Surveillance deel 1
start operatie - diensten

LIMC

LAND INFORMATION MANOEUVRE CENTRE

Koninklijke Landmacht

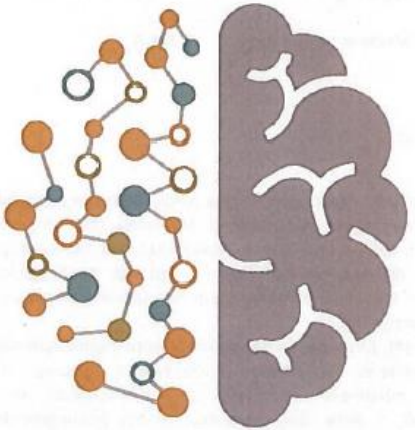
COVID-19

LIMC update XX

31 03 2020 - XX

Koninklijke Landmacht

LIMC



LIMC

LAND INFORMATION MANOEUVRE CENTRE

Informatierapport

Verwachting IC bezetting covid-19
met behulp van *Artificial Intelligence* (AI)

27 juli 2020

WHO WE ARE

- Het LIMC genereert in een **experimentele** vorm **situational awareness (SA)** en **situational understanding (SU)** voor het CLAS en civiele overheden over de COVID-19 crisis. Hierdoor worden militaire en civiele besluitvormingsprocessen gevoed met **inzicht** en waar mogelijk **handelingsperspectief**.

- Met het LIMC kan de Koninklijke Landmacht **ervaring opdoen** met het samenbrengen van **information manoeuvre** capaciteiten die insight, foresight en doorlopend handelingsperspectief bieden in drie dimensies (cognitief, virtueel en fysiek).

LIMC

CCIR

(DV) Druk op de Nederlandse voedselbanken neemt op middellange termijn waarschijnlijk toe

(DV) Gezien het toenemend aantal WW- en bijstandsuitkeringen is het mogelijk dat de stijgende trend in hulpaanvragen van mensen bij de voedselbanken, zal doorzetten. Ten gevolge daarvan is het waarschijnlijk dat de vraag naar ondersteuning van de voedselbanken zal toenemen. Het is mogelijk dat deze ondersteuning bij defensie wordt gezocht.

(DV) Meerdere voedselbanken in Nederland melden dat het aantal mensen dat gebruik maakt van de voedselbanken in het afgelopen kwartaal sterk is gestegen. Vergeleken met eind 2019 is er gemiddeld een stijging van 5% van mensen die geholpen worden, met regionale percentages die variëren tussen de 5% en 32%. Dit betekent dat er wekelijks 5.000 mensen meer geholpen worden ten opzichte van eind 2019. Op dit moment helpen de voedselbanken in totaal 93.000 mensen. Er zijn meerdere redenen voor deze toename.

(Vervolg op volgende pagina)

VOEDSELBANKEN.NL

Het LIMC is een experimentele capaciteit die is opgezet bij de start van de Coronacrisis om, binnen de wettelijke kaders, het TOC te voorzien van Situational Awareness en Understanding. Dit LIMC tracht op basis van open bronnen en met gebruik van rudimentaire datascience, binnen wettelijke kaders (WIV/AVG), een beter begrip en inzicht te verzorgen. Dit inzicht draagt vervolgens bij aan handelingsperspectieven. Tevens is het LIMC al experimenterend steeds beter in staat om beperkte

forecasting te doen. De combinatie van analyse capaciteit, gedragswetenschap en datascience leiden tot andere en vaak opmerkelijke inzichten. De producten van het LIMC werden dagelijks gebruikt in het TOC en werden gedeeld met het LOTC. Daarnaast maken zij een wekelijks rapportage over bepaalde trends en duiden deze in een scenario/narratief. Dit is gerelateerd aan COVID en daarmee samenhangende gebeurtenissen waaronder een duiding van nep informatie (zoals relatie COVID en 5G).

Een MSOB vanuit NCTV waarbij de opgedane kennis van het LIMC gebruikt wordt door het civiel gezag- en deze capaciteit zich verder kan ontwikkelen- Art 11 , om beleidsmatige redenen niet in behandeling genomen. Ik hoor vanuit de wandelgangen Art 11 . Laat ik vooropstellen dat de producten die het LIMC nu wekelijks levert resultaten zijn van een lerende experimentele capaciteit. Dat deze binnen strikte wettelijk kaders tot stand komen en dat deze producten veel waardering krijgen.

Opbouw LIMC

- Analyse cel: desinformatie – MSOB → NCTV, OM, NP
  - Social media monitoring (binnen grenzen van de wet)
  - Data mining & cleansing
    - Voor partners zoals NCTV, LOTC, NP etc.
  - Software engineering / programming (ICT/IM initieel beheer)

Opmerking [redacted]: "we hebben geen bevoegdheid, dus we leggen het terug bij NCTV, NP of anders"

Vragen vanuit Nationale Politie

- Houden jullie je aan de kaders van de wet? : "Ja, we slaan dus geen persoonsgegevens op. Bedoeling is dat de NCTV mandaat verstrekt om in samenwerking de gegevens te verzamelen en op te slaan. We monitoren de groei van een Facebook Groep, wat niet specifiek ziet op een individu"
- Vanuit de politie bestond de verwachting dat defensie een taakstelling had of zou krijgen om ondergrondse (digitale) vijand preventief tegen te gaan, maar concludeert dat deze taak er nog niet ligt. Waarom? [redacted] "de vraag is wat onder ondergronds oorlog voeren valt, waardoor er een grey zone ontstaat voorafgaand aan het conflict. Er bestaat een mogelijkheid om in het voortraject onderzoek te doen naar informatiestromen en prikkels en daarop data-analyses los te laten. Op dit moment is dit in het kader van COVID-19. Wellicht in het najaar voor ongewenste beïnvloeding."

Begrip desinformatie

De vraag waarmee men aan de slag wil is: in hoeverre beïnvloedt des-/misinformatie in relatie tot COVID-19 de NL samenleving? (Dit biedt een breder draagvlak zonder dat er sprake is van persoonsgericht onderzoek).

[redacted]

Hoofdkwartier OOCL — Bureau Juridische Zaken
Operationeel Ondersteuningscommando Land
Koninklijke Landmacht
Frank van Bijnenkazerne | Frankenlaan 70 | 7312 TG | Apeldoorn | [redacted]
Postbus 9019 | 7300 EA | Apeldoorn | MPC 39A

MDTN [redacted]
T [redacted]
M [redacted]
[redacted]@mindef.nl (functioneel)
[redacted]@mindef.nl (persoonlijk)
www.landmacht.nl

Op maandag en dinsdag werkzaam vanaf de Tonnetkazerne in 't Harde.

Van: "[redacted] CLAS/OOCL/CMD TEAM/JZ ADV" [redacted]@mindef.nl>
Datum: maandag 9 maart 2020 om 17:22:00
Aan: [redacted], CLAS/OOCL/JISTARC/DIVI" [redacted]@mindef.nl>
Cc: [redacted] CLAS/OOCL/JISTARC" [redacted]@mindef.nl>
Onderwerp: Opzet nota OSINT

[redacted]

Zoals vanochtend besproken gevoegd een eerste opzetje voor een nota t.a.v. de OSINT problematiek. Ik heb wat opmerkingen in het document ingevoegd op de vlakken waar ik input kan gebruiken. Overige op- en aanmerkingen uiteraard ook meer dan welkom.
Fijne avond,

[redacted]

From: [redacted] BS/AL/HDB/Belmdwrs <[redacted]@mindef.nl>
Sent: dinsdag 17 maart 2020 16:11
To: [redacted] BS/AL/DJZ/Cl. NTRH [redacted]@mindef.nl>; [redacted] BS/AL/DJZ/Clust. INT [redacted]@mindef.nl>
Cc: [redacted] BS/AL/DJZ/Clust. INT [redacted]@mindef.nl>
Subject: Re: Advies - verzoek onderzoek JISTARC desinformatie

Beste [redacted],
Veel dank voor jullie snelle respons.
Misschien heb ik twee zaken niet helder verwoord:
1) Het zou in dit geval gaan om een verzoek wat ik, namens de CHU, aan JISTARC zou doen. NCTV bracht het onder de aandacht, maar het verzoek zou vanuit mij komen. Is dit ook een steunverzoek in nationaal belang?
De resultaten zou ik wel breder interdepartementaal willen delen.
2) Het gaat mij expliciet niet om e-mailadressen, IP-adressen en persoonsinformatie etc. maar alleen om berichten die open source (bijv. op social media) de ronde doen, zodat ik een beeld krijg van de soort desinformatie die verspreid wordt. Ik hoef niet te weten wie hier achter zit, maar wil een beeld krijgen van de narratieven - een soort social media analyse dus. Opsporing en attributie is ook uitdrukkelijk niet het doel.
Is voor bovenstaande een wettelijke basis?
Alvast heel veel dank voor jullie hulp.
Hartelijke groet,
[redacted]

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: [redacted]@rijksoverheid.nl>
Datum: dinsdag 17 mrt. 2020 5:56 PM
Aan: [redacted]@nctv.minjenv.nl>, [redacted]@minbzk.nl>, [redacted]@minbzk.nl>, [redacted]@minbuza.nl>, [redacted]@minbuza.nl' [redacted]@minbuza.nl>, [redacted]@minocw.nl>, [redacted]@nctv.minjenv.nl>, [redacted]@mindef.nl [redacted]@mindef.nl>, [redacted]@minvws.nl>, [redacted]@nctv.minjenv.nl>, [redacted]@nctv.minjenv.nl> [redacted]@minezk.nl' [redacted]@minezk.nl>, [redacted]@minezk.nl>, [redacted]@minezk.nl' [redacted]minezk.nl>, [redacted]@rvo.nl' [redacted]@rvo.nl>, [redacted]@rvo.nl' [redacted]@rvo [redacted]@mindef.nl' [redacted]@mindef.nl>, [redacted]i@minvws.nl>, [redacted]@minvws.nl>, [redacted]@minvws.nl>, [redacted]@minbzk.nl>
Kopie: [redacted]@minbzk.nl>, [redacted]@nctv.minjenv.nl>, [redacted]@minbzk.nl> [redacted]@minbzk.nl>
Onderwerp: Bijeenkomst MID - 23 maart - COVID19

Beste allen,

In het kader van COVID-19 roepen wij maandag 23 maart om **15.00** uur het MID bij elkaarbij de NCTV (Turfmarkt 147, middenbouw 7e etage). Voorafgaand wordt jullie gevraagd om informatie die jullie hebben over des/misinformatie over COVID-19 uiterlijk **donderdag 19 maart om 18.00** uur te delen per mail (waar dit kan) en anders 23/3 ter plekke op papier uit te reiken en evt. na bespreking weer in te nemen. Hierbij valt te denken aan informatie over:

- Inhoud: wat wordt er voor nepbericht verspreid
- Verzender: is duidelijk wie het bericht verzonden heeft

[Paginanummer]

Van: [redacted] BS/AL/DJZ/Clust. INT" [redacted]@mindef.nl>
Datum: woensdag 18 maart 2020 om 10:32:00
Aan: [redacted] BS/AL/HDB/Belmdwrs" <[redacted]@mindef.nl>, [redacted] BS/AL/DJZ/Cl. NTRH" [redacted]@mindef.nl>
Cc: "[redacted] BS/AL/DJZ/Clust. INT" [redacted]@mindef.nl>
Onderwerp: RE: Advies - verzoek onderzoek JISTARC desinformatie

Beste [redacted]
Dit klinkt een beetje als een u-bocht: de NCTV heeft belangstelling maar laat jou het verzoek doen, om vervolgens wel van jou de opbrengst te krijgen. Wellicht chargeer ik het een beetje, maar helaas zien we wel vaker varianten hierop. Ik begrijp dat het alleen om de berichten gaat en niet om de

"daders", maar (a) er ontbreekt nog steeds een grondslag – dit is geen taak van Defensie, maar van de NCTV; (b) het duiden van informatie als zijnde desinformatie vereist nog steeds meer dan alleen rondkijken op internet en daarvoor zijn de Diensten echt aan zet; (c) rondkijken op social media en het verzamelen van berichten daaruit zonder tot personen herleidbare gegevens is best een uitdaging en ik heb grote twijfels of dat op de juiste wijze zal worden uitgevoerd zonder verdere toezichtmechanismes – en die ontbreken voor JISTARC.
Kortom, ik vraag me in gemoede af waarom dit een rol of taak voor Defensie zou zijn en ik zie geen (wettelijke) grondslag om dit op eigen initiatief (al dan niet daartoe aangezet door de NCTV) te gaan uitvoeren.
Met vriendelijke groet,

[redacted]

Van: [redacted] BS/AL/DJZ/Clust. INT
Verzonden: donderdag 19 maart 2020 11:14
Aan: [redacted], BS/AL/HDB/Belmdwrs
Onderwerp: RE: Advies - verzoek onderzoek JISTARC desinformatie

Beste [redacted]

Voor inzet van inlichtingenmiddelen – waaronder OSINT – is een wettelijke grondslag nodig. Zonder de notitie te herhalen of het al te juridisch te maken, komt het erop neer dat als de overheid inbreuk maakt op de privacy van burgers (beschermd door de Grondwet en door artikel 8 van het EVRM), het legaliteitsbeginsel vereist dat daarvoor een wettelijke basis bestaat en dat bepaalde waarborgen van toepassing zijn. Die waarborgen zijn in de jurisprudentie, zowel Nederlandse als die van het Europese Hof, nader gepreciseerd. De eis voor een wettelijke basis vloeit overigens ook voort uit het EVRM en de jurisprudentie en is de belangrijkste waarborg dat e.e.a. niet op basis van willekeur of opportuniteit plaatsvindt.

De wettelijke basis bepaalt ook wie de opdracht mag geven, wie daarop toezicht houdt en hoe de (democratische) verantwoording achteraf zal plaatsvinden. In Nederland zijn er twee wettelijke bases voor (feitelijk) inlichtingenwerk:

(1) Het Openbaar Ministerie en, in opdracht van het OM, de Nationale Politie mogen in het kader van strafvordering bepaalde bevoegdheden inzetten, waaronder bevoegdheden die neerkomen op criminele inlichtingen verzamelen, verwerken, enz.

Er zijn nog een derde en een vierde optie: de KMar kan wel bijstand aan de politie vragen, die dat op hun beurt weer aan Defensie kunnen vragen, waarna deze bijstand aan ons kan worden geleverd. Absurd en niet wat de wetgever beoogt, maar wel mogelijk. De vierde optie is gewoonweg aan de politie vragen of zij bijstand willen vragen en daarmee de OSINT capaciteit langs die kant op de gezamenlijke informatie-organisatie van de politie en de KMar laten aansluiten.

1) Ik zal mijn [redacted]-JZ vragen een werkverbandje te vormen. Wel moet je me dan nog even adviseren, namelijk, of we daar dan meteen ook een DJZ-rep in zouden moeten laten participeren.

2) Verder zou ik willen voorstellen om optie 4. ook te helpen verkennen. Uiteindelijk is dat waar de NCTV op hintte toen we spraken over het in kaart brengen van nep-berichten die op social media rondgaan. Is het dan niet handig om meteen een politiejurist aan tafel hebben?

@[redacted], ik begrijp dat hierover vandaag in de RVI wordt gesproken. Mocht dat zo zijn, willen jullie dit dan in het achterhoofd houden?

@[redacted] graag een print van deze mail meegeven aan [redacted] voor de RVI

Van: [redacted]/OOCL/JISTARC/DIVI/IGP D
Verzonden: maandag 23 maart 2020 11:09
Aan: [redacted], BS/AL/DS/DOPS/J3 OPS/SieNatOps/LOCC
Onderwerp: [redacted]LIMC

Goedemorgen [redacted],

Vanochtend is het Land Information Manoeuvre Centre (LIMC) onder leiding van [redacted] in 't Harde opgestart.

Ik ben aangewezen om als [redacted] op te treden tussen het LOCC en het LIMC. Het LIMC in 't Harde gaat zich bezighouden het verzorgen van informatieproducten op de volgende gebieden:

Civiel
1) Inzetbaarheid zorgcapaciteit / IC-capaciteit in NL
2) Continuïteit vitale processen in NL
3) Zorg voor kwetsbare doelgroepen in NL
4) Financieel-economische stabiliteit in NL
5) Caribisch gebied (geen zelfredzaamheid)
6) Ondermijning door fakenews/ acceptatie maatregelen overheid onder bevolking

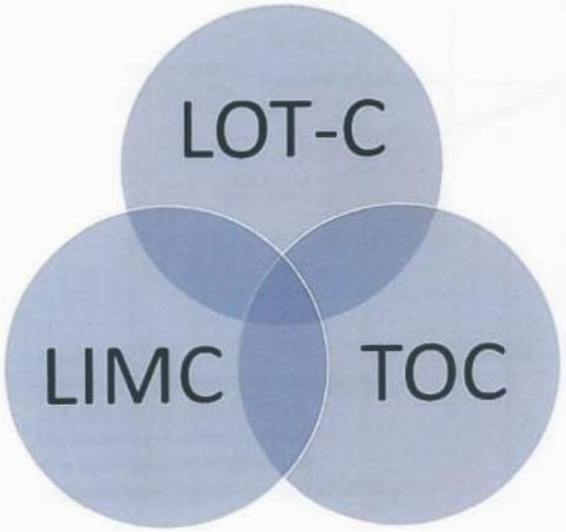
Militair
1) Inzetbaarheid krijgsmacht
2) Kunnen anticiperen op de vraag vanuit civiele autoriteiten

De intentie van mijn functie is dat ik de intermediair wordt tussen enerzijds de informatiebehoefte van het LOCC en het opstellen van producten door het LIMC om aan deze informatiebehoefte te voldoen. Ik heb inmiddels gesproken met collega [redacted]. Kan ik morgenochtend op een tijdstip dat het u uitkomt langskomen om nader kennis te maken en verdere afspraken te maken over mijn taakinvulling?

Agenda 22 april 2020

Opening en welkom	organisatie
Deel 1	
- Huidige scenario	LOT-C
- Tijdlijnen en IM proces	LOT-C
- Ontwikkeling LIMC	LIMC
Lunchpauze	
Deel 2	
- 10 factoren, wat verstaan we eronder?	Allen
- Wat loopt er al, wat missen wij? Per tijdlijn	Allen
- Vervolgafspraken	Allen

Zoeken naar overlap - werkafspraken



- Informatie:
  - IVP – vragen – indicatoren - frequentie
  - Uitvraag
  - Bundeling/aggregatie
  - Presentatie
- Duiding
  - Tijdsspanne
  - Combinatie van factoren
  - Weging
- Rapportage


Rijksoverheid
LOT-C
Gedrag:
Maatregelen en naleving
07 mei 2020

Guido Veldhuis

- TNO, LOT-C sectie scenario's, plannen en handelingsprotocollen
- Researcher & Project leader Military Operations

- Guido.Veldhuis@tno.nl

Guido Veldhuis · 3rd

Researcher at TNO Defence, Security and Safety

Analyseren voor toekomstig optreden

August 2021

Authors:

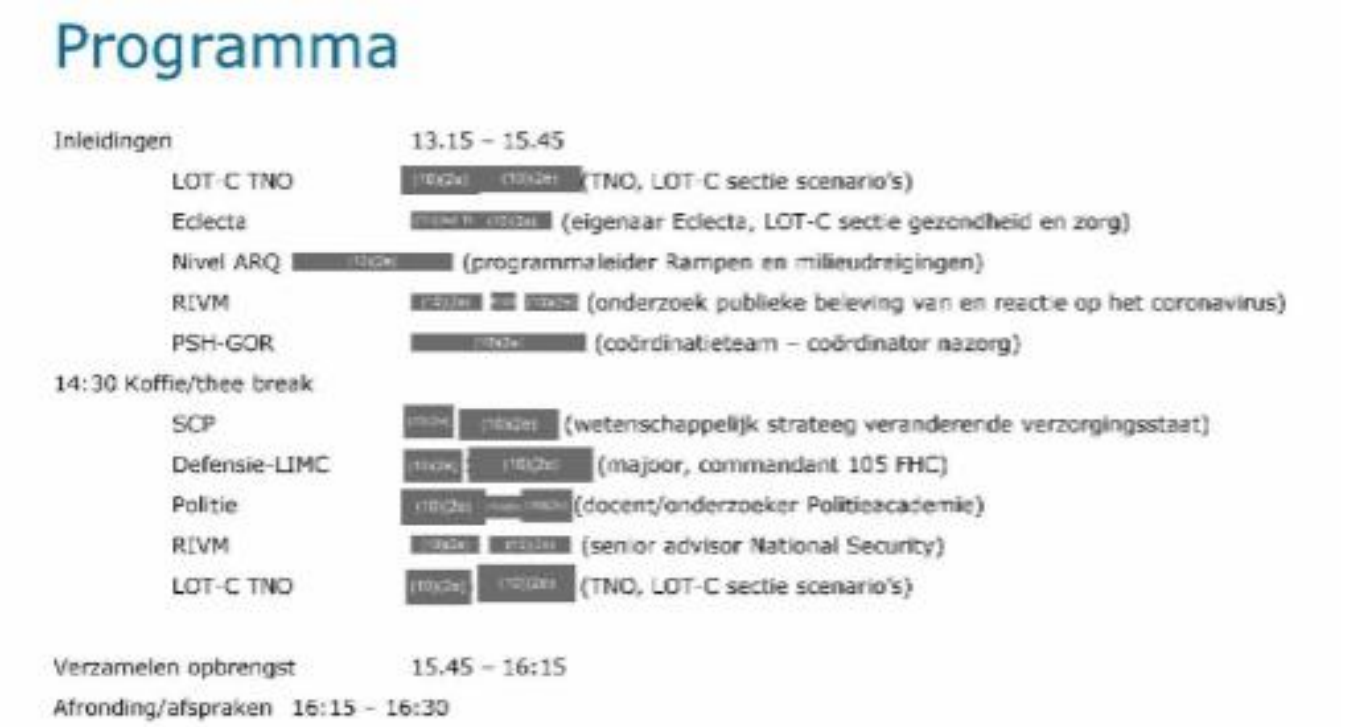
Guido Veldhuis
TNO

Bas Keijser
TNO

Download citation | Copy link

Abstract

Een veranderende wereld, dreiging en operatieconcept vragen om nieuwe (methoden voor) omgevingsanalyse. In het TNO-onderzoeksprogramma Mastering the Littoral is gekeken naar manieren waarop drie sleutelconcepten uit FLitOC geanalyseerd kunnen worden: flows, veerkracht en optreden met JIMP-partners. We hebben in dit artikel praktische handvatten geboden voor de analyse met flows en veerkracht. Dit vormt een eerste stap en een basis voor CZSK en de rest van Defensie om op verder te bouwen. Daarbij moet het FLitOC-concept zelf ook beproefd worden. Is de wijze van optreden en daaraan gekoppelde conceptualisatie van de omgeving voor elke situatie en tegen elke dreiging geschikt? En welke analyse is vervolgens benodigd bij verschillende missietypen, omgevingen en dreigingen? Het moge duidelijk zijn dat dit nog geen eindstation is. Een dieper begrip van de operatieomgeving opbouwen en dit ook nog eens sneller doen zal meer innovatie vragen in kennis en kunde, middelen en analyseondersteuning.



105 Field HUMINT Squadron (105 Field Humint-eskadron): The 105 Field HUMINT Squadron consists of personnel of all four branches. The Field HUMINT Teams (FHTs) of the squadron gather intelligence through contacts in their area of operations, draft reports and report their findings to higher echelons.

Human intelligence (intelligence gathering)

Human intelligence (abbreviated **HUMINT** and pronounced as *hyoo-mint*) is intelligence gathered by means of interpersonal contact, as opposed to the more technical intelligence gathering disciplines such as signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signature intelligence (MASINT).[1]

A United States Marine asks a local woman about weapons in Fallujah, Iraq

NATO defines HUMINT as "a category of intelligence derived from information collected and provided by human sources."[1] HUMINT, as the name suggests, is mostly done by people rather than any technical means, and is commonly provided by covert agents and spies. For instance, Oleg Penkovsky was a Soviet military intelligence (GRU) colonel who served as a source to the UK and the United States by informing them of the precise knowledge necessary to address rapidly developing military tensions with the Soviet Union. A typical HUMINT activity consists of interrogations and conversations with persons having access to information.

The manner in which HUMINT operations are conducted is dictated by both official protocol and the nature of the source of the information. Within the context of the U.S. military, HUMINT activity may involve clandestine activities, however these operations are more closely associated with CIA projects.[2] Both counterintelligence and HUMINT include clandestine HUMINT and clandestine HUMINT operational techniques.

Gert Sanderman

- Defensie-LIMC
- Majoor, Commandant 105 FHC

- g.sanderman@mindef.nl

VELDERVARINGEN VAN EEN OFFICIER

DONDERDAG 31 MEI

KUNDUZ LIFE

Spreker : Gert Sanderman
Locatie : Trouwzaal Noorderkerk
Aanvang : 20:00 uur

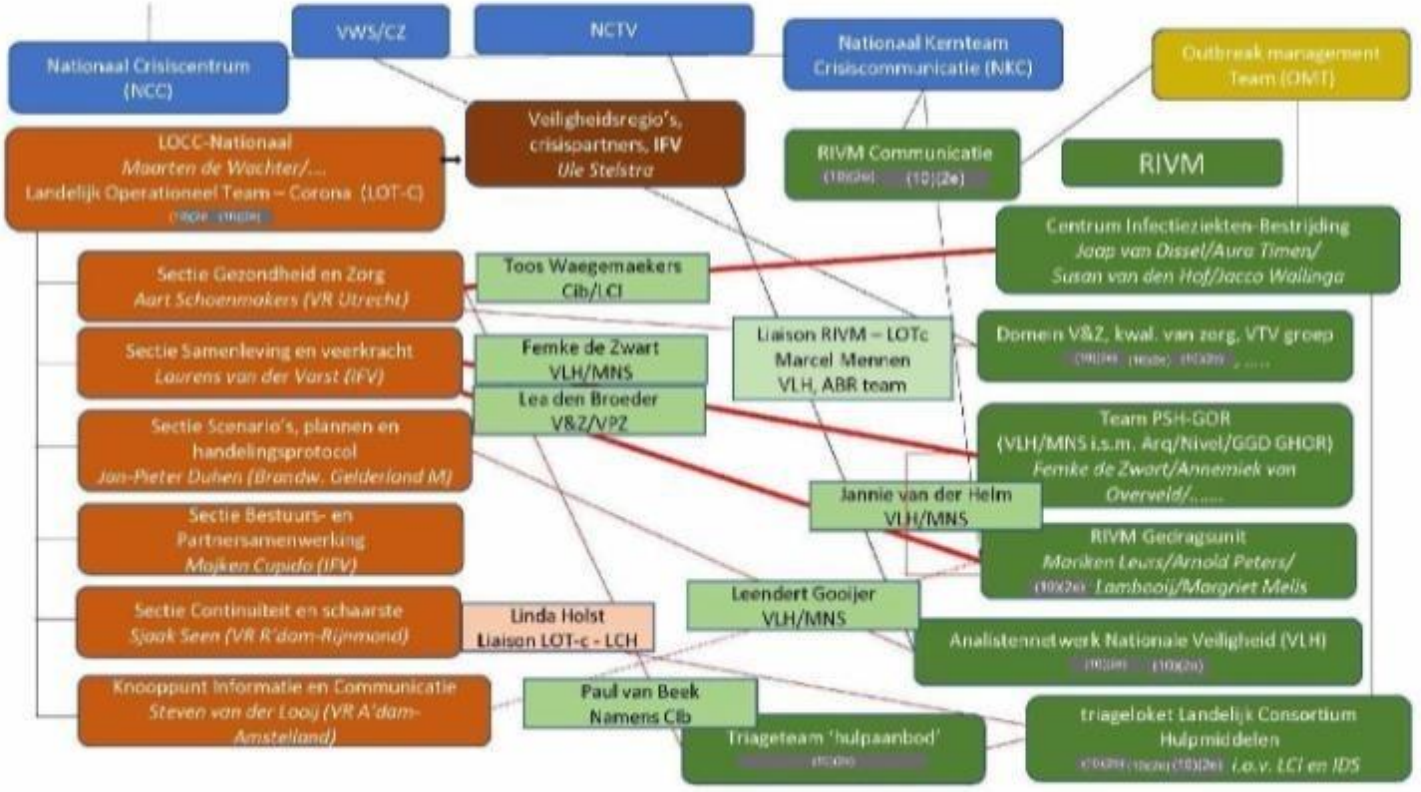
da costa sgp-j

Soldaat en politiek

Christen in het leger

Iedereen welkom!

Samenwerking LOT-C en RIVM



Van [redacted] CLAS
Verzonden: woensdag 25 maart 2020 07:38
Aan: [redacted] CLAS/ST CLAS/KAB/SIE JZ [redacted]@mindef.nl>
CC: [redacted] CLAS/ST CLAS/KAB/SIE JZ/BUR O&I [redacted]@mindef.nl>; [redacted]
CLAS/ST CLAS/KAB [redacted]@mindef.nl>; [redacted], CLAS [redacted]@mindef.nl>
Onderwerp: FW: OSINTCIE

[redacted]

Zie maildiscussie hieronder.

Voor de duidelijkheid: bij het LIMC heb ik gisteren expliciet duidelijk gemaakt dat hier – zonder de wettelijke basis – geen ruimte is voor welke commandant dan ook. Dat is iedereen in die lijn duidelijk. In het TOCC heb ik zelf C-109 OSINT-cie gesproken en die is zich van deze cap meer dan bewust.

Maar … ik doek wel die wettelijke basis. En potentiele vraagstellers helpen een steunvraag te stellen.

Zelf zie ik het meest in optie 4. (zie hieronder).

Lees het nog eens en ik stel voor dat [redacted] me daarna nog even opzoekt voor een bilat (bellen, facetimen, kijk maar). Ik heb nog wat mensen op de BS die wellicht zouden kunnen helpen.

Inleiding

Vanwege mogelijke onduidelijkheden over het wettelijk kader van de modus operandi van twee nieuwe JISTARC-onderdelen is besloten geen publiciteit te geven aan de symbolische oprichting op dinsdag 3 december 2019. Dit memo beschrijft op welke wijze en momenten de landmacht alsnog de publicitaire kansen kan verzilveren en zowel intern als extern doelgroepen kan informeren over de organisatie.

Beschouwing

Met de oprichting van 108 Technical Exploitation Intelligence-compagnie en 109 Open Sources Intelligence-compagnie bij het JISTARC beschikt de Koninklijke Landmacht over twee nieuwe/uitgebreide capaciteiten voor het verzamelen van informatie en inlichtingen. De oprichting van deze eenheden vormt een publicitaire kans, want het toont zowel het nut van investeringen in de landmacht, alsook vernieuwing: een landmacht die met zijn tijd mee gaat. De nieuwe eenheden zijn dinsdag 3 december 2019 met militair ceremonieel symbolisch opgericht. De formele (administratieve) oprichting vindt plaats op 1 februari 2020.

Reden om de ceremoniële oprichting begin december publicitair niet breed uit te meten is dat het werk van zowel 108 TeXINT-cie als 109 OSINT-cie het verzamelen informatie behelst, op - voor militaire begrippen - relatief nieuwe wijze en nieuwe terreinen, zoals forensisch onderzoek en informatie over (mogelijk) non-combattanten in inzetgebieden. Vanwege de maatschappelijke aandacht voor privacy en de strikte wet- en regelgeving inzake het verzamelen, gebruiken en bewaren van persoonsgebonden informatie (denk aan: AVG) dient voor alle betrokkenen (en daarmee 'ambassadeurs' van de nieuwe eenheden) duidelijk te zijn wat we als militaire organisatie in bepaalde situaties wel en niet kunnen, mogen en doen, zeker voordat we hier publicitair mee naar buiten gaan.

[redacted]

Dank voor de beantwoording.

De reeds opgestelde DPIA behandeld niet het afstaan van biometrisch/genetisch materiaal van eigen personeel t.b.v. de eliminatie-database. De DPIA handelt alleen over O&T-biometrie. Het toepassen van de eliminatie-database ten behoeve van de bescherming van eigen personeel heeft een bredere toepassing en heb ik hier bewust buiten gelaten.
Het opstellen van een DPIA-deconflictie (eliminatie-database) is zowel voor O&T als voor operationele inzet van toepassing. Beide vallen onder de AVG en niet onder de RGMO.

Ik heb inderdaad eind 2018 gesproken over AVG-zaken m.b.t. biometrie. Hier waren aanwezig:
- [redacted] CLAS/Dir Plannen/Landoptreden
- [redacted] BS/Dir K&I/Afd Pri&A
- [redacted] BS/DJZ/Intern Recht
- [redacted] BS/Dir M&B Gegevensbescherming
- [redacted] JKC I&V
- [redacted] 108 TEXINT
- [redacted] ICT ABIS/biometrie

Mijn kennis van de AVG was destijds minimaal. Echter, deze bespreking heeft mij genoodzaakt om hier zelf in te duiken. De voorstellen die geopperd werden voor O&T-biometrie en de daarop volgende discussie waren verre van realistisch. Dit heeft geleid tot een DPIA O&T-biometrie welke meer in de richting komt van realistische O&T.

Voor het eliminatie-database/deconflictie-probleem heeft [redacted] tijdens deze bespreking het idee geopperd voor een AMAR-wijziging. Hij gaf daarbij aan dat dit wel een lange weg is. Hier moeten ook de bonden etc. mee eens zijn. Tijdens deze bespreking is niet naar voren gekomen dat een DPIA opgesteld moet worden om dit traject in te zetten. Voordat we overgaan tot AMAR-wijzigingen moeten we eerst goed de bestaande mogelijkheden van de AVG afwegen.

- **108 Technical Exploitation Intelligence-compagnie** (108 TeXInt): 108 TeXInt is opgericht op 20 februari 2020 als inlichtingeneenheid die is gespecialiseerd om militaire commandanten in inzetgebieden extra forensische inlichtingen te bieden.[14]
- **109 Open Sources Intelligence-compagnie** (109 OSINT): 109 OSINT is opgericht op 20 februari 2020 als inlichtingeneenheid die is gespecialiseerd in de doelmatige detectie en verzameling van informatie uit openbare bronnen in inzetgebieden.[14]

MIVD-directeur generaal-majoor Jan Swillens.

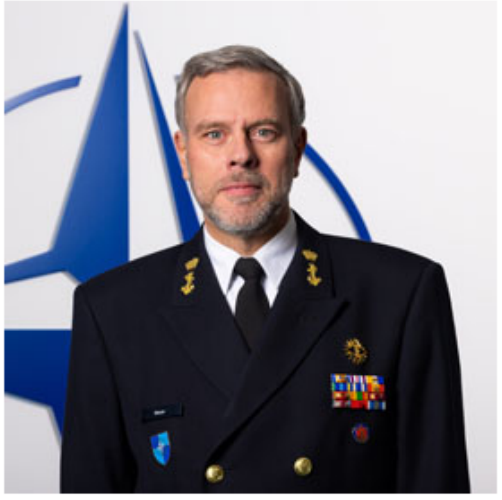
Ongekende dreiging gekend maken

Die gegevens zijn hard nodig, benadrukt Swillens, cruciaal zelfs. “Om onze opdracht ‘een ongekende dreiging gekend maken’ goed uit te voeren. Dit belang wordt ook bevestigd door de toezichthouder de CTIVD en de onafhankelijke Evaluatiecommissie. Het is ontzettend moeilijk om de ongekende dreiging gericht te lijf te gaan, je weet immers niet waar je naar zoekt.”

De MIVD doet dat door zoveel mogelijk data te verzamelen voor een zo betrouwbaar mogelijk voorspellend inlichtingenproduct. Om te beginnen open bronnen. Maar ook informatie van menselijke bronnen, cyber en ‘signal intelligence’, zoals satellieten en internationale partners.

Nu was het woord aan de Lkol Patrick Dekker, commandant van het Defensie Inlichtingen & Veiligheidsinstituut (DIVI), om met een militaire blik te kijken naar deze informatie–oorlog. De grote uitdagingen liggen op het vlak van afstemming binnen Defensie: de vakgebieden van elektronische oorlogsvoering, psyops en cyber overlappen en zouden moeten samenwerken om elkaars effecten te versterken. Aan de andere kant is er een grote onbekendheid bij commandanten in het veld, die zich een betere voorstelling kunnen maken van kinetische effecten.

Commandant Landstrijdkrachten luitenant-generaal Martin Wijnen.



Admiral Rob Bauer (Royal Netherlands Navy) is the 33rd Chair of the Military Committee of the North Atlantic Treaty Organization (NATO). As the Military Adviser to the Secretary General and the North Atlantic Council, Admiral Bauer is NATO's most senior military officer.

He is the conduit through which advice from NATO's 30 Chiefs of Defence is presented to the political decision-making bodies; and guidance and directives are issued to the Supreme Allied Commander Europe, Supreme Allied Commander Transformation and the Director General of the International Military Staff.

General

Tom Middendorp

Middendorp in 2015

Chief of Defence	
In office	
28 June 2012 – 3 October 2017	
Preceded by	General Peter van Uhm
Succeeded by	Lieutenant admiral Rob Bauer

TOM MIDDENDORP

Oud Commandant der Strijdkrachten Tom Middendorp was de voorzitter van het bestuur van Stichting Open Nederland tot aan 30 juni 2021. Sinds de start van het coronavirus COVID-19 zette Tom zich in voor het opschalen van de testcapaciteit in Nederland en hij gaf tevens leiding aan de operatie Fastlane die eind 2020 vanuit het bedrijfsleven hielp de testcapaciteit voor de GGD te verdrievoudigen met de bouw van de (X)L-testlocaties. Vervolgens ondersteunde hij ook bij de invoering van preventief testen voor werkgevers en zelftesten in de onderwijssector. Vanuit die rollen werd hij gevraagd leiding te geven aan de Stichting Open Nederland om een test-infrastructuur op te zetten teneinde het sociale leven weer op gang te brengen. Sinds dit is opgezet richt hij zich weer op zijn functies als Speciaal Gezant voor het ministerie van EZK en als voorzitter van de Internationale Militaire Raad voor Klimaat en Veiligheid (IMCCS). Tom blijft daarnaast aan als adviseur van de Stichting.

Bestuur [bewerken | brontekst bewerken]

Het bestuur van de stichting[6] bestaat sinds de oprichting op 16 februari 2021 uit:

- Pier Eringa (voorzitter per 1 juli 2021)
- Tom Middendorp (oprichtend voorzitter, tot 1 juli 2021), voormalig Commandant der Strijdkrachten
- Chris Smulders, voormalig financieel directeur van NS en Abellio
- Paul van Roozendaal, voormalig ICT-ondernemer.

De raad van toezicht bestaat uit de volgende leden[7]:

- Marjanne Sint, Oud-PvdA politica
- Margot Scheltema
- Paul Verheul

De Wet Bestuur en Toezicht Rechtspersonen is sinds 1 juli 2021 van toepassing op de stichting. De Wet Openbaarheid Bestuur is niet van toepassing op de Stichting.[bron?]

Testen voor toegang [bewerken | brontekst bewerken]

De gehele organisatie van de testevenementen zou initieel van april tot eind augustus 2021 duren. Uiteindelijk was het project 'Testen voor toegang' tot eind maart 2022 actief.[8] Stichting Open Nederland draagt per 1 september 2022 haar taken over aan het Ministerie van Volksgezondheid, Welzijn en Sport, dienst Testen.[9]

De Stichting heeft er voor gekozen om geselecteerde testaanbieders een gegarandeerde vergoeding te betalen van 387 euro per testafnameplek per dag tot in ieder geval 1 augustus 2021 (een testlocatie bestaat doorgaans uit meerdere testafnameplekken), ongeacht of er enige test wordt afgenomen.[10] Daarbovenop vergoedt de Stichting voor het uitvoeren van testen.

Tot en met maart 2022 zegt de stichting dat er meer dan 9,4 miljoen testen zijn afgenomen binnen het kader van Testen voor toegang.[9]

Controverse [bewerken | brontekst bewerken]

In april 2021 ontstond er commotie over het gebruik van de Stichting en het feit dat het project tot augustus al in totaal 925 miljoen euro zou gaan kosten.[11][12][13] Deze controverse heeft geleid tot kamervragen.[14]

Op 14 april 2021 gaf minister De Jonge in een toelichting aan de Tweede Kamer aan dat voor het organiseren van toegangstesten voor fieldlab-evenementen een bedrag van 1,1 miljard euro is gereserveerd: circa 900 miljoen voor de realisatie en exploitatie van de toegangstestlocaties - georganiseerd door Stichting Open Nederland, en circa 200 miljoen voor de kosten van antigeentesten en de opbouw van XL-straten waar de

OM en NFI starten pilot met genealogische DNA-databanken

Nieuwsbericht | 06-03-2023 | 08:00

Het Openbaar Ministerie (OM) en het Nederlands Forensisch Instituut (NFI) gaan gebruik maken van genealogische DNA-databanken voor het oplossen van volledig vastgelopen ernstige strafzaken, in de hoop een doorbraak te forceren. Binnenkort start een pilot waarin die opsporingsmethode ingezet gaat worden in twee cold casezaken. Dat zou voor het eerst zijn in Nederland. Voor het zover is, wordt deze opsporingsmethode nog wel voorgelegd aan de rechter.

Irakli Beridze
Head of the Centre for Artificial Intelligence and Robotics, UNICRI

Marjolein Smit-Arnold Bik
Head of the Special Operations Division, Police of the Netherlands

Kay Firth-Butterfield
Head of Artificial Intelligence and Machine Learning; Member of the Executive Committee, World Economic Forum

Cyril Gout
Director of Operational Support and Analysis, INTERPOL

https://www3.weforum.org/docs/WEF_A_Policy_Framework_for_Responsible_Limits_on_Facial_Recognition_2021.pdf

Artikel 126g

69

1 In geval van verdenking van een misdrijf, kan de officier van justitie in het belang van het onderzoek bevelen dat een opsporingsambtenaar stelselmatig een persoon volgt of stelselmatig diens aanwezigheid of gedrag waarneemt.

2 Indien de verdenking een misdrijf betreft als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie in het belang van het onderzoek bepalen dat ter uitvoering van het bevel een besloten plaats, niet zijnde een woning, wordt betreden zonder toestemming van de rechthebbende.

3 De officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel wordt aangewend, voor zover daarmee geen vertrouwelijke communicatie wordt opgenomen. Een technisch hulpmiddel wordt niet op een persoon bevestigd, tenzij met diens toestemming dan wel in het geval, bedoeld in artikel 126nba, eerste lid, onder c.

Open Source Intelligence

Open Source Intelligence, vaak afgekort als OSINT, is het legaal verzamelen van data en informatie uit open en publiek beschikbare bronnen. Deze gegevens worden verzameld, geanalyseerd en op een begrijpbare manier gerapporteerd of gepubliceerd.

De onderstaande gegevens en informatie worden als Open Source beschouwd:

- Open of semi-gesloten databases;
- Overheidsrapporten, documenten en websites;
- Het internet;
- Massamedia (zoals kranten, tv, radio, tijdschriften en websites);
- Sociale netwerken en sociale mediasites;
- Kaarten en commerciële afbeeldingen;
- Afbeeldingen, foto's en video's;
- Het Dark Web.

AIVD
@AIVD

Als Internet Investigator bij de afdeling OSINT van de AIVD ga je online op zoek naar puzzelstukjes die onze onderzoeken verder helpen. Iets voor jou? Bekijk de vacature:
werkenvoornederland.nl/vacatures/inte...

10:07 a.m. · 27 jan. 2020

De Koninklijke Marechaussee start vanaf volgende week met de uitrol van de landelijke opsporingsapplicatie SUMM-IT. De applicatie ondersteunt collega's die werkzaam zijn binnen de opsporing en intell bij het verwerken van gegevens en dossiervorming in de breedste zin van het woord. SUMM-IT vervangt op termijn het bestaande systeem RBS (Recherche Basis Systeem) en de dossiervorming op de zogenaamde confiserver. De Nationale Politie, de bijzondere opsporingsdiensten en de Rijksrecherche zijn al eerder overgestapt op SUMM-IT.

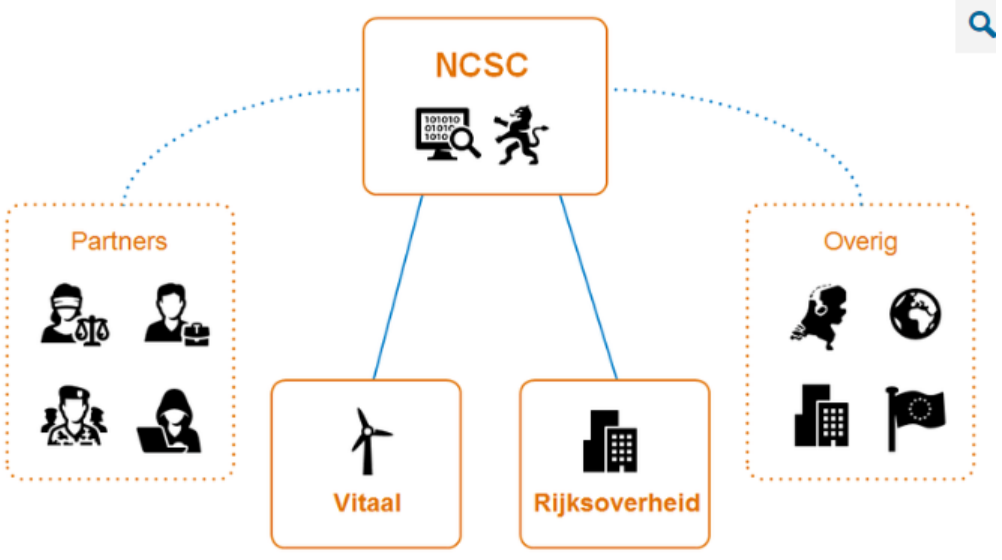
Een van de grootste voordelen van SUMM-IT is dat alle informatie binnen de opsporing en de bijbehorende intell-processen van de KMar op 1 plek en op een eenduidige manier samen wordt gebracht en niet meer is versnipperd over verschillende systemen. De applicatie stuurt de collega door alle stappen tussen een onderzoekdossier en procesdossier heen en legt alle handelingen vast. Daarnaast kunnen coördinatoren werkopdrachten uitzetten, bewaakt SUMM-IT de termijnen van documenten, is al het bewijsmateriaal, zoals foto's, video's op te slaan en zijn altijd de laatste versies van formulieren beschikbaar.

Klik op de plus-tekens hieronder om meer te weten te komen over SUMM-IT.

INFORMATIE-GESTUURD OPTREDEN

Informatiegestuurd optreden: SUMM-IT levert een bijdrage aan het informatiegestuurd optreden van de Koninklijke Marechaussee. Omdat alle opsporingshandelingen op een eenduidige manier in 1 systeem worden verwerkt, versterkt SUMM-IT het intell-beeld. Door afzonderlijke stukjes informatie nader te onderzoeken en te veredelen (verrijken en stapelen van informatie) kunnen de Intell-medewerkers de grotere verbanden tussen verschillende incidenten en onderzoeken zichtbaar maken. Zo kunnen criminele samenwerkingsverbanden in kaart worden gebracht, waarna op basis van die informatie de Recherche nieuwe onderzoeken start.

Door samenwerking geeft het NCSC invulling aan haar missie om een bijdrage te leveren aan het vergroten van de digitale weerbaarheid van Nederland. Een gezamenlijk doel van het NCSC en haar partners is om in een veilige, open en stabiele informatiesamenleving te leven, wonen en werken.



Partners en doelgroepen

Nationaal Coördinator Terrorismebestrijding en Veiligheid

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) beschermt Nederland tegen bedreigingen die de maatschappij kunnen ontwrichten. Samen met partners binnen overheid, wetenschap en bedrijfsleven zorgt de NCTV ervoor dat de Nederlandse vitale infrastructuur veilig is én blijft. Voor cybersecurity is de NCTV de beleidsopdrachtgever van het NCSC.

NEXIS: Nederlands-Europees Kruispunt voor Cybersecurity-Innovatie en Samenwerking

Gepubliceerd op: 24 januari 2023
Laatst gecontroleerd op: 12 april 2023
Hoort bij: Ondernemen en bedrijfsvoering

De snelle digitalisering in Nederland biedt u nieuwe kansen, maar ook zéker de nodige aandachtspunten. Het vergroten van de cyberweerbaarheid en de samenwerking met EU-lidstaten is voor ons allemaal van groot belang om heel Europa digitaal veilig en veerkrachtig te houden. Het nieuwe Nederlandse loket NEXIS ondersteunt u vanaf 2023 bij uw aanvraag van (Europese) vormen van financiering en de verbinding met andere, relevante stakeholders.

NCI AGENCY | Cyber Security

Welcome to the portal of the NATO Cyber Security Centre - NATOs first line of cyber defence.
The NATO Cyber Security Centre, formerly known as the NATO Computer Incident Response Capability Technical Centre (NCIRC TC), is responsible for the full lifecycle of NATO's Cyber Security activities, designing, implementing and operating:

- Scientific and technical expertise
- Supporting Acquisition, Maintenance and Sustainment
- Conducting Operations and Incident Response / CERT

Norwegian National Cyber Security Centre (NCSC) and NorCERT

NCSC is a part of the Norwegian Security Authority (NSM). We are Norway's national cyber security centre and home to the national CERT*; NorCERT. We handle severe computer attacks against critical infrastructure and information. Our mission is to enhance Norway's resilience in the digital domain.

INFORMATION SECURITY NOW!

The National Cyber Security Centre Finland's weekly review – 17/2023

Published 02.05.2023 11:33

This week we talk about technical support scam calls and phishing messages impersonating the suomi.fi service.

National Cyber Security Centre under the Ministry of National Defence (NCSC) is the main Lithuanian cyber security institution, responsible for unified management of cyber incidents, monitoring and control of the implementation of cyber security requirements, accreditation of information resources.

www.ncsc.admin.ch

Homepage NCSC DE FR IT EN

National Cyber Security Centre NCSC

Information for

Individuals

Te Tira Tiaki
Government Communications Security Bureau

NCSC

National Cyber Security Centre

We are part of the Government Communications Security Bureau. Our mission is to protect Aotearoa New Zealand's wellbeing and prosperity through trusted cyber security services.

Welcome to the NCSC Ireland website

The National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) was founded in 2011 and is an operational arm of the Department of the Environment, Climate and Communications (DECC). The NCSC is responsible for advising and informing Government IT and Critical National Infrastructure providers of current threats and vulnerabilities associated with network information security.

The main roles of the NCSC are to lead in the management of major cyber security incidents across government, provide guidance and advice to citizens and businesses on major cyber security incidents, and develop strong international relationships in the global cyber security community for the purposes of information sharing. In the period since 2011, the unit has focused its efforts on building capacity and establishing a stable base for its operational work.

Alert - Vulnerabilities exploited in VPN products used worldwide (NCSC Alert)

From: Canadian Centre for Cyber Security

Number: AL19-017

Date: 3 October 2019

AUDIENCE

This Alert is intended for IT professionals and managers of notified organizations.

www.ncsc.gov.uk

National Cyber Security Centre

Menu

The National Cyber Security Centre

Helping to make the UK the safest place to live and work online.

Featured

The role of the National Cyber Security Centre (NCSC)

At a glance

- The NCSC is the UK's technical authority for cyber threats. It is part of the Government Communications Headquarters (GCHQ) and has several roles in NIS.
- It acts as the 'computer security incident response team' or CSIRT. This means it monitors incidents, provides early warnings, disseminates information, conducts cyber threat assessments and provides general technical support to competent authorities.
- It is also the 'single point of contact' (SPOC). In this role it receives information on NIS incidents from all competent authorities and co-ordinates with its counterparts in other Member States.
- The NCSC has published a 'NIS guidance collection', primarily for OES.


www.dni.gov
Office of the Director of National Intelligence
The National Counterintelligence and Security Center
NCSC
WE LEAD THE EFFORT TO PROTECT OUR NATION AGAINST INTELLIGENCE AND SECURITY THREATS
Lead and support the U.S. Government's counterintelligence (CI) and security activities critical to protecting our nation; provide CI outreach to U.S. private sector entities at risk of foreign intelligence penetration; and issue public warnings regarding intelligence threats to the U.S.

OFFICE *of the* DIRECTOR *of* NATIONAL INTELLIGENCE

Our mission is to **lead intelligence integration** and forge an **intelligence community** that delivers the most insightful intelligence possible

Office *of the*
Director *of* National Intelligence

Contact ODNI

ODNI Centers

National Counterterrorism Center

National Counterintelligence and Security Center

National Counterproliferation and Biosecurity Center

Cyber Threat Intelligence Integration Center

Foreign Malign Influence Center

Oversight

Leading Intelligence Integration

Equal Employment Opportunity

IC Inspector General

IC Diversity Equity Inclusion and Accessibility

Civil Liberties, Privacy, and Transparency

Office of General Counsel

More Offices

ODNI, DOJ, and DHS Release Unclassified Summary of Assessment on Domestic Violent Extremism

Release Date: March 17, 2021

WASHINGTON – The Office of the Director of National Intelligence (ODNI), the Department of Justice (DOJ), and the Department of Homeland Security (DHS) today released an unclassified summary of the joint comprehensive threat assessment on domestic violent extremism. The unclassified summary is attached and will be available on DNI.gov later today.

James Robert Clapper Jr. (born March 14, 1941) is a retired lieutenant general in the United States Air Force and former Director of National Intelligence. Clapper has held several key positions within the United States Intelligence Community. He served as director of the Defense Intelligence Agency (DIA) from 1992 until 1995. He was the first director of defense intelligence within the Office of the Director of National Intelligence and simultaneously the Under Secretary of Defense for Intelligence.[1] He served as the director of the National Geospatial-Intelligence Agency (NGA) from September 2001 until June 2006.

James Clapper

Clapper to replace Dennis C. Blair as United States Director of National Intelligence. Clapper was unanimously confirmed by the Senate for the position on August 5, 2010.

Following the June 2013 leak of documents detailing the NSA practice of collecting telephone metadata on millions of Americans' telephone calls, Clapper was accused of perjury for telling a congressional committee hearing that the NSA does not collect any type of data on millions of Americans earlier that year. One senator asked for his resignation, and a group of 26 senators complained about Clapper's responses under questioning. In November 2016, Clapper resigned as director of national intelligence, effective at the end of President Obama's term. In May 2017, he joined the Washington, D.C.–based think tank the Center for a New American Security (CNAS) as a Distinguished Senior Fellow for Intelligence and National Security.[2] In August 2017, CNN hired Clapper as a national security analyst.[3]

called the firing of FBI director James Comey "inexcusable", and warned of an "internal assault on our institutions".[100]

In June 2017, Clapper opined that Trump-Russia scandal is more serious than the Watergate scandal of the 1970s.[101] In December 2017, Clapper said that Russian President Vladimir Putin "knows how to handle an asset, and that's what he's doing with" President Trump.[102] In his 2018 memoir *Facts and Fears: Hard Truths from a Life in Intelligence*, Clapper further addressed the issue.[103]

In an August 2017 interview, Clapper stated that U.S. President Donald Trump having access to the nuclear codes is "pretty damn scary" and he questioned his fitness to be in office.[104]

In October 2018, Clapper alongside several Democratic officials and other critics of Trump was targeted by a mailed pipe bomb.[105]

In February 2019, Clapper said he agreed with former acting FBI Director Andrew McCabe's opinion that President Donald Trump could be a "Russian asset".[106]

In October 2020, Clapper and more than 50 former intelligence officials signed a letter stating the disclosure of emails in the Hunter Biden laptop story "has the classic earmarks of a Russian information operation".[107]

President's Statement on Senate Confirmation of John D. Negroponte

April 21, 2005

"I commend the Senate for moving quickly to confirm John Negroponte as the first Director of National Intelligence. I congratulate John on his confirmation, and I look forward to working closely with him. As the DNI, Ambassador Negroponte will lead a unified intelligence community as it reforms and adapts to the new challenges of the 21st century. The United States continues to make progress in the global war on terror against the enemies of freedom who target innocent civilians and seek weapons of mass destruction. I appreciate John's willingness to once again serve his country and the many men and women who serve in the intelligence community."

Robert Michael Gates (born September 25, 1943) is an American intelligence analyst and university president who served as the twenty-second United States secretary of defense from 2006 to 2011. He was originally appointed by President George W. Bush and was retained by President Barack Obama. Gates began his career serving as an officer in the United States Air Force but was quickly recruited by the Central Intelligence Agency (CIA).[2] Gates served for twenty-six years in the CIA and at the National Security Council, and was director of central intelligence under President George H. W. Bush. After leaving the CIA, Gates became president of Texas A&M University and was a member of several corporate boards. Gates served as a member of the Iraq Study Group, the bipartisan commission co-chaired by James A. Baker III and Lee H. Hamilton that studied the lessons of the Iraq War.

Robert Gates

Career after leaving the CIA

1993–1999

After retiring from the CIA in 1993, Gates worked as an academic and lecturer. He evaluated student theses for the International Studies Program of the University of Washington. He lectured at Harvard, Yale, Johns Hopkins, Vanderbilt, Georgetown, Indiana, Louisiana State, Oklahoma, and the College of William & Mary. Gates served as a member of the Board of Visitors of the University of Oklahoma International Programs Center and a trustee of the endowment fund for the College of William & Mary, his alma mater, which in 1998 conferred upon him honorary degree of Doctor of Humane Letters.[32] In 1996, Gates' autobiography, *From the Shadows: The Ultimate Insider's Story of Five presidents and How They Won the Cold War*, was published. Gates has also written numerous articles on government and foreign policy and has been a frequent contributor to the op-ed page of *The New York Times*.[33]