Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW

On 13 April 2018, with support from the Netherlands General Intelligence and Security Service and UK counterparts, the Netherlands Defence Intelligence and Security Service (DISS) disrupted a cyber operation being carried out by a Russian military intelligence (GRU) team. The Russian operation had targeted the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague.

The 4 Russian intelligence officers at Schiphol Airport.
To conduct their operation, 4 Russian intelligence officers had set up specialised equipment in the vicinity of the OPCW offices and were preparing to hack into OPCW networks. As host country the Netherlands bears responsibility for ensuring the organisation’s security. In order to protect the security of the OPCW it therefore pre-empted the GRU operation and escorted the Russian intelligence officers out of the country.

“The cyber operation targeting the OPCW is unacceptable. Our exposure of this Russian operation is intended as an unambiguous message that the Russian Federation must refrain from such actions,” said Defence Minister Ank Bijleveld in her response. “The OPCW is a respected international institution representing 193 nations around the globe and was established to rid the world of chemical weapons. The Netherlands is responsible for protecting international organisations within its borders, and that is what we have done.”

**Equipment**

The 4 Russian intelligence officers entered the Netherlands via Schiphol Airport, travelling on diplomatic passports. They subsequently hired a car which they positioned in the parking lot of the Marriot Hotel in The Hague, which is adjacent to the OPCW offices.

Equipment was set up in the boot of the car with which the officers intended to hack into wifi networks and which was installed for the purpose of infiltrating the OPCW’s network. The antenna for this equipment lay hidden under a jacket on the rear shelf and the equipment was operational when DISS interrupted the operation.

“Digital manipulation and sabotage pose a serious threat. Today, we have shown that the ongoing threat posed by the GRU extends into the Netherlands to affect international organisations that have their offices here,” said the director of DISS, Major General Onno Eichelsheim. “It is therefore vitally important that we deflect this threat – which we did. I am proud of our intelligence personnel,” he concluded.

Further investigation revealed that one of the Russian intelligence officers operating in the Netherlands had also been active in Malaysia, targeting the investigation of the crash of Malaysia Airlines flight MH17. Bijleveld adds, “We had previously informed the Dutch House of Representatives of the Russian Federation’s interest in the MH17 investigation. As we stated earlier, manipulation and influencing are among the potential threats to the MH17 investigation. All of the organisations involved in the criminal investigation into the MH17 crash are aware of the digital threats that they face and have taken appropriate measures to address these threats.”

Only rarely are the findings of intelligence services brought to the attention of the public. The Cabinet has, in this case, taken the deliberate step of exposing this operation and, by extension, the Russian intelligence officers involved in it, since this will hamper any further attempts by them to operate internationally.

**Undermined**

“Any incident in which the integrity of international organisations is undermined is unacceptable,” stresses Bijleveld. “We have therefore summoned the Russian ambassador to remind him of this.” The Netherlands
shares the concerns of other international partners regarding the damaging and undermining the GRU’s actions. It supports the conclusion, presented today by the UK, that GRU cyber operations such as this one undermine the international rule of law.

Today, the US publicly brings charges against a number of Russian intelligence officers. On 6 August 2018 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 unauthorised Russian cyber operations. In response to this request, the Public Prosecutor supplied information based on an official report by DISS as well as launching its own investigation.

Downloads

› Disruption of a GRU cyber operation in The Hague

Letter of 4 October 2018 from the Minister of Defence Ank Bijleveld-Schouten, Minister of Foreign Affairs Stef Blok and ...

Parliamentary document | 04-10-2018

See also

› Russian cyber operation disrupted
› Cyber security