VIPS Memorandum til præsidenten: »Var det 'russiske hack' et inside-job?«

Tekniske undersøgelser af »russisk hacking« af den Demokratiske Nationalkomites (DNC) computere sidste år afslører, at, den 5. juli, 2016, blev data ***lækket (ikke hacket)*** *af en person, der havde fysisk adgang til DNC's computere. Efter at have undersøgt metadata fra »Guccifer 2.0«'s indbrud den 5. juli, 2016, i DNC-serveren, har uafhængige cyber-efterforskere konkluderet, at en insiderperson kopierede DNC-data over på en ekstern lagerfacilitet.*

VIPS Memorandum til præsidenten: »Var det 'russiske hack' et inside-job?«

Den 24. juli, 2017, offentliggjorde consortiumnews.com et memorandum, som Veteran Intelligence Professionals for Sanity, VIPS, havde udarbejdet til USA's præsident, og til offentliggørelse. I sin artikel, under overskriften, *»Intel Vets Challenge 'Russia Hack Evidence«*, kommer de med redaktionelle bemærkninger, der går ud på, at VIPS-memoet indeholder to forkerte datoer, som dog ikke påvirkede memoets hovedkonklusion, nemlig, at indbruddet i DNC-e-mails, som Rusland fik skyld for, ikke kunne have været et hack – fra Rusland eller nogen anden. De dele af memoet, der vedrører de forkerte datoer, er blevet rettet (af consortiumnews.com).

Dernæst følger en kort redegørelse for rettelserne:

- Den 14. juni, 2016 (og ikke, som VIPS-memoet fejlagtigt

siger, den 15.) var den dag, hvor Crowdstrike sagde, skadelig software var blevet fundet i DNC-serveren og hævdede, der forelå beviser for, at den skadelige software var indført af russere. (Den følgende dag – den 15. – tog »Guccifer 2.0« ansvaret for »hacket« og hævdede at være WikiLeaks' kilde.)

- Selv om VIPS-memoet korrekt anførte, at, den 15. juni, 2016 udlægger … »Guccifer 2.0 et dokument, som de tekniske undersøgelser viser, var kunstigt manipuleret med 'russiske fingeraftryk'«, så indikerer anden tekst i memoet fejlagtigt, at beviser for sådan manipulation *også* blev fundet i »Guccifer 2.0« metadata fra kopieringsbegivenheden den 5. juli.

MEMORANDUM TIL: Præsidenten

FRA: Veteran Intelligence Professionals for Sanity (VIPS)

EMNE: Var det »russiske hack« et inside-job?

Kort resume

Tekniske undersøgelser af »russisk hacking« af den Demokratiske Nationalkomites (DNC) computere sidste år afslører, at, den 5. juli, 2016, blev data ***lækket (ikke hacket)*** af en person, der havde fysisk adgang til DNC's computere. Efter at have undersøgt metadata fra »Guccifer 2.0«'s indbrud den 5. juli, 2016, i DNC-serveren, har uafhængige cyber-efterforskere konkluderet, at en insiderperson kopierede DNC-data over på en ekstern lagerenhed.

Et hovedresultat af de uafhængige kriminaltekniske undersøgelser er den konklusion, at DNC-data blev kopieret over på en lagerenhed ***med en hastighed, der overstiger***

kapaciteten ved et udefrakommende Internet-hack. Hvad der er lige så vigtigt, så viser de tekniske undersøgelser, at kopieringen fandt sted på østkysten af USA. Hidtil har mainstream-medierne ignoreret resultaterne af disse uafhængige undersøgelser. [se her og her].

Den uafhængige analytiker Skip Folden, der trak sig tilbage efter 25 år som IBM Program Manager for Information Technology, USA, og som undersøgte de nylige kriminaltekniske resultater, er medforfatter af dette Memorandum. Han har udarbejdet en mere detaljeret teknisk rapport med titlen, *»Cyber-Forensic Investigation of 'Russian Hack' and Missing Intelligence Community Disclaimers«* (Kriminalteknisk cyber-undersøgelse af 'russisk hack' og manglende dementi fra efterretningssamfundet), og har sendt den til den særlige rådgivers kontor og justitsministerens kontor. VIPS-medlem William Binney, en tidligere teknisk direktør i National Security Agency (NSA), samt andre senior-NSA-»alumner« i VIPS, bevidner de uafhængige, tekniske resultaters professionalisme.

De nylige kriminaltekniske undersøgelser udfylder et afgørende hul. Hvorfor FBI forsømte at udføre uafhængige, kriminaltekniske undersøgelser af det oprindelige »Guccifer 2.0«-materiale, er fortsat et mysterium – og det samme er manglen på ethvert tegn på, at de »håndplukkede analytikere« fra FBI, CIA og NSA, der skrev »Vurderingen fra Efterretningssamfundet«, dateret 6. januar, 2017, ofrede kriminaltekniske undersøgelser nogen som helst opmærksomhed.

BEMÆRK: Der har været så megen sammenblanding af anklager om hacking, at vi ønsker at gøre dette Memorandas primære fokus helt klart. Vi fokuserer specifikt på det angivelige »hack« den 5. juli, udført af Guccifer 2.0, af DNC-serveren. I tidligere VIPS-memoranda adresserede vi manglen på ethvert bevis, der forbinder de angivelige Guccifer 2.0-hacks og WikiLeaks, og vi bad specifikt præsident Obama om at afsløre eventuelt bevis på, at WikiLeaks fik DNC-data fra russerne [se her og her].

Han adresserede dette punkt under sin sidste pressekonference (18. januar) og beskrev »efterretningssamfundets konklusioner« som »ikke endegyldige«, selv om Vurderingen fra Efterretningssamfundet af 6. januar gav udtryk for »stor overbevisning« om, at russisk efterretning »videresendte materiale, det fik fra DNC … til WikiLeaks«.

Obamas indrømmelse kom ikke som en overraskelse for os. Det har længe stået os klart, at grunden til, at den amerikanske regering mangler endegyldigt bevis på en overførsel af et »russisk hack« til WikiLeaks skyldes, at der ikke fandt en sådan overførsel sted. For det meste baseret på den kumulativt unikke, tekniske erfaring hos vore eks-NSA-kolleger, har vi i næsten et år sagt, at DNC-data kom til WikiLeaks via en kopi/et læk fra en DNC-insider (men næsten med sikkerhed ikke fra den samme person, der kopierede DNC-data den 5. juli, 2016).

Ud fra det tilgængelige materiale konkluderer vi, at den samme *proces* med en inside-DNC-kopi/et læk blev brugt på to forskellige tidspunkter, af to forskellige enheder, og til to klart forskellige formål:

- Et inside-læk til WikiLeaks, før Julian Assange den 12. juni meddelte, at han var i besiddelse af DNC-dokumenter og planlagde at offentliggøre dem (hvilket han gjorde den 22. juli) – hvor det formodede formål var at afsløre en stærk partiskhed til fordel for Clinton-kandidaturet, og
- Et særskilt læk den 5. juli, 2016, for på forhånd at forfalske noget, WikiLeaks senere måtte offentliggøre, ved at »vise«, at det kom fra et »russisk hack«.

Hr. præsident,

Dette er vores første VIPS-memorandum til Dem, men vi har en historie for at lade amerikanske præsidenter vide, hvornår vi

mener, vore tidligere efterretningskolleger har taget fejl i noget, der er vigtigt, og hvorfor. For eksempel advarede vores første sådant memorandum, en kommentar til præsident George W. Bush om Colin Powells tale i FN den 5. februar, 2003, om, at de »utilsigtede konsekvenser sandsynligvis ville blive katastrofale«, ifald USA angreb Irak og »retfærdiggjorde« krigen ved hjælp af efterretninger, som vi pensionerede efterretningsofficerer let kunne se, var svindel og drevet af en krigsdagsorden.

»Vurderingen fra Efterretningssamfundet« den 6. januar, af »håndplukkede« analytikere fra FBI, CIA og NSA, synes at passe ind i den samme kategori med at være drevet af en dagsorden. Den er i vid udstrækning baseret på en »vurdering«, og ikke støttet af nogen øjensynlige beviser, der går ud på, at en dunkel enhed med tilnavnet »Guccifer 2.0«, hackede DNC på vegne af russisk efterretning og gav DNC-e-mails til WikiLeaks.

De nylige, ovenfor nævnte resultater har slået et enormt skår i denne vurdering og sået alvorlig tvivl om fundamentet for den usædvanligt succesfulde kampagne for at lægge skylden på den russiske regering for hacking. De lærde hoveder og politikere, der har anført angrebet mod russisk »indblanding« i det amerikanske valg, kan forventes at forsøge at så tvivl om disse kriminaltekniske resultater, skulle disse nogensinde finde på at boble op til overfladen i mainstream-medierne. Men de tekniske begrænsninger af nutidens Internet forstås bredt. Vi er parat til at besvare alle substantielle udfordringer på basis af deres fortjenester.

De kunne måske tænke Dem at spørge CIA-direktør Mike Pompeo om, hvad han ved om dette. Vores egen lange erfaring i efterretningssamfundet indikerer, at det er muligt, at hverken tidligere CIA-direktør John Brennan, eller de cyber-krigere, der arbejdede for ham, har været fuldstændig oprigtige over for deres nye direktør med hensyn til, hvordan alt dette fandt sted.

Kopieret, ikke hacket

Som ovenfor anført, så fokuserede det netop afsluttede, uafhængige, kriminaltekniske arbejde på data, der var *kopieret (ikke hacket)* af et dunkelt individ ved navn »Guccifer 2.0«. De kriminaltekniske beviser reflekterer det, der synes at have været en desperat bestræbelse på at »give russerne skylden« for at offentliggøre særdeles pinlige DNC-e-mails tre dage før det Demokratiske partikonvent sidste juli. Eftersom indholdet af DNC-e-mailene stank af partiskhed til Clintons fordel, så hendes kampagne det tvingende nødvendigt at aflede opmærksomheden fra indhold til herkomst – som i hvem »hackede« disse DNC-e-mails? Kampagnen blev entusiastisk støttet af de føjelige »mainstream«-medier; det kører stadig for dem.

»Russerne« var den ideelle synder. Og, efter at WikiLeaks redaktør Julian Assange den 12. juni, 2016, meddelte, »Vi har e-mails relateret til Hillary Clinton, der afventer offentliggørelse«, havde hendes kampagne mere end en måned før konventet til at indskyde sine egne »kriminaltekniske fakta« for at forberede medie-pumpen til at lægge skylden på »russisk indblanding«. Fr. Clintons PR-chef Jennifer Palmieri har forklaret, hvordan hun brugte golfvogne til at foretage runderne under konventet. Hun skrev, at hendes »mission var at få pressen til at fokusere på noget, som selv vi fandt vanskeligt at forarbejde: nemlig udsigten til, at Rusland ikke alene havde hacket og stjålet e-mails fra DNC, men at det havde gjort det for at hjælpe Donald Trump og skade Hillary Clinton«.

Uafhængige cyber-efterforskere har nu fuldført den form for kriminalteknisk arbejde, som efterretningsvurderingen ikke gjorde. Mærkeligt nok stillede disse »håndplukkede« efterretningsanalytikere sig tilfredse med at »vurdere« dit og »vurdere« dat. I modsætning hertil gravede efterforskerne dybt og kom op med verificerbare beviser fra metadata, der blev

fundet i registreringen af det angivelige russiske hack.

De fandt, at det påståede »hack« af DNC af Guccifer 2.0 ikke var noget hack, af Rusland eller af nogen andre. Det stammede snarere fra en kopiering (over på en ekstern lagerenhed – som f.eks. et USB-stik) udført af en insider. Data blev lækket for at involvere Rusland. Vi ved ikke, hvem eller hvad, den skumle Guccifer 2.0 er. Vi foreslår, De spørger FBI.

Den kronologiske rækkefølge

12. juni, 2016: Assange meddeler, at WikiLeaks står foran at offentliggøre »e-mails relateret til Hillary Clinton«.

14. juni, 2016: DNC-kontrahent Crowdstrike (der har en tvivlsom professionel historie og utallige interessekonflikter) meddeler, at skadelig software er blevet fundet på DNC-serveren og hævder, der er beviser for, at det blev indført af russere.

15. juni, 2016: »Guccifer 2.0« bekræfter DNC-erklæringen; påtager sig ansvaret for »hacket«; hævder at være en kilde til WikiLeaks; og udlægger et dokument, som tekniske undersøgelser viser, er forfalsket med »russiske fingeraftryk«.

Vi mener ikke, at timingen med den 12., 14. og 15. juni var rent tilfældig. Det antyder snarere begyndelsen af et forebyggende træk for at associere Rusland til det, WikiLeaks måske stod for at offentliggøre, og »vise«, at det kom fra et russisk hack.

Hovedbegivenheden

5. juli, 2016: I de tidlige aftentimer, Eastern Daylight Time (EDT), kopierede nogen i EDT-tidszonen med en computer, der var direkte tilsluttet DNC-serveren eller DNC Local Area

network, 1.976 megabyte data på 87 sekunder over på en ekstern lagerenhed. ***Denne hastighed er langt hurtigere end det, der er muligt med et hack*.**

Det fremstår således som, at det påståede »hack« af DNC af Guccifer 2.0 (den selvudråbte kilde til WikiLeaks) ikke var et hack af Rusland eller nogen anden, men snarere var en kopiering af DNC-data over på en ekstern lagerenhed.

»Tilsløring & af-tilsløring«

Hr. præsident, den neden for beskrevne afsløring kan være relateret. Selv om det ikke skulle være det, mener vi, det er noget, De bør gøres opmærksom på i denne generelle forbindelse. Den 7. marts begyndte WikiLeaks at offentliggøre en skattekiste af originale CIA-dokumenter, som WikiLeaks markerede med navnet »Vault 7«. WikiLeaks sagde, det havde fået skattekisten fra en nuværende eller tidligere CIA-kontrahent og beskrev den som sammenlignelig i omfang og betydning med den information, Edward Snowden gav reportere i 2013.

Der er ingen, der har sat spørgsmålstegn ved ægtheden af de originale dokumenter i Vault 7, der afslører et stort spektrum af redskaber til cyber-krigsførelse, der sandsynligvis var blevet udviklet med hjælp fra NSA, af CIA's Tekniske Udviklingsgruppe. Denne gruppe var en del af det vidtstrakte CIA Direktorat for Digital Innovation – en vækstindustri etableret af John Brenan i 2015.

Digitale redskaber, man næppe forestiller sig – som kan tage kontrol over din bil og få den til at køre med over 100 miles/timen, for eksempel, eller som kan gøre det muligt at spionere gennem et Tv-apparat – blev beskrevet og behørigt rapporteret i *New York Times* og andre medier i hele marts måned. Men offentliggørelsen af Vault 7, del 3 den 31. marts, der afslørede programmet »Marble Framework«, blev

tilsyneladende vurderet til at være for delikat til at kunne kvalificere som »nyheder, der kunne trykkes« og blev holdt ude af *New York Times*.

Ellen Nakashima fra *Washington Post*, tilsyneladende, »fik ikke memoet« i tide. Hendes artikel af 31. marts havde den opsigtsvækkende (og korrekte) overskrift: »**WikiLeaks' seneste offentliggørelse af CIA's cyber-redskaber kunne afsløre tjenestens hacking-operationer«.**

WikiLeaks' offentliggørelse indikerede, at Marble var designet til fleksibel og brugervenlig »tilsløring«, og at Marble-kildekoden inkluderer en »af-tilsløring«, der kan omstøde CIA's tekst-tilsløring.

Hvad der er vigtigere, så skal CIA angiveligt have brugt Marble i løbet af 2016. Nakashima udelod dette i sin *Washington Post* rapport, men inkluderede en anden, betydningsfuld pointe, som WikiLeaks fastslog; nemlig, at tilslørings-redskabet kunne bruges til at udføre et »dobbeltspil mht. tilskrivning til tekniske undersøgelser« eller operation under falsk flag, fordi det inkluderer prøver på kinesisk, russisk, koreansk, arabisk og persisk.

CIA's reaktion var skarp. Direktør Mike Pompeo gik til angreb to uger senere og kaldte Assange og hans medarbejdere for »dæmoner« og fremførte; »Tiden er inde til at udråbe WikiLeaks som det, det virkeligt er, nemlig en ikke-statslig, fjendtlig efterretningstjeneste, der ofte tilskyndes af statslige aktører som Rusland.«

Hr. præsident, vi ved ikke, om CIA's Marble Framework, eller lignende redskaber, spillede en eller anden rolle i kampagnen med at give Rusland skylden for at hacke DNC. Vi ved heller ikke, hvor oprigtige skabningerne i CIA's Digital Innovation Direktorate har været over for Dem, og over for direktør Pompeo. Dette er områder, der måske ville have gavn af Det Hvide Hus' snarlige gennemgang.

Putin og teknologi

Vi ved heller ikke, om De har haft en grundig diskussion om cyber-spørgsmål med præsident Putin. I sit interview til NBC's Megyn Kelly synes han ganske villig til – endda ivrig for – at adressere spørgsmål med relation til den form for cyber-redskaber, der afsløres i Vault 7-afsløringerne, om ikke for andet, så for at indikere, at han er blevet briefet om dem. Putin påpegede, at nutidens teknologi gør det muligt at »maskere og kamuflere hacking i en grad, hvor ingen kan forstå oprindelsen [af hackingen] … Og, vice versa, så er det muligt at skabe en enhed eller et individ, som alle vil tro på, er den nøjagtige kilde til dette angreb.«

»Hackere kan være overalt«, sagde han. »Der kunne for øvrigt være hackere i USA, der meget dygtigt og professionelt gav sorteper videre til Rusland. Kan I ikke forestille jer et sådant scenarie?… Det kan jeg.«

Fuld afsløring: I løbet af de seneste årtier er ånden i vores efterretningsprofession udhulet i offentlighedens mening til et punkt, hvor man vurderer, at en analyse, der ikke har en dagsorden, er noget nær en umulighed. Vi tilføjer derfor dette dementi, som gælder for alt, vi i VIPS siger og gør: Vi har ingen politisk dagsorden; vores eneste formål er at udbrede sandhed og, når det er nødvendigt, stille vore tidligere efterretningskolleger til ansvar.

Vi taler og skriver uden frygt eller fordel. Som følge heraf er enhver lighed mellem det, vi siger, og det, præsidenter, politikere og lærde eksperter siger, rent tilfældig. Den kendsgerning, at vi finder det nødvendigt at inkludere denne påmindelse, siger meget om disse højst politiserede tider. Dette er vores 50. VIPS-memorandum siden den eftermiddag, Powell holdt sin tale i FN. Links til de forudgående 49 memoer

kan findes her.

FOR STYRELSESGRUPPEN, VETERAN INTELLIGENCE PROFESSIONALS FOR SANITY:

William Binney, tidligere NSA teknisk direktør for World Geopolitical & Military Analysis; medstifter af NSA's Signals Intelligence Automation Research Center

Skip Folden, uafhængig analytiker, pensioneret IBM Program Manager for Information Technology US (Medarbejder VIPS)

Matthew Hoh, tidligere kaptajn, USMC, Irak & Udenrigstjenesteofficer, Afghanistan (medarbejder VIPS)

Larry C. Johnson, CIA & Udenrigsministeriet (pensioneret)

Michael S. Kearns, Efterretningsofficer i Flyvevåbnet (pensioneret), Master SERE Resistance to Interrogation Instructor

John Kiriakou, tidligere CIA-kontraterrorofficer og tidligere seniorefterforsker, Senatskomite for Udenrigsrelationer

Linda Lewis, analytiker af politik for beredskab af masseødelæggelsesvåben (WMD), USDA (Landbrugsministeriet), pensioneret

Lisa Ling, TSgt (Teknisk sergent) USAF (USA's Luftvåben) (pensioneret), (medarbejder VIPS)

Edward Loomis, jr., tidligere NSA tekniks direktør for Office of Signals Processing

David MacMichael, National Intelligence Council, (pensioneret)

Ray McGovern, tidligere U.S. Army Infantry/efterretningsofficer og CIA-analytiker

Elizabeth Murray, tidligere Deputy National Intelligence Officer for Mellemøsten, CIA

Coleen Rowley, FBI Special Agent og tidligere Minneapolis Division Legal Counsel (pensioneret)

Cian Westmoreland, tidligere USAF Radio Frequency Transmission Systems tekniker og Unmanned Aircraft Systems whistleblower (medarbejder VIPS)

Kirk Wiebe, tidligere senioranalytiker, SIGINT Automation Research Center, NSA

Sarah G. Wilton, efterretningsofficer, DIA (pensioneret); kommandør, US Naval Reserve (pensioneret)

Ann Wright, U.S. Army reserveoberst (pensioneret) og tidligere amerikansk diplomat