

Ministry of Defence

## GRU close access cyber operation against OPCW

Genmaj. O. Eichelsheim

Defence Intelligence &  
Security Service

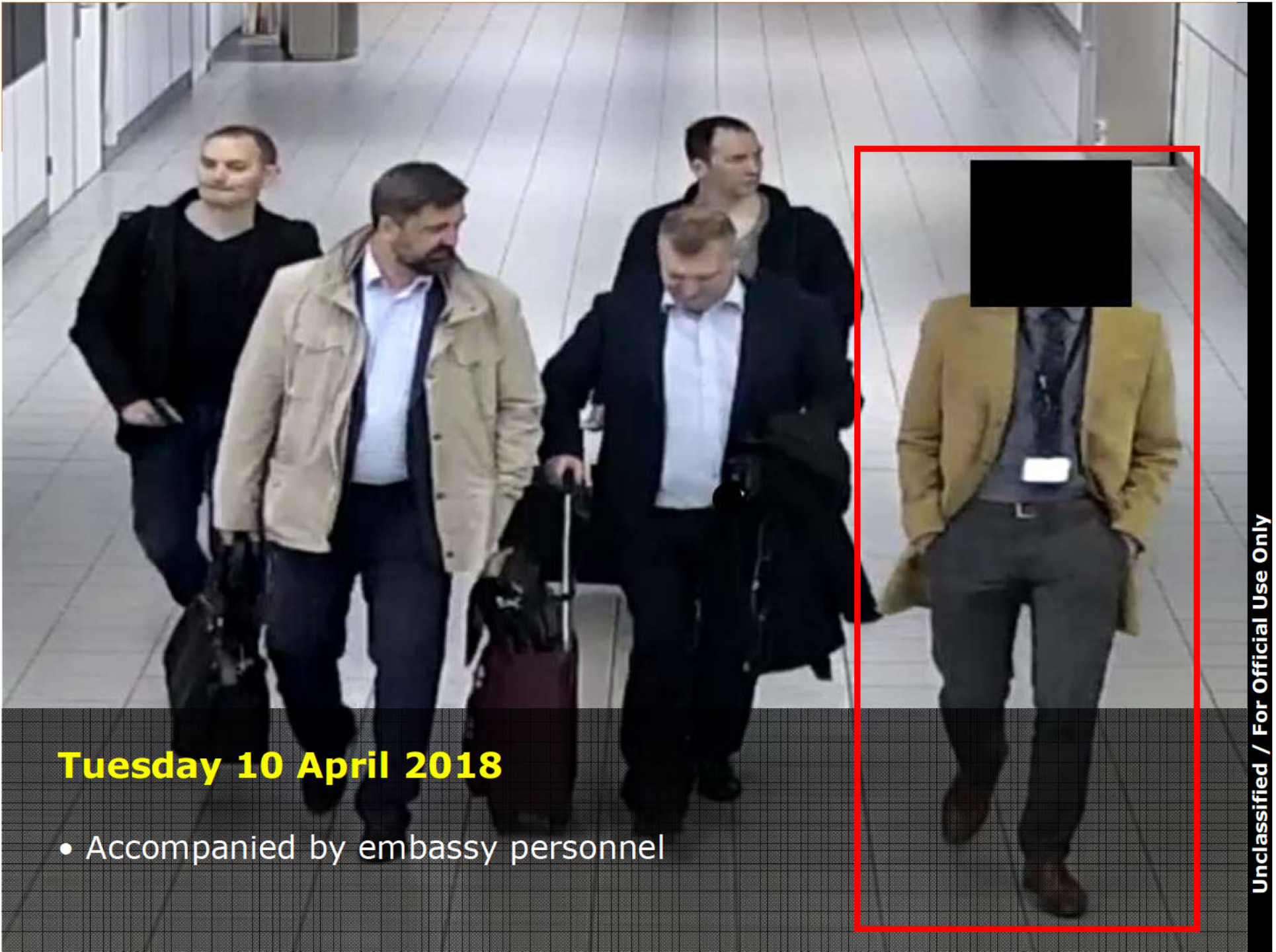
4 October 2018



**Tuesday 10 April 2018**

- Arrival from Moscow at Amsterdam Schiphol Airport

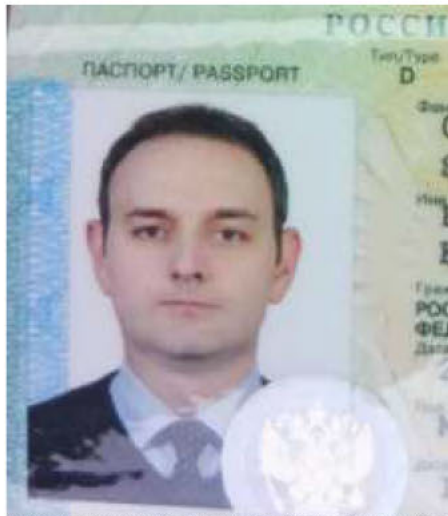




**Tuesday 10 April 2018**

- Accompanied by embassy personnel





## Overview of Russian persons

- Diplomatic passports









## Evgenii SEREBRIAKOV



**Name:** Evgenii Mikhaylovich SEREBRIAKOV  
(a.k.a. SEREBRYAKOV)

**Date of birth:** 26-07-1981

**Place of birth:** Kursk

**Passport nr:** 100135555

**Role:** cyber operator





# Oleg SOTNIKOV



**Name:** Oleg Mikhaylovich SOTNIKOV

**Date of birth:** 24-08-1972

**Place of birth:** Ulyanovsk

**Passport nr:** 120018866

**Role:** HUMINT support







# Car rental agreement Citroën C3, PF-934-R

Naam O.M. Sotnikov  
 Adres Podmoscown Street 10-211  
 Postcode / plaats RUSS IA RUSSIA  
 Land Russia  
 Telefoon 0617671589  
 verklaren dat zij een overeenkomst hebben gesloten tot huur en verhuur van

Bestuurder 2: Minin, 27-05-1972

Contractnummer: H76786 VERHUUROVEREENKOMST Pagina 1 van 2

Naam: O.M. Sotnikov  
 Adres: Podmoscown Street 10-211  
 Postcode / plaats: RUSS IA RUSSIA  
 Land: Russia  
 Telefoon: 0617671589

GSM: 061074565  
 E-mail: p.o.s.7@spjsoel.nl  
 Referentie / extern reserveringsnummer: 24-05-1972  
 Geboortedatum: 24-05-1972  
 Rijbewijs categorie: B

Alleen huurder of de hier vermelde bestuurder(s) mogen het voertuig besturen,mits in bezit van een geldig rijbewijs.

Extra bestuurder(s):

Bestuurder 2: Minin, 27-05-1972

Categorie berekend: ECVR Peugeot 208  
 Categorie werkdag: ECVR Peugeot 208  
 Huurperiode: 11 apr. 2018 12:30 uur tot 18 april 2018 12:30 uur  
 Ritprijs: 700,- Euro (indien overeenkomsten na verlooprijd per schakelgeval)

In bepaalde gevallen is huurder aansprakelijk voor de volledige schade van de Algemere Voorwaarden, artikel 11 en bijgeschikschrijving:

	KORTING	KORTING	EURO
Huurprijs berekende huurperiode, inclusief 1000 kilometers uit			145,25
Dagwaarschuldiging 5 dagen			35,26
PK & per extra kilometer: 0,120 Euro		29,59,5	58,55
Verplichting de Bestuurder			
Totaalbedrag 8 euro			
Afdringkosten excl. btw bij retour zonder volle tank: 6,00			
Huurkosten exclusief btw en brandstof			135,69
Btw bedrag			22,41
Huurkosten inclusief btw en exclusief brandstof			154,10
EURO	5212*****7192	Autob. code: 02753	900,00

Dit bedrag met creditcard, gaat de huurder vakkoud met volledige afschrijving van de uit deze huur voortvloeiende kosten.

Op deze huurovereenkomst na van toepassing de algemene voorwaarden Boordj Verhuurbedrijven voor Continenten, daterende november 2012. Huurder heeft een exemplaar van deze voorwaarden ontvangen.  
 Huurder verklaart kennis te zullen nemen van het Nederlandse staatsrechtelijke welke zich in het voertuig bevindt.  
 Huurder dient het voertuig te retourneren met dezelfde hoeveelheid benzine in de tank als waarmee de auto is afgeleverd. Bij niet nakoming is de huurder de door Europcar gehanteerde brandstofkosten verschuldigd, vormdegrond met uitankkosten.  
 Dit contract bestaat uit 2 formulieren en vormt samen de huurovereenkomst.

Handtekening huurder: [Redacted] Huurder: O.M. Sotnikov  
 11-04-2018 12:31 11-04-2018 12:31





# Car rental agreement Citroën C3, PF-934-R

Huurder : Aleksey Minin  
 Adres : Micknouslay str 8  
 Plaats : 1735 NOBODW  
 Russia  
 Bestuurder : Aleksey Minin  
 Afleveradr. :

RENTAL-AGREEMENT  
 INNAME / INNAME

Contractnr : 498794  
 Telefoon : 061745365

Beoordelst: 27-05-78  
 Geo.plaats : RUSSIA  
 Rijbewijs : 771756/019  
 Rijb. cat. : 3  
 Telefoon : 061745365

Huurauto : CITROEN C3 (HD)  
 Kenteken : PF-934-R (NX-508-T)  
 Sublocatie :

Huurperiode: 16 april 2018 12:30 tot 16 april 2018 12:30  
 OORZAKEN schade : 1  
 OORZAKEN schade : 1

ACCESSOIRES  
 check-out check-in  
 schoon  
 autoplegen  
 radio / CD / DVD  
 navigatie  
 handreuk  
 kiel / gereedschap  
 wieloppen/vegen  
 rijschool  
 zomer/winterbanden  
 sanitair toilet  
 overige:

DAMAGE: YES / NO  
 Het voertuig is zonder schade afgegeven  
 Het voertuig is zonder schade ingekomen

INNAME / CHECK-IN  
 = 0000 0 = 0000  
 FRONT FRONT  
 BACK BACK

Huurder verklaart afbreken te gaan met de hand gemaakte algemene voorwaarden van de BOVAG Verhuurbedrijven. Huurder verklaart akkoord te gaan met alle conditions van de overeenkomst en van de algemene voorwaarden van de overeenkomst. Huurder verklaart akkoord te gaan met alle conditions van de overeenkomst en van de algemene voorwaarden van de overeenkomst. Huurder verklaart akkoord te gaan met alle conditions van de overeenkomst en van de algemene voorwaarden van de overeenkomst. Huurder verklaart akkoord te gaan met alle conditions van de overeenkomst en van de algemene voorwaarden van de overeenkomst.

Indien u niet in de gelegenheid bent geweest dit formulier te ondertekenen en u heeft een opmerking over de staat van het voertuig, dan dient u dit binnen 2 uur na aflevering van het voertuig te melden aan onze vestiging.

CHECK OUT  
 Handtekening en naam huurder/bestuurder  
 Handtekening en naam verhuurder

CHECK IN  
 Handtekening en naam huurder/bestuurder  
 Handtekening en naam verhuurder

BOVAG



## Reconnaissance of OPCW and surroundings

- Photos taken on 11 April, found on MININ's camera





## Reconnaissance of OPCW and surroundings

- Photo taken on 12 April, found on MININ's camera



## Reconnaissance of OPCW and surroundings

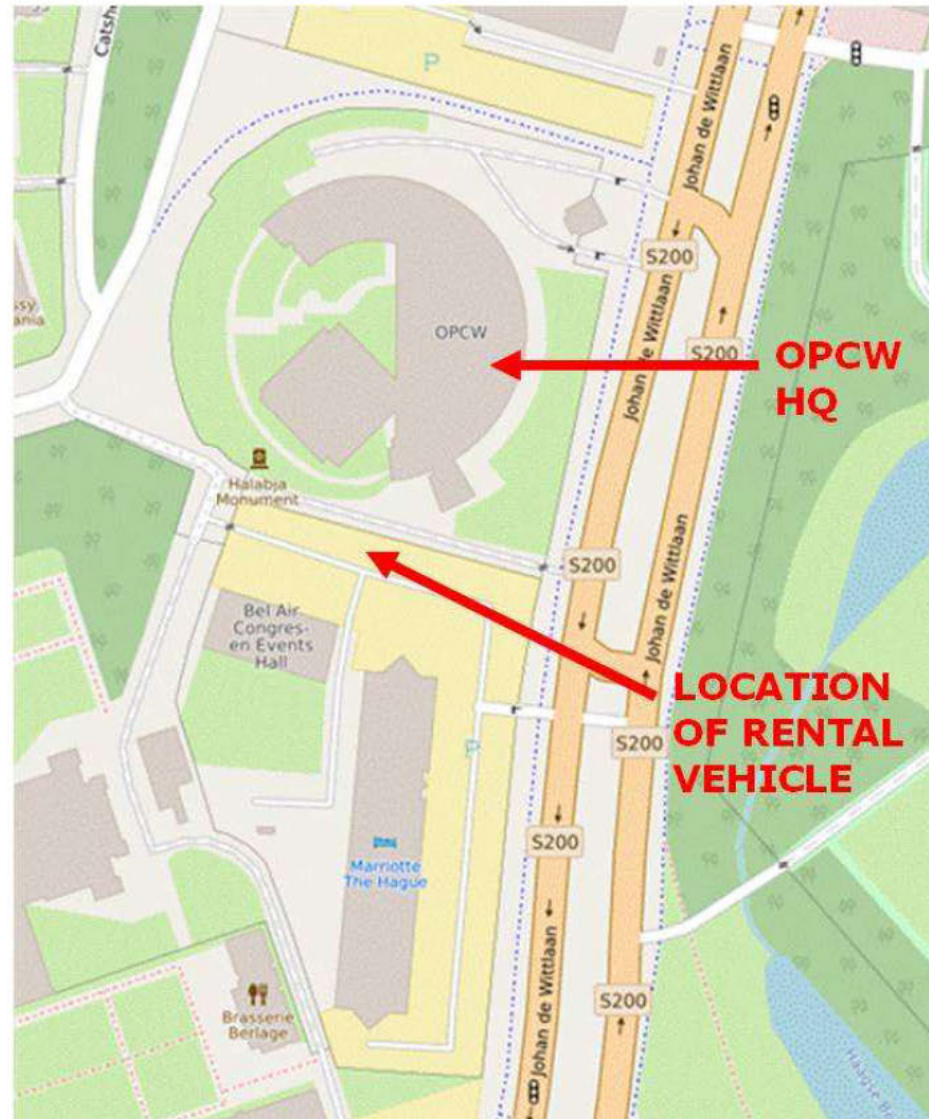
- Photo taken on 13 April, found on MININ's camera



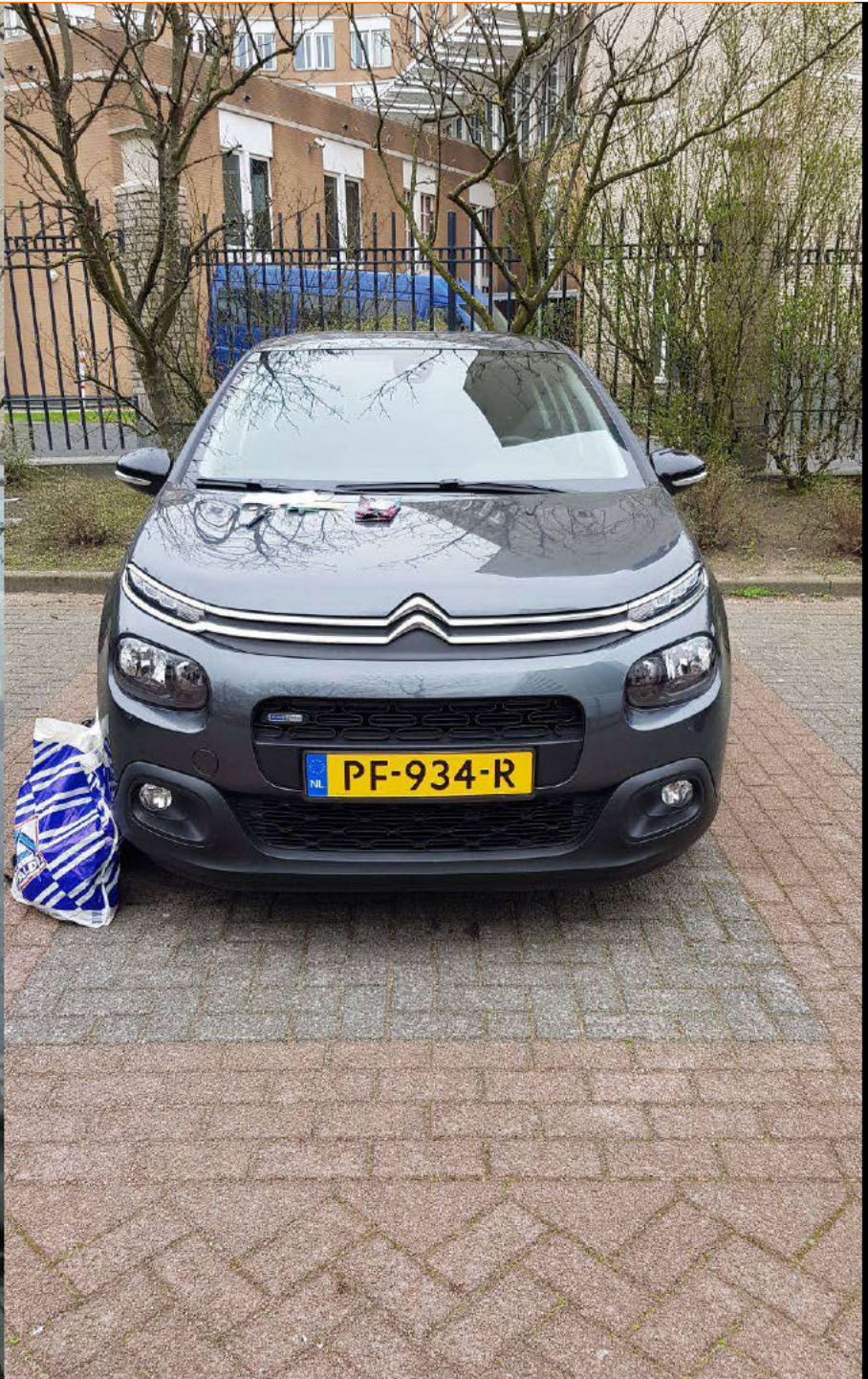
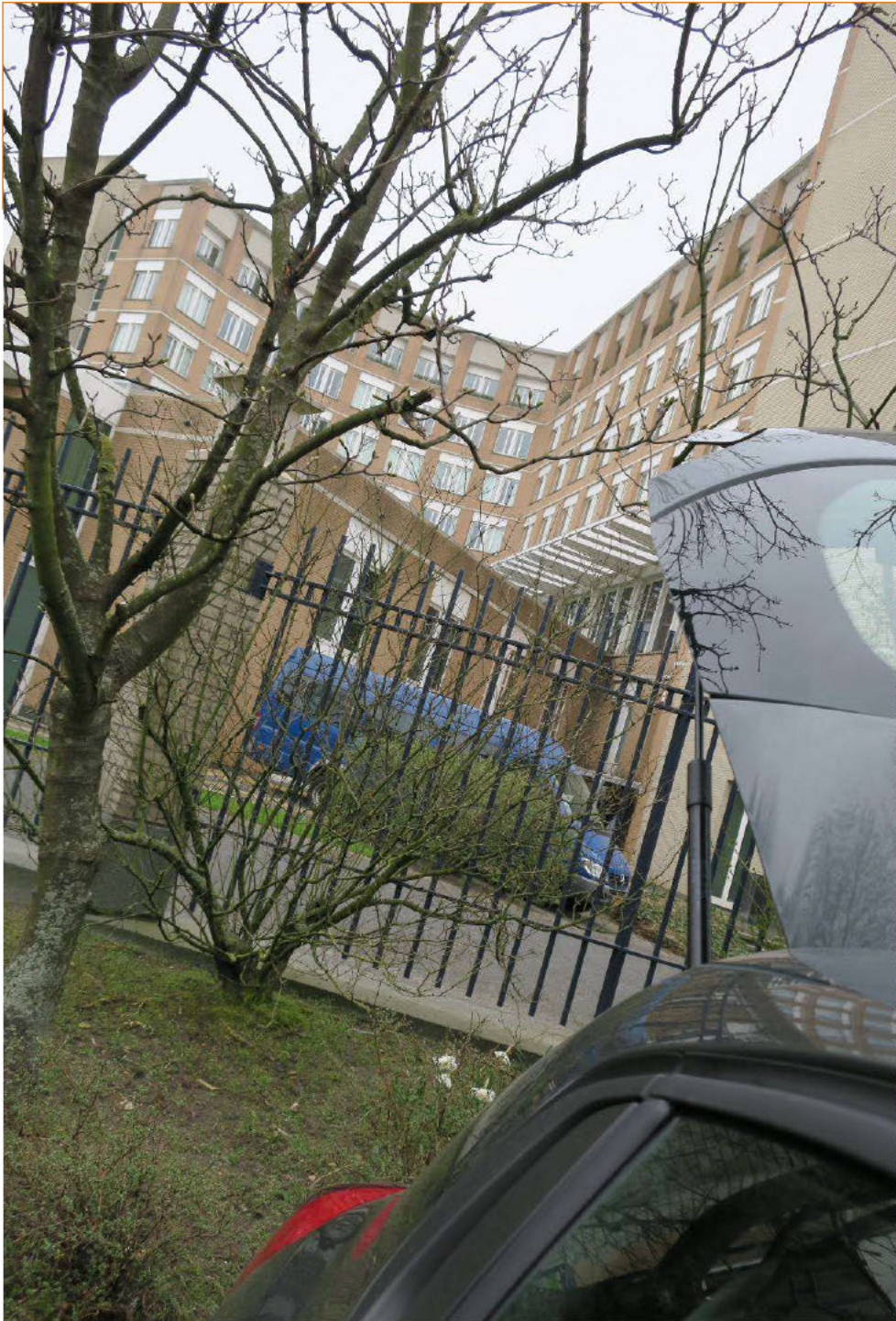


## Situation map

- Location of rental vehicle on Friday 13 April









Connected to:

-Smartphone  
(4G)

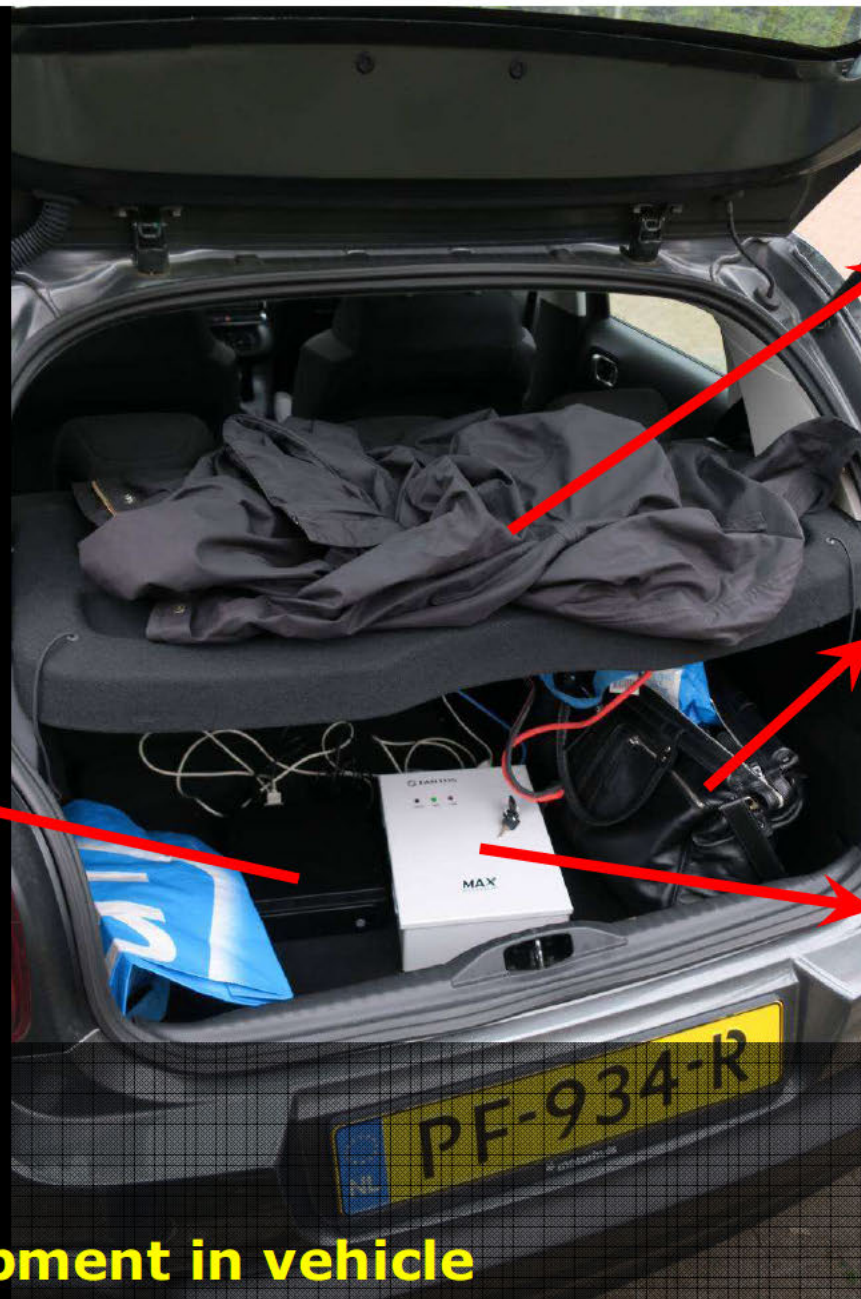
-WiFi panel  
antenna

Computer

WiFi panel  
antenna  
(covered)

Bag with  
battery

Transformer

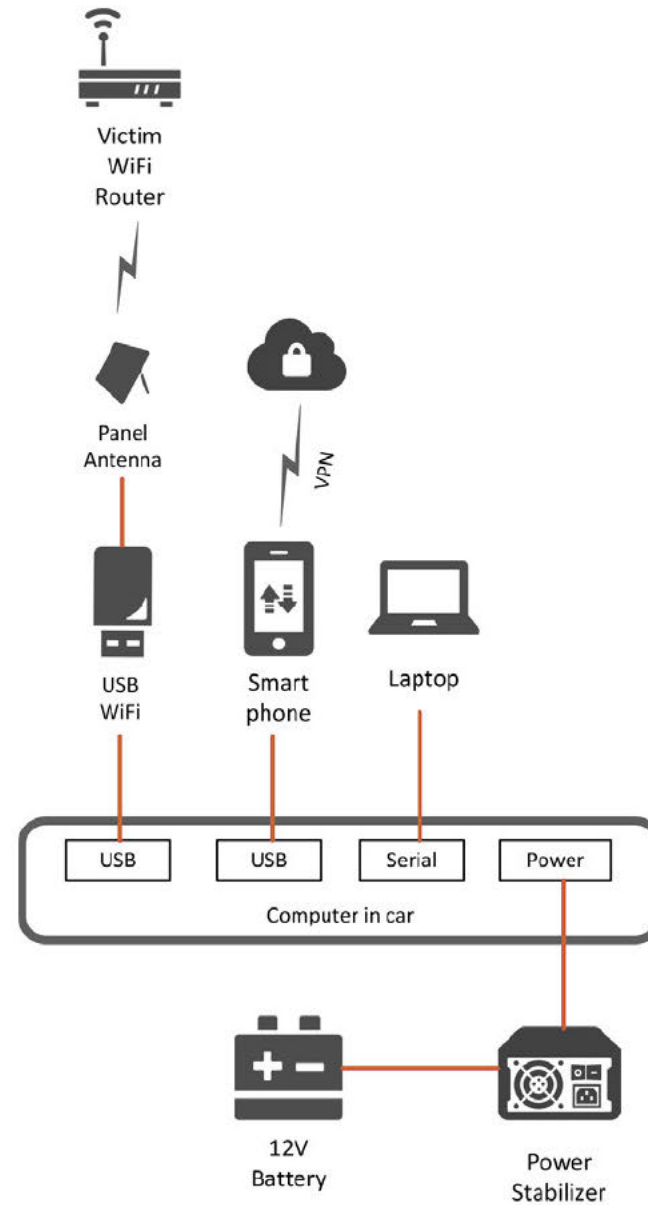


### Specialist equipment in vehicle

- Setup for hacking WiFi connections



# Schematische weergave

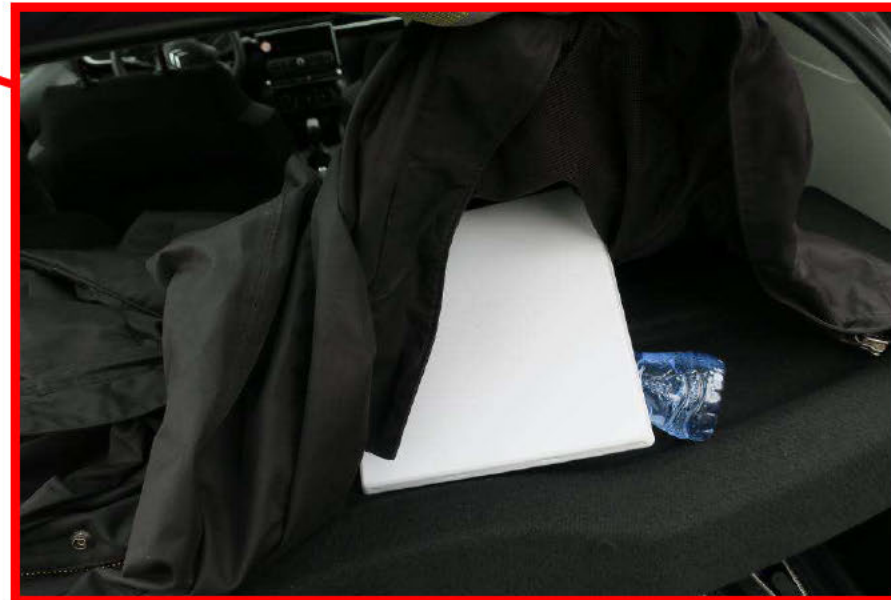






## WiFi panel antenna

- Hidden under coat





## Battery

- Power supply for equipment
- Purchased in The Hague



SPORT BV

10-04-2018 16:14  
REG 000004

VERKOOP €219,65  
EX. BTW 2 €181,53  
BTW 2 €38,12  
CONTANT €219,65

TEN, MOTOREN & WATERSPORTARTIKELEN

KONTANTBON: 624399 Datum: 10/04/18 Pagina 1

Artikel	Omschrijving	Aantal	Prijs	Kort.	Bedrag
GR008100	53 Ah onderhoudsvrij	1,00	100,65		100,65
00449007	MinnKota MK-110PE Acculader po	1,00	119,00		119,00

Exclusief BTW 181,53    BTW hoog 38,12    BTW laag    TOTAAL INCL. € 219,65











### **Operational modus operandi**

- Security awareness
- Tried to destroy smartphone during disruption operation





### **Operational modus operandi**

- Security awareness
- GRU intelligence officers took their trash out of their hotel rooms





## Operational modus operandi

- Cash money: 20.000 Euro's and 20.000 dollars



OPCW	09-04-2018 07:09:46
<a href="https://www.google.ru/maps/search/OPCW/@42.7111121,3.5078125,3z">https://www.google.ru/maps/search/OPCW/@42.7111121,3.5078125,3z</a>	09-04-2018 07:09:46
Organization for the Prohibition Chemical Weapos	09-04-2018 07:10:16
Organization for the Prohibition Chemical Weapos	09-04-2018 07:10:16
<a href="https://www.google.ru/maps/search/Organization+for+the+Prohibition+Chemical+Weapos/@42.7111121,3.5078125,3z">https://www.google.ru/maps/search/Organization+for+the+Prohibition+Chemical+Weapos/@42.7111121,3.5078125,3z</a>	09-04-2018 07:10:16
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:17
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:17
<a href="https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.09096,4.2810983,17z/data=!4m1!4m5!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287">https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.09096,4.2810983,17z/data=!4m1!4m5!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287</a>	09-04-2018 07:10:17
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:27
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:27
<a href="https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.090136,4.281903,17z/data=!4m1!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287">https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.090136,4.281903,17z/data=!4m1!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287</a>	09-04-2018 07:10:27
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:32
Organisation for the Prohibition of Chemical Weapons	09-04-2018 07:10:32
<a href="https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.0900569,4.2822248,17z/data=!4m1!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287">https://www.google.ru/maps/place/Organisation+for+the+Prohibition+of+Chemical+Weapons/@52.0900569,4.2822248,17z/data=!4m1!3m4!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!8m2!3d52.09096!4d4.283287</a>	09-04-2018 07:10:32
The Hague Marriott Hotel	09-04-2018 07:10:39
The Hague Marriott Hotel	09-04-2018 07:10:39
The Hague Marriott Hotel	09-04-2018 07:10:39
The Hague Marriott Hotel	09-04-2018 07:10:39
<a href="https://www.google.ru/maps/place/The+Hague+Marriott+Hotel/@52.0900569,4.2822248,17z/data=!4m12!1m6!3m5!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!2sOrganisation+for+the+Prohibition+of+Chemical+Weapons!8m2!3d52.09096!4d4.283287!3m4!1s0x0:0xc44f7f20fe9c5077!8m2!3d52.0900298!4d4.2824558">https://www.google.ru/maps/place/The+Hague+Marriott+Hotel/@52.0900569,4.2822248,17z/data=!4m12!1m6!3m5!1s0x47c5b0c7e15ee87f:0xfa7c7523f39a9e0c!2sOrganisation+for+the+Prohibition+of+Chemical+Weapons!8m2!3d52.09096!4d4.283287!3m4!1s0x0:0xc44f7f20fe9c5077!8m2!3d52.0900298!4d4.2824558</a>	09-04-2018 07:10:39

Unclassified / For Official Use Only

## Online searches from SEREBRIAKOV's laptop

- Indicating interest in OPCW headquarters building and immediate surroundings





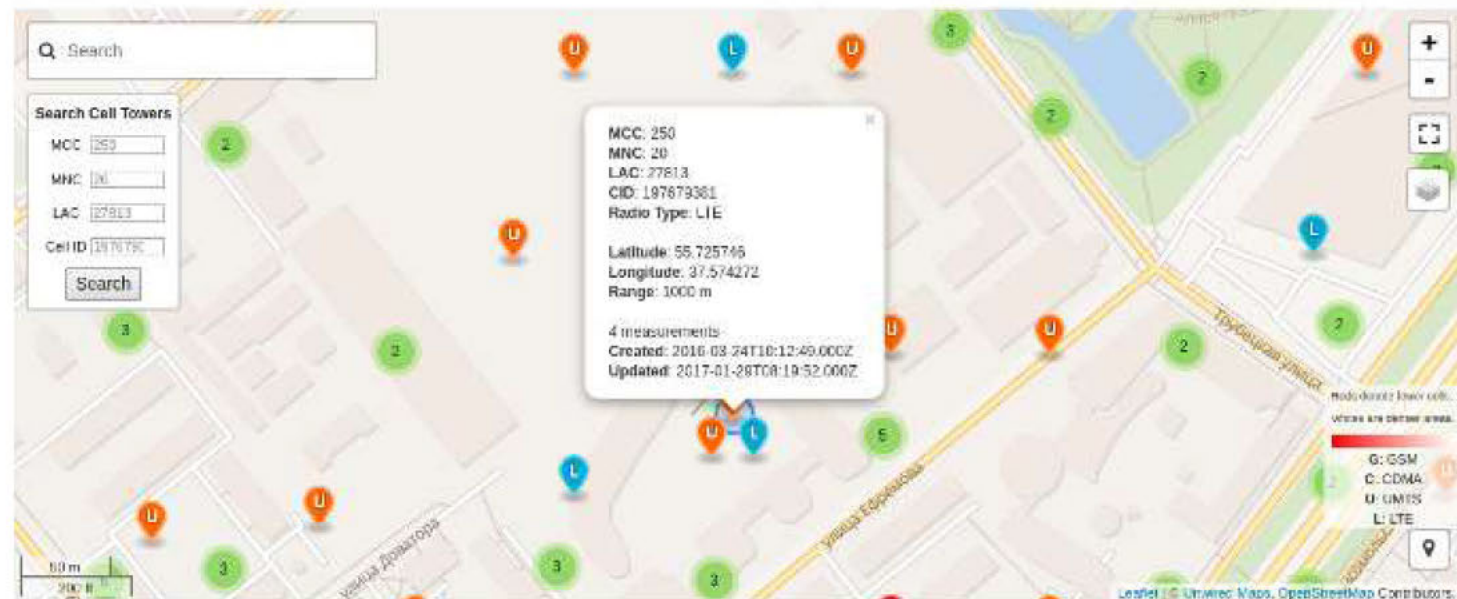
## Additional specialist equipment

- Carried by SEREBRIAKOV
- Intended for hacking WiFi networks



## The world's largest Open Database of Cell Towers

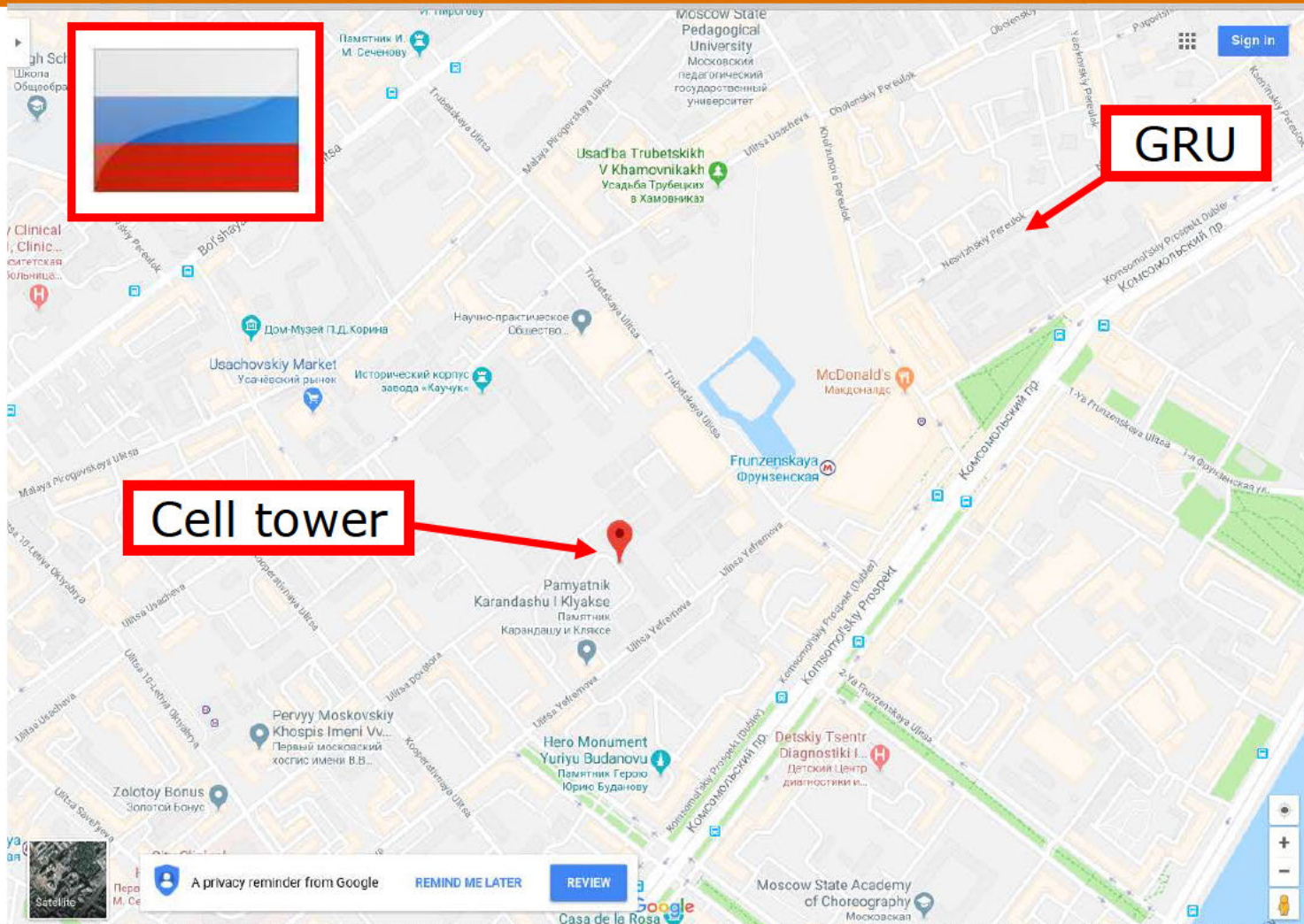
Locate devices without GPS, explore Mobile Operator coverage and more!



### Sony Xperia F3311

- Activated on 9 April, through cell tower in Moscow (GSM MCC: 250 MNC: 20 LAC: 27813 CID: 197679381)





**CID: 197679381**

- Nearest cell tower to known GRU barracks at Komsomolsky Prospekt 20, Moscow





ИП Шагинян Бениамин Нариманович  
 Адрес регистрации: 125252, г. Москва,  
 ул. 2-я Песчаная, д. 3, кв. 128 8-495-205-€3-39  
 ИНН 402900885858  
 ОГРНИП 313774628000948

**Квитанция ГР № 001832**  
 Дата выдачи "10" апреля 2018 г.

Откуда / Starting point  
 Несвижский переулоч

Куда / Point of destination  
 Аэропорт Шереметьево  
 терминал F

Показания таксометра

Пробег	32 км	Простой	—
Итого	842,00 руб.	Восемьсот сорок два рубля 00 коп.	

(сумма прописью)

Водитель подпись  
 Сидоров С.В.

Заказчик подпись  
 Моренц

М.П.

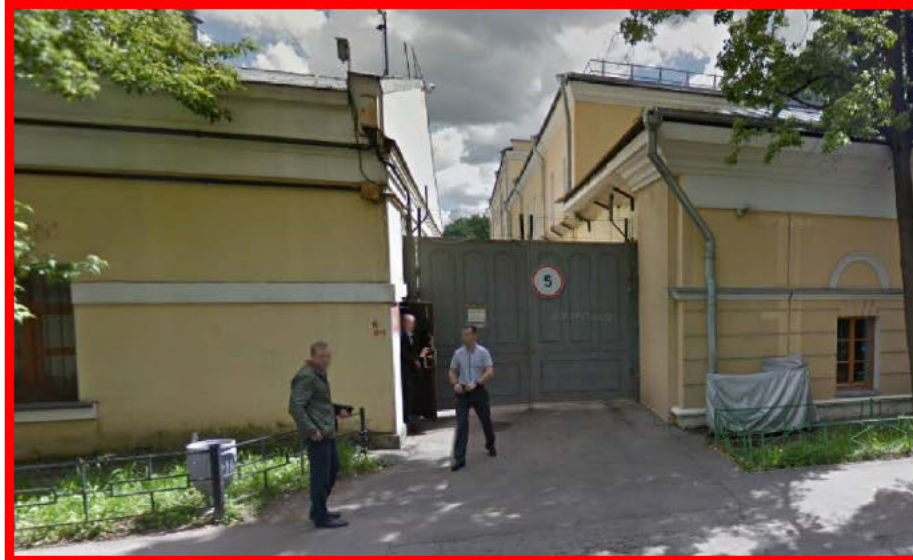
Опечатано ООО "01-Принт" www.print.ru Тел.: 737-72-40  
 115191, г. Москва, ул. Большая Тульская, д. 10, стр. 5 ИНН 772507046  
 Заг. № 1168259 Тираж 1800 штук



## MORENETS' taxi receipt

- From Nesvizhskiy Pereulok to Moscow Sheremetyevo airport
- Date: 10 April 2018

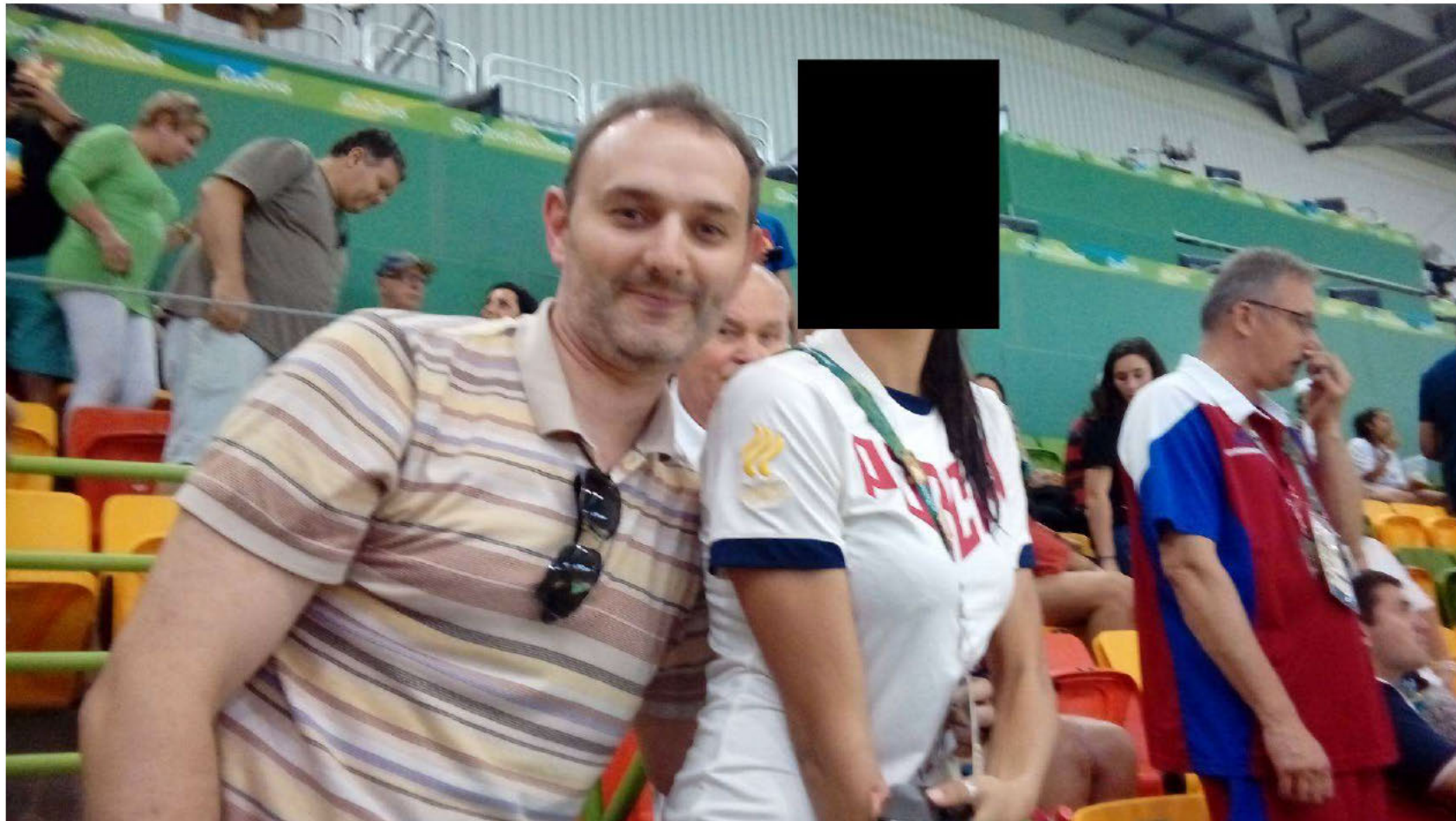




## Rear entrance of GRU barracks

- Opening onto Nesvizhskiy Pereulok





**Previous operations: photo on SEREBRIAKOV's laptop**

- 14 August 2016: Olympic Games in Brazil (picture above taken on 16.39, 14-08-2016 with LG-K350ds)





Network Name	Name Type	First Connect	Last Connected	Managed	DNS Suffix	Gateway Mac Address	Profile GUID	Location (LAT/LON)
Sheremetyevo Wi-Fi	Wireless	2016-09-17 19:10:57 +00:00	2016-09-17 19:10:57 +00:00	Unchecked	<о т с у т с т в у е т >	B4-E9-B0-C9-1E-40	{7D30FD49-1E32-4618-8278-AFF127C2F288}	Airport, Khimki, Russia
LP_Public	Wireless	2016-09-20 20:17:39 +00:00	2016-09-20 20:29:12 +00:00	Unchecked	lausanne-palace.net	00-90-0B-29-02-D7	{FC1F8A2C-7959-4C0A-AE0D-6ACAAA049420}	Lausanne, Switzerland
Hotel Alpha-Palmiers	Wireless	2016-09-20 21:26:51 +00:00	2016-09-22 08:59:34 +00:00	Unchecked	monzoon.net	00-1A-A2-9F-9C-AE	{7E6EC1D0-6B1A-467E-A81D-DFFFF2375E69}	Lausanne, Switzerland
GMKLhotel	Wireless	2017-12-16 03:21:01 +00:00	2017-12-22 12:39:21 +00:00	Unchecked	localdomain	90-E2-BA-58-ED-FB	{64746B9B-1E16-4366-AE08-38596037B691}	Kuala Lumpur, Malaysia
Palace-Hotel-Guests	Wireless	2018-04-10 22:58:44 +00:00	2018-04-12 09:53:14 +00:00	Unchecked	hotspot.internet-for-guests.com	D0-BF-9C-3A-66-B5	{2B8E00FF-9942-4818-A5B9-B0FC6DB523D2}	Noordwijk, Netherlands
Marriott_GUEST	Wireless	2018-04-12 19:08:00 +00:00	2018-04-13 14:12:52 +00:00	Unchecked	<о т с у т с т в у е т >	50-9A-4C-6A-F0-E5	{01E8FAC9-4419-4B38-80B9-9A9F896A5415}	The Hague, Netherlands

## Previous operations: WiFi connections made by SEREBRIAKOV's laptop

- Grand Millenium Hotel (Kuala Lumpur, Malaysia) from 16 to 22 December 2017;
- Alpha Palmiers Hotel (Lausanne, Switzerland) from 20 to 22 September 2016;
- Palace Hotel (Lausanne, Switzerland) on 20 September 2016.





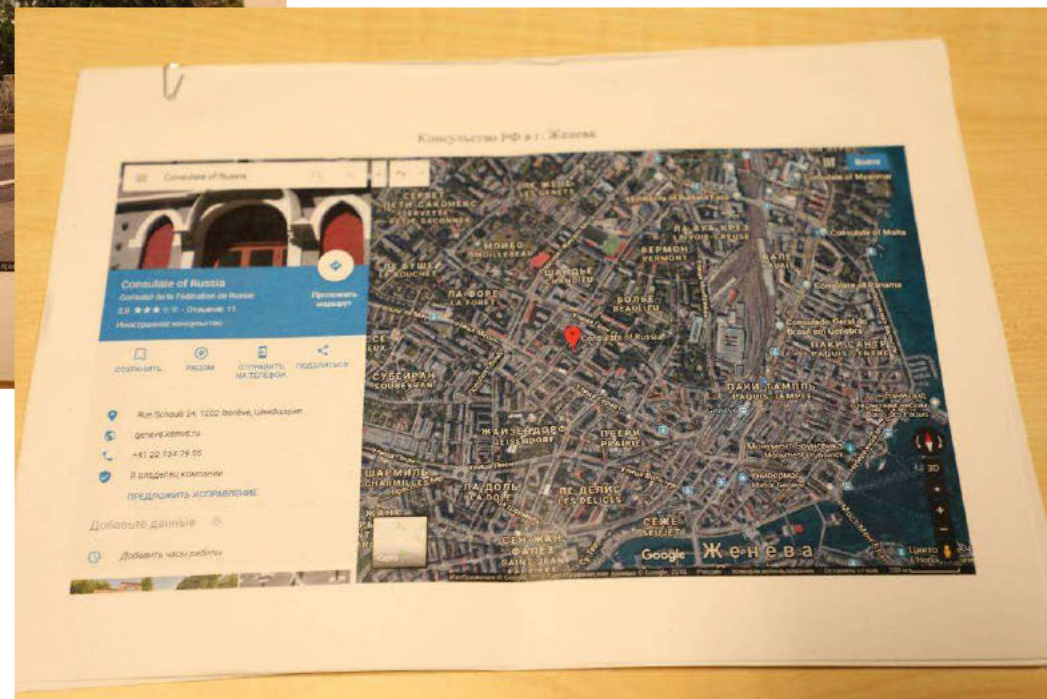
```
Opera web visits.csv:3274,https://www.google.ru/url?sa=t&rc=tj&q=&esrc=s&source=web&cd=1&ved=0ahUKew1r7eaA0azaAhwTY
Opera web visits.csv:3275,https://www.opcw.org/ru/09-04-2018 07:09:33,?????????????? ?? ?????????????? ?????????????? ??????
Opera web visits.csv:3561,https://www.opcw.org/ru/headadmin/OPCW/Fact_Sheets/Russian/Fact_Sheet_3_-_OPCW_Structure.pdf
Opera web visits.csv:3930,https://www.opcw.org/ru/headadmin/OPCW/Fact_Sheets/Russian/Fact_Sheet_3_-_OPCW_Structure.pdf
Opera web visits.csv:2999,https://www.google.ru/url?sa=t&rc=tj&q=&esrc=s&source=web&cd=1&ved=0ahUKewio7-7wxazaAhvsE
Opera web visits.csv:3000,https://www.labor-spiez.ch/09-04-2018 06:17:17,LABOR SPIEZ - SPIEZ LABORATORY,0,LINK,, "d
Opera web visits.csv:3001,https://www.labor-spiez.ch/enindex.htm,09-04-2018 06:18:16,LABOR SPIEZ - SPIEZ LABORATORY
Opera web visits.csv:3012,https://www.labor-spiez.ch/enindex.htm,09-04-2018 06:20:00,LABOR SPIEZ - SPIEZ LABORATORY
Opera web visits.csv:3028,http://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-t
Opera web visits.csv:3029,https://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-
Opera web visits.csv:3271,http://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-t
Opera web visits.csv:3272,https://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapon
Opera web visits.csv:3931,https://www.swissinfo.ch/eng/safety-assessment---_spiez-laboratory-aces-chemical-weapons-
Opera web visits.csv:3932,https://www.labor-spiez.ch/enindex.htm,09-04-2018 12:14:28,LABOR SPIEZ - SPIEZ LABORATORY
```

Austrasse, 3700 Spiez, Швейцария	09-04-2018 07:03:01
<a href="https://www.google.ru/maps/place/Austrasse,+3700+Spiez,+%D0%A8%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D0%B8%D1%8F/@46.6931311,7.6467636,19.05z/data=!4m5!3m4!1s0x478fad1ff520c9b:0xc55f8d818b681645!8m2!3d46.6913408!4d7.6432401?dcr=0">https://www.google.ru/maps/place/Austrasse,+3700+Spiez,+%D0%A8%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D0%B8%D1%8F/@46.6931311,7.6467636,19.05z/data=!4m5!3m4!1s0x478fad1ff520c9b:0xc55f8d818b681645!8m2!3d46.6913408!4d7.6432401?dcr=0</a>	09-04-2018 07:03:01
<a href="https://www.google.ru/maps/place/Austrasse,+3700+Spiez,+%D0%A8%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D0%B8%D1%8F/@46.6931311,7.6467636,19.03z/data=!4m5!3m4!1s0x478fad1ff520c9b:0xc55f8d818b681645!8m2!3d46.6913408!4d7.6432401?dcr=0">https://www.google.ru/maps/place/Austrasse,+3700+Spiez,+%D0%A8%D0%B2%D0%B5%D0%B9%D1%86%D0%B0%D1%80%D0%B8%D1%8F/@46.6931311,7.6467636,19.03z/data=!4m5!3m4!1s0x478fad1ff520c9b:0xc55f8d818b681645!8m2!3d46.6913408!4d7.6432401?dcr=0</a>	09-04-2018 07:03:01
<a href="https://www.google.ru/maps/@46.6931311,7.6467636,19.03z?dcr=0">https://www.google.ru/maps/@46.6931311,7.6467636,19.03z?dcr=0</a>	09-04-2018 07:03:07
hotels	09-04-2018 07:03:14
<a href="https://www.google.ru/maps/search/hotels/@46.6931311,7.6467636,19.03z?dcr=0">https://www.google.ru/maps/search/hotels/@46.6931311,7.6467636,19.03z?dcr=0</a>	09-04-2018 07:03:14

### Target: Spiez Laboratory

- Train tickets to Bern
- Online searches for Spiez laboratory
- Google-maps print-outs of Russian diplomatic facilities in Bern





## Google Maps print-outs

- Russian diplomatic facilities in Bern and Geneva





DNR: FCTDHXS ID:0

RESERVERING  
RESERVATION  
InterCityExpress

CIV 1184

0107 954536  
130418 11:37 AA0C CA CASH

Den Haag

NS International

Sotnikov, O  
04PERSONEN

AFREIS	VERTREK	AANKOMST	KLASSE
17/04	07:36	UTRECHT CENTRAAL -> BASEL SBB	1

TREIN 255 ICE RIJTUIG 39 ZITPLAATS

NIET ROKEN MET MIDDENGANG 02GANG 02RAAM

04 RESERVERING ALLEEN ICM EEN GELDIG VERVOERBEWIJS

849830087650 IR DNR:FCTDHXS Ref:

Den Haag 130418 11:37 CACASH 1/1

PRJIS: EUR \*\*\*\*\*0.00

Passagierslijst:

Naam	Voornaam
Sotnikov	O
Minin	A
Serebriakov	E
Morenets	A

## Train tickets to Switzerland

- Departure from Utrecht for Bern via Basel
- Planned date: 17 April 2018