THE YAHOOS IN BRAZIL IDENTIFIED IN SERGEY CHERKASOV'S COMPLAINT

There's a detail in Greg Miller's profile of Sergey Cherkasov, the Russian accused of posing under an assumed Brazilian identity and using a SAIS degree to get an internship at the ICC, that confirms something I've long assumed: the US has had a hand in the recent roll-up of Russian spies, mostly in Europe.

> He was due to start a six-month internship there last year — just as the court began investigating Russian war crimes in Ukraine — only to be turned away by Dutch authorities acting on information relayed by the FBI, according to Western security officials.
>
> [snip]
>
> His arrest last April came at the outset of an ongoing roll-up of Russian intelligence networks across Europe, a crackdown launched after Russia's invasion of Ukraine that officials say has inflicted greater damage on Kremlin spy agencies than any other effort since the end of the Cold War.
>
> The FBI and CIA have played extensive behind-the-scenes roles in this wave of arrests and expulsions, according to Western officials.

As Miller describes, the Dutch realized that Russians stationed in the Hague were preparing to welcome a new agent, but by then, the US already had an incredibly detailed dossier on him.

> On March 31, as he boarded a flight to Amsterdam, neither Cherkasov nor his GRU

> handlers seemed aware of the net closing in on him. By then, the Dutch intelligence service had picked up its own signals that the Russian Embassy in The Hague was making preparations for the arrival of an important new illegal, according to a Western security official.
>
> Authorities in the Netherlands then received a dossier from the FBI with so much detail about Cherkasov's identity and GRU affiliation that they concluded the bureau and the CIA had been secretly monitoring Cherkasov for months if not years, according to a Western official familiar with the matter.

Until DOJ charged him last week, this had been largely a European story, with Dutch intelligence crowing about their success at foiling his plans and Bellingcat serially unpacking his public life (though CNN published this story at the time). Significantly, the Dutch published his legend and an explanation of how it might be used, with translations into Dutch and English from the original Portuguese.

As noted below, the US would later source its own possession of the legend to devices seized from Cherkasov on arrest in Brazil.

However, as Brazil gets closer to extraditing Cherkasov back to Russia on a trumped up narcotics trafficking charge, the US stepped in to make their own claim with the criminal charges: multiple counts of fraud, as well as acting as an unregistered foreign power. It's not yet clear how Brazil will respond to the competing charges. Contrary to some reporting on the charges, DOJ has not yet indicted the case. The complaint has not yet been docketed.

Which is why I wanted to look at the sourcing for the complaint.

Many of the sources in the complaint come via way of Brazil, temporally after the Dutch

deported him and the Brazilians arrested him, and so long past the time the US shared "a dossier" from the FBI reflecting months if not years of review. Brazil-sourced evidence includes:

- A picture taken on Cherkasov's 2011 immigration into Brazil
- His Brazilian birth certificate
- The details behind Brazil's identity theft charges
- Items collected — as if for the first time — from devices Cherkasov had with him when he arrived in Brazil, including:
    - The hard drive
        - His legend
        - His 2018 acceptance into SAIS
        - His 2018 receipt of visa
    - Thumb drive 1
        - November 29, 2021 draft message about US policy in advance of Ukraine invasion
    - Thumb drive 2
        - December 21, 2021 electronic communications about conversations

with US persons, including about Ukraine

- Thumb drive 3, including:
  - March 2022 emails of unknown provider with details about a dead drop
  - Details about his dead drop site
  - March 2022 emails about paying for false Portuguese citizenship
  - March 2022 mails about establishing a meeting place
- Samsung Galaxy Note phone
  - His mother’s Kaliningrad contact
  - 90 contacts with someone whose Telegram account and VKontakte account lead to a 2011 picture of Cherkasov in military uniform and a 2008

        - picture with friends
        - Contacts from one of those friends to a posted picture in military uniform (a picture also shown in the original Bellingcat profile)
    - Devices collected from the dead drop shared by Brazilian authorities
    - Correspondence between Brazil and Russia about Cherkasov
    - Audio messages between Cherkasov and his fiancée from immediately after his arrest in the Netherlands
    - Post-arrest communications between Cherkasov and his one-time fiancée, at least some of which were photographs of hand-written notes
    - Validation of Cherkasov's ID in certain photos from FBI agents who met him in 2022 (though these meetings are not explicitly described to have taken place in Brazil)
    - A Bellingcat story debunking the Russian narcotics

The focus on the phone, especially, cites evidence that would be fairly easily collected via other sources, but attributes that evidence to analysis the FBI did only downstream from the Brazilian arrest, and with the assent of Brazil. The complaint doesn't explain whether these devices were encrypted or even what messaging applications were used, at least on the thumb drives including communications with his handlers. But there's at least some reason to believe Brazil let FBI take the lead on exploiting those devices.

To be sure, there are items that the US could have collected in the US, whether before or after Cherkasov flew to the Hague, such as an Uber receipt timed to his travel to the dead drop in Brazil and IP addresses tied to US-based cloud providers like Yahoo and Google. Just once does the complaint reference using legal process — a 2017 video from a Moscow airport restaurant, obtained using legal process, reflecting Cherkasov saying goodbye to his mother — though it doesn't describe what kind (it sounds like it could be iCloud content).

Still, the emphasis on material obtained with subpoenas and investigative steps done while Cherkasov has been in Brazilian custody — whether or not that was the first that FBI obtained such evidence — is one reason I'm interested in the outliers.

This is a document that could form basis to extradite Cherkasov to the US — it seems more than sufficient to make that case. But it's also a document that might reflect on the kinds of investigations that have contributed to efforts to roll up spies outside of the US.

First, there are details about communications that Cherkasov had, while studying at Trinity College in Ireland and so not a US person at all — via known Section 702 participant, Yahoo!!! — with a tour agent who wrote recommendations for Cherkasov then later worked in Russia's Consul

General and, apparently, the General Consul himself.

> CHERKASOV used the Yahoo 1 Account on multiple occasions to contact individual "C2" who was communicating with CHERKASOV from Brazil. C2 communicated with CHERKASOV on numerous matters, including financial matters, between at least July 22, 2016, and December 27, 2019. According to a translation of C2's curriculum vitae, C2 worked in Brazil at "The General Consulate of the Russian Federation," for "General Consul [M.G.]"
>
> [snip]
>
> 35. Other emails show C2 took direction from another person, M.G., about financial payments that C2 sent to CHERKASOV. In correspondence between C2 and M.G., C2 refers to M.G. as "Mikhail" and the email address is identified in C2's contacts as "MikhailRussia." For example, on or about November 30, 2016, C2 forwarded M.G. correspondence from CHERKASOV that indicated another payment to CHERKASOV was imminent. M.G. responded by sending an email to C2 instructing C2 to make a payment to CHERKASOV: "Friend; thank you very much. Let's do another one on the 14th of December." According to further correspondence, CHERKASOV was able to receive the original transaction intended via MoneyGram. However, after corresponding to CHERKASOV that C2 would attempt to make transactions via Western Union the following day, financial records indicate C2 attempted to make two separate transactions via Western Union shortly after on December 16 and 18, 2016, for $842.65 and $867.55, respectively, but the funds were never transferred to CHERKASOV. CHERKASOV corresponded on December 19, 2016, that Western Union would not work properly

> and moving forward, the transactions should be made via Moneygram. C2 corresponded back to CHERKASOV on December 20, 2016, that C2 had sent €750 again via Moneygram to CHERKASOV.
>
> 36. C2 also stated in other emails that C2 previously owned a travel agency in Brazil, and that the Russian Federation was one of C2's best clients. C2 later moved to the Russian Consulate after C2 closed the travel agency.
>
> 37. On or about March 8, 2017, C2 wrote a letter of recommendation for CHERKASOV for a university located in Canada. In the letter, C2 indicated FERREIRA worked as a travel consultant for C2 from May 2014 until March 2017, and as a senior event manager in

It's possible that something Cherkasov did while at SAIS triggered a larger investigation that worked its way back to two likely Russian spies in Brazil. It's also possible that the investigation started from known subjects in Brazil and thereby discovered Cherkasov.

But one thing these two references do — aside from identify the travel agent later made part of the official Russian delegation, aside from making Cherkasov's tie to Russian government officials necessary for the 18 USC 951 charge — is put both Brazil and Russia on notice that the US is aware of these two suspected intelligence officers who were or are in Brazil.

Both C2 and the Consult General would have been legal targets for the entirety of the period in question and (as noted) Cherkasov was while he was in both Ireland or Brazil.

Another of the relatively few pieces of evidence unmoored from the Brazil arrest pertains to collection Cherksov shared after taking a SAIS trip to Israel. The details around the reporting — the single use email directing Cherkasov to fly to the Philippines to meet — definitely give

the story spy drama.

Just as interesting, however, are the descriptions of the identifiable US (and Israeli) subjects targeted by Cherksov's collection.

> 45. On or about January 16, 2020, CHERKASOV, using his D.C.-based phone number, texted with M.S. at a Philippines-based number for M.S. the following:
>
> CHERKASOV: Hey [M],7 I arrived…Where do you want to meet?
>
> [M.S.]: Grab a taxi and ask to drive via skyway.
>
> CHERKASOV: On my way. Will be there in approx. 15 min.
>
> [M.S.]: Ok. Here
>
> CHERKASOV: I can't find it
>
> [M.S.]: Names?
>
> CHERKASOV: Yea, I'll text you then when I'm in the airport.
>
> CHERKASOV: Texting you the names.
>
> CHERKASOV: Sent you a list there. Now whom we met.
>
> CHERKASOV: All people from the Jerusalem Embassy, literally every single one, even LGBTQ advisor. [N.G.]8 – security expert, local. I think he is a spook. [?.L.]9 kingmaker' – [Israeli political] party leader
>
> CHERKASOV: The previous list didn't sent [sic], I'll retype it.
>
> CHERKASOV: Can I send it to you email?
>
> CHERKASOV: This SMS shit kills me
>
> [M.S.]: Sure.
>
> 46. On or about January 17, 2020,

> CHERKASOV sent M.S. an email with a screen shot of names, mostly U.S. persons ("USP"), stating the following: Just a list of interesting people that I was talking to you about Experts side: [USP 1]10– DoS, middle Eastern direction advisor the president admin, former [University 1] student.
>
> [USP 2]11– FDD, military security adviros [sic] to the Congress Committee on Intelligence, [USP 3]'s12 assistant. ["TT1"] 13 group: [USP 4]14– [USP 5]15 chair, came only for a day though, [USP 6]16– main guy to call shots, Israeli expert came with small team of his own. [University 1, University 2] student leader: [USP 7]17– Anapolis [sic] Naval Academy Cyber Sec instructor

While just one of the people involved in Cherkasov's targeting — his SAIS professor, Eugene Finkel — has explicitly spoken out about being duped by Cherkasov, virtually all of these people (and a bunch more described later in the complaint) are likely to be able to identify themselves.

There are a few I suspect I recognize and, if I'm right, they've been apologists for Trump's propaganda about Russia.

Notably, this messaging involved a US-based phone, one not obviously included among the devices seized from Cherkasov when he returned to Brazil. The FBI Agent who wrote the affidavit couldn't have obtained the messaging in real time — he or she has only worked at the FBI since 2021, and the messaging dates to early 2020. But the affidavit does reference "surveillance that I have conducted."

In general, the FBI is revealing almost nothing obtained via sensitive sources and methods — that's one reason the reliance on evidence obtained via Brazil is of interest to me. Given how the US has allowed European countries to

take credit for these stings, I find it interesting that the US almost creates the misimpression that it only discovered Cherkasov — that it accessed his legend that the Dutch had upon his arrest — when he arrived in Brazil.

But in just a few spots, the affidavit gives a glimpse of what else the US Intelligence Community might know.

The US has not really taken much credit for helping a bunch of European countries roll up Russian spies (though they're likely reminding them of the role Section 702 plays in the process). But this document, seemingly released because they had reason to exert legal pressure with a country that is fairly close to Russia, likely serves multiple purposes. While it doesn't give away a lot, it does hint at far more.

Update, 4/6: The Guardian reported that two suspected Russian illegals, one presenting as Brazilian and the other presenting as Greek-Mexican, disappeared in January.

> Halfway through a trip to Malaysia in January, Gerhard Daniel Campos Wittich stopped messaging his girlfriend back home in Rio de Janeiro and she promptly launched a frantic search for her missing partner.
>
> A Brazilian of Austrian heritage, Campos Wittich ran a series of 3D printing companies in Rio that made, among other things, novelty resin sculptures for the Brazilian military and sausage dog key chains.
>
> [snip]
>
> The Brazilian foreign ministry and Facebook communities in Malaysia mobilised to look for the missing man. But Campos Wittich had simply disappeared.
>
> Greece believes Campos Wittich was a

> Russian illegal with the surname Shmyrev, said the official, while his wife, “Maria Tsalla”, was born Irina Romanova. She married him in Russia before their missions began and took his surname, the Greeks claim. She left Athens in a hurry in early January, just after Campos Wittich left Brazil. Neither have returned.

If I’m right that the FBI chose to use the Cherkasov complaint in part to identify those in Brazil who were running illegals, it may be because the disappearance of another Brazilian illegal in January led the US Intelligence Community to believe Russia had figured out what the US knew.