Ministerie van Defensie

Ministerie van Defensie

Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

>RetouradresPostbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Plein 2
2511 CR Den Haag

Onze referentie
2018024323

Bij beantwoording datum, onze referentie en betreft vermelden.

Datum 4 oktober 2018
Betreft Disruption of a GRU cyber operation in The Hague

On behalf of the Minister for Foreign Affairs, the Minister for Justice and Security and others, I am writing to inform you regarding a cyber operation orchestrated in The Hague by the Russian military intelligence service (GRU). Together with the director of the Netherlands Defence Intelligence and Security Service (DISS) and the Ambassador to the United Kingdom, I presented a press conference on this topic today. Initially I would have been accompanied by the UK's Minister of State for Europe and the Americas, but unfortunately the minister was not able to attend due to the cancelling of his flight.

With support from the Netherlands General Intelligence and Security Service (GISS), DISS disrupted a GRU cyber operation in The Hague on Friday 13 April 2018 which targeted the international Organisation for the Prohibition of Chemical Weapons (OPCW). Russian intelligence officers had moved to a location close to the OPCW headquarters in The Hague and were making preparations to hack into OPCW networks. The officers were in possession of specialist equipment with which to intercept and manipulate wifi traffic. In order to protect the integrity of the OPCW, DISS pre-empted the GRU cyber operation and escorted the Russian intelligence officers out of the Netherlands that same day. DISS is currently investigating the equipment that the intelligence officers left behind in the Netherlands.

The investigation of this equipment has revealed that it has also been in active use in Brazil, Switzerland and Malaysia. As discussed in the press conference by the UK Minister of State, one of the Russian intelligence officers involved in this operation in the Netherlands was also actively involved in a GRU operation

focusing on Malaysia's investigation of the crash of Malaysia Airlines flight MH17. As the Dutch House of Representatives has been informed, the Russian Federation takes a particular interest in certain dossiers and political and other processes, and these therefore entail a conceivable risk of manipulation and influencing. One of these dossiers is the one pertaining to flight MH17 (Parliamentary Paper 26643, No. 496). The organisations involved in the criminal investigation into the crash and the claim for liability against the Russian Federation are aware of potential digital threats and have taken appropriate measures against such threats. Together with its partners, the Dutch Public Prosecutor, as part of the Joint Investigation Team, will continue its criminal investigation into the shooting down of flight MH17.

Bringing the concrete findings of intelligence services into the public arena is an unusual step. However, the Cabinet has come to the deliberate decision to expose this operation and, by extension, the Russian intelligence officers involved in it, since this will hamper any further attempts at international operations. Undermining the integrity of an international organisation is an unacceptable activity, and as a host country the Netherland bears the particular responsibility of ensuring that international organisations can carry out their duties both freely and safely. This is the message that will be imparted today to the Russian Federation's chargé to the Netherlands after having been summoned to the Ministry of Foreign Affairs. Furthermore, the Netherlands will address the undermining nature of the Russian military intelligence service in the forums of its international partnerships, which include the EU and NATO.

The Netherlands shares the concerns of its international partners with regard to the GRU's damaging and undermining activities in the digital domain. Moreover, the Netherlands supports the conclusion that the UK has presented today, which is that GRU cyber operations such as this one are at odds with the international rule of law. This development is in line with the threat assessment set out by the annual reports of DISS and GISS and in the Cyber Security Picture for the Netherlands, as well as with the pattern set out in earlier findings by the UK. State actors are shifting their focus increasingly towards digital espionage, and they constitute the greatest threat to digital security in the Netherlands.

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.

By bringing this operation to public attention, the Cabinet wishes to make clear that the actors behind cyber attacks such as this will no longer be able to operate with impunity. As set out in the Netherlands Cyber Security Agenda and the Integrated Foreign and Security Strategy, the threat posed by cyber operations requires a clear national and international response. In the interest of national security, the Cabinet has allocated additional resources to bodies including the National Cyber Security Centre and to the intelligence and security services. The Netherlands is committed to maintaining international agreements entered into on the basis of international law and to investing in cyber capabilities with which

to promptly detect and robustly deflect cyber threats and to take appropriate measures in response, all with a view to preventing cyber attacks.

MINISTER OF DEFENCE

A.Th.B. Bijleveld-Schouten