FRIVÄRLD
STOCKHOLM FREE WORLD FORUM

PATRIK OKSANEN

DEN RYSKA CYBERATTACKEN MOT STORTINGET

Sammanfattning

Den 13 oktober, drygt ett år före valet till det norska Stortinget, pekade den norska regeringen ut den Ryska federationen som skyldig till ett cyberangrepp mot Stortinget med syfte att komma över information från norska politiker.

Mönstret att hacka andra länders politiker för att påverka den politiska debatten är återkommande från rysk underrättelsetjänst. Så skedde med den tyska förbundsdagen 2016, Demokraternas e-post i USA inför presidentvalet 2016 och Macrons presidentvalskampanj i Frankrike 2017.

Ryssland har i skarpa ordalag förnekat hackningen. Ryssland genomförde också en flygning med strategiskt bombflyg med nukleär kapacitet i norska havet efter att norska regeringen pekat ut Ryssland. Enligt ryska försvarsministeriets hemsida var detta en planerad flygning.[1]

För att bygga avskräckning mot cyberangrepp behöver västliga demokratier bygga upp en trovärdig respons som går längre än ”name and shame” från enskilda länder. Agerandet behöver utföras i solidaritet mellan olika länder för att skapa avskräckning. I dag är priset för angrepp i gråzonen alldeles för lågt.

Ad notam: Norska citat är på originalspråk. Övriga är översatta.

[1] Ryska försvarsministeriet, 2020. ”Два стратегических ракетоносца Ту-160 выполнили плановый полет над нейтральными водами Баренцева, Норвежского и Северного морей”, 15 oktober.

Detta har hänt

Det var i slutet av augusti som Stortinget, Norges parlament, upptäckte att e-postsystemet hade hackats. En vecka senare gick Stortinget ut och berättade att det skett ett omfattande cyberangrepp, där ett antal stortingsledamöter och anställda drabbats. Stortingets direktör Marianne Andreassen sade på presskonferensen att *"Vi vet at data er hentet ut, men vet ikke hva slags data".* Arbeiderpartiet (S) och Senterpartiet (C) berättade i samband med presskonferensen att de hade drabbade ledamöter. Övriga partier hänvisade till Stortingets direktion eller kände inte till att de varit utsatta.[2]

Kort därefter meddelade norska säkerhetspolisen, PST, att myndigheten misstänkte en statlig aktör och en underrättelseoperation. Kring samma tid kom nyheten att e-postadresser för 10 000 anställda i sju inlandskommuner i Norge utsatts för intrångsförsök. E-posten såg ut att komma från kollegor men innehöll skadlig kod.[3]

Den Nationella Säkerhetsmyndigheten (Norges motsvarighet till MSB) gick den 7 september ut i ett pressmeddelande att myndigheten *"ser nå lignende mistenkelig aktivitet hos andre. Både private og offentlige virksomheter er berørt."* Dock specificeras inte vilka som angripits.[4]

Senare uppgav Stortinget för NTB, Norsk telegrambyrån, att angriparna kan ha fått "*tilgang til private opplysninger om flere representanter". [5]*

Historien tog en ny vändning då Norges regering officiellt gick ut och namngav Ryssland 13 oktober i ett pressmeddelande: "*Basert på det informasjonsgrunnlaget regjeringen besitter, er det vår vurdering at Russland står bak denne aktiviteten."* [6]

Agerandet var oväntat snabbt i ett internationellt perspektiv, ofta har det tagit betydligt längre tid innan gärningspersonerna kartlagts och offentliggjorts. Norges utrikesminister Ine Eriksen Søreide utvecklade det för NRK och kallade dataangreppet mot Stortinget för *"ei veldig alvorleg hending, og at det er viktig å halde Russland ansvarleg for angrepet. Å gå ut offentleg og legge skulda på Russland er ein del av ansvarleggjeringa."* Bakom utpekandet ligger underrättelseanalys som inte närmare specificeras.[7] Dagen efter kommenterade Norges statsminister Erna Solberg angreppet med *"det er viktig at Noreg reagerer tydeleg når me opplever at andre land handlar feil".[8]*

Vilka ligger bakom?

Norska regeringen har pekat ut Ryssland som ansvarigt, utan att närmare ange vilken gruppering som utfört angreppet. Sett till tidigare cyberangrepp är det något som både SVR, utrikesunderrättelsetjänsten, och GRU, den militära underrättelsetjänsten, ägnat sig åt. Aftenposten har i en artikel pekat ut "Kremls superhackare" från GRU: s avdelning 26165 som huvudmisstänkta för angreppet.

---

[2] Kalajdzic, P., mfl., 2020 "Stortinget utsatt for et omfattende IT-angrep", NRK, 1 september.
[3] Krantz, A., mfl., 2020 "Dataangrepet: Kan skade Korona-beredskapen", NRK, 2 september.
[4] 2020, "Flere norske virksomheter ramme av datorinbrudd", Nasjonal Sikkerhetsmyndighet, 7 september.
[5] 2020, "Kan ha fatt tilgang til privat info", NRK, 8 oktober.
[6] 2020, "Datainbruddet i Stortinget,Regjeringen, 13 oktober.
[7] 2020, "Viktig å halde Russland ansvarleg", NRK, 13 oktober.
[8] 2020, "Viktig at Noreg seier frå", NRK, 14 oktober.

En av GRU: s cyberoperatörer nämns vid namn i artikeln, en person som är efterlyst av både tysk och amerikansk polis. I Tyskland ska han ha varit inblandad i hackningen av den tyska förbundsdagen 2015 och i USA handlar det både om demokraternas e-post 2016 och angrepp på antidopningsbyrån. Det sistnämnda cyberangreppet var en del i en kampanj mot det internationella arbetet mot dopning för att relativisera den ryska dopningen. I den kampanjen har även svenska Riksidrottsförbundet angripits.[9]

Nyligen blev sex av den namngivne GRU-hackarens kollegor i GRU åtalade i USA, misstänkta för cyberangrepp bland annat mot OS, Macronkampanjen och det georgiska parlamentet.[10]

Ryska reaktioner

De ryska reaktionerna har följt det klassiska mönstret av förnekelse, motangrepp och anklagelser. Den ryska ambassaden i Oslo skrev på sin Facebooksida att *”sådana anklagelser om vårt land är oacceptabla”* och att Ryssland betraktar det ”*som en seriös avsiktlig provokation, destruktiv för bilaterala förbindelser.”*[11] Norge anklagas också för bristande vilja att föra dialog om cyberintrång.

Samma kväll som norska regeringen pekade ut Ryssland kom reaktioner från Moskva. Ordförande i Federationsrådets utrikesutskott Konstantin Kosatsjov hävdade att beskyllningarna var grundlösa till ryska statliga nyhetsbyrån Tass: *”Som alltid kommer det beskyllningar mot Ryssland, utan att man bryr sig om att bevisa dessa och utan att man föreslår att dryfta det på expertnivå”.*[12] Kosatsjov tog också upp händelsen från 2018 då en rysk medborgare satt i norskt häkte en månad efter misstänkt spioneri vid en konferens i Stortinget. Mannen var seniorrådgivare när det gäller informationsteknologi i Federationsrådet.

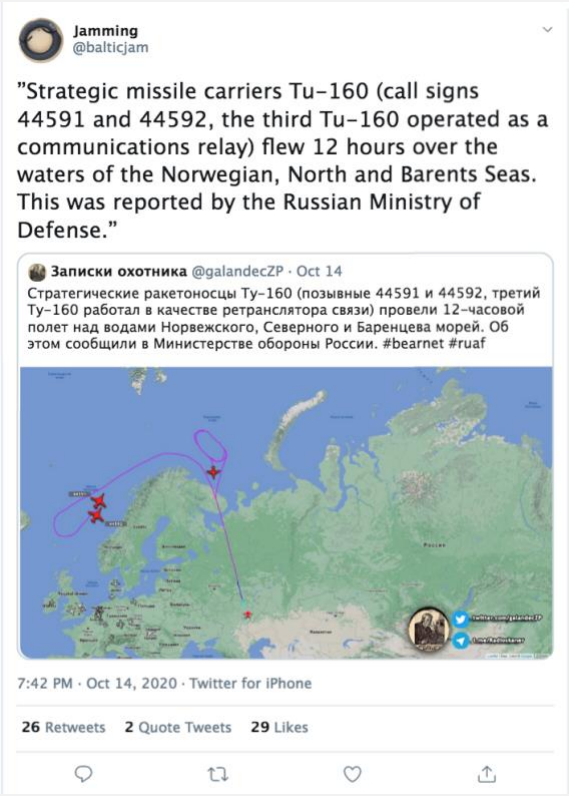
Rådgivaren vid det ryska säkerhetsrådet Andrej Manoilo anklagade USA för att ligga bakom tonläget: *”Norska UD har antagligen inte önskat att uttrycka sig så skarpt, men uttalandet kan ha kommit till stånd genom kraftiga påtryckningar från USA”.* Vidare kom Manoilo med påståendet att det var *”ointressant och meningslöst”* att gräva i folkvaldas e-poster.[13] Ett uttalande som bygger på att alla plötsligt skulle ha glömt de tidigare e-post-attackerna i USA och Frankrike.

---

[9] 2020, ”Er dette de russiske hackerne som angrep Stortinget? De elsker bandet Queen. Putin kaller dem kunstnere”, Aftenposten, 14 oktober.
[10] 2020, ”Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace”, Department of Justice, 19 oktober.

[11] 2020, ”Комментарий Посольства России в Норвегии”, Russian Embassy in Norway, 13 oktober.
[12] 2020, ”Russisk etterretningsekspert: Uinteressant og meningsløst å grave i Stortingets e-post”, NRK, 14 oktober.
[13] Ibid.

En händelse att notera inträffade dagen därpå, 14 oktober, men som enligt ryska försvarsministeriet var planerad sedan tidigare. Det ryska strategiska bombflyget gick upp och flög med TU-160. TU-160 är ett flygplan med kapacitet att bära kärnvapen. Flygningen pågick i tolv timmar och skedde framför allt i Norska havet och Barents hav.[14] Ryssland kommunicerar återkommande på olika sätt för att påminna om sin nukleära kapacitet i både ord och handling, och här går det inte att bortse från tidpunkten då detta skedde.



Därefter gick ryska UD:s presstalesperson Maria Zakharova till angrepp mot Norge med anklagelser om att Norge brukar destruktiva metoder som skadar de redan dåliga bilaterala relationerna ytterligare. Zakharova hävdade också att Norge inte har några bevis.[15]

Övriga reaktioner

Nyheten har fått stor uppmärksamhet i internationell press. Men det enda landet, förutom Norge och Ryssland, som Frivärld har kunnat hitta som uttalat sig officiellt med anledning av cyberattacken är Ukraina. Landets utrikesminister Dmytro Kuleba gick ut och krävde att Ryssland måste hållas ansvarig för angreppet och att *"Euro-Atlantisk solidaritet och ömsesidigt stöd är nyckeln för att möta utmaningar från hybridkriget".*[16]

På direkt fråga till norska UD vilka länder som uttryckt stöd till Norge efter angreppet så svarar presstjänsten att det inte är några uppgifter som Norge sammanställer öppet.

Slutsats

Cyberoperationen mot Stortinget följer ett klassiskt ryskt mönster, att attackera politiska församlingar för att skaffa underlag både för analys om svagheter, men också information som på olika sätt kan användas i påverkansoperationer. Information som kan utnyttjas och manipuleras för att undergräva tilltron till det demokratiska systemet och elda på konflikter inom demokratier. Operationerna har haft blandad framgång, där interventionen i det amerikanska presidentvalet 2016 får betraktas som det för Ryssland mest lyckade exemplet.

Relationerna mellan Norge och Ryssland har varit ansträngda ett tag. Här finns både misstänkta spionaffärer och geopolitiska spänningar som ökar friktionen. Ryssland har på olika sätt ifrågasatt norsk suveränitet på Svalbard och vill nu även föra in säkerhet i det

[14] Ryska försvarsministeriet, 2020. "Два стратегических ракетоносца Ту-160 выполнили плановый полет над нейтральными водами Баренцева, Норвежского и Северного морей", 15 oktober.
[15] 2020, "Russland: Noreg skadar forholdet", NRK, 15 oktober.
[16] 2020, " Ukraine's MFA calls for Russia's responsibility for cyberattack on Norway", 112 UA, 15 oktober

Arktiska rådet.[17] Även om Ryssland försöker lägga skulden på Norge är det Kremls agerande som steg för steg höjer temperaturen. Det är en medveten strategi från Putin-regimen.

Men frågan handlar inte bara om Norge. Det ryska agerandet är desamma mot hela västvärldens demokratier; i syfte att underminera statsskicket, försvaga beslutsfattande, skapa splittring i länderna och bryta ned multilaterala samarbeten som EU och Nato.

Det finns två sätt att stoppa cyberangrepp. Det ena är att ha ett tillräckligt robust cyberförsvar att det är omöjligt att komma åt informationen. Tyvärr är det en kapplöpning mellan angripare och försvarare, där angriparen ligger före och tvingar försvararen att försöka parera. Det går alltså att göra det svårare och mer tidskrävande för angriparen, men det går inte att i alla lägen stoppa en potentiell cyberangripare.

Det andra handlar om att skapa ett politiskt pris där statsaktörer följaktligen, antingen direkt eller via ombud, väljer att avstå. Tröskeln – och därmed kostnaden - måste alltså höjas avsevärt. Enbart utpekande från Oslo kommer inte att räcka, även om ”name och shame” är bättre än att tiga om vem som ligger bakom. Ukrainas stöduttalande borde ha upprepats av Sveriges utrikesminister Ann Linde och samtliga utrikesministrar i EU och Nato. Ett unilateralt agerande visar ingen styrka och skapar inte den avskräckningseffekt som behövs.

Naturligtvis är det kombinationen av ett bra cyberförsvar och ett tydligt pris för angriparen som ger effekt. Det ska vara svårt att ta sig in och det ska vara kännbart smärtande när man försöker. Det ska understrykas att det inte bara är Ryssland som ägnar sig åt cyberangrepp, utan även Kina, Iran och en rad andra länder.

Utan kostnad och internationella ramverk för konsekvenser kommer det inte finnas något incitament för statsaktörer att upphöra med cyberangreppen. Det här problemet kommer inte att minska under 2020-talet.

Rekommendationer

- Sverige bör ta initiativ i den baltisk-nordiska kretsen att skapa ett protokoll för snabba stöduttalande vid cyberangrepp där främmande makt pekas ut. Det här bör sedan etableras på EU-nivå, eller med en ”coalition of the willing” där Ukraina finns med. Andra tänkbara länder utanför Norden och EU-kretsen är Storbritannien, Kanada, Sydkorea, Japan, Australien, Nya Zeeland och Taiwan.

- Sanktionsverktyg mot ansvariga individer bakom statsaktörers cyberangrepp bör införas.

- Utvisning av diplomater bör ske koordinerat och i solidaritet som svar på cyberangrepp mot demokratiska institutioner och nationella säkerhetsstrukturer.

[17] 2020, ”Se upp för Svalbard”, HBL, 16 oktober.