

Virus som herjet med det iranske atomprogrammet

# Digitalt angrep mot Iran

**Datavirus.** Samtidig som forhandlingene om Irans atomprogram startet i Istanbul i januar, dukket det opp noen sensasjonelle avsløringer: Dataviruset Stuxnet som rammet Iran skal ha blitt utviklet i Israel med amerikansk hjelp.

**PHILIPPE RIVIÈRE**

Journalist, franske Le Monde diplomatique.

«**ET NYTT** Tsjernobyll!» Nylig skapte Russlands NATO-ambassadør, Dimitrij Rogozin, sensasjon da han ba om en granskning av Stuxnet, dataviruset som har angrepet iranske atomanlegg de siste månedene. Viruset kunne ifølge ham ha ført til en kjernefysisk nedsmelting i atomreaktoren i Busher sør i Iran.

En «virtuell» og «fullstendig ubegrunnet» påstand, svarer den tyske sikkerhetseksperten Ralph Langner, som i september laget den første komplette studien av viruset. «For det første var ikke Busher målet til Stuxnet.» Målet var faktisk Natanz, der 7000 sentrifuger for anrikning av uran ble rammet. «For det andre, selv om dette var tilfellet, ville det ikke kunne nå systemene i fremste krets [som er i kontakt med det radioaktive materialet]. Det morsomme er at russerne vet dette svært godt.» For Russland er Irans viktigste partner på dette området. Stuxnet-saken, historien om en høyteknologisk sabotasje, er som en roman der handlingen glir rask fra datakode til et skyggespill av IT og diplomati.

**NOEN FAKTA** later til å være etablert. De som laget viruset har brukt mye tid på det (kildekoden på rundt 15 000 linjer må ha krevd rundt ti «ingeniør-år») og hatt avansert kunnskap (ormen brukte fire ukjente hull i operativsystemet Windows for å overføre viruset). «Analysen av koden indikerer tydelig at Stuxnet ikke har som mål å sende et budskap eller demonstrere et konsept,» skriver Langner. «Det dreier seg om å ødelegge målene, med en militær besluttsomhet.» Ifølge en rapport fra antivirusselskapet Kaspersky i Moskva har Stuxnet-ormen som dukket opp i 2009 spredt seg i en rekke land, særlig i India, som er hardest rammet med 8565 infiserte maskiner (i september 2010), og Indonesia (5148), mens Iran kommer på tredjeplass med 3062 kjente tilfeller.

Var målet de iransk atominstallasjonene? Det hevder en svært detaljert artikkel i New York Times 15. januar 2011. Ifølge anonyme amerikanske og israelske kilder skal viruset ha blitt utviklet for formering i et system med samme størrelse som nettverket av sentrifuger i Natanz. Og arbeidet skal ha blitt utført i atomanlegget Dimona, i hjertet av det israelske militære atomprogrammet i Negevørkenen. Artikkelen avslutter med at «det hemmelige kappløpet for å skape Stuxnet var et samarbeidspro-



Ahmadinejad på besøk i atomanlegget i Natanz, som Stuxnet etter all sannsynlighet var programmert til å ramme. Foto: Irans pressetjeneste.

sjeikt mellom amerikanerne og israelerne, med bevisst eller ubevisst bistand fra tyskerne og britene».<sup>2</sup>

Tyskerne det her dreier seg om er firmaet Siemens som lager IT-systemene for industriell overvåkning («Scada») som brukes i det iranske atomanlegget. Ifølge enkelte scenarier skal Stuxnet ha trengt seg inn i Natanz gjennom en USB-nøkkel som ble infisert av de russiske leverandørene. Deretter skal viruset, etter å ha gjenkjent sitt mål (merket til enkelte frekvenskontroller), aktivert en angrepsseseks verdig en hollywoodfilm: Mens det viste tilsynelatende normale data på sikkerhetsskjermene, skal viruset gjentatte ganger ha økt rotasjonsfrekvensen til sentrifugene og kjørt rotorene til tålegrensen for å skape en unormal mengde skader.

skal Teheran ha blitt rammet av «en stadig økende tilbakeslag».<sup>4</sup> Rapporten lister opp: «økende vansker med å få tak i uunnværlige deler på det internasjonale markedet, driftsproblemer for et stort antall av sentrifugene, og noe som kan ligne på hemmelige aksjoner utført av utenlandske etterretningsorganisasjoner». Blant de sistnevnte finner vi «dataangrep, sabotasje på nøkkelutstyr Iran leter etter i utlandet, infiltrasjon og forstyrrelse av Irans smuglernetverk, og mord på atomekspertene». Det siste rammet fysikeren Majid Shahriari som døde 29. november 2010 da bilen hans eksploderte. Men ifølge rapportens forfattere, David Albright og Andrea Stricker, «virker det som om de største problemene har blitt forårsaket av Stuxnet, som begynte å ramme gassentrifugene i anrikningsan-

«**Etter først å ha kalt det et eventyr, innrømmet Ahmadinejad at dataormen hadde skapt «enkelte problemer».**

**ISRAEL** har ikke sagt at de står bak viruset, men de har heller ikke benektet det. Stuxnet inngår i utbudet av sabotasjehandling mot det iranske atomprogrammet som tidligere Mossad-sjef Meir Dagan nylig skrøt av å ha forsinket «med flere år: iranerne vil ikke ha atomvåpen før i 2015».<sup>3</sup> Ifølge en rapport fra American Peace Institute

legget Natanz i 2009». Etter først å ha kalt det hele et eventyr, innrømmet den iranske statslederen Mahmoud Ahmadinejad høsten 2010 at dataormen hadde skapt «enkelte problemer», som var «blitt løst».

I en artikkel i tidsskriftet Nuclear Intelligence Weekly trekker tidligere FN-våpeninspektør for Irak (1991-1998), Scott Rit-

ter, fram noen besynderlige variasjoner i de ulike framstillingene av saken: «Både amerikanske og israelske talspersoner har antydnet at Stuxnet for øyeblikket har hemmet Irans anrikningsprogram. [...] Men en nylig gjennomgang utført av Federation of American Scientist, på bakgrunn fra data fra FN's atominspektører, indikerer at Iran i 2010 faktisk økte omfanget og effektiviteten til anrikningen, på tross av Stuxnet-angrepet.»

**DISSE FORSKJELLENE** skyldes ifølge Ritter «kappløpet» mellom Iran og «P5+1» (de fem permanente medlemmene i FN's sikkerhetsråd – Kina, USA, Frankrike, Storbritannia og Russland – og Tyskland). «Slike faktabaserte gjennomganger har blitt ignorert til fordel for spekulasjoner om potensielle scenarier». Siden diplomatene i snart tjue år har hevdet at Iran er på nippet til å skaffe seg en atombombe, har de «begrenset de politiske valgmulighetene til de som dreier seg om disse overdrevne hypotesene» hevder Ritter. Dermed skal de ha innsnevret debatten. Forsinkelsen som tilskrives sabotasjeoperasjonen gir rom for å fortsette forhandlingene uten å miste ansikt.

Skal man dermed hylle Stuxnet for å ha minket farene for et «preventivt angrep»? Foruten den åpenbare asymmetrien mellom de to naboene – de israelske atombombene er verdens «dårligst bevarte hemmelighet», mens det iranske programmet virker å ha et godt stykke igjen – kan sabotasjeaksjoner i fredstid føre til represalier eller opptrapping. Det er altså paradoksal om de mest avanserte landene, som i utgangspunktet har mest å tape, skulle legitimere slike aksjoner. Men datapiratvirksomhet er en kampsport, der angrep er det beste forsvar.

I Washington, der man har friskt i minne hvordan Googles e-postsystem ble hacket (sannsynligvis av kineserne, har presidenten bedt om en knapp som kan stenge internettet, som en siste forsvarslinje i tilfelle «dataangrep fra utlandet». Estland, som i 2007 ble rammet av et ukjent «dataangrep» (som de fleste tror stammet fra Russland), huser nå Natos forsvarssenter for dataangrep.

Oversatt av R.N.

→ og presidenter, næringslivsledere, militærdere og kirkeledere som hadde nær tilknytning til pressen. I mai 2008 ble overvåkingen avslørt av en varsler. Like etter ble fem ledere og flere andre ansatte permittert. Tyskland implementerte EUs datalagringsdirektiv i 2008, men begrenset lagringstiden til seks måneder. I mars 2010 vendte imidlertid det tyske rettsvesenet ryggen til direktivet, da den tyske forfatningsdomstolen erklærte datalagringsdirektivet grunnlovstridig i forbindelse med en lov som ga myndighetene rett til å lagre data om borgere for anti-terrorismeformål. Domstolen kalt loven «en alvorlig innblanding» i enkeltborgeres personvern.<sup>16</sup>

Etter at direktivet ble innført gikk antall alvorlige forbrytelser i Tyskland opp fra 1,36 millioner saker i 2007 til 1,42 millioner i 2009,<sup>17</sup> mens oppklaringsprosenten sank fra 77,6 prosent til 76,3 prosent i samme periode.

Szymielewicz fra Panoptikon Foundation mener EU med datalagringsdirektiv har gitt seg selv et mektig overvåkningsredskap, samtidig som det mangler gode mekanismer for å beskytte personvernet. «Hvis EU ikke ønsker at direktivet i praksis forblir et undertrykkende og kontroversielt instrument som begrenser våre grunnleggende rettigheter, må det innføres effektive beskyttelsestiltak. Mangelen på slike tiltak åpner for misbruk,» sier Szymielewicz.

Foreløpig ser hun ikke annen utvei enn å kjempe lokalt og nasjonalt for å kunne begrense direktivets konsekvenser i Polen. «Staten vil alltid være sterkere enn det sivile samfunnet når det gjelder å utforme lovene. Direktivet burde heller omformes til et verktøy for å begrense statens makt til å overvåke. Hvis EU velger å beholde datalagringsdirektivet, burde de påkrevne rettslig kontroll over anmodninger om tilgang til trafikkdata,

begrense antallet instanser som kan søke om slik adgang og under hvilke omstendigheter slike data kan bli brukt til å oppklare forbrytelser,» mener Szymielewicz.

Arnbak fra Bits of Freedom håper EU i større grad vil legge begrensninger på bruken av datalagringsdirektivet i fremtiden. Han mener det allerede er endringer på vei etter Lisboa-traktaten. «Det store problemet med datalagringsdirektivet i 2005 var at det var det mest enorme stykket EU-lovgiving som har blitt iverksatt. Ingen direktiv har blitt framforhandlet raskere. Det demokratiske underskuddet har blitt fjernet fordi Europaparlamentet har fått en mer likverdig status i forhold til medlemsstatene, og vil ha medvirkning i hva som skjer videre. Jeg tror debatten vil bli mer balansert og mer basert på fakta heller enn politiske argumenter,» konkluderer Arnbak.

© norske LMD

1 «The Virtual Chernobyl», 1. februar 2011, www.langner.com.  
2 William J. Broad, John Markoff og David E. Sanger, «Israeli Test on Worm Called Crucial in Iran Nuclear Delay», New York Times, 15. januar 2011.  
3 Haaretz, Tel-Aviv, 7. januar 2011.  
4 «Iran's Nuclear Setbacks: A Key for U.S. Diplomacy», 18. januar 2011, United States Institute of Peace, www.usip.org.  
5 Scott Ritter, «In Perspective: The Stuxnet Effect», Nuclear Intelligence Weekly, New York, 31. januar 2011.

1 Det dreier seg om dokumentet «Room document. Evaluation of directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications».  
2 Pressemelding 14. juli 2010  
3 Åpent brev til EU-kommisjonær Cecilia Malmström 22. juni 2010  
4 AK Vorrat, «There is no such thing as secure data. Refuting the myths of secure IT systems», www.vorratsdatenspeicherung.de  
5 Panoptikon og Den polske helseforskningskomité, «Joint statement regarding the evaluation of directive 2006/24/EC», 5. november 2010  
6 PCWorld, 27. januar 2011  
7 Panoptikon, «Åpent brev til statsminister Donald Tusk», 13. oktober 2010.  
8 Gazeta Wyborcza 8. oktober 2010  
9 Human Rights House Foundation, «Surveillance of Polish journalists case - new developments», 14. januar 2011.  
10 Privacy International, «PHR2006: Republic of Poland», 18. desember 2007  
11 Polsk radio 3. oktober 2009  
12 Bits of Freedom, «What the European Commission owes 500 million Europeans».  
13 Nieuwe Revu nr. 51, 2008  
14 «Bits of Freedom strikes again: Dutch government cancels national database on bank data», 18. november 2010, www.bof.nl.  
15 Alternet, 25. november 2008.  
16 European Digital Rights, «German Federal Constitutional Court rejects data retention law», 10. mars 2010.  
17 AK Vorrat, «Registered Serious Crime in Germany».