Remarks Minister of Defense, 4 October in The Hague

Check against delivery

Ladies and gentlemen of the national and international media:

Welcome.

Welcome also to the United Kingdom‘s Minister of State for Europe and the Americas, Sir Alan Duncan, who joins us today in connection with the joint nature of the intelligence operation we are about to share with you.

His presence is also an expression of the joint efforts of our two countries and other international partners to address the threats I will now inform you about.

We have invited you here today to describe how the Netherlands Defence Intelligence and Security Service, or DISS, disrupted a cyber operation conducted by the Russian military intelligence service – GRU – in the Netherlands.

On the 13th of April this year, DISS carried out an operation to disrupt a GRU operation targeting the Organisation for the Prohibition of Chemical Weapons – the OPCW – in The Hague.

General Eichelsheim will explain further details of the operation in a few moments.

The Dutch Cabinet considers it a matter of extreme concern that the Russian military intelligence GRU has targeted the OPCW with an operation aimed at undermining it. As a host country the Netherlands has the responsibility to protect organisations such as the OPCW, which are of fundamental importance to maintaining international law.

We have duly offered such protection.

The Netherlands Defence Intelligence and Security Service, or DISS, disrupted the Russian cyber operation and escorted the four Russian intelligence officers involved in the operation out of the country that same day, thus preventing OPCW systems from being hacked.

I am proud of DISS for the work it has carried out.

I would like to emphasise that cooperation played a major role in achieving this successful resolution.

Cooperation in the Netherlands…… but certainly also with our international intelligence partners.… sound international cooperation is crucial for tackling threats such as those posed by GRU.

A continued commitment to investing in international cooperation in the field of intelligence now and in the future is therefore crucial.

Ladies and gentlemen,

Since the operation conducted in April this year, the Netherlands has continued its intelligence investigation.

It has revealed that the laptop of one of the four Russian intelligence officers……indicates that he had previously been active in Brazil, Switzerland and Malaysia. General Eichelsheim and Sir Alan Duncan will elaborate on this in their presentations.

The activities of the GRU in Malaysia targeted the investigation into the shooting down of Malaysian Airlines flight MH17, an extremely sensitive subject for the Netherlands.

So let me reiterate what the Dutch authorities have said before, namely that all organisations involved in the MH17 investigation …
have long been aware of the Russian intelligence services' interest in this investigation and have implemented appropriate measures.

We are and will remain highly alert to such threats.

Ladies and gentlemen,

Today we will expose the GRU cyber operation in conjunction with our UK partners …and also with the US Department of Justice.

In August the US Department of Justice submitted a request for legal assistance to the Dutch Public Prosecutor's office in connection with a criminal investigation into Russian cyber operations …In response to this request the Public Prosecutor supplied information based on an official report by DISS, which clearly names the four men and describes their activities in great detail.

This afternoon the US Department of Justice will make a related announcement. This means that the details of our operation to disrupt the men's activities will be brought to public attention, and that is precisely why we have chosen this moment to expose the Russian cyber operation.

I am aware that exposing the GRU's cyber operation is a highly unusual step for the Netherlands to take, as is providing details of a Dutch counter-intelligence operation.

We do not normally do this.

Nonetheless, in collaboration with our international partners the Dutch government has decided to take this step in order to send a clear message to the Russian military intelligence service that it must put a stop to its undermining cyber operations.

By exposing the GRU's modus operandi we are hampering its operations and simultaneously boosting our own resilience.

This is why we have today taken the highly unusual step of publicly identifying these Russian intelligence officers. So bear with me for a moment as I invite DISS's director General Eichelsheim to provide you with the details of the DISS operation that disrupted the GRU's cyber operation in The Hague.

General…

Presentation general Eichelsheim

Thank you, Minister,

Ladies and gentlemen,

As the minister just informed you, at a quarter to five in the afternoon on 13 April 2018 my service disrupted an operation being conducted by a GRU team in the immediate vicinity of the OPCW offices in The Hague.

The GRU operation was focused on hacking into and infecting the OPCW's wifi network from close by in what is referred to as a close access hacking operation.

I will now guide you through our findings, which are based not only on our counter-intelligence operation but also on the data and equipment left behind by the GRU officers.

1. On 10 April four Russian individuals travelled from Moscow to Amsterdam Airport Schiphol on diplomatic passports. Over the course of the week DISS identified these persons as intelligence officers working for the Russian military intelligence service GRU. <**slide 2**>
2. At Schiphol Airport the Russian intelligence officers were escorted by an assistant employed by the Russian embassy, as you can see in this photo. <**slide 3**>
3. All four men were in possession of a diplomatic passport. <**slide 4**>.
4. They were 1. Aleksei MORENETS <**slide 5**>
5. Evgenii SEREBRIAKOV.
    a. Note that their passport numbers differ from each other by only one digit. <**slide 6**>
6. Oleg SOTNIKOV<**slide 7**>
7. Aleksey MININ <**slide 8**>
8. They subsequently rented a Citroen C3 from Wednesday 11 April to Monday 16 April <**slide 9**>

9. The rental agreement clearly shows that both SOTNIKOV and MININ were registered as the drivers of this vehicle <**slide 10**>
10. On Wednesday 11 April, the four GRU intelligence officers came to the attention of DISS in the course of its regular counter-intelligence activities, which are aimed at continually tracking the activities of state actors.
11. Based in part on intelligence supplied by a partner service, it became clear that they were reconnoitring in preparation for a close-access hacking operation. The technology they were using to conduct the operation was also revealed.
12. On 11 and 12 April we established that they were targeting the OPCW.
13. Photos produced by Minin's camera confirm this. <**slides 11, 12, 13, 14>**
14. On Friday 13 April the rental vehicle, a Citroen C3 with registration PF-934-R, was positioned in the car park of the Marriott Hotel in The Hague. <**slide 14**>

    The parking lot directly abuts the OPCW headquarters. <**slide 15**>

15. The back of the vehicle was positioned towards the OPCW building. <**slide 15**>
16. Set up in the boot of this hired car was specialist equipment intended to hack into wifi networks of the OPCW, to identify users and to intercept their log-in data. <**slide 16 and 17**>
17. The antenna for this equipment was oriented towards the OPCW headquarters and lay hidden under a jacket. <**slide 18**>
18. The Russians purchased the battery charger for their equipment in The Hague. <**slide 19**>

    The equipment was in operation on Friday afternoon.

In other words, it posed a direct threat to the OPCW's digital communication networks.

As an intelligence service, it is our task to prevent cyber operations such as this from succeeding.
We therefore disrupted the GRU operation **<slide 20>**
and escorted the four men out of the Netherlands,
thus protecting the OPCW and preventing serious damage.

…

Ladies and gentlemen,

What else do we know about these four GRU intelligence officers?

We have established that:

19. … their operational intelligence techniques included the use of a large number of separate telephones and other devices. <**slide 21**>…
20. … they attempted to evade surveillance and to disable their equipment after we disrupted their operation. <**slide 22**>
21. … they demonstrated a considerable degree of security awareness, for example by removing discarded items from their hotel room and disposing of them elsewhere. **<slide 23>**
22. … they travelled with an unusually large amount of cash. **<slide 24>**

23. … one of their laptops was used to research details of the OPCW, including its location. **<slide 25**>
24. … besides the specialist equipment found in the hire car, SEREBRIAKOV also had items in his backpack that could be added to the hacking equipment and used to infiltrate networks; these included a wifi pineapple, signal repeaters and various antennas. <**slide 26**>
25. … logs from some of the intelligence officers' phones indicated that the phones were initially activated on 9 April via a telephone tower in Moscow. <**slide 27**>
26. … this telephone tower was the one closest to a known GRU barracks, which is located at 20 Komsomolsky Prospekt. This is also the address of the GRU's 85th Main Special Service Centre, military unit 26165. <**slide 28**>
27. … one of the Russian intelligence officers, Aleksei MORENETS, was carrying a taxi receipt for his journey to the airport to catch his flight to Amsterdam on the morning of Tuesday 10 April. According to the receipt, the taxi collected him from a street named Nesvizhskiy pereulok. <**slide 29**>
28. … a back entrance to the GRU barracks at 20 Komsomolsky Prospekt gives onto Nesvizhskiy pereulok. <**slide 30**>
    … the GRU's 85th Main Special Service Centre is the same unit that was recently charged by the US in connection with its involvement in hacking into Democratic Party systems in 2016.
    … this same GRU unit was responsible for the digital espionage campaign known as APT28, or Fancy Bear. This morning, our UK colleagues attributed a number of cyber operations to this unit.

SEREBRIAKOV's laptop also contained indications of other cyber operations by this GRU unit.

29. For example, SEREBRIAKOV's laptop contained a photo of SEREBRIAKOV and a Russian athlete that was taken in Brazil during the August 2016 Olympic Games. <**slide 31**>

30. Log details from SEREBRIAKOV's laptop also show that he was in Lausanne, Switzerland in September 2016. <**slide 32**>

… The log details show further that SEREBRIAKOV was in Kuala Lumpur in December 2017, in a district that is home to many of the government organisations involved in the investigation into the crash of Malaysia Airlines flight MH17. Sir Alan Duncan will elaborate on this shortly.

31. … Further intelligence investigations reveal that the GRU intelligence officers were planning to travel from The Hague to Switzerland to carry out another cyber operation there. SEREBRIAKOV's laptop showed evidence of online research into an OPCW-accredited Swiss laboratory in Spiez that carries out chemical weapons investigations. <**slide 33**>
32. The intelligence officers also had printed images of Russian diplomatic facilities in Geneva and Bern. <**slide 34**>
33. Finally, the intelligence officers had purchased train tickets for a journey to Switzerland on Tuesday 17 April. <slide 35>

Ladies and gentlemen,

Digital manipulation and sabotage pose a serious threat that is not limited to countries beyond our borders. The GRU is also active here in the Netherlands, the site of many international organisations.
It is therefore vital that we continue to combat this threat.
We can only do so in close cooperation with our intelligence partners here in the Netherlands and our international partners. Today, once again, we have seen the crucial value of this cooperation.
…
I am incredibly proud of the people who have made this counter-intelligence operation possible.
…
I now invite the UK Minister of State for Europe and the Americas, Sir Alan Duncan, to speak.

Statement Sir Alan Duncan

…..

Closing remarks by the Minister of Defence

Thank you, Sir Alan Duncan.

Ladies and gentlemen,

In April 2018 a team of four Russian military intelligence officers targeted the offices of the OPCW in The Hague in a cyber operation.

This afternoon, the US Justice Ministry will make public its charges against a number of Russian intelligence officers.

The Dutch government is deeply concerned at the GRU's targeting of an international organisation such as the OPCW in a cyber operation.

The OPCW is situated within the borders of the Netherlands. As the host country, we bear a particular responsibility to ensure that the international organisations residing here are able to do their work safely and freely.

We fulfilled this responsibility by disrupting the GRU's cyber operation before it could inflict serious damage.

Today, the Netherlands and its international partners have shone a light on the undermining cyber operations that the GRU conducts.

By bringing these events to the attention of the general public, the Netherlands is issuing a clear signal to the Russian Federation that it must refrain from such actions.

Just now the Russian ambassador was summoned to the Ministry of Foreign Affairs and instructed as such.

We have today informed the EU, NATO and our other international partners of these unacceptable actions by the Russian Federation.

Together with our partners, we will continue our efforts to eliminate cyber threats such as this one.

-0-0-0-