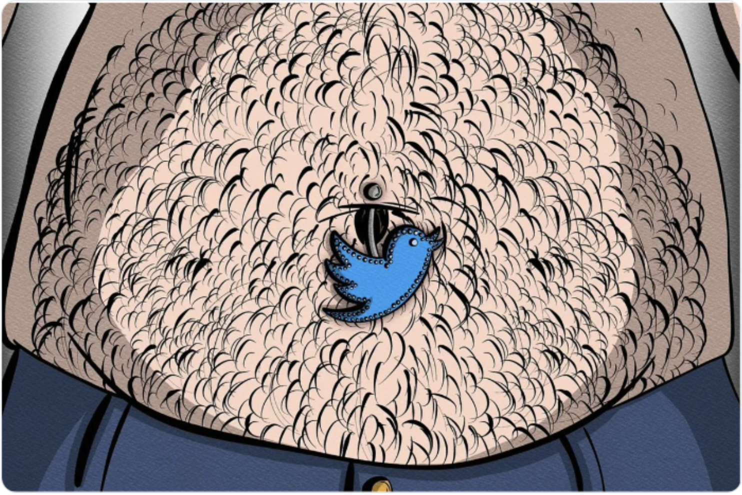
THREAD BY MATT TAIBII

‹ TWITTER FILES ›

#13 TWITTER AND THE FBI "BELLY BUTTON"

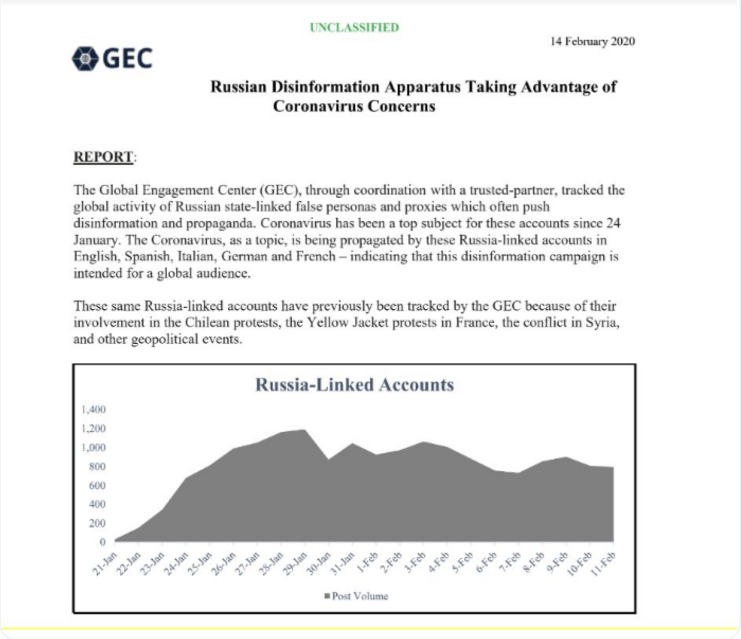
@UNGATHEGREAT

1.THREAD: The Twitter Files
Twitter and the FBI "Belly Button"



2.By 2020, Twitter was struggling with the problem of public and private agencies bypassing them and going straight to the media with lists of suspect accounts.

3.In February, 2020, as COVID broke out, the Global Engagement Center – a fledgling analytic/intelligence arms of the State Department – went to the media with a report called, "Russian Disinformation Apparatus Taking Advantage of Coronavirus Concerns."



UNCLASSIFIED

GEC

14 February 2020

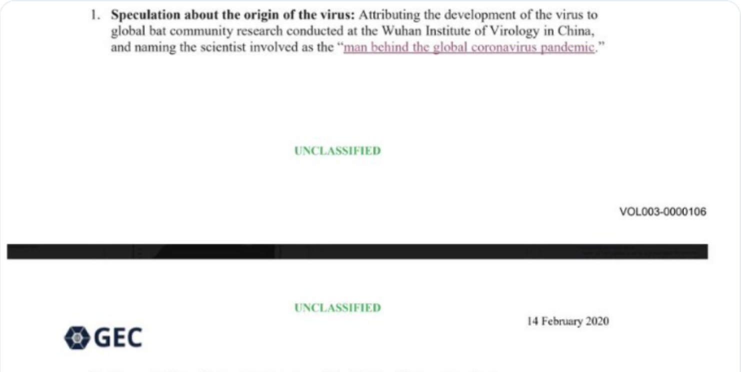
Russian Disinformation Apparatus Taking Advantage of Coronavirus Concerns

REPORT:

The Global Engagement Center (GEC), through coordination with a trusted-partner, tracked the global activity of Russian state-linked false personas and proxies which often push disinformation and propaganda. Coronavirus has been a top subject for these accounts since 24 January. The Coronavirus, as a topic, is being propagated by these Russia-linked accounts in English, Spanish, Italian, German and French – indicating that this disinformation campaign is intended for a global audience.

These same Russia-linked accounts have previously been tracked by the GEC because of their involvement in the Chilean protests, the Yellow Jacket protests in France, the conflict in Syria, and other geopolitical events.

4.The GEC flagged accounts as “Russian personas and proxies” based on criteria like, “Describing the Coronavirus as an engineered bioweapon,” blaming “research conducted at the Wuhan institute,” and “attributing the appearance of the virus to the CIA.”



1. **Speculation about the origin of the virus:** Attributing the development of the virus to global bat community research conducted at the Wuhan Institute of Virology in China, and naming the scientist involved as the “man behind the global coronavirus pandemic.”

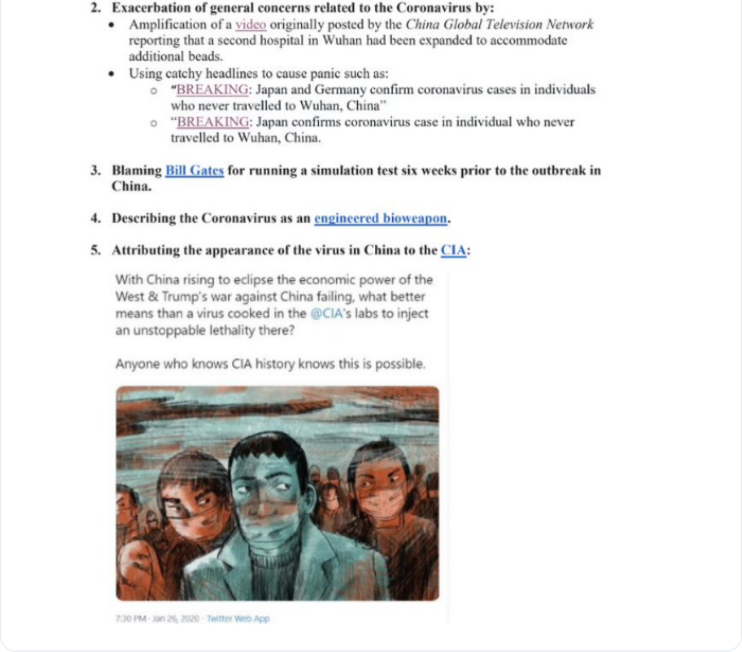
UNCLASSIFIED

VOL003-0000106

UNCLASSIFIED

GEC

14 February 2020



2. **Exacerbation of general concerns related to the Coronavirus by:**
   - Amplification of a video originally posted by the *China Global Television Network* reporting that a second hospital in Wuhan had been expanded to accommodate additional beads.
   - Using catchy headlines to cause panic such as:
     - "BREAKING: Japan and Germany confirm coronavirus cases in individuals who never travelled to Wuhan, China"
     - "BREAKING: Japan confirms coronavirus case in individual who never travelled to Wuhan, China.

3. **Blaming Bill Gates for running a simulation test six weeks prior to the outbreak in China.**

4. **Describing the Coronavirus as an engineered bioweapon.**

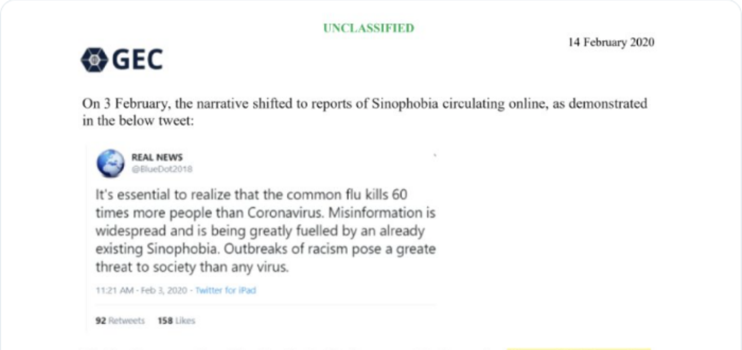
5. **Attributing the appearance of the virus in China to the CIA:**

With China rising to eclipse the economic power of the West & Trump's war against China failing, what better means than a virus cooked in the @CIA's labs to inject an unstoppable lethality there?

Anyone who knows CIA history knows this is possible.

7:30 PM · Jan 26, 2020 · Twitter Web App

5.State also flagged accounts that retweeted news that Twitter banned the popular U.S. ZeroHedge, claiming the episode "led to another flurry of disinformation narratives." ZH had done reports speculating that the virus had lab origin.



UNCLASSIFIED

GEC

14 February 2020

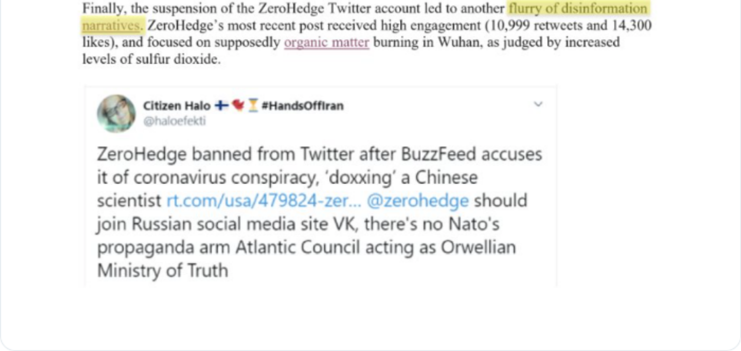
On 3 February, the narrative shifted to reports of Sinophobia circulating online, as demonstrated in the below tweet:

REAL NEWS
@BlueDot2018

It's essential to realize that the common flu kills 60 times more people than Coronavirus. Misinformation is widespread and is being greatly fuelled by an already existing Sinophobia. Outbreaks of racism pose a greate threat to society than any virus.

11:21 AM · Feb 3, 2020 · Twitter for iPad

92 Retweets **158** Likes

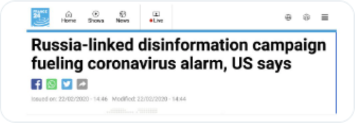


Finally, the suspension of the ZeroHedge Twitter account led to another flurry of disinformation narratives. ZeroHedge's most recent post received high engagement (10,999 retweets and 14,300 likes), and focused on supposedly organic matter burning in Wuhan, as judged by increased levels of sulfur dioxide.

Citizen Halo 🇫🇮 ❤ ⏳ #HandsOffIran
@haloefekti

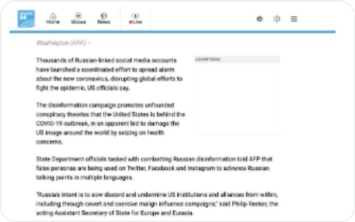
ZeroHedge banned from Twitter after BuzzFeed accuses it of coronavirus conspiracy, 'doxxing' a Chinese scientist rt.com/usa/479824-zer... @zerohedge should join Russian social media site VK, there's no Nato's propaganda arm Atlantic Council acting as Orwellian Ministry of Truth

6.The GEC still led directly to news stories like the AFP's headline, "Russia-linked disinformation campaign led to coronavirus alarm, US says," and a Politico story about how "Russian, Chinese, Iranian Disinformation Narratives Echo One Another."



Russia-linked disinformation campaign fueling coronavirus alarm, US says

Issued on: 22/02/2020 - 14:46 Modified: 22/02/2020 - 14:44



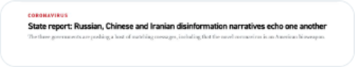
Washington (AFP) –

Thousands of Russian-linked social media accounts have launched a coordinated effort to spread alarm about the new coronavirus, disrupting global efforts to fight the epidemic, US officials say.

The disinformation campaign promotes unfounded conspiracy theories that the United States is behind the COVID-19 outbreak, in an apparent bid to damage the US image around the world by seizing on health concerns.

State Department officials tasked with combatting Russian disinformation told AFP that false personas are being used on Twitter, Facebook and Instagram to advance Russian talking points in multiple languages.

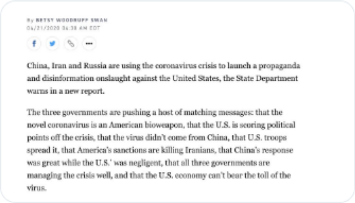
"Russia's intent is to sow discord and undermine US institutions and alliances from within, including through covert and coercive malign influence campaigns," said Philip Reeker, the acting Assistant Secretary of State for Europe and Eurasia.



CORONAVIRUS

State report: Russian, Chinese and Iranian disinformation narratives echo one another

The three governments are pushing a host of matching messages, including that the novel coronavirus is an American bioweapon.

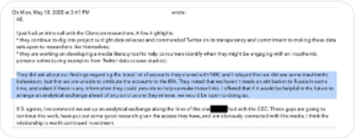


By BETSY WOODRUFF SWAN
04/21/2020 04:38 AM EDT

China, Iran and Russia are using the coronavirus crisis to launch a propaganda and disinformation onslaught against the United States, the State Department warns in a new report.

The three governments are pushing a host of matching messages: that the novel coronavirus is an American bioweapon, that the U.S. is scoring political points off the crisis, that the virus didn't come from China, that U.S. troops spread it, that America's sanctions are killing Iranians, that China's response was great while the U.S.' was negligent, that all three governments are managing the crisis well, and that the U.S. economy can't bear the toll of the virus.

7."YOU HAVEN'T MADE A RUSSIA ATTRIBUTION IN SOME TIME" When Clemson's Media Forensics Hub complained Twitter hadn't "made a Russia attribution" in some time, Trust and Safety chief Yoel Roth said it was "revelatory of their motives."



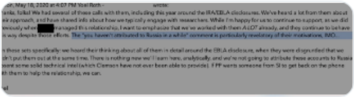
On Mon, May 18, 2020 at 3:41 PM wrote:

All,

I just had an intro call with the Clemson researchers. A few highlights:
* they continue to dig into project sunlight data releases and commended Twitter on its transparency and commitment to making these data sets open to researchers like themselves;
* they are working on developing a media literacy tool to help consumers identify when they might be engaging with an inauthentic persona online (using examples from Twitter data as case studies).

They did ask about our findings regarding the latest list of accounts they shared with NBC and I relayed that we did see some inauthentic behaviour, but that we are unable to attribute the accounts to the IRA. They noted that we haven't made an attribution to Russia in some time, and asked if there is any information they could provide to help us make those links. I offered that if it would be helpful in the future to arrange an analytical exchange ahead of any conclusions they release, we would be open to doing so.

If SI agrees, I recommend we set up an analytical exchange along the lines of the one [redacted] had with the GEC. These guys are going to continue this work, have put out some good research given the access they have, and are obviously connected with the media. I think the relationship is worth continued investment.

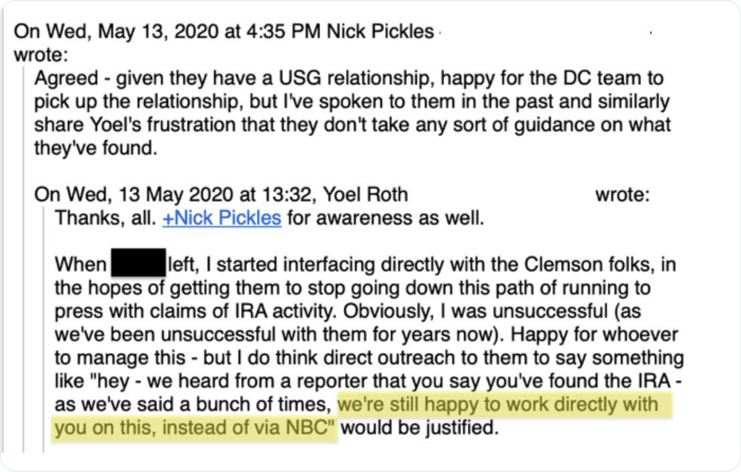


on, May 18, 2020 at 4:07 PM Yoel Roth - wrote:
anks, folks! We had several of these calls with them, including this year around the IRA/EBLA disclosures. We've heard a lot from them about eir approach, and have shared info about how we typically engage with researchers. While I'm happy for us to continue to support, as we did eviously when [redacted] managed this relationship, I want to emphasize that we've worked with them A LOT already, and they continue to behave is way despite those efforts. The "you haven't attributed to Russia in a while" comment is particularly revelatory of their motivations, IMO.

n these sets specifically: we heard their thinking about all of them in detail around the EBLA disclosure, when they were disgruntled that we dn't put them out at the same time. There is nothing new we'll learn here, analytically, and we're not going to attribute these accounts to Russia sent some solid technical intel (which Clemson have not ever been able to provide). If PP wants someone from SI to get back on the phone th them to help the relationship, we can.

el

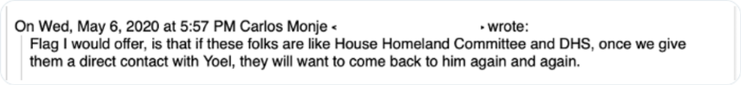
8.“WE’RE HAPPY TO WORK DIRECTLY WITH YOU ON THIS, INSTEAD OF NBC.” Roth tried in vain to convince outsider researchers like the Clemson lab to check with them before pushing stories about foreign interference to media.



On Wed, May 13, 2020 at 4:35 PM Nick Pickles wrote:

> Agreed - given they have a USG relationship, happy for the DC team to pick up the relationship, but I've spoken to them in the past and similarly share Yoel's frustration that they don't take any sort of guidance on what they've found.
>
> On Wed, 13 May 2020 at 13:32, Yoel Roth wrote:
>
> > Thanks, all. +Nick Pickles for awareness as well.
> >
> > When [redacted] left, I started interfacing directly with the Clemson folks, in the hopes of getting them to stop going down this path of running to press with claims of IRA activity. Obviously, I was unsuccessful (as we've been unsuccessful with them for years now). Happy for whoever to manage this - but I do think direct outreach to them to say something like "hey - we heard from a reporter that you say you've found the IRA - as we've said a bunch of times, we're still happy to work directly with you on this, instead of via NBC" would be justified.

9.Twitter was also trying to reduce the number of agencies with access to Roth. “If these folks are like House Homeland Committee and DHS, once we give them a direct contact with Yoel, they will want to come back to him again and again,” said policy director Carlos Monje.

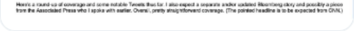


On Wed, May 6, 2020 at 5:57 PM Carlos Monje < • wrote:

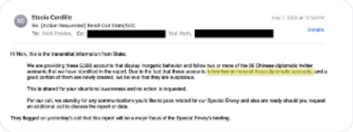
> Flag I would offer, is that if these folks are like House Homeland Committee and DHS, once we give them a direct contact with Yoel, they will want to come back to him again and again.

10.When the State Department/GEC – remember this was 2020, during the Trump administration – wanted to publicize a list of 5,500 accounts it claimed would “amplify Chinese propaganda and disinformation” about COVID, Twitter analysts were beside themselves.

11.The GEC report appeared based on DHS data circulated earlier that week, and included accounts that followed “two or more” Chinese diplomatic accounts. They reportedly ended up with a list “nearly 250,000” names long, and included Canadian officials and a CNN account:



Here's a round-up of coverage and some notable Tweets thus far. I also expect a separate and/or updated Bloomberg story and possibly a piece from the Associated Press who I spoke with earlier. Overall, pretty straightforward coverage. (The pointed headline is to be expected from CNN.)



Stacia Cardille
Re: [Action Requested] Read-Out State/GEC
To: Nick Pickles, Cc: [redacted] Yoel Roth, [redacted]

May 7, 2020 at 12:54 PM

Hi Nick, this is the transmittal information from State:

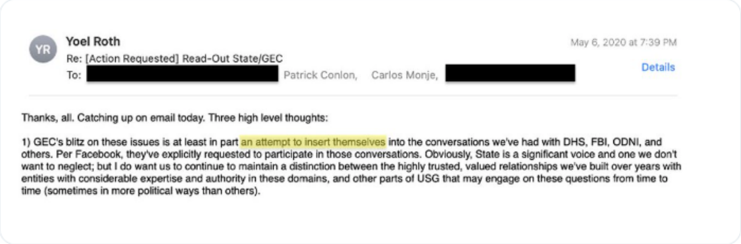
We are providing these 5,500 accounts that display inorganic behavior and follow two or more of the 56 Chinese diplomatic twitter accounts that we have identified in the report. Due to the fact that these accounts follow two or more of those diplomatic accounts, and a good portion of them are newly created, we believe that they are suspicious.

This is shared for your situational awareness and no action is requested.

Per our call, we standby for any communications you'd like to pass related for our Special Envoy and also are ready should you request an additional call to discuss the report or data.

They flagged on yesterday's call that this report will be a major focus of the Special Envoy's briefing.

12.Roth saw GEC's move as an attempt by the GEC to use intel from other agencies to "insert themselves" into the content moderation club that included Twitter, Facebook, the FBI, DHS, and others:



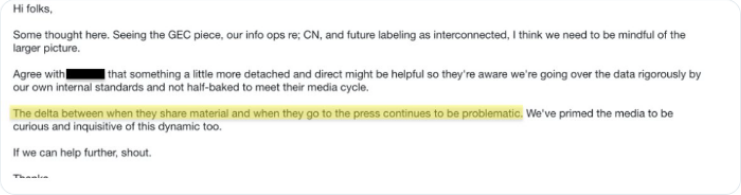
Yoel Roth
Re: [Action Requested] Read-Out State/GEC
To: [redacted] Patrick Conlon, Carlos Monje, [redacted]

May 6, 2020 at 7:39 PM

Thanks, all. Catching up on email today. Three high level thoughts:

1) GEC's blitz on these issues is at least in part an attempt to insert themselves into the conversations we've had with DHS, FBI, ODNI, and others. Per Facebook, they've explicitly requested to participate in those conversations. Obviously, State is a significant voice and one we don't want to neglect; but I do want us to continue to maintain a distinction between the highly trusted, valued relationships we've built over years with entities with considerable expertise and authority in these domains, and other parts of USG that may engage on these questions from time to time (sometimes in more political ways than others).

13.The GEC was soon agreeing to loop in Twitter before going public, but they were using a technique that had boxed in Twitter before. "The delta between when they share material and when they go to the press continues to be problematic," wrote one comms official.



Hi folks,

Some thought here. Seeing the GEC piece, our info ops re; CN, and future labeling as interconnected, I think we need to be mindful of the larger picture.

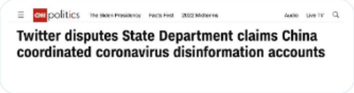
Agree with [redacted] that something a little more detached and direct might be helpful so they're aware we're going over the data rigorously by our own internal standards and not half-baked to meet their media cycle.

The delta between when they share material and when they go to the press continues to be problematic. We've primed the media to be curious and inquisitive of this dynamic too.

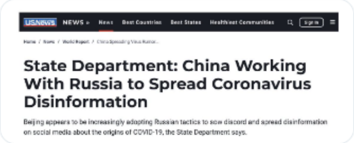
If we can help further, shout.

Thanks

14.The episode led to a rare public disagreement between Twitter and state officials:



Twitter disputes State Department claims China coordinated coronavirus disinformation accounts

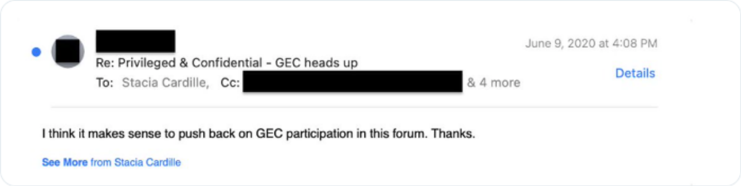


State Department: China Working With Russia to Spread Coronavirus Disinformation

Beijing appears to be increasingly adopting Russian tactics to sow discord and spread disinformation on social media about the origins of COVID-19, the State Department says.

15."IT MAKES SENSE TO PUSH BACK ON GEC PARTICIPATION IN THIS FORUM"

When the FBI informed Twitter the GEC wanted to be included in the regular “industry call” between companies like Twitter and Facebook and the DHS and FBI, Twitter leaders balked at first.



[redacted]

[redacted]

Re: Privileged & Confidential - GEC heads up

To: Stacia Cardille, Cc: [redacted] & 4 more

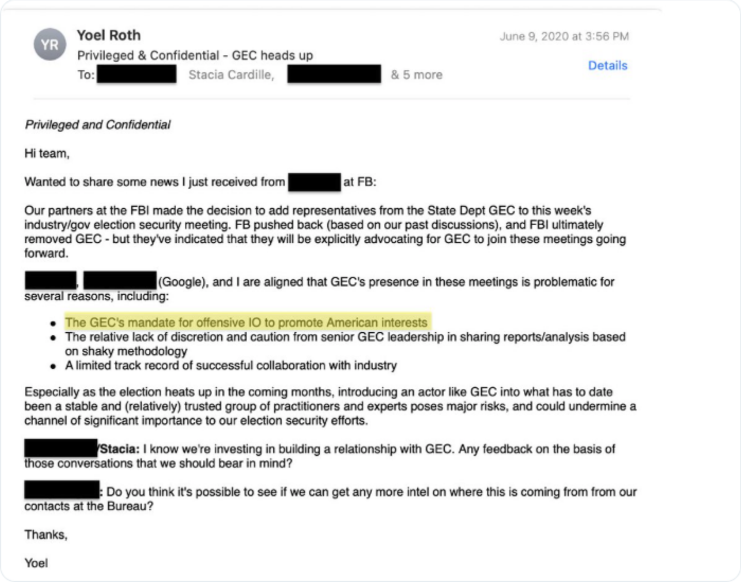
June 9, 2020 at 4:08 PM

Details

I think it makes sense to push back on GEC participation in this forum. Thanks.

See More from Stacia Cardille

16.Facebook, Google, and Twitter executives were united in opposition to GEC’s inclusion, with ostensible reasons including, “The GEC’s mandate for offensive IO to promote American interests.”



YR

Yoel Roth

Privileged & Confidential - GEC heads up

To: [redacted] Stacia Cardille, [redacted] & 5 more

June 9, 2020 at 3:56 PM

Details

Privileged and Confidential

Hi team,

Wanted to share some news I just received from [redacted] at FB:

Our partners at the FBI made the decision to add representatives from the State Dept GEC to this week's industry/gov election security meeting. FB pushed back (based on our past discussions), and FBI ultimately removed GEC - but they've indicated that they will be explicitly advocating for GEC to join these meetings going forward.

[redacted], [redacted] (Google), and I are aligned that GEC's presence in these meetings is problematic for several reasons, including:

- The GEC's mandate for offensive IO to promote American interests
- The relative lack of discretion and caution from senior GEC leadership in sharing reports/analysis based on shaky methodology
- A limited track record of successful collaboration with industry

Especially as the election heats up in the coming months, introducing an actor like GEC into what has to date been a stable and (relatively) trusted group of practitioners and experts poses major risks, and could undermine a channel of significant importance to our election security efforts.

[redacted]**/Stacia:** I know we're investing in building a relationship with GEC. Any feedback on the basis of those conversations that we should bear in mind?

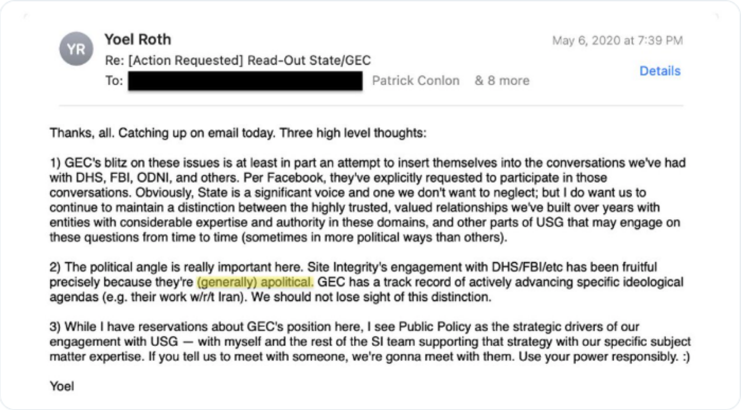
[redacted]: Do you think it's possible to see if we can get any more intel on where this is coming from from our contacts at the Bureau?

Thanks,

Yoel

17.A deeper reason was a perception that unlike the DHS and FBI, which were “apolitical,” as Roth put it, the GEC was “political,” which in Twitter-ese appeared to be partisan code.

“I think they thought the FBI was less Trumpy,” is how one former DOD official put it.



Yoel Roth
May 6, 2020 at 7:39 PM
Re: [Action Requested] Read-Out State/GEC
To: [redacted] Patrick Conlon & 8 more

Thanks, all. Catching up on email today. Three high level thoughts:

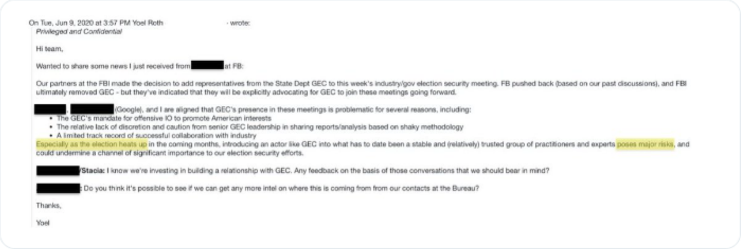
1) GEC's blitz on these issues is at least in part an attempt to insert themselves into the conversations we've had with DHS, FBI, ODNI, and others. Per Facebook, they've explicitly requested to participate in those conversations. Obviously, State is a significant voice and one we don't want to neglect; but I do want us to continue to maintain a distinction between the highly trusted, valued relationships we've built over years with entities with considerable expertise and authority in these domains, and other parts of USG that may engage on these questions from time to time (sometimes in more political ways than others).

2) The political angle is really important here. Site Integrity's engagement with DHS/FBI/etc has been fruitful precisely because they're (generally) apolitical. GEC has a track record of actively advancing specific ideological agendas (e.g. their work w/r/t Iran). We should not lose sight of this distinction.

3) While I have reservations about GEC's position here, I see Public Policy as the strategic drivers of our engagement with USG — with myself and the rest of the SI team supporting that strategy with our specific subject matter expertise. If you tell us to meet with someone, we're gonna meet with them. Use your power responsibly. :)

Yoel

18.After spending years rolling over for Democratic Party requests for “action” on “Russia-linked” accounts, Twitter was suddenly playing tough. Why? Because, as Roth put it, it would pose “major risks” to bring the GEC in, “especially as the election heats up.”



On Tue, Jun 9, 2020 at 3:57 PM Yoel Roth - wrote:

Privileged and Confidential

Hi team,

Wanted to share some news I just received from [redacted] at FB:

Our partners at the FBI made the decision to add representatives from the State Dept GEC to this week's industry/gov election security meeting. FB pushed back (based on our past discussions), and FBI ultimately removed GEC - but they've indicated that they will be explicitly advocating for GEC to join these meetings going forward.

[redacted], [redacted] (Google), and I are aligned that GEC's presence in these meetings is problematic for several reasons, including:

- The GEC's mandate for offensive IO to promote American interests
- The relative lack of discretion and caution from senior GEC leadership in sharing reports/analysis based on shaky methodology
- A limited track record of successful collaboration with industry

Especially as the election heats up in the coming months, introducing an actor like GEC into what has to date been a stable and (relatively) trusted group of practitioners and experts poses major risks, and could undermine a channel of significant importance to our election security efforts.

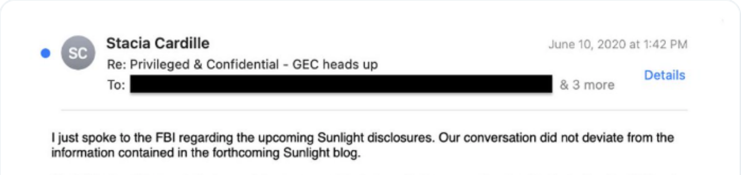
[redacted]/**Stacia:** I know we're investing in building a relationship with GEC. Any feedback on the basis of those conversations that we should bear in mind?

[redacted]: Do you think it's possible to see if we can get any more intel on where this is coming from from our contacts at the Bureau?

Thanks,

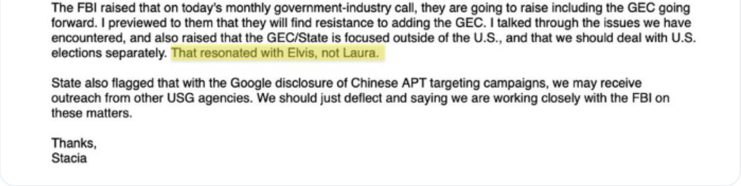
Yoel

19.When senior lawyer Stacia Cardille tried to argue against the GEC’s inclusion to the FBI, the words resonated “with Elvis, not Laura,” i.e. with agent Elvis Chan, not Foreign Influence Task Force (FITF) unit chief Laura Dehmlow:



Stacia Cardille
June 10, 2020 at 1:42 PM
Re: Privileged & Confidential - GEC heads up
To: [redacted] & 3 more

I just spoke to the FBI regarding the upcoming Sunlight disclosures. Our conversation did not deviate from the information contained in the forthcoming Sunlight blog.

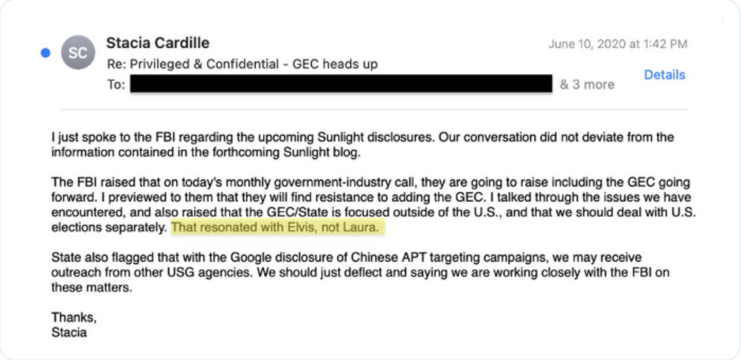


The FBI raised that on today's monthly government-industry call, they are going to raise including the GEC going forward. I previewed to them that they will find resistance to adding the GEC. I talked through the issues we have encountered, and also raised that the GEC/State is focused outside of the U.S., and that we should deal with U.S. elections separately. That resonated with Elvis, not Laura.

State also flagged that with the Google disclosure of Chinese APT targeting campaigns, we may receive outreach from other USG agencies. We should just deflect and saying we are working closely with the FBI on these matters.

Thanks,
Stacia

20.Eventually the FBI argued, first to Facebook, for a compromise solution: other USG agencies could participate in the "industry" calls, but the FBI and DHS would act as sole "conduits."



Stacia Cardille June 10, 2020 at 1:42 PM
Re: Privileged & Confidential - GEC heads up
To: [redacted] & 3 more Details

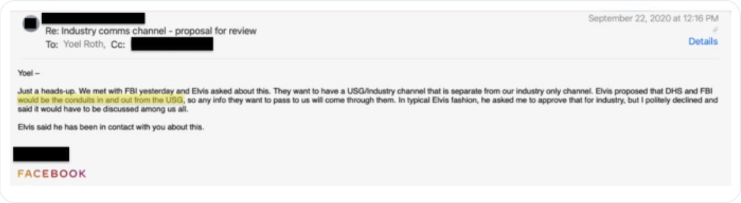
I just spoke to the FBI regarding the upcoming Sunlight disclosures. Our conversation did not deviate from the information contained in the forthcoming Sunlight blog.

The FBI raised that on today's monthly government-industry call, they are going to raise including the GEC going forward. I previewed to them that they will find resistance to adding the GEC. I talked through the issues we have encountered, and also raised that the GEC/State is focused outside of the U.S., and that we should deal with U.S. elections separately. That resonated with Elvis, not Laura.

State also flagged that with the Google disclosure of Chinese APT targeting campaigns, we may receive outreach from other USG agencies. We should just deflect and saying we are working closely with the FBI on these matters.

Thanks,
Stacia

21.Roth reached out to Chan with concerns about letting the "press-happy" GEC in, expressing hope they could keep the "circle of trust small."



[redacted] [redacted] September 22, 2020 at 12:16 PM
Re: Industry comms channel - proposal for review
To: Yoel Roth, Cc: [redacted] Details

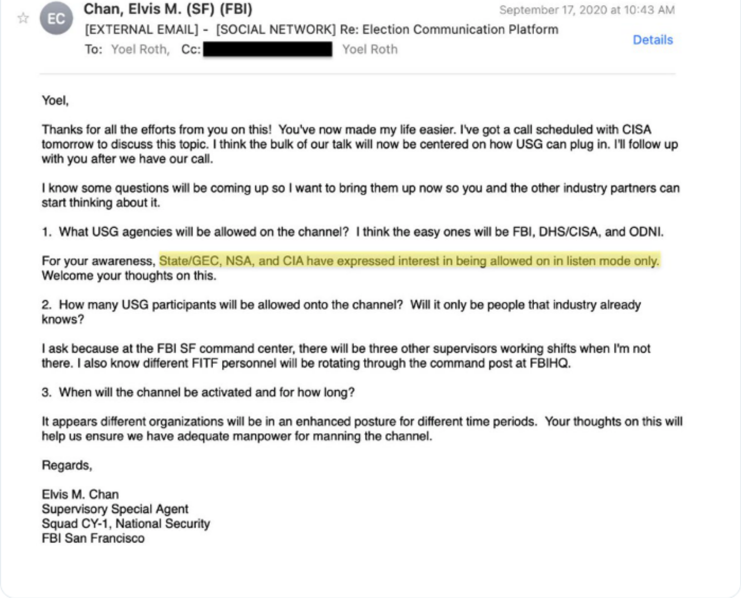
Yoel –

Just a heads-up. We met with FBI yesterday and Elvis asked about this. They want to have a USG/Industry channel that is separate from our industry only channel. Elvis proposed that DHS and FBI would be the conduits in and out from the USG, so any info they want to pass to us will come through them. In typical Elvis fashion, he asked me to approve that for industry, but I politely declined and said it would have to be discussed among us all.

Elvis said he has been in contact with you about this.

[redacted]
FACEBOOK

22."STATE… NSA, and CIA" Chan reassured him it would be a "one-way" channel, and "State/GEC, NSA, and CIA have expressed interest in being allowed on in listen mode only."



Chan, Elvis M. (SF) (FBI) September 17, 2020 at 10:43 AM

[EXTERNAL EMAIL] - [SOCIAL NETWORK] Re: Election Communication Platform

To: Yoel Roth, Cc: [redacted] Yoel Roth

Yoel,

Thanks for all the efforts from you on this! You've now made my life easier. I've got a call scheduled with CISA tomorrow to discuss this topic. I think the bulk of our talk will now be centered on how USG can plug in. I'll follow up with you after we have our call.

I know some questions will be coming up so I want to bring them up now so you and the other industry partners can start thinking about it.

1. What USG agencies will be allowed on the channel? I think the easy ones will be FBI, DHS/CISA, and ODNI.

For your awareness, State/GEC, NSA, and CIA have expressed interest in being allowed on in listen mode only. Welcome your thoughts on this.

2. How many USG participants will be allowed onto the channel? Will it only be people that industry already knows?

I ask because at the FBI SF command center, there will be three other supervisors working shifts when I'm not there. I also know different FITF personnel will be rotating through the command post at FBIHQ.

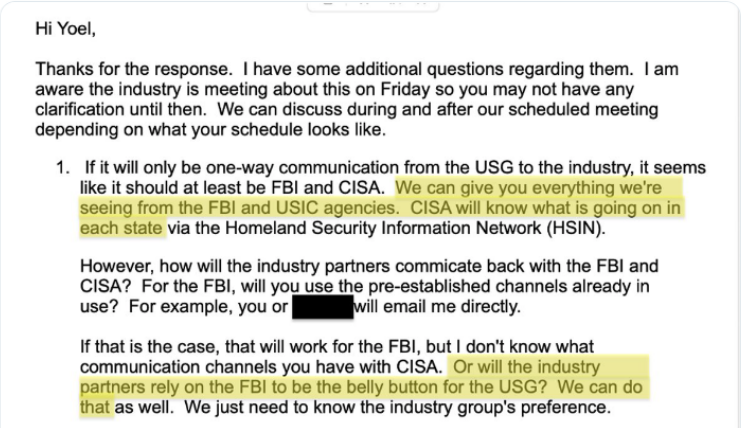
3. When will the channel be activated and for how long?

It appears different organizations will be in an enhanced posture for different time periods. Your thoughts on this will help us ensure we have adequate manpower for manning the channel.

Regards,

Elvis M. Chan
Supervisory Special Agent
Squad CY-1, National Security
FBI San Francisco

23."BELLY BUTTON" “We can give you everything we’re seeing from the FBI and USIC agencies,” Chan explained, but the DHS agency CISA “will know what’s going on in each state.” He went on to ask if industry could “rely on the FBI to be the belly button of the USG."



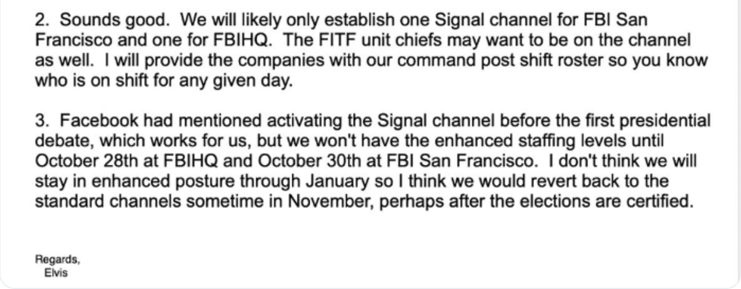
Hi Yoel,

Thanks for the response. I have some additional questions regarding them. I am aware the industry is meeting about this on Friday so you may not have any clarification until then. We can discuss during and after our scheduled meeting depending on what your schedule looks like.

1. If it will only be one-way communication from the USG to the industry, it seems like it should at least be FBI and CISA. We can give you everything we're seeing from the FBI and USIC agencies. CISA will know what is going on in each state via the Homeland Security Information Network (HSIN).

   However, how will the industry partners commicate back with the FBI and CISA? For the FBI, will you use the pre-established channels already in use? For example, you or [redacted] will email me directly.

   If that is the case, that will work for the FBI, but I don't know what communication channels you have with CISA. Or will the industry partners rely on the FBI to be the belly button for the USG? We can do that as well. We just need to know the industry group's preference.

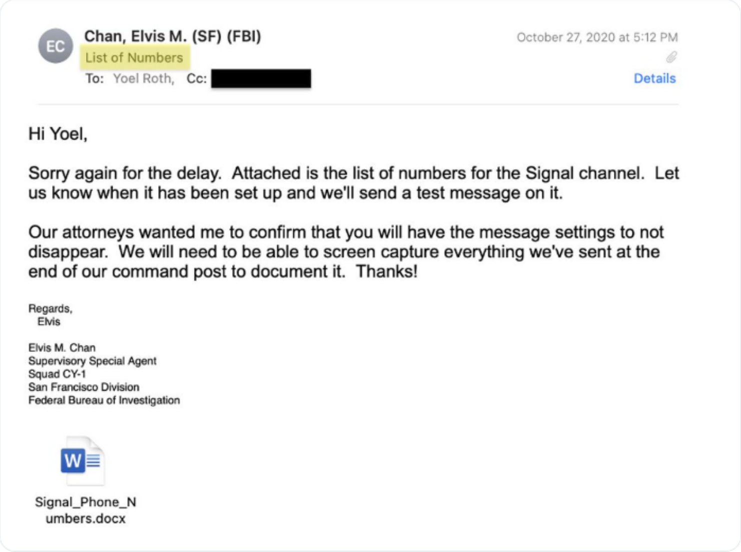


2. Sounds good. We will likely only establish one Signal channel for FBI San Francisco and one for FBIHQ. The FITF unit chiefs may want to be on the channel as well. I will provide the companies with our command post shift roster so you know who is on shift for any given day.

3. Facebook had mentioned activating the Signal channel before the first presidential debate, which works for us, but we won't have the enhanced staffing levels until October 28th at FBIHQ and October 30th at FBI San Francisco. I don't think we will stay in enhanced posture through January so I think we would revert back to the standard channels sometime in November, perhaps after the elections are certified.

Regards,
Elvis

24.They eventually settled on an industry call via Signal. In an impressive display of operational security, Chan circulated private numbers of each company's chief moderation officer in a Word Doc marked "Signal Phone Numbers," subject-lined, "List of Numbers."



Chan, Elvis M. (SF) (FBI)
List of Numbers
To: Yoel Roth, Cc: [redacted]

October 27, 2020 at 5:12 PM

Hi Yoel,

Sorry again for the delay. Attached is the list of numbers for the Signal channel. Let us know when it has been set up and we'll send a test message on it.

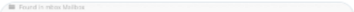
Our attorneys wanted me to confirm that you will have the message settings to not disappear. We will need to be able to screen capture everything we've sent at the end of our command post to document it. Thanks!

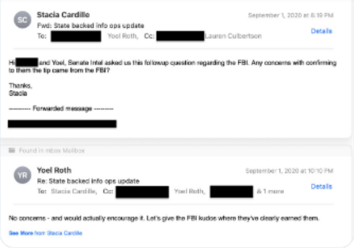
Regards,
Elvis

Elvis M. Chan
Supervisory Special Agent
Squad CY-1
San Francisco Division
Federal Bureau of Investigation

Signal_Phone_Numbers.docx

25.Twitter was taking requests from every conceivable government body, beginning with the Senate Intel Committee (SSCI), which seemed to need reassurance Twitter was taking FBI direction. Execs rushed to tell "Team SSCI" they zapped five accounts on an FBI tip:





Stacia Cardille September 1, 2020 at 8:19 PM
Fwd: State backed info ops update
To: [redacted] Yoel Roth, Cc: [redacted] Lauren Culbertson

Hi [redacted] and Yoel, Senate Intel asked us this followup question regarding the FBI. Any concerns with confirming to them the tip came from the FBI?

Thanks,
Stacia

---------- Forwarded message ---------

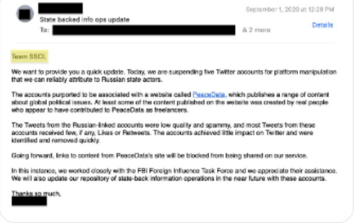
[redacted]

Found in mbox Mailbox

Yoel Roth September 1, 2020 at 10:10 PM
Re: State backed info ops update
To: Stacia Cardille, Cc: [redacted] Yoel Roth, [redacted] & 1 more

No concerns - and would actually encourage it. Let's give the FBI kudos where they've clearly earned them.

See More from Stacia Cardille



[redacted] September 1, 2020 at 12:28 PM
State backed info ops update
To: [redacted] & 2 more

Team SSCI,

We want to provide you a quick update. Today, we are suspending five Twitter accounts for platform manipulation that we can reliably attribute to Russian state actors.

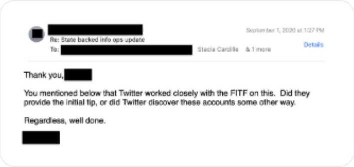
The accounts purported to be associated with a website called PeaceData, which publishes a range of content about global political issues. At least some of the content published on the website was created by real people who appear to have contributed to PeaceData as freelancers.

The Tweets from the Russian-linked accounts were low quality and spammy, and most Tweets from these accounts received few, if any, Likes or Retweets. The accounts achieved little impact on Twitter and were identified and removed quickly.

Going forward, links to content from PeaceData's site will be blocked from being shared on our service.

In this instance, we worked closely with the FBI Foreign Influence Task Force and we appreciate their assistance. We will also update our repository of state-back information operations in the near future with these accounts.

Thanks so much,
[redacted]



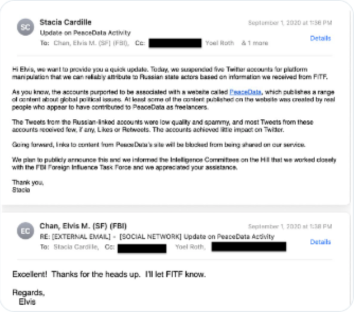
[redacted] September 1, 2020 at 1:27 PM
Re: State backed info ops update
To: [redacted] Stacia Cardille & 1 more

Thank you, [redacted]

You mentioned below that Twitter worked closely with the FITF on this. Did they provide the initial tip, or did Twitter discover these accounts some other way.

Regardless, well done.

[redacted]



Stacia Cardille September 1, 2020 at 1:36 PM
Update on PeaceData Activity
To: Chan, Elvis M. (SF) (FBI), Cc: [redacted] Yoel Roth & 1 more

Hi Elvis, we want to provide you a quick update. Today, we suspended five Twitter accounts for platform manipulation that we can reliably attribute to Russian state actors based on information we received from FITF.

As you know, the accounts purported to be associated with a website called PeaceData, which publishes a range of content about global political issues. At least some of the content published on the website was created by real people who appear to have contributed to PeaceData as freelancers.

The Tweets from the Russian-linked accounts were low quality and spammy, and most Tweets from these accounts received few, if any, Likes or Retweets. The accounts achieved little impact on Twitter.

Going forward, links to content from PeaceData's site will be blocked from being shared on our service.

We plan to publicly announce this and we informed the Intelligence Committees on the Hill that we worked closely with the FBI Foreign Influence Task Force and we appreciated your assistance.

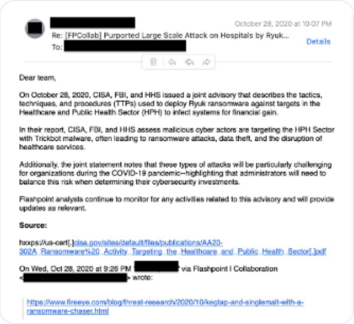
Thank you,
Stacia

Chan, Elvis M. (SF) (FBI) September 1, 2020 at 1:38 PM
RE: [EXTERNAL EMAIL] - [SOCIAL NETWORK] Update on PeaceData Activity
To: Stacia Cardille, Cc: [redacted] Yoel Roth, [redacted]

Excellent! Thanks for the heads up. I'll let FITF know.

Regards,
Elvis

26.Requests arrived and were escalated from all over: from Treasury, the NSA, virtually every state, the HHS, from the FBI and DHS, and more:



[redacted] October 28, 2020 at 10:07 PM
Re: [FPCollab] Purported Large Scale Attack on Hospitals by Ryuk...
To: [redacted]

Dear team,

On October 28, 2020, CISA, FBI, and HHS issued a joint advisory that describes the tactics, techniques, and procedures (TTPs) used to deploy Ryuk ransomware against targets in the Healthcare and Public Health Sector (HPH) to infect systems for financial gain.

In their report, CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with Trickbot malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.

Additionally, the joint statement notes that these types of attacks will be particularly challenging for organizations during the COVID-19 pandemic--highlighting that administrators will need to balance this risk when determining their cybersecurity investments.

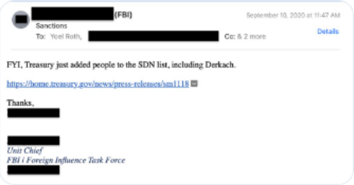
Flashpoint analysts continue to monitor for any activities related to this advisory and will provide updates as relevant.

Source:

hxxps://us-cert[.]cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector[.]pdf

On Wed, Oct 28, 2020 at 9:26 PM [redacted] via Flashpoint | Collaboration <[redacted]> wrote:

> https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html



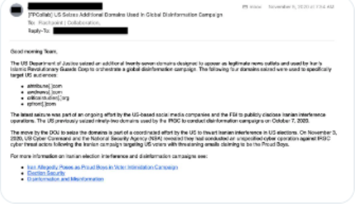
[redacted] (FBI) September 10, 2020 at 11:47 AM
Sanctions
To: Yoel Roth, [redacted] Cc: & 2 more

FYI, Treasury just added people to the SDN list, including Derkach.

https://home.treasury.gov/news/press-releases/sm1118

Thanks,
[redacted]

[redacted]
Unit Chief
FBI | Foreign Influence Task Force
[redacted]



[redacted]
[FPCollab] US Seizes Additional Domains Used In Global Disinformation Campaign
To: Fastpoint | Collaboration,
Reply-To: [redacted]

Good morning Team,

The US Department of Justice seized an additional twenty-seven domains designed to appear as legitimate news outlets and used by Iran's Islamic Revolutionary Guards Corp to orchestrate a global disinformation campaign. The following four domains seized were used to specifically target US audiences:

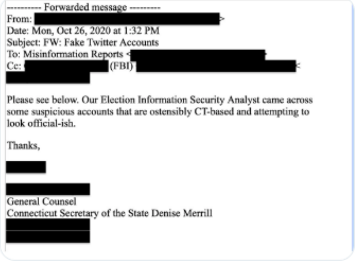
- [illegible][.]com
- [illegible][.]com
- criticalstudies[.]org
- [illegible][.]com

The latest seizure was part of an ongoing effort by the US-based social media companies and the FBI to publicly disclose Iranian interference operations. The US previously seized ninety-two domains used by the IRGC to conduct disinformation campaigns on October 7, 2020.

The move by the DOJ to seize the domains is part of a coordinated effort by the US to thwart Iranian interference in US elections. On November 3, 2020, US Cyber Command and the National Security Agency (NSA) revealed they had conducted an unspecified cyber operation against IRGC cyber threat actors following the Iranian campaign targeting US voters with threatening emails claiming to be the Proud Boys.

For more information on Iranian election interference and disinformation campaigns see:

- Iran Allegedly Poses as Proud Boys in Voter Intimidation Campaign
- Election Security
- Disinformation and Misinformation



---------- Forwarded message ---------
From: [redacted]>
Date: Mon, Oct 26, 2020 at 1:32 PM
Subject: FW: Fake Twitter Accounts
To: Misinformation Reports <[redacted]>
Cc: [redacted](FBI) [redacted]>
[redacted]

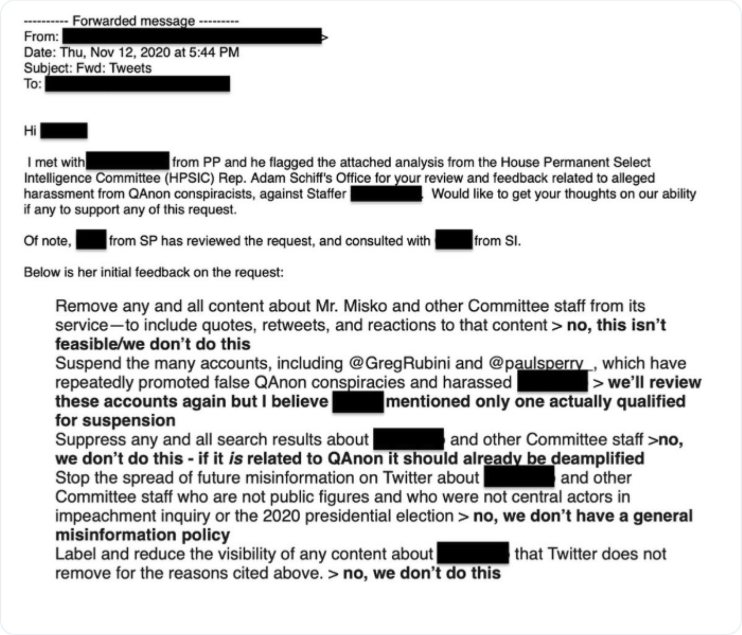
Please see below. Our Election Information Security Analyst came across some suspicious accounts that are ostensibly CT-based and attempting to look official-ish.

Thanks,

[redacted]

[redacted]
General Counsel
Connecticut Secretary of the State Denise Merrill
[redacted]

27.They also received an astonishing variety of requests from officials asking for individuals they didn't like to be banned. Here, the office for Democrat and House Intel Committee chief Adam Schiff asks Twitter to ban journalist Paul Sperry:



---------- Forwarded message ---------
From: [redacted]>
Date: Thu, Nov 12, 2020 at 5:44 PM
Subject: Fwd: Tweets
To: [redacted]

Hi [redacted]

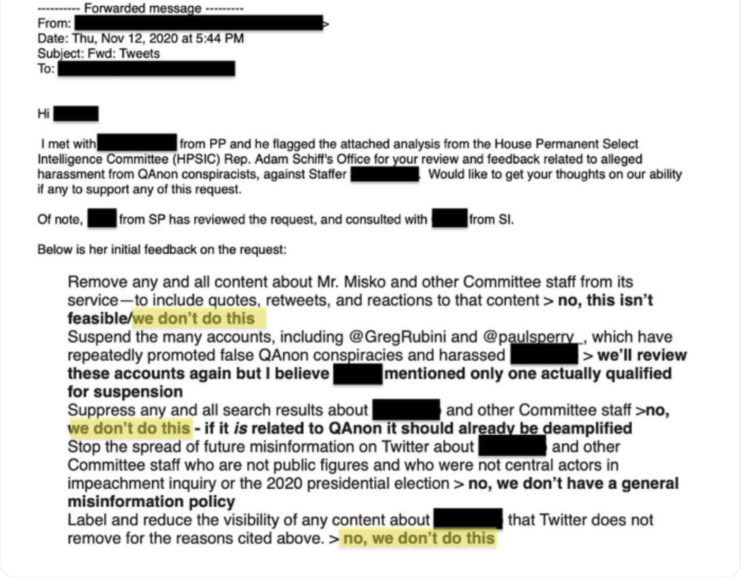
I met with [redacted] from PP and he flagged the attached analysis from the House Permanent Select Intelligence Committee (HPSIC) Rep. Adam Schiff's Office for your review and feedback related to alleged harassment from QAnon conspiracists, against Staffer [redacted]. Would like to get your thoughts on our ability if any to support any of this request.

Of note, [redacted] from SP has reviewed the request, and consulted with [redacted] from SI.

Below is her initial feedback on the request:

> Remove any and all content about Mr. Misko and other Committee staff from its service—to include quotes, retweets, and reactions to that content > **no, this isn't feasible/we don't do this**
> Suspend the many accounts, including @GregRubini and @paulsperry_, which have repeatedly promoted false QAnon conspiracies and harassed [redacted] > **we'll review these accounts again but I believe [redacted] mentioned only one actually qualified for suspension**
> Suppress any and all search results about [redacted] and other Committee staff >**no, we don't do this - if it *is* related to QAnon it should already be deamplified**
> Stop the spread of future misinformation on Twitter about [redacted] and other Committee staff who are not public figures and who were not central actors in impeachment inquiry or the 2020 presidential election > **no, we don't have a general misinformation policy**
> Label and reduce the visibility of any content about [redacted] that Twitter does not remove for the reasons cited above. > **no, we don't do this**

28."WE DON'T DO THIS" Even Twitter declined to honor Schiff's request at the time. Sperry was later suspended, however.



---------- Forwarded message ---------
From: [redacted]>
Date: Thu, Nov 12, 2020 at 5:44 PM
Subject: Fwd: Tweets
To: [redacted]

Hi [redacted]

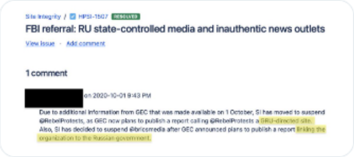
I met with [redacted] from PP and he flagged the attached analysis from the House Permanent Select Intelligence Committee (HPSIC) Rep. Adam Schiff's Office for your review and feedback related to alleged harassment from QAnon conspiracists, against Staffer [redacted]. Would like to get your thoughts on our ability if any to support any of this request.

Of note, [redacted] from SP has reviewed the request, and consulted with [redacted] from SI.

Below is her initial feedback on the request:

Remove any and all content about Mr. Misko and other Committee staff from its service—to include quotes, retweets, and reactions to that content > **no, this isn't feasible/we don't do this**
Suspend the many accounts, including @GregRubini and @paulsperry_, which have repeatedly promoted false QAnon conspiracies and harassed [redacted] > **we'll review these accounts again but I believe [redacted] mentioned only one actually qualified for suspension**
Suppress any and all search results about [redacted] and other Committee staff >**no, we don't do this - if it *is* related to QAnon it should already be deamplified**
Stop the spread of future misinformation on Twitter about [redacted] and other Committee staff who are not public figures and who were not central actors in impeachment inquiry or the 2020 presidential election > **no, we don't have a general misinformation policy**
Label and reduce the visibility of any content about [redacted] that Twitter does not remove for the reasons cited above. > **no, we don't do this**

29.Twitter honored almost everyone else's requests, even those from GEC – including a decision to ban accounts like @RebelProtests and @bricsmedia because GEC identified them as "GRU-controlled" and linked "to the Russian government," respectively:

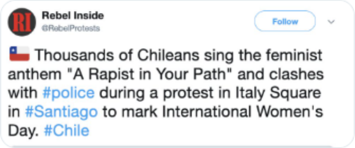


FBI referral: RU state-controlled media and inauthentic news outlets

1 comment

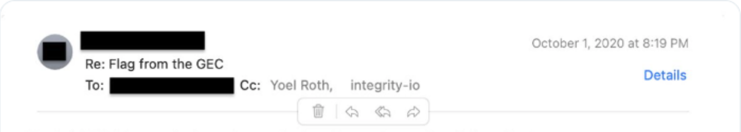
[redacted] on 2020-10-01 8:43 PM

Due to additional information from GEC that was made available on 1 October, SI has moved to suspend @RebelProtests, as GEC now plans to publish a report calling @RebelProtests a GRU-directed site. Also, SI has decided to suspend @bricsmedia after GEC announced plans to publish a report linking the organization to the Russian government.

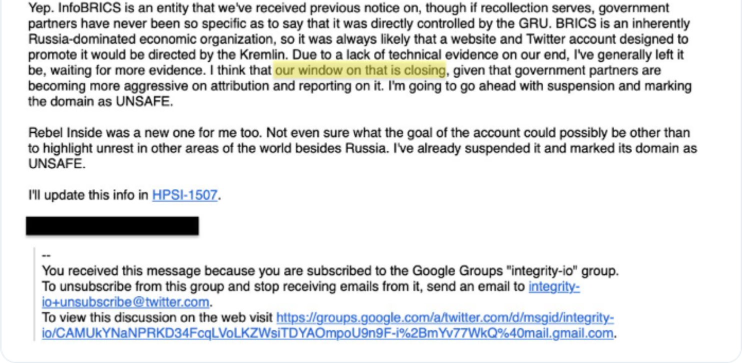


🇨🇱 Thousands of Chileans sing the feminist anthem "A Rapist in Your Path" and clashes with #police during a protest in Italy Square in #Santiago to mark International Women's Day. #Chile

30.The GEC requests were what a former CIA staffer working at Twitter was referring to, when he said, "Our window on that is closing," meaning they days when Twitter could say no to serious requests were over.



[redacted]
October 1, 2020 at 8:19 PM
Re: Flag from the GEC
To: [redacted] Cc: Yoel Roth, integrity-io



Yep. InfoBRICS is an entity that we've received previous notice on, though if recollection serves, government partners have never been so specific as to say that it was directly controlled by the GRU. BRICS is an inherently Russia-dominated economic organization, so it was always likely that a website and Twitter account designed to promote it would be directed by the Kremlin. Due to a lack of technical evidence on our end, I've generally left it be, waiting for more evidence. I think that our window on that is closing, given that government partners are becoming more aggressive on attribution and reporting on it. I'm going to go ahead with suspension and marking the domain as UNSAFE.

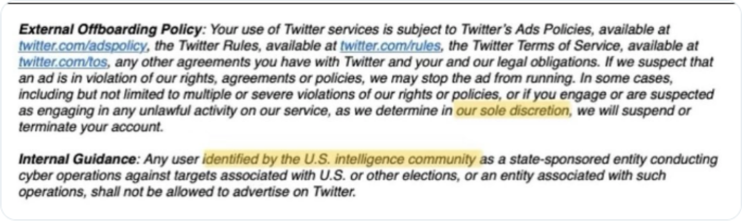
Rebel Inside was a new one for me too. Not even sure what the goal of the account could possibly be other than to highlight unrest in other areas of the world besides Russia. I've already suspended it and marked its domain as UNSAFE.

I'll update this info in HPSI-1507.

[redacted]

> --
> You received this message because you are subscribed to the Google Groups "integrity-io" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to integrity-io+unsubscribe@twitter.com.
> To view this discussion on the web visit https://groups.google.com/a/twitter.com/d/msgid/integrity-io/CAMUkYNaNPRKD34FcqLVoLKZWsiTDYAOmpoU9n9F-i%2BmYv77WkQ%40mail.gmail.com.

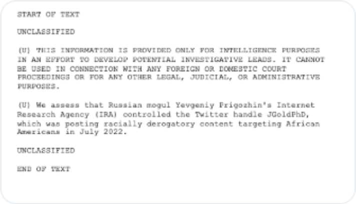
31.Remember the 2017 "internal guidance" in which Twitter decided to remove any user "identified by the U.S. intelligence community" as a state-sponsored entity committing cyber operations? By 2020 such identifications came in bulk.



***External Offboarding Policy**: Your use of Twitter services is subject to Twitter's Ads Policies, available at twitter.com/adspolicy, the Twitter Rules, available at twitter.com/rules, the Twitter Terms of Service, available at twitter.com/tos, any other agreements you have with Twitter and your and our legal obligations. If we suspect that an ad is in violation of our rights, agreements or policies, we may stop the ad from running. In some cases, including but not limited to multiple or severe violations of our rights or policies, or if you engage or are suspected as engaging in any unlawful activity on our service, as we determine in our sole discretion, we will suspend or terminate your account.*

***Internal Guidance**: Any user identified by the U.S. intelligence community as a state-sponsored entity conducting cyber operations against targets associated with U.S. or other elections, or an entity associated with such operations, shall not be allowed to advertise on Twitter.*

32."USIC" requests often simply began "We assess" and then provided lists (sometimes, in separate excel docs) they believed were connected to Russia's Internet Research Agency and committing cyber ops, from Africa to South America to the U.S.:



START OF TEXT

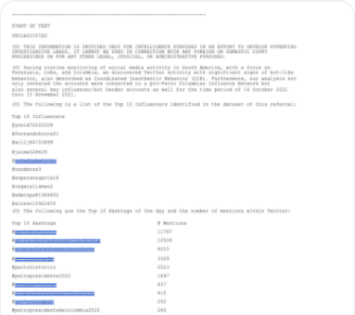
UNCLASSIFIED

(U) THIS INFORMATION IS PROVIDED ONLY FOR INTELLIGENCE PURPOSES IN AN EFFORT TO DEVELOP POTENTIAL INVESTIGATIVE LEADS. IT CANNOT BE USED IN CONNECTION WITH ANY FOREIGN OR DOMESTIC COURT PROCEEDINGS OR FOR ANY OTHER LEGAL, JUDICIAL, OR ADMINISTRATIVE PURPOSES.

(U) We assess that Russian mogul Yevgeniy Prigozhin's Internet Research Agency (IRA) controlled the Twitter handle JGoldPhD, which was posting racially derogatory content targeting African Americans in July 2022.

UNCLASSIFIED

END OF TEXT



START OF TEXT

UNCLASSIFIED

(U) THIS INFORMATION IS PROVIDED ONLY FOR INTELLIGENCE PURPOSES IN AN EFFORT TO DEVELOP POTENTIAL INVESTIGATIVE LEADS. IT CANNOT BE USED IN CONNECTION WITH ANY FOREIGN OR DOMESTIC COURT PROCEEDINGS OR FOR ANY OTHER LEGAL, JUDICIAL, OR ADMINISTRATIVE PURPOSES.

(U) During routine monitoring of social media activity in South America, with a focus on Venezuela, Cuba, and Columbia, we discovered Twitter activity with significant signs of bot-like behavior, also described as Coordinated Inauthentic Behavior (CIB). Furthermore, our analysis not only revealed the accounts were connected to a pro-Petro Columbian Influence Network but also several key influencer/bot herder accounts as well for the time period of 14 October 2021 thru 15 November 2021.

(U) The following is a list of the Top 10 Influencers identified in the dataset of this referral:

Top 10 Influencers

@yesid70282528

@fernandchinca21

@willy84753699

@jaime528629

@[illegible]

@nanderas3

@esperanzapriel6

@cepatallemen2

@edwinpa81364652

@alonso15822455

(U) The following are the Top 10 Hashtags of the day and the number of mentions within Twitter:

Top 10 Hashtags	# Mentions
#[illegible]	11767
#[illegible]	10508
#[illegible]	8215
#[illegible]	3329
#pactohistorico	2523
#petropresidente2022	1697
#[illegible]	637
#[illegible]	615
#[illegible]	252
#petropresidentedecolombia2022	245

#[illegible] 230

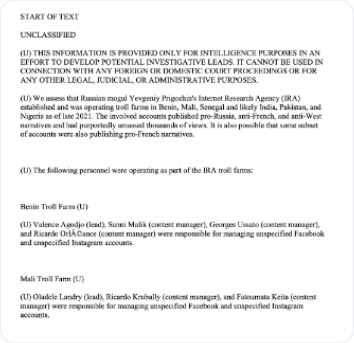
#[illegible] 223

(U) The attached excel file contains a list of 500 potential bot account, but also a compilation of over 50,000 posts and engagements.

(U) Any feedback you can provide regarding these identifiers and any violations of your company's terms of service would be greatly appreciated.

UNCLASSIFIED

END OF TEXT



START OF TEXT

UNCLASSIFIED

(U) THIS INFORMATION IS PROVIDED ONLY FOR INTELLIGENCE PURPOSES IN AN EFFORT TO DEVELOP POTENTIAL INVESTIGATIVE LEADS. IT CANNOT BE USED IN CONNECTION WITH ANY FOREIGN OR DOMESTIC COURT PROCEEDINGS OR FOR ANY OTHER LEGAL, JUDICIAL, OR ADMINISTRATIVE PURPOSES.

(U) We assess that Russian mogul Yevgeniy Prigozhin's Internet Research Agency (IRA) established and was operating troll farms in Benin, Mali, Senegal and likely India, Pakistan, and Nigeria as of late 2021. The involved accounts published pro-Russia, anti-French, and anti-West narratives and had purportedly amassed thousands of views. It is also possible that some subset of accounts were also publishing pro-French narratives.

(U) The following personnel were operating as part of the IRA troll farms:

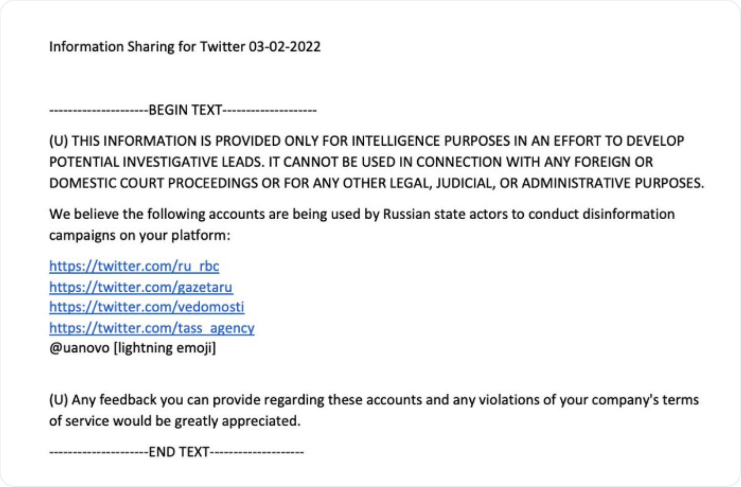
Benin Troll Farm (U)

(U) Valence Agodjo (lead), Sanni Malik (content manager), Georges Ussato (content manager), and Ricardo OrlÃ©ance (content manager) were responsible for managing unspecified Facebook and unspecified Instagram accounts.

Mali Troll Farm (U)

(U) Oladele Landry (lead), Ricardo Krubally (content manager), and Fatoumata Keita (content manager) were responsible for managing unspecified Facebook and unspecified Instagram accounts.

33.One brief report, sent right after Russia's invasion of Ukraine early last year, flagged major Russian outlets like Vedomosti and Gazeta.ru. Note the language about "state actors" fits Twitter's internal guidance.



Information Sharing for Twitter 03-02-2022

---------------------BEGIN TEXT--------------------

(U) THIS INFORMATION IS PROVIDED ONLY FOR INTELLIGENCE PURPOSES IN AN EFFORT TO DEVELOP POTENTIAL INVESTIGATIVE LEADS. IT CANNOT BE USED IN CONNECTION WITH ANY FOREIGN OR DOMESTIC COURT PROCEEDINGS OR FOR ANY OTHER LEGAL, JUDICIAL, OR ADMINISTRATIVE PURPOSES.

We believe the following accounts are being used by Russian state actors to conduct disinformation campaigns on your platform:

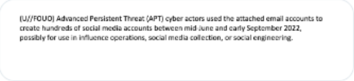
https://twitter.com/ru_rbc
https://twitter.com/gazetaru
https://twitter.com/vedomosti
https://twitter.com/tass_agency
@uanovo [lightning emoji]

(U) Any feedback you can provide regarding these accounts and any violations of your company's terms of service would be greatly appreciated.

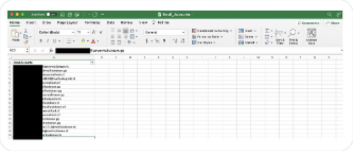
---------------------END TEXT--------------------

Главные новости – Газета.Ru
Главные новости дня из Москвы и регионов, информационная лента новостей, новости России и мира, события дня и последнего часа, аналитика, комментарии…
http://Gazeta.ru

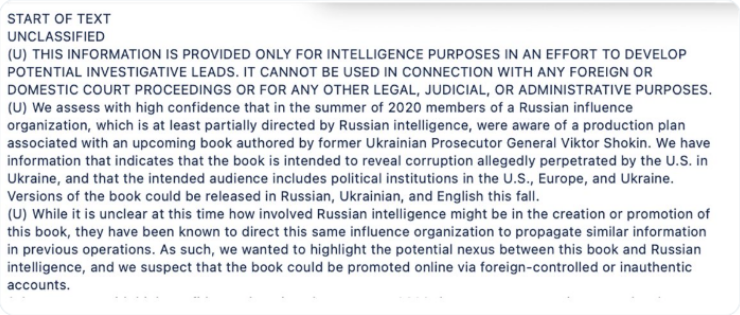
34.Some reports were just a paragraph long and said things like: "The attached email accounts… were possibly used for "influence operations, social media collection, or social engineering." Without further explanation, Twitter would be forwarded an excel doc:



(U//FOUO) Advanced Persistent Threat (APT) cyber actors used the attached email accounts to create hundreds of social media accounts between mid-June and early September 2022, possibly for use in influence operations, social media collection, or social engineering.

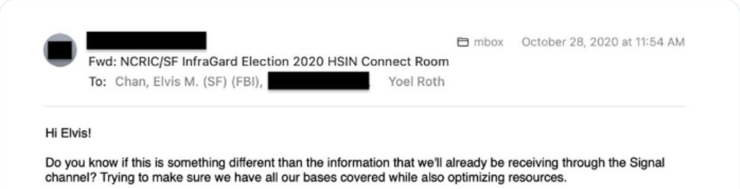


35.They were even warned about publicity surrounding a book by former Ukraine prosecutor Viktor Shokhin, who alleged "corruption by the U.S. government" – specifically by Joe Biden.



START OF TEXT
UNCLASSIFIED
(U) THIS INFORMATION IS PROVIDED ONLY FOR INTELLIGENCE PURPOSES IN AN EFFORT TO DEVELOP POTENTIAL INVESTIGATIVE LEADS. IT CANNOT BE USED IN CONNECTION WITH ANY FOREIGN OR DOMESTIC COURT PROCEEDINGS OR FOR ANY OTHER LEGAL, JUDICIAL, OR ADMINISTRATIVE PURPOSES.
(U) We assess with high confidence that in the summer of 2020 members of a Russian influence organization, which is at least partially directed by Russian intelligence, were aware of a production plan associated with an upcoming book authored by former Ukrainian Prosecutor General Viktor Shokin. We have information that indicates that the book is intended to reveal corruption allegedly perpetrated by the U.S. in Ukraine, and that the intended audience includes political institutions in the U.S., Europe, and Ukraine. Versions of the book could be released in Russian, Ukrainian, and English this fall.
(U) While it is unclear at this time how involved Russian intelligence might be in the creation or promotion of this book, they have been known to direct this same influence organization to propagate similar information in previous operations. As such, we wanted to highlight the potential nexus between this book and Russian intelligence, and we suspect that the book could be promoted online via foreign-controlled or inauthentic accounts.

36.By the weeks before the election in 2020, Twitter was so confused by the various streams of incoming requests, staffers had to ask the FBI which was which:

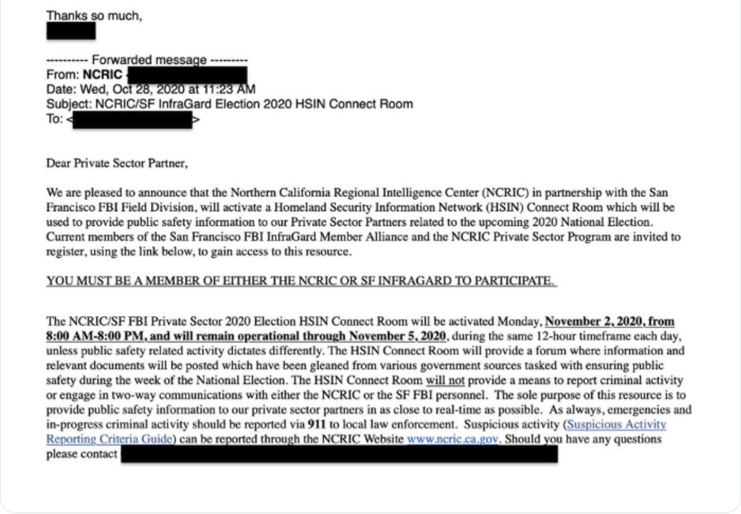


[redacted]
Fwd: NCRIC/SF InfraGard Election 2020 HSIN Connect Room
To: Chan, Elvis M. (SF) (FBI), [redacted] Yoel Roth

October 28, 2020 at 11:54 AM

Hi Elvis!

Do you know if this is something different than the information that we'll already be receiving through the Signal channel? Trying to make sure we have all our bases covered while also optimizing resources.



Thanks so much,
[redacted]

---------- Forwarded message ---------
From: **NCRIC** [redacted]
Date: Wed, Oct 28, 2020 at 11:23 AM
Subject: NCRIC/SF InfraGard Election 2020 HSIN Connect Room
To: <[redacted]>

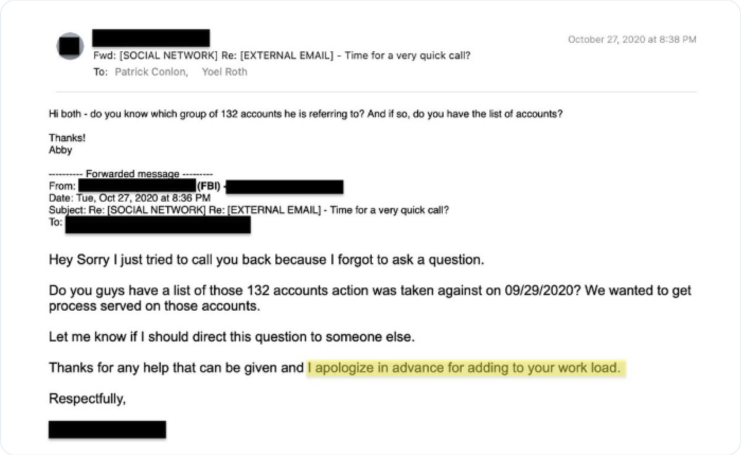
Dear Private Sector Partner,

We are pleased to announce that the Northern California Regional Intelligence Center (NCRIC) in partnership with the San Francisco FBI Field Division, will activate a Homeland Security Information Network (HSIN) Connect Room which will be used to provide public safety information to our Private Sector Partners related to the upcoming 2020 National Election. Current members of the San Francisco FBI InfraGard Member Alliance and the NCRIC Private Sector Program are invited to register, using the link below, to gain access to this resource.

YOU MUST BE A MEMBER OF EITHER THE NCRIC OR SF INFRAGARD TO PARTICIPATE.

The NCRIC/SF FBI Private Sector 2020 Election HSIN Connect Room will be activated Monday, **November 2, 2020, from 8:00 AM-8:00 PM, and will remain operational through November 5, 2020**, during the same 12-hour timeframe each day, unless public safety related activity dictates differently. The HSIN Connect Room will provide a forum where information and relevant documents will be posted which have been gleaned from various government sources tasked with ensuring public safety during the week of the National Election. The HSIN Connect Room will not provide a means to report criminal activity or engage in two-way communications with either the NCRIC or the SF FBI personnel. The sole purpose of this resource is to provide public safety information to our private sector partners in as close to real-time as possible. As always, emergencies and in-progress criminal activity should be reported via **911** to local law enforcement. Suspicious activity (Suspicious Activity Reporting Criteria Guide) can be reported through the NCRIC Website www.ncric.ca.gov. Should you have any questions please contact [redacted]

37.“I APOLOGIZE IN ADVANCE FOR YOUR WORK LOAD”: Requests poured in from FBI offices all over the country, day after day, hour after hour: If Twitter didn’t act quickly, questions came: “Was action taken?” “Any movement?”



[redacted] [redacted]
Fwd: [SOCIAL NETWORK] Re: [EXTERNAL EMAIL] - Time for a very quick call?
To: Patrick Conlon, Yoel Roth

October 27, 2020 at 8:38 PM

Hi both - do you know which group of 132 accounts he is referring to? And if so, do you have the list of accounts?

Thanks!
Abby

---------- Forwarded message ---------
From: [redacted] **(FBI)** [redacted]
Date: Tue, Oct 27, 2020 at 8:36 PM
Subject: Re: [SOCIAL NETWORK] Re: [EXTERNAL EMAIL] - Time for a very quick call?
To: [redacted]

Hey Sorry I just tried to call you back because I forgot to ask a question.

Do you guys have a list of those 132 accounts action was taken against on 09/29/2020? We wanted to get process served on those accounts.

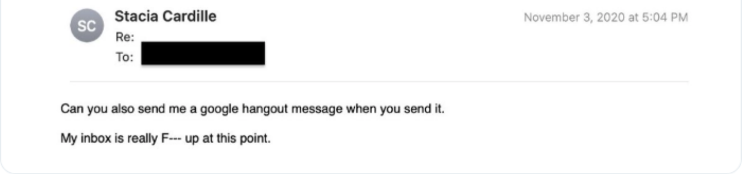
Let me know if I should direct this question to someone else.

Thanks for any help that can be given and I apologize in advance for adding to your work load.

Respectfully,

[redacted]

38.Wrote senior attorney Stacia Cardille: “My in-box is really f--- up at this point.”



SC **Stacia Cardille** November 3, 2020 at 5:04 PM
Re:
To: [redacted]

Can you also send me a google hangout message when you send it.

My inbox is really F--- up at this point.

39.It all led to the situation described by @ShellenbergerMD two weeks ago, in which Twitter was paid $3,415,323, essentially for being an overwhelmed subcontractor.

Twitter wasn't just paid. For the amount of work they did for government, they were underpaid.

40.For more on the #TwitterFiles, check out @bariweiss, @ShellenbergerMD, @lhfang, and @davidzweig. For more on this story, read

TK News by Ma
Taibbi
Regular news and features b
winning author and investig
Subscribe

TK News by Matt Taibbi

Regular news and features by award-winning author and investigative reporter. Click to read TK News by Matt Taibbi, a Substack publication with hundreds of thousands …

http://www.taibbi.substack.com