как агентство может и должно бороться с высказываниями американцев, которые правительство считает неправильной, недостоверной или вредоносной информацией. SHS создало, а затем расформировало после возмущения общественности недолговечный Совет по управлению дезинформацией.

Но к 2023 году, когда республиканцы вновь получили большинство в Палате представителей и начали осуществлять надзор за цензурно-промышленным комплексом, CISA очистила свой сайт от ссылок на внутреннюю цензуру. Комитет и специальный подкомитет получили и раскрыли информацию о том, как Facebook изменила свою политику из-за давления со стороны администрации Байдена. Внутренние документы Facebook показали, что Белый дом Байдена, в частности, хотел, чтобы правдивая информация и сатира подвергались цензуре со скоростью, которую даже Big Tech считает неприемлемой. По результатам работы Комитета и специального подкомитета, даже основные средства массовой информации больше не могли игнорировать эти нарушения Конституции. Истцы по делу «*Миссури против Байдена*» одержали победу в федеральном окружном суде и Апелляционном суде США по Пятому округу, а теперь их дело будет рассмотрено в Верховном суде. Публичные сообщения показывают, что университеты пересматривают свое мнение о том, стоит ли разрешать своим профессорам получать финансирование и заниматься цензурой.

Но работа еще не закончена. Расследование Комитета и специального подкомитета продолжается. Чтобы лучше обосновать законодательные усилия по прекращению государственной цензуры и защите прав американцев, гарантированных Первой поправкой, Комитет и Подкомитет продолжают расследование масштабов взаимодействия CISA и других ведомств исполнительной власти с платформами социальных сетей и третьими сторонами, в том числе с теми, которые используются для облегчения цензуры по доверенности.

ПРИЛОЖЕНИЕ I

Судебный комитет Палаты представителей и его специальный подкомитет по вооружению федерального правительства получили от Стэнфордского университета документы и информацию в соответствии с повесткой, из которых следует, что аналитики и сотрудники EIP давали четкие рекомендации платформам социальных сетей по принятию конкретных мер принуждения по меньшей мере в 75 случаях в течение четырех месяцев в преддверии и во время выборов 2020 года. В этом приложении собраны эти 75 рекомендаций в порядке возрастания номера тикета EIP Jira. Весь тикет Jira, включая комментарии социальных медиаплатформ, можно найти по перекрестным ссылкам на архивные данные тикетов Jira, представленные в Приложении II.

Тикет #	Сообщения
EIP-166	«Здравствуйте, Google... Мы рекомендуем удалить это объявление».
EIP-279	«Мы рекомендуем Twitter пометить или удалить этот твит».
EIP-307	«Мы рекомендуем следующим платформам предпринять следующие действия: *Twitter* - отключить аккаунт».
EIP-321	«Рекомендуемые действия: запретить обмен ссылками на следующие сайты:»
EIP-329	«Мы сообщаем о двух случаях предвыборной дезинформации, представляющей собой вмешательство в участие и делегитимацию. Мы отмечаем пост и аккаунт в Twitter и рекомендуем следующее:»
EIP-330	«Мы рекомендуем Twitter и Facebook удалить эти сообщения. Если вы не можете удалить эти сообщения, мы предлагаем пометить их как вводящие в заблуждение».
EIP-345	«Статьей делятся на Facebook, и хотя она была помечена, когда ею поделились в группе, официальные акции на странице не получили такой пометки... Мы рекомендуем маркировать все случаи распространения статьи на Facebook».
EIP-348	«Рекомендую наклеить ярлык».
EIP-378	«Это распространилось в протрамповских консервативных группах и под-сообществах... Мы рекомендуем вам отметить как ложные или удалить приведенные ниже сообщения.»

EIP-389	«Мы также рекомендуем расширить правоприменительную практику в отношении дезинформации о выборах, содержащейся на неанглийских языках».
EIP-396	«Привет Facebook, Reddit и Twitter... мы рекомендуем удалить его с ваших платформ».

EIP-397	«Привет, Facebook, вот два сообщения, утверждающие о проблемах с машинами для голосования, мы рекомендуем их заклеить:».
EIP-402	«Twitter и Reddit, мы передаем вам полные ссылки, которые мы нашли, для наглядности, и рекомендуем вам пометить их информацией о голосовании».
EIP-407	«Привет команда Twitter - пожалуйста, посмотрите тикет выше, который мы рекомендуем поместить в информацию, относящуюся к голосованию по почте».
EIP-417	«В этом видео утверждается, что оно демонстрирует доказательства мошенничества с избирателями в Мэриленде, однако на самом видео (кадры с работником избирательной комиссии) не видно ничего, что мы могли бы интерпретировать как мошенничество с избирателями. Мы рекомендуем удалить это видео или наклеить на него ярлык».
EIP-421	«Мы рекомендуем пометить подобные сообщения, если они содержат утверждения о мошенничестве, и принимать дальнейшие меры, если это сообщение действительно свидетельствует о мошенничестве».
EIP-450	«Как минимум, мы рекомендуем наклеить на столбы ярлыки, разъясняющие, что голосование по почте безопасно».
EIP-451	«Мы рекомендуем предпринять те же действия с новым объявлением».

EIP-455	«+*Платформенные рекомендации*+ +*Twitter*+», где повествованиеполучает наибольшее количество взаимодействий, отметить видео и хэштег и продолжить мониторинг на предмет возможные версии наблюдения за опросом и подстрекательства».
EIP-460	«Хакаби не сказал, был ли этот твит шуткой или нет... Мы рекомендуемTwitter пометить сообщение (а) надлежащей информацией о голосовании».

EIP-461	«Привет команда Twitter - ряд высокопоставленных лиц, включая президента, выдвигают обвинения в фальсификации результатов голосования. . . Учитывая большую аудиторию и статус Пенсильвании как поворотного штата, мы бы рекомендовали принять меры в отношении этого контента».
EIP-479	«Мы рекомендуем наносить соответствующую маркировку».
EIP-483	«Мы рекомендуем twitter удалить твит, так как это довольно явнонарушение».
EIP-489	«Мы рекомендуем Twitter удалить эти твиты».
EIP-503	«Мы рекомендуем удалить следующие твиты как вводящие в заблуждение».
EIP-511	Мы рекомендуем маркировать этот контент и отслеживать ключевые слова на китайском языке, такие как «фальсификация выборов» и «QAnon», для принятия мер в отношении будущего контента».

EIP-512	«Мы рекомендуем Twitter удалить этот твит»; «Мы рекомендуем удалить эти твиты»; «Я рекомендую Twitter и Facebook удалить эти сообщения или добавить ярлык».
EIP-537	«Здравствуйте команды Youtube и Facebook: Мы добавляем вас в этот тикет, так как видеоролики, о которых идет речь, содержат несколько вводящих в заблуждение утверждений о бюллетенях, отправленных по почте, а также о голосовании лично. Мы рекомендуем применить к этим постам специальный ярлык».
EIP-559	«Мы рекомендуем удалить или заклеить этот твит»; «Поскольку это явно ложная информация о выборах, мы рекомендуем удалить ее с помощью Twitter».
EIP-575	«Мы рекомендуем Twitter принять меры в отношении этого аккаунта за делегитимацию выборов».

EIP-581	«Мы рекомендуем вам пометить или уменьшить обнаруживаемость сообщения».
EIP-585	«Мы рекомендуем удалить связанный твит.»; «Рекомендуем также удалить связанные твиты с цитатами».

EIP-589	«Поскольку это ложное утверждение, подрывающее доверие кизбирательному процессу, мы рекомендуем удалить его».
EIP-608	«Рекомендую наклеить ярлык».
EIP-614	«Мы рекомендуем, по крайней мере, наклеить ярлык, поскольку этоопрровергнутое заявление о преступлении на выборах».
EIP-615	«Мы рекомендуем удалить эти сообщения и сообщим вам о новых».
EIP-638	«Мы рекомендуем помечать его [sic] твиты и следить за тем, не ретвититли его какой-нибудь из отмеченных аккаунтов влиятельных лиц».
EIP-639	«Мы рекомендуем удалить или пометить эти твиты».
EIP-656	«@SeanHannity публикует частичное заявление представителя Ильхана Омара... мы рекомендуем Twitter добавить метку к твитам, содержащимссылку на статью».
EIP-664	«Twitter, рекомендуем удалить:».
EIP-668	«Мы повторяем нашу рекомендацию приостановить действие этого аккаунта на время дня выборов, чтобы он не размещал дополнительнуювводящую в заблуждение информацию о голосовании».

EIP-673	«Мы рекомендуем удалить этот твит и другие твиты, содержащие эту ложную информацию»; «Мы рекомендуем принять конкретные меры вотношении этого аккаунта, например, приостановить его возможностьпродолжать писать твиты в течение 12 часов».
EIP-680	«Мы рекомендуем удалить этот твит, а также твиты с оригинальнымвидео или пометить их как вводящие в заблуждение».
EIP-698	«Рекомендую удалить для некоторых, наклеить ярлык для других твитов».

EIP-705	«Мы рекомендуем удалить этот твит или отметить его за вводящее заблуждение содержание».
EIP-706	«Поскольку в счетах содержатся необоснованные утверждения, подрывающие доверие к избирательному процессу, мы рекомендуем принять меры». 100

EIP-715	«Этот аккаунт в приведенном выше твите пытается делегитимизировать процесс голосования без доказательств. Мы рекомендуем принять меры».
EIP-746	«Мы рекомендуем удалить это содержимое».
EIP-767	«Мы рекомендуем Twitter удалить эти сообщения».
EIP-779	«Мы рекомендуем удалять сообщения, содержащие ссылки на эту историю, и сообщения, содержащие скриншоты этой истории. Если их невозможно удалить, следует добавить баннер, объясняющий, что они являются ложным или вводящим в заблуждение контентом».
EIP-780	«Мы знаем, что вы в курсе акции #stopthesteal, но мы собрали здесь некоторые из основных факторов, способствующих этому... Мы рекомендуем принять меры в кратчайшие сроки».
EIP-789	«Эти сообщения быстро растут, и мы рекомендуем их удалить, потому что они подрывают веру людей в легитимность результатов выборов».
EIP-790	Они делятся этим видео, чтобы предположить, что Байден участвует в подтасовке голосов, но это вводит в заблуждение...». Facebook разместил предупреждающий баннер на подобных сообщениях (см. ссылку и мы предлагаем Twitter либо удалить эти сообщения, либо сделать то же самое».
EIP-795	«Мы рекомендуем немедленно удалить эти сообщения».
EIP-798	«Мы рекомендуем удалить этот твит или, по крайней мере, закрыть его баннером с вводящим в заблуждение/спорным содержанием. Он ложно подрывает веру людей в легитимность результатов выборов».
EIP-811	«Пользователи Twitter и Facebook делятся манипулированными изображениями людей, перевозящих коробки в грузовиках с надписью «Чрезвычайные голоса демократов». Мы предлагаем пометить или удалить твиты, в которых используется эта фотография, поскольку она может подрывать веру людей в легитимность избирательного

	процесса».
--	------------

EIP-817	«Поскольку это бездоказательное утверждение подрывает доверие квыборам, мы рекомендуем принять меры».
EIP-847	«Мы рекомендуем наклеить ярлык (как уже было сделано) или удалить этитвиты».

EIP-853	«Рекомендуем наклеить или удалить:».
EIP-867	«Мы рекомендуем пометить эти заявления как необоснованные».
EIP-868	«Мы настоятельно рекомендуем платформам принять меры в отношении этого контента и любого другого контента с таким скриншотом. Эти сообщения должны быть удалены или помечены соответствующим образом».
EIP-869	«Мы рекомендуем как минимум наклеить ярлык, поскольку этоопрровергнутое заявление о преступлении на выборах».
EIP-879	«Мы рекомендуем удалить или пометить этот контент».
EIP-890	«Мы рекомендуем отмечать (или удалять) сообщения, в которыхсодержатся такие утверждения:».
EIP-909	«Мы рекомендуем удалить».
EIP-920	«Рекомендуем ограничить распространение прикрепленных твитов».

EIP-949	«Мы завершили анализ приложенной статьи Breitbart и рекомендуем пометить или удалять любые ссылки на нее в соответствии с политикой.»; «рекомендуем применять тот же ярлык к другим/новым случаям повествования».
EIP-952	«Мы рекомендуем принять меры по проверке фактов».
EIP-969	«Facebook: пожалуйста, посмотрите эту вводящую в заблуждение историю в Instagram... Рекомендуем наклеить ярлык или предпринять другие действия, так как она уже попала в Twitter».
EIP-970	«Facebook и Twitter: эта история от предполагаемого «разоблачителя» из Невады, утверждающего о нарушениях в ходе голосования, не была проверена или обоснована. Она получила значительное вирусное распространение. Мы рекомендуем пометить эти ссылки».
EIP-987	«Мы работаем над решением проблемы, но рекомендуем Twitter/Facebook удалить (или хотя бы пометить) эти видео».
EIP-989	«Мы рекомендуем удалить его как нарушающий условия предоставления услуг».
EIP-996	«Мы рекомендуем удалить или пометить этот контент соответствующим образом».
EIP-998	«Мы рекомендуем отметить их для маркировки или удаления».
EIP-1020	«Мы рекомендуем пометить или удалять ссылки на его содержание».