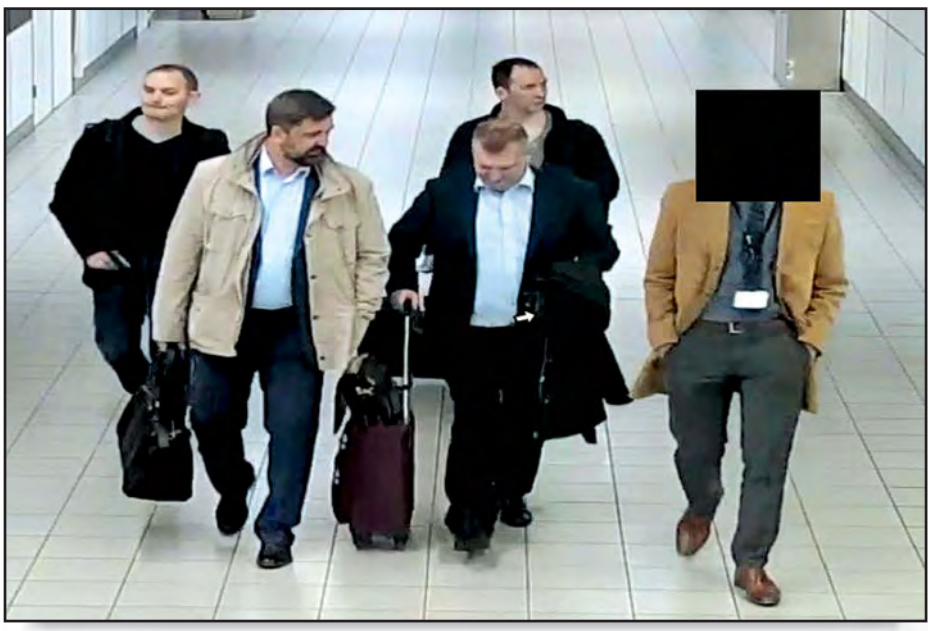
THE GRU CLEANERS

RUSSIA'S GLOBAL CYBER ATTACK UNITS EXPOSED IN JOINT MIVD-MI6 OPERATION

Dutch Intelligence supported by MI6 have foiled attempted GRU operations at the Hague and in Switzerland, both are relevant to Britain's investigation into the attempted assassination of former MI6 agent Sergei Skripal, in Salisbury, England on 4 March 2018.

At a joint Dutch-UK government news conference held in The Hague, officials and intelligence chiefs from Holland's MIVD (Military Intelligence and Security Service) revealed details of "brazen attempts" by Russia to manipulate international affairs. Much of the information revealed the extent of a GRU 'clean-up unit' despatched in April to help conceal Moscow's alleged involvement in the operation against Skripal, .

The Dutch accused the GRU of targeting the world's chemical weapons watchdog, the Organisation for the Prohibition of Chemical Weapons (OPCW), through a foiled cyber operation. The OPCW was working to independently verify the UK's analysis of the chemical used in the poisoning of the Skripals in Salisbury. The OPCW was also due to conduct analysis of a chemical weapons attack in Douma, Syria on 7 April.



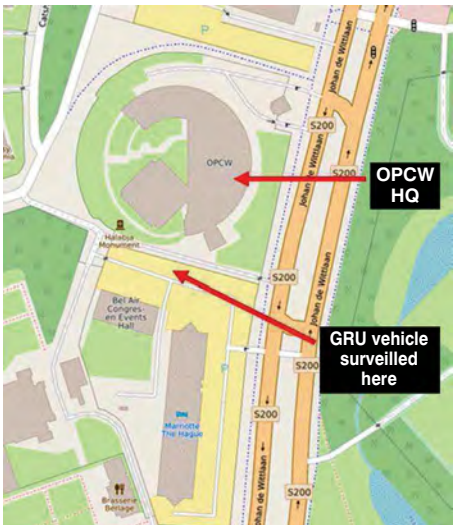
10 April 2018. The GRU team arrive at Amsterdam's Schiphol Airport and are greeted by a diplomat from Russia's Embassy in Holland

On Friday 13 April, Dutch authorities escorted four Russian intelligence officers out of the country just hours after the car they had rented was found parked near the OPCW's building in The Hague. Its boot was packed with equipment for hacking WiFi networks. A large antenna was also discovered concealed under a coat. The assembly was in operation targeting login details when security services, who had been surveilling the team, detained the GRU officers. One Russian operative attempted to destroy his cell phone, but it was to no avail. Analysis of the subsequent equipment, including computers, revealed a plethora of incriminating evidence that the team was operational, and had plans to visit another OPCW facility relevant to the Skripal investigation in Switzerland.

Passports of the four GRU operatives detained near the Hague

The four GRU officers had entered Holland on diplomatic passports, according to the Dutch

Major General Onno Eichelsheim, Director MIVD, addresses the media

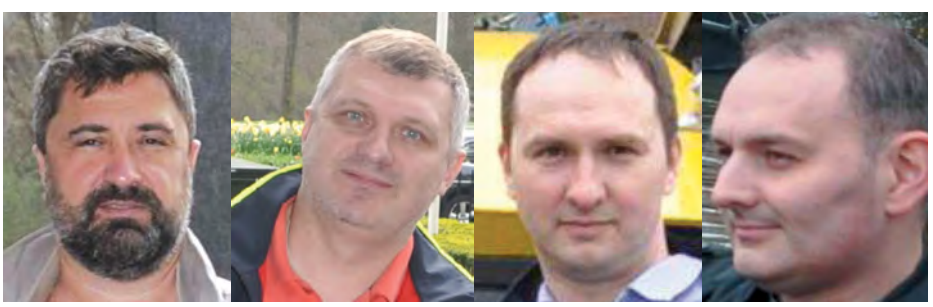


Location of rental vehicle and OPCW headquarters on 13 April

The rental vehicle used by the GRU operatives was packed with equipment capable of engaging with computer systems

Defense Ministry, which acknowledged British Intelligence had worked with the MIVD to disrupt the operation. The head of Dutch counter-intelligence, Major General Onno Eichelsheim, named the four Russian officers as Aleksei Morenets, Evgenii Serebriakov, Oleg Sotnikov and Alexey Minin. Eye Spy understands both GCHQ and the NSA helped to expose the attempted "cyber break-in."

UK Ambassador to The Netherlands Peter Wilson, supported by a diplomatic team was unequivocal in his condemnation of Russia: "This operation in The Hague by the GRU was not an isolated act. The Unit involved, known in the Russian military as Unit 26165 (also known as APT 28 and GRU 85 Main Special Service Centre), has sent officers around the world to conduct brazen close access cyber operations."



Alexey Minin, Oleg Sotnikov, Aleksei Morenets and Evgeni Serebriakov

OPCW HQ, The Hague

Reconnaissance photographs of the OPCW building found on Alexey Minin's camera taken on 11 April

Reconnaissance photographs of the OPCW building found on Alexey Minin's camera taken on 13 and 14 April

A confiscated laptop computer contained information that they planned to travel on to the OPCW designated laboratory - Spiez in Switzerland. This facility was analysing a sample of the Novichok nerve agent used in the Salisbury attack. In addition, investigators found out about their past activities, including a record of connecting to a WiFi network at a hotel in Lausanne, Switzerland, in September of 2016, as the World Anti-Doping Agency was holding a conference at the hotel. An Olympic Committee laptop was compromised, and the APT 28 malware infection that resulted spread widely, eventually compromising the IP addresses of the International Olympic Committee, Wilson said.

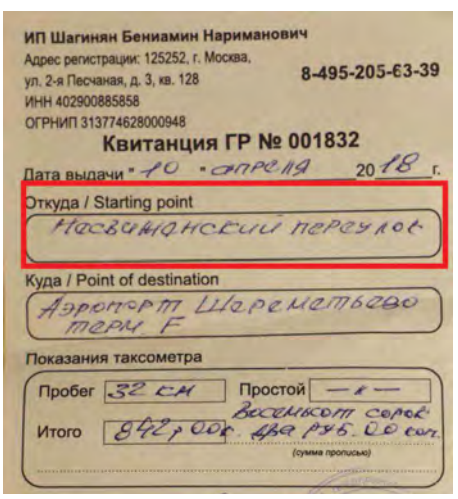
During the press briefing, officials also said the GRU had attempted to engage with computer systems at Porton Down, the UK's Defence Science and Technology Laboratory (Dstl), Wiltshire, which has been active in the investigation of the Novichok incident.

Wilson added: "One of the GRU team also conducted malign activity in Malaysia," in an operation that targeted the inquiry into Malaysia Airlines Flight MH17, the airliner that was shot down in eastern Ukraine on 17 July 2014, after being hit by a missile. Hours earlier, it had taken off from Amsterdam. This case is still under investigation, though intelligence watchers are satisfied the aircraft was brought down by a Russian-controlled Buk surface-to-air missile.

Various high-end specialist equipment was recovered from the rental vehicle

Ambassador Wilson concluded: "The GRU is an aggressive, well-funded, official body of the Russian State. It can no longer be allowed to act aggressively across the world, and against

UK Ambassador to The Netherlands Peter Wilson



ИП Шагинян Бениамин Нариманович
Адрес регистрации: 125252, г. Москва,
ул. 2-я Песчаная, д. 3, кв. 128
8-495-205-63-39
ИНН 402900885858
ОГРНИП 313774628000948

Квитанция ГР № 001832

Дата выдачи "10" апреля 2018 г.

Откуда / Starting point
Новинский переулок

Куда / Point of destination
Аэропорт Шереметьево терм. F

Показания таксометра

Пробег 32 км Простой —"—

Итого 842,00 Восемьсот сорок два руб. 00 коп.
(сумма прописью)

Taxi receipt found by the MIVD showing one of the operatives had travelled from the GRU HQ in Moscow to Moscow's Sheremetyevo Airport on 10 April

PUTIN PRIVATELY FURIOUS WITH GRU FOR EXPOSURE

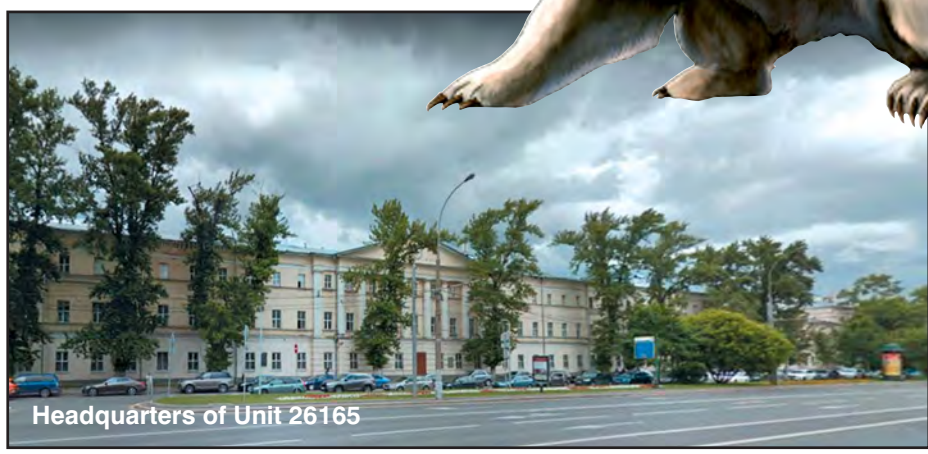
MOSCOW: The intelligence secured by the MIVD was described as "remarkable" by senior officials. Perhaps more extraordinary is the fact that British and Dutch Intelligence officials agreed to make much of it public. Amongst the treasure trove - documents revealing the GRU agents inadvertently exposed the identity of more than 300 colleagues, many still operational. Two of the men caught in The Hague used their real names on diplomatic passports - both registered as living at the GRU's Military Academy in Moscow.

Alexey Morenets' Lada vehicle is also registered at GRU's cyber warfare department - and investigators say by searching other vehicles registered to the same address they have identified an astonishing 305 other operatives of the 26165 unit accused of cyber attacks all over world.

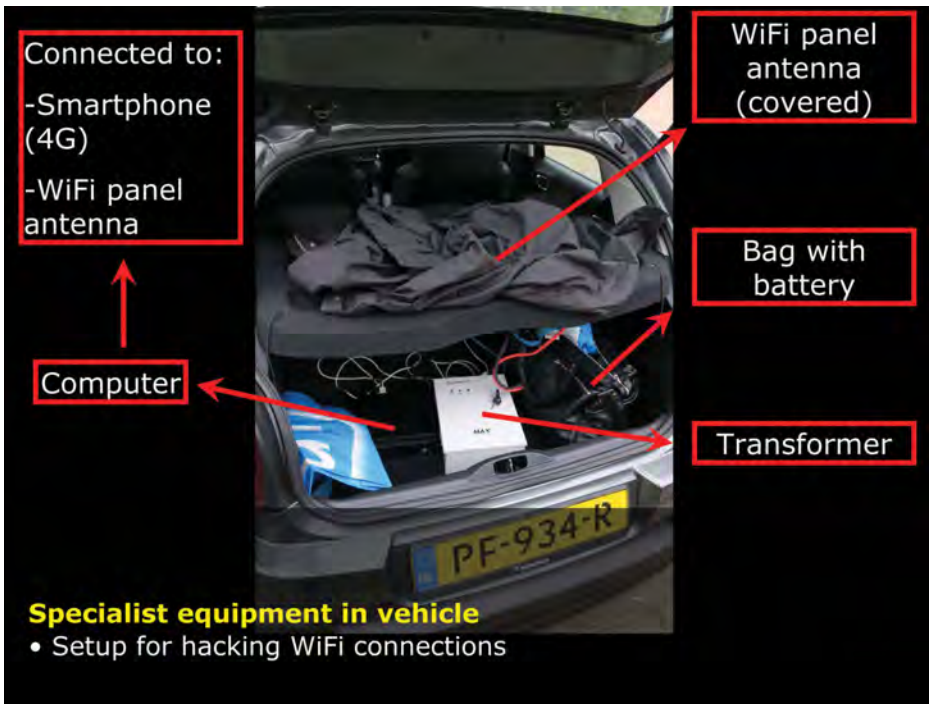
Perhaps more embarrassingly for Russian Intelligence, the lists are believed to contain authentic and accurate names, including birth dates and cell phone numbers. Some intelligence sources have already stated that following the failed April operation, a furious President Putin instructed senior officials to investigate the Hague debacle. Speculation is rife in Moscow that "repercussions" are imminent and some senior GRU officials may be purged.


GRU chief Igor Korobov

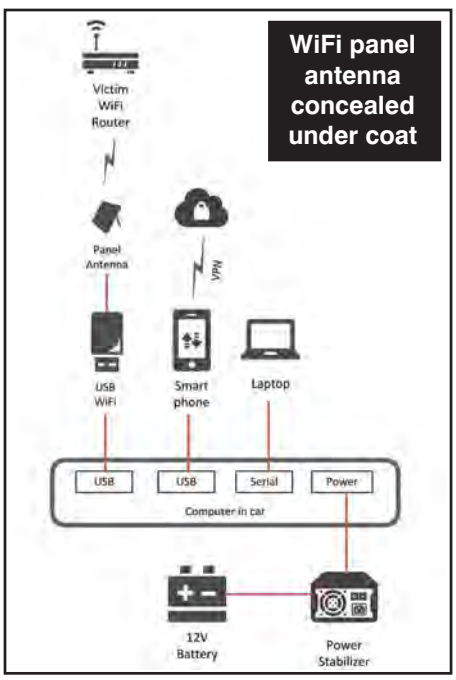

Dutch security personnel detain the GRU operatives. Right: Logo of the cyber hacking group Fancy Bear which is almost certainly a GRU outfit


Headquarters of Unit 26165

Incriminating web search data uncovered by the MIVD includes references to the Spiez Laboratory in Switzerland which was examining samples of the Novichok nerve agent used in the Salisbury attack



Holland's Defence Minister Ank Bijleveld-Schouten - she is responsible for the running and activities of the MIVD



The GRU cyber element was accused of attempting to engage with computer systems operated by Britain's Porton Down Defence Science and Technology Laboratory (Dstl)

vital international organisations, with apparent impunity. With its aggressive cyber campaigns, we see the GRU trying to clean up Russia's own mess... be it the doping uncovered by WADA (World Anti-Doping Agency) or the nerve agent identified by the OPCW.

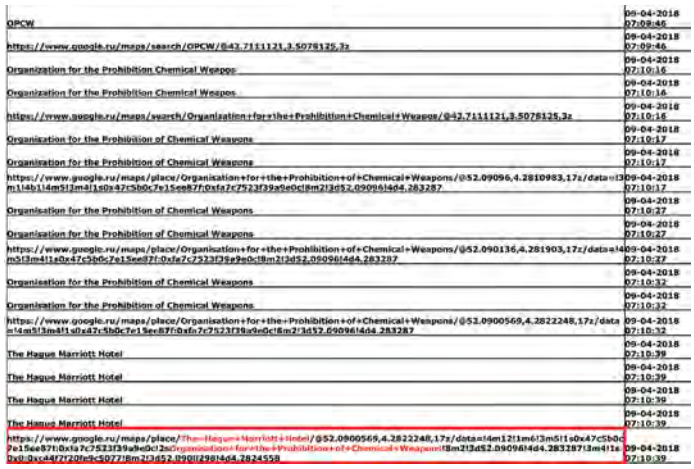
"The GRU is an aggressive, well-funded, official body of the Russian State. It can no longer be allowed to act aggressively across the world, and against vital international organisations, with apparent impunity.

"We are now stepping up our collective efforts against malign activity, and specifically against the GRU. We will increase further our understanding of what the GRU is doing, and attempting to do, in our countries. We will shine a light on their activities. We will expose their methods and we will share this with our allies. This includes strengthening international organisations, and working to protect other potential targets from further harm."

Holland's Defence Minister Ank Bijleveld-Schouten said: "By revealing this Russian action, we send out a clear message - Russia

Google Street Map print outs of Russian diplomatic missions in Bern and Geneva, Switzerland, found on the GRU team

Various cell phones and cameras recovered by the Dutch Intelligence service provided a plethora of information



A revealing image showing search records of OPCW headquarters found on Serebriakov's laptop computer

must stop this." Dutch officials defended their decision not to charge and prosecute the GRU team. Prime Minister Mark Rutte (left) said the men had been ejected immedi-

The GRU team was carrying 20,000 Euros and 20,000 Dollars in cash

The GRU team were careful not to leave any evidence at their hotel, including rubbish (above) found by the MIVD. However, it was the items discovered on their persons, electronic devices and in the hire vehicle that exposed their activities

As investigators detained the GRU team, one agent attempted to crush his cell phone

ately because it was "not a criminal inquiry." Intelligence officials backed the premier by stating that the evidence is sufficient to damage the reputation and hamper further operations attempted by one of Russia's leading spy agencies. Other officials said the operatives should have been charged.

THE AMERICAN RESPONSE

The Dutch decision not to prosecute the GRU team contrasts greatly to the actions taken by US law officials. Twelve men were recently indicted in the United States following the US 2016 General Election hacking by GRU units 26165 and 74455. The indictment describes the activities of each department in a way that generally suggests a division of labour, with Unit 26165 carrying out core hacking activities and Unit 74455 carrying out information operations.

US Assistant Attorney General for National Security John Demers said the attacks were "altering perceptions of the truth." Interestingly, four of the men indicted by the US, were also involved in the Hague OPCW operation to source information on Britain's Skripal investigation.

OPCW STATEMENT
GRU CYBER ATTACK

THE HAGUE: The Director-General of the Organisation for the Prohibition of Chemical Weapons (OPCW) was briefed by officials of the Ministry of Foreign Affairs of the Kingdom of the Netherlands about a cyber operation targeting the OPCW that was disrupted by the Netherlands Defence Intelligence and Security Service.

The Netherlands is the OPCW's host country and, as such, is in charge of ensuring and exercising due diligence in protecting the OPCW Headquarters. The OPCW thanks the Netherlands for its actions and will remain in contact in regards to any further developments.

The OPCW takes very seriously the security of its information systems and networks. Since early 2018, the Organisation has observed increased cyber-related activities. The Director-General has informed OPCW Member States about these activities and the OPCW Technical Secretariat has undertaken measures to mitigate them.

Director-General OPCW Ahmet Uzumcu

US Assistant Attorney General for National Security John Demers

THE RUSSIAN TWELVE

UNIT 26165

VIKTOR NETYKSHO: Commands Unit 26165

BORIS ANTONOV: Head of Department that oversees spear-phishing targeting

DMITRIY BADIN: Assistant Head of Department conducting spear-phishing targeting

IVAN YERMAKOV: Works for Antonov, uses identities Kate Milton, Kames McMorgans, Karen Millen. Hacked at least two email accounts the contents of which were released by DCLeaks. Helped hack DNC emails server released through WikiLeaks

ALEKSEY LUKASHEV: Senior Lieutenant in Antonov's department. Uses identities Den Katenberg, Yuliana Martynova. Sent spear-phishing emails to Clinton campaign, including one to John Podesta (head of 2016 campaign)

SERGEY MORGACHEV: Lieutenant Colonel who oversaw department that developed and managed X-Agent

NIKOLAY KOZACHEK: Lieutenant Captain. Used monikers including 'kazak' and 'blablabla1234565'. Developed, customised, and monitored X-Agent used to hack DCCC

PAVEL YERSHOV: Helped customise and text X-Agent before deployment against DCCC

ARTEM MALYSHEV: Second Lieutenant in Morgachev's department. Used handles 'djangomagicdev' and 'realblatr'. Monitored X-Agent implanted in DCCC and DNC servers

UNIT 74455

ALEKSANDR OSADCHUK: Colonel and commanding officer of 74455, which assisted in release of stolen documents through DCLeaks, Guccifer 2.0, and the publication of anti-Clinton propaganda on social media

ALEKSEY POTEMKIN: A supervisor responsible for administration of computer infrastructure used to assist in release in DCLeaks and Guccifer 2.0 documents

ANATOLIY KOVALEV: Assigned to 74455 involved in hacks of State Boards of Election

FBI Cyber Division Deputy Assistant Director Eric Welling discusses computer intrusion and related charges against seven Russian GRU officers as Western District of Pennsylvania US Attorney Scott W. Brady (left) and Royal Canadian Mounted Police Director General Mark Flynn look on

KREMLIN RESPONSE

Russia's response to the findings of British and American Intelligence was swift and uncompromising. Foreign Minister Sergey Lavrov dismissed reports that the GRU was involved in the attempted cyber operation at the Hague. He said the reports were a "conspiracy to "distract people from stark divisions between Western nations."

Mr Lavrov said: "They weren't hiding from anyone when they arrived at the airport, settled in a hotel and visited our embassy. They were detained without any explanation, denied a chance to contact our embassy in Holland and then asked to leave. It all looked like a misunderstanding." He said the four Russians were on a routine trip to the Hague. Lavrov also accused the Dutch authorities of using "loudspeaker diplomacy," instead over quiet diplomatic channels to address its concerns.

President Putin's spokesman Dmitry Peskov challenged the West to provide "specific information" also using official channels.

Relevant to the equipment discovered in the vehicle used by the GRU team, a report was circulated amongst Russian media. Russian intelligence officials said it was to be used to "test the resilience of the embassy's cyber counter-measures," and not against the OPCW.

The Kremlin has also rejected the FBI's impressive investigative findings.

An ironic meeting - Sergey Lavrov with Hillary Clinton at the 2011 Munich Security Conference. Just five years later Russia's cyber elements would engage in an operation that some believe derailed her ambition to become President of the United States