Statements betreffende de verstoring van een cyberoperatie van de GRU door de MIVD op 4 oktober in Den Haag

Let op: Alleen gesproken woord geldt!

Ladies and gentlemen of the national and international media:

Welcome.

Welcome also to the United Kingdom's ambassador Peter Wilson, 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.

Please allow me to continue in Dutch…

Het Nederlandse kabinet vindt het zeer zorgelijk dat de OPCW doelwit is van ondermijning door de Russische militaire inlichtingendienst.
Als gastland heeft Nederland de taak om organisaties als de OPCW - van fundamenteel belang voor de internationale rechtsorde - te beschermen.

Die bescherming hebben we dan ook geboden.

De MIVD heeft de cyberoperatie verstoord en de vier betrokken Russische inlichtingenofficieren zijn nog dezelfde dag het land uit begeleid.

Hierdoor is voorkomen dat de systemen van de OPCW zijn gehackt.

Ik ben trots op de MIVD voor hun werk.

Ik wil benadrukken dat samenwerking bij dit succes een grote rol heeft gespeeld.

Samenwerking in Nederland…
… maar zeker ook samenwerking met onze internationale inlichtingenpartners…
…goede internationale samenwerking is cruciaal bij het aanpakken van dreigingen als de GRU.

Het laat ook zien hoe belangrijk het is dat we nu en in de toekomst blijven investeren in de internationale samenwerking op het gebied van inlichtingen.

Dames en heren,

Sinds de verstoring in april heeft Nederland het inlichtingenonderzoek voortgezet.

Dit nadere onderzoek heeft uitgewezen dat de laptop van één van de vier Russische inlichtingenofficieren…
…eerder ook verbindingen heeft gemaakt in Brazilië, Zwitserland en Maleisië.
Zowel generaal Eichelsheim als ambassadeur Wilson zullen hier in hun presentaties verder op in gaan.

De activiteit van de GRU in Maleisië was gericht op het MH17-onderzoek.

Dit is voor Nederland uiteraard een heel gevoelige kwestie.

Laat ik daarom herhalen wat de Nederlandse autoriteiten eerder hebben gezegd: álle organisaties die betrokken zijn bij het MH17-onderzoek…
…zijn zich al langer bewust van de interesse van Russische inlichtingendiensten in dit onderzoek en hebben gepaste maatregelen genomen.

Wij zijn en blijven zeer alert op dergelijke dreigingen.

Dames en heren,

Wij maken deze GRU-cyberoperatie vandaag openbaar samen met onze Britse partners…
…Maar ook samen met het Amerikaanse *Department of Justice*.

In augustus heeft de Amerikaanse justitie in het kader van een strafrechtelijk onderzoek naar Russische cyberoperaties…
…een rechtshulpverzoek ingediend bij het Nederlandse Openbaar Ministerie.
Het OM heeft informatie aan de VS verstrekt, gebaseerd op een ambtsbericht van de MIVD.
In dit ambtsbericht hebben we klip en klaar de vier mannen benoemd en uitgebreid hun acties beschreven.
Het Amerikaanse *Department of Justice* zal de aanklacht vanmiddag openbaar maken en op een persconferentie verdere details verstrekken.
Dit betekent dat de details van de verstoring in de openbaarheid komen.
Dat verklaart ook waarom we nu in de openbaarheid treden.

Ik ben me ervan bewust dat het onthullen van deze cyberoperatie door de GRU een buitengewone stap is voor Nederland.
Dat geldt ook voor het verstrekken van details over een Nederlandse contra-inlichtingenoperatie.

Wij doen dat normaal niet.

Toch heeft de Nederlandse regering, samen met internationale partners, besloten deze stap te zetten…
Wij geven hiermee een duidelijke boodschap af: dat de Russische militaire inlichtingendienst moet stoppen met deze ondermijnende cyberoperaties.

Met het onthullen van de werkwijze van de GRU maken we het de GRU moeilijker en vergroten we tegelijkertijd onze eigen weerbaarheid.

Dat is de reden dat wij vandaag de buitengewone stap nemen om deze Russische inlichtingenofficieren publiekelijk te identificeren. U gaat dat zo zien.

Ik nodig nu generaal Eichelsheim, de directeur van de MIVD, uit om u te voorzien van de details van de verstoring van de cyber operatie van de GRU in Den Haag.

Generaal…

Presentatie generaal Eichelsheim

Dank u, excellentie,
Dames en heren,

Zoals zojuist uiteengezet door de minister heeft mijn dienst op 13 april om kwart voor vijf in de middag een operatie verstoord van een team van de GRU in Den Haag…
…naast het gebouw van de OPCW.

De GRU-operatie was erop gericht om van korte afstand het WiFi-netwerk van de OPCW te hacken en te infecteren.
Een zogenaamde '*close access hack operatie'*.

Ik wil u stapsgewijs meenemen door onze bevindingen.
Deze bevindingen zijn gebaseerd op onze contra-inlichtingenoperatie maar ook op de gegevens en de apparatuur die zijn achtergelaten door de GRU-officieren.

1. Op 10 april reisden vier Russische personen op een diplomatiek paspoort van Moskou naar Amsterdam Schiphol. Gedurende deze week heeft de MIVD deze personen geïdentificeerd als inlichtingenofficieren van de Russische militaire inlichtingendienst GRU
2. Op Schiphol werden de Russische inlichtingenofficieren begeleid door een assistent van de Russische ambassade, zoals u hier op deze foto kunt zien.
3. Alle vier de inlichtingenofficieren waren in bezit van een diplomatiek paspoort .
4. Het betreft: 1. Aleksei MORENETS
5. Evgenii SEREBRIAKOV.
    a. Merk hierbij op dat hun paspoorten maar twee cijfers van elkaar verschillen
6. Oleg SOTNIKOV
7. Aleksey MININ
8. Zij huurden een Citroen C3 vanaf woensdag 11 April tot maandag 16 April
9. De huurovereenkomst laat duidelijk zien dat zowel SOTNIKOV als MININ als chauffeur geregistreerd waren voor dit voertuig.
10. Op woensdag 11 april kreeg de MIVD door regulier contra-inlichtingenwerk – waarmee we voortdurend zicht willen houden op de activiteiten van statelijke actoren - deze vier GRU inlichtingenofficieren in het vizier.
11. Mede op basis van inlichtingen van een partnerdienst werd duidelijk dat zij bezig waren met verkenningen voor een *close-acces-hack operatie*. De techniek die zij daarvoor konden inzetten werd ook duidelijk.
12. In de dagen 11 en 12 april werd duidelijk dat zij hun focus richten op de OPCW.
13. Beelden van de camera van Minin bevestigen dit ook.
14. Op vrijdag 13 april stond de gehuurde Citroen C3 met kenteken PF-934-R geparkeerd op de parkeerplaats van het Marriott Hotel in Den Haag.

    Dit parkeerterrein grenst direct aan het hoofdkantoor van de OPCW.

15. De achterkant van het voertuig was gericht op het OPCW gebouw.
16. In de kofferbak van deze huurauto zat specialistische apparatuur, bedoeld om via WiFi-verbindingen het OPCW netwerk te hacken, gebruikers te identificeren en hun inloggegevens te onderscheppen.
17. De antenne van deze opstelling was bedekt met een jas en gericht op het OPCW hoofdkwartier
18. De benodigde acculader hebben de Russen hier in Den Haag gekocht.

    De opstelling was actief vrijdagmiddag.

Er was dus sprake van een directe dreiging tegen de digitale communicatienetwerken van de OPCW.

Onze taak als inlichtingendienst is voorkomen dat dergelijke cyberoperaties slagen.

We hebben daarom de GRU-operatie verstoord.

De vier heren zijn het land uit begeleid.

Hierdoor hebben we de OPCW beschermd en ernstige schade voorkomen.

Dames en heren,

Wat weten we nog meer over deze vier GRU-inlichtingenofficieren?

We hebben vastgesteld dat:

19. …zij operationele inlichtingentechnieken toepasten, zoals het gebruiken van een grote hoeveelheid verschillende telefoons en andere *devices*.
20. … zij probeerden surveillance te voorkomen en hun apparatuur onbruikbaar probeerden te maken nadat wij ze verstoord hadden
21. … zij een groot veiligheidsbewustzijn hadden en bijvoorbeeld hun afval meenamen van hun hotelkamer om dit elders weg te gooien.
22. … ze een ongebruikelijk grote hoeveelheid cash geld bij zich hadden.
23. … op één van hun laptops zoekslagen waren uitgevoerd naar de OPCW en de locatie van de OPCW

24. … naast de specialistische apparatuur die in de huurauto was opgesteld droeg SEREBRIAKOV in zijn rugtas accessoires die aan de WiFi hackingopstelling kon worden toegevoegd en gebruikt kon worden om netwerken binnen te dringen, zoals een wifi pineapple, signaalversterkers en diverse antennes.
25. …logging van sommige van hun telefoons liet zien dat deze voor het eerst geactiveerd zijn via een telefoonmast in Moskou op 9 april.
26. … Dit bleek de dichtstbijzijnde telefoonmast bij een bekende GRU-kazerne te zijn, namelijk op Komsomolsky Prospekt 20. Op dit adres is het 85th Main Special Service Center gevestigd, met militair veldpostnummer 26165.
27. … Eén van de Russische inlichtingenofficieren, Aleksei MORENETS, had een taxibonnetje bij zich voor een rit naar het vliegveld voor zijn vlucht naar Amsterdam op dinsdagochtend 10 april. Dit bonnetje laat zien dat hij is opgepikt van een straat genaamd Nesvizhskiy pereulok.
28. … Aan de straat Nesvizhskiy pereulok zit een een achteruitgang van de eerder genoemde GRU-kazerne op Komsomolsky Prospekt 20

    … Het genoemde 85e Main Special Service Center van de GRU is dezelfde eenheid die recent is aangeklaagd in de Verenigde Staten voor zijn betrokkenheid bij het hacken van de Democratische Partij in 2016.
    … Dit is dezelfde GRU-eenheid die verantwoordelijk is voor de digitale spionagecampagne die bekend staat als APT28 of Fancy Bear, aan wie onze Britse collega's vanochtend een aantal cyberoperaties hebben toegerekend.

De laptop van SEREBRIAKOV wijst ook op andere cyber operaties door deze GRU-eenheid.

29. De laptop van SEREBRIAKOV bevatte bijvoorbeeld een foto van SEREBRIAKOV met een Russische atlete die genomen is in Brazilië ten tijde van de Olympische Spelen in augustus 2016.
30. Ook laat de logging van SEREBRIAKOV's laptop zien dat SEREBRIAKOV aanwezig was in Lausanne, Zwitserland in September 2016.

… Daarnaast laat de logging ook zien dat SEREBRIAKOV in december 2017 aanwezig was in het district van Kuala Lumpur waar veel overheidsorganisaties gevestigd zijn die te maken hebben met het MH17-onderzoek. Sir Alan Duncan zal hier zo dadelijk meer over vertellen.

31. … Verder heeft het nadere inlichtingenonderzoek uitgewezen dat de GRU-inlichtingenofficieren van plan waren om van Den Haag naar Zwitserland door te reizen, om daar een andere cyberoperatie uit te voeren. De laptop van SEREBRIAKOV bevatte online zoekslagen naar het door de OPCW-geaccrediteerde Zwitserse laboratorium in Spiez, dat onderzoek doet naar chemische strijdmiddelen.
32. De inlichtingenofficieren hadden ook geprinte afbeeldingen bij zich van Russische diplomatieke faciliteiten in Genève en Bern.
33. Tot slot hebben de inlichtingenofficieren treintickets gekocht voor een reis naar Zwitserland op dinsdag 17 april.

Dames en heren,

Digitale manipulatie en sabotage vormen een serieuze dreiging. Deze dreiging speelt zich niet alleen ver van ons bed af. De GRU is ook hier in Nederland, met al zijn internationale organisaties, actief.
Het is belangrijk dat we deze dreiging blijven bestrijden.
Dat kan alleen in nauwe samenwerking met onze inlichtingenpartners, zowel nationaal als internationaal.
Het grote belang van die samenwerking is vandaag opnieuw aangetoond.
…
En ik ben echt super trots op mijn mensen die deze contra-inlichtingenoperatie mogelijk hebben gemaakt.
…
Dan geef ik nu graag het woord aan ambassadeur Peter Wilson.

Statement ambassadeur Peter Wilson

Conclusie minister van Defensie

Thank you ambassador Wilson,

Dames en heren,

Een team van vier Russische militaire inlichtingen officieren heeft afgelopen april het OPCW in Den Haag als doelwit gekozen voor een cyber operatie.

Het Amerikaanse ministerie van Justitie maakt vanmiddag een aanklacht openbaar tegen diverse Russische inlichtingenofficieren.

De Nederlandse regering vindt het zeer zorgelijk dat de OPCW, een internationale organisatie, doelwit was van deze cyberoperatie door de GRU.
Het OPCW is gevestigd op Nederlands grondgebied.

Als gastland hebben wij een speciale verantwoordelijkheid om internationale organisaties vrij en veilig hun werk te kunnen laten doen.

Die verantwoordelijkheid hebben we genomen.

We hebben de cyber operatie verstoord voordat de GRU grote schade kon toebrengen.

Vandaag zet Nederland samen met internationale partners de schijnwerper op deze ondermijnende cyberoperaties van de GRU.

Door hiermee naar buiten te treden geeft Nederland een duidelijk signaal af: Rusland moet hiermee ophouden.

De Russische ambassadeur is zojuist ontboden bij het ministerie van Buitenlandse Zaken om hem deze boodschap over te brengen.

Vandaag worden onze internationale partners in de EU en NAVO en daarbuiten geïnformeerd over deze onacceptabele actie.

Met deze partners werken we samen om cyberdreigingen als deze een halt toe te roepen.

-0-0-0-