FORSVARSAKADEMIET

BRIEF

Irans cyberkapabiliteter og offensive operationer på internettet

Af Asbjørn Thranov, cand.jur.

FORSVARET

FORSVARSAKADEMIETS FORLAG

BRIEF

Irans cyberkapabiliteter og offensive operationer på internettet

Af Asbjørn Thranov, cand.jur.

Forsvarsakademiet er Danmarks førende forskningsinstitution inden for militære studier. Vi forsker i et bredt felt af militære kerneområder såsom militære operationer, strategi, sikkerheds- og forsvarspolitik, militær ledelse, tværkulturel forståelse og militærhistorie. Akademiets fælles omdrejningspunkt er anvendt forskning i fremtidens konflikter.

Forsvarsakademiets forskning og forskningsbaserede uddannelser skal være med til at sikre, at dansk forsvar kan kæmpe og vinde i morgendagens konflikter. Men den omfattende viden på akademiet skal ikke alene stilles til rådighed for forsvaret. Gennem publikationer bidrager akademiet også til at informere og nuancere den offentlige debat om danske og internationale forsvars- og sikkerhedspolitiske forhold.

God fornøjelse ved læsning af Forsvarsakademiets publikationer!

København december 2014
Forsvarsakademiet
Svanemøllens Kaserne
2100 København Ø
Tlf.: 3915 1515
Fax: 3929 6172
Redaktør: Fung. Chef for Institut for Strategi, Michael Jedig Jensen, Major & militæranalytiker
Layout: FAK
ISBN: 978-87-7147-084-0
Udkommer kun i elektronisk form

Forsvarsakademiets forlag

Indhold

Forord

Iran bliver ofte nævnt på linje med Kina og Rusland som et af de lande, der for Vesten udgør en sikkerhedsmæssig risiko i cyberspace[1]. Formålet med dette brief er at beskrive Irans evne, vilje og kapabiliteter til at udføre offensive operationer og spionage i cyberspace. Indledningsvis opridser briefet kort baggrunden for den iranske trussel i cyberspace. Dernæst følger en overordnet gennemgang af en række forskellige iranske myndigheder med ansvar for at beskytte Iran mod cyberangreb. Briefet giver desuden en detaljeret beskrivelse af Revolutionsgarden og den iranske efterretningstjeneste, som anses for at være de to mest centrale aktører bag Irans offensive og defensive cyberaktiviteter. Endelig sætter briefet fokus på Irans brug af private hackere samt på flere af de offensive aktioner i cyberspace, som Iran er mistænkt for at stå bag.

Hovedkonklusioner

- Iran er gået fra primært at forsvare sig selv mod angreb i cyberspace til at indtage en mere offensiv rolle, hvor landet udfører cyberoperationer og -spionage mod andre lande. Det er meget sandsynligt, at skiftet skyldes, at Iran i de seneste år har været udsat for en række cyberangreb.
- Iran har på nuværende tidspunkt ikke kapacitet til at udføre større cyberangreb, der kan forårsage omfattende ødelæggelse af it- og teleinfrastruktur eller fysisk skade på tilknyttet infrastruktur såsom industrielle systemer. Iran har derimod kapacitet til at forårsage kortvarige forstyrrelser af og sabotage mod it-systemer og hjemmesider. Iran udnytter desuden internettet til spionage og propagandavirksomhed.
- Danmark er ikke i særlig risiko for at blive udsat for et iransk cyberangreb, medmindre landet deltager direkte i en væbnet konflikt med Iran. Den største trussel mod Danmark synes at være private iranske hackergrupper, der lejlighedsvist og lidt tilfældigt hacker danske hjemmesider eller udnytter dansk it-infrastruktur som platform for angreb rettet mod andre lande. Danske selskaber inden for primært forsvarsindustrien er desuden i risiko for at blive genstand for iransk cyberspionage.

Briefets kildegrundlag

Briefet bygger på offentligt tilgængelige kilder: internationale aviser, artikeldatabaser og offentlige efterretningsrapporter. Desuden udgør officielle udtalelser fra iranske myndighedspersoner en væsentlig del af briefets kildegrundlag. Det er imidlertid vanskeligt at validere oplysningerne, og det må formodes, at de ofte ikke afspejler virkeligheden i et land, hvor pressefriheden har trange kår.[2]

Dertil kommer, at den iranske regering - og i særlig grad Irans efterretningstjeneste - bevidst bruger medier til at sprede falske informationer om landets militære kapa-

(1) Der skelnes i briefet ikke mellem begreberne "cyberspace" og "internettet".

(2) Iran indtager ifølge den franskbaserede organisation Reportere uden Grænser i 2014 en bundplacering på det såkaldte pressefrihedsindeks: http://rsf.org/index2014/en-index2014.php

citeter.3 Det er således sandsynligt, at iranske myndigheder forsøger at overdrive omfanget af landets cyberkapabiliteter. Derudover kan retorikken betragtes dels som sabelraslen rettet mod landets fjender, dels som en forsikring til den iranske befolkning om, at Iran kan forsvare sig mod angreb i cyberspace. Oplysningerne giver ikke desto mindre et indblik i Irans syn på og strategier for udnyttelsen af cyberspace til offensive formål.

Indledning

Iran har i de seneste år arbejdet aktivt på at udvikle både defensive og offensive cyberkapabiliteter, og landet er mistænkt for at udføre cyberangreb mod andre lande. Iran har selv været udsat for flere tilfælde af cyberspionage og -angreb, hvoraf det mest kendte angreb er den såkaldte Stuxnet-virus, der i 2010 ødelagde plutonium-centrifuger i uranberigelsesanlægget ved Natanz i Iran. Stuxnet-angrebet var ikke alene en *game changer* inden for cyberkrigsførelse, men også en advarsel til det iranske styre om landets sårbarhed i cyberspace. I januar 2013 udtalte chefen for den amerikanske Air Force Space Command, William L. Shelton, som har ansvaret for flyvevåbnets cyberoperationer, at Stuxnet-angrebet havde fået Iran til at udvide sine cyberkapabiliteter.[4]

Flere efterretnings- og sikkerhedstjenester advarer offentligt om Irans tiltagende udvikling af landets cyberkapabiliteter. James R. Clapper, director of national intelligence, betegner i sin trusselsvurdering for 2014 Iran som en stadig mere aggressiv cyberaktør.[5] Chefen for den svenske sikkerhedstjeneste Säpo, Anders Thornberg, har udtalt, at Iran sammen med Rusland og Kina er en hovedaktør bag spionage på internettet.[6] Den hollandske efterretningstjeneste AIVD estimerer, at Iran har moderate cyberkapabiliteter, men at landet arbejder på at udvikle sine kapaciteter yderligere. Ifølge chefen for Tysklands indlands-efterretningstjenesten Verfassungsschutz, Hans-Georg Maassen, har Iran ressourcer til at udføre cyberangreb- og spionage.[7]

Cyberangreb mod Iran

Iranske myndigheder har rapporteret, at Iran – foruden Stuxnet-angrebet – har været udsat for flere cyberangreb med skadelig software. Eksempelvis har computervirusseerne Duqu og Flame haft til formål sabotere it-systemer og udføre spionage mod Iran.

(3) "Iran's Ministry of Intelligence And Security: A Profile", The Library of Congress (december 2012)

(4) "Iran strengthened cyber capabilities after Stuxnet", Reuters World Service (17. januar 2013)

(5) US Intelligence Community Worldwide Threat Assessment (29. januar 2014) http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

(6) "Swedish spy chief warns of rise of Islamist threat", Reuters (27. maj 2014) http://www.reuters.com/article/2014/05/27/us-sweden-security-idUSKBN0E720A20140527

(7) "Cyber-Attacken; Spione aus dem Iran greifen deutsche Firmen an", Welt Online, 13. november 2014.

Herhjemme har hverken Politiets Efterretningstjeneste eller Forsvarets efterretningstjeneste offentligt beskrevet den iranske trussel i cyberspace.

Iranske medier rapporterer jævnligt om landets evne til at forsvare sig i cyberspace, og præsident Hassan Rohani understregede i begyndelsen af februar 2014 vigtigheden af, at Iran kan modstå angreb i cyberspace.[8] Iran følger en toleddet strategi: Dels opbygger landet foranstaltninger, der skal sikre den nationale cybersikkerhed og begrænse befolkningens adgang til uvildige informationer på internettet, herunder adgangen til sociale medier som Facebook og Twitter. Dels udvikler iranske myndigheder kapabiliteter, der kan anvendes til at udføre offensive handlinger i cyberspace.

Defensiv cyberstrategi

Iran har ikke offentliggjort en egentlig samlet national cyberstrategi, men lederen af Irans civile forsvarsorganisation, Gholamreza Jalali, udtalte i januar 2013, at organisationens cyberhovedkvarter havde udarbejdet det første udkast til en cyberstrategi[9], som afventede godkendelse hos den iranske ledelse. En sammenstykning af en række forskellige nyhedsartikler fra iranske medier viser, at Iran særligt har fokus på at beskytte landets kritiske infrastruktur såsom olieproduktion og nukleare faciliteter mod cyberangreb.[10] Det sker blandt andet ved at:

- Udvikle og producere software og it-systemer, der skal gøre Iran mindre sårbar over for angreb.[11] Antivirusprogrammet Padvish er et eksempel på software udviklet i Iran, der skal beskytte iranske it-systemer.[12]
- Opstille it-netværk, der skal danne skjold mod cyberangreb.[13] Sensornetværket Shahpad advarer eksempelvis iranske organisationer om ondsindede cyberaktiviteter.[14]
- Indføre et nationalt såkaldt halal-internet, som er isoleret fra resten af internettet.[15]

(8) "President says Iran must remain calm, hopeful in face of the 'enemy threats'", BBC Monitoring Trans Caucasus Unit (3. februar 2014)

(9) "Iran defence official says most advanced economic war waged against Iran", BBC Monitoring Middle East (14. januar 2013)

(10) "Iran's nuclear sites safe against quakes, cyber attacks: Iran official", Islamic Republic of Iran Broadcasting (17. maj 2013)

(11) "Iran Defense Ministry to unveil 12 cyber products", Islamic Republic of Iran Broadcasting (14. december 2013)

(12) "Iran unveils first indigenous antivirus", BBC Monitoring Middle East (Mehr News Agency) (7. december 2013)

(13) "Iran unveils its first cyber defense shield", Islamic Republic of Iran Broadcasting (13. december 2013)

(14) "Iran launches home-made defense shield", Iranian Students News Agency (9. december 2013)

(15) "Iran to launch 'halal' internet network – official", (BBC Monitoring Middle East) (IRNA) (15. april 2011)

Et andet centralt element i Irans cyberstrategi er, at landet skal kunne forsvare sig mod cyberangreb fra ærkefjenderne USA og Israel.[16] Det er opfattelsen, at USA officielt har erklæret Iran krig i cyberspace, og at Iran derfor er berettiget til at svare igen.[17] I september 2011 varslede en general fra Irans væbnede styrker, at cyberangreb fra USA og landets allierede ville blive gengældt. Den advarsel blev i maj 2014 gentaget af Gholamreza Jalali på en national kongres om cyberforsvar.[18] Det er uklart, om et gengældelsesangreb vil blive gennemført i cyberspace, eller om Iran også er parat til at reagere med traditionelle militære midler i tilfælde af et cyberangreb. Det er muligt, at Iran allerede har gjort alvor af sin trussel om at svare igen, idet landet er mistænkt for at stå bag flere cyberangreb.

Den bløde krig

Blød krig (*soft war*) er et centralt begreb i Irans cyberstrategi, og det dækker over det iranske styres bestræbelser på at hindre vestlig samfundsundergravende indflydelse på landets befolkning.[19] Iranske magthavere frygter, at Vesten gennem psykologiske operationer, økonomiske sanktioner og cyberangreb forsøger at drive en kile ind mellem befolkningen og regeringen.[20] Begrebet dækker også over Irans forsvar mod angreb i cyberspace og forsøg på at hindre cyberspionage. Den bløde krig udkæmpes navnlig i medierne og på internettet, og det iranske styre forsøger som nævnt at overvåge og kontrollere begge dele.

Konceptet blød krig har eksisteret længe i Iran, men det var først i forbindelse med omfattende demonstrationer ved præsidentvalget i 2009, den såkaldte Grønne Revolution, at iranske myndigheder udvidede overvågningen af internettet.[21] Demonstranterne anvendte blandt andet sociale medier til at kommunikere, hvilket resulterede i den alternative betegnelse Twitter-revolutionen. Det iranske styre har ligeledes anerkendt værdien af cyberspace som en platform til at udbrede propaganda med henblik på at påvirke mange mennesker.[22]

Kludetæppe af myndigheder

Iran har en række forskellige organer og myndigheder, der formelt varetager og koordinerer landets cybersikkerhed. Det Øverste Råd for Cyberspace blev nedsat i

(16) "Iran develops new defensive doctrine to 'confront' US", BBC Monitoring Middle East (Tasnim News Agency) (24. februar 2014)

(17) "US officially started cyber war against Iran", BBC Monitoring Middle East (ISNA website) (11. maj 2014)

(18) "Iran to give reciprocal reaction to possible cyber attacks", Iranian Government News (14. maj 2014)

(19) "Iran details 'soft warfare' activities of Western-backed 'opposition media'", BBC Monitoring Middle East, Fars News Agency website (13. april 2009)

(20) "Iranian official says cyber war more dangerous than conventional war", BBC Monitoring Trans Caucasus Unit (ISNA website) (22. juni 2012)

(21) Daniel Baldion, "Iran and the emergence of information and communications technology: the evolutions of revolution?", vol. 68, issue 1, 2014

(22) Gabi Siboni og Sami Kronenfeld, "Iran and Cyberspace Warfare, Military and Strategic Affairs", vol. 4, no. 3 (december 2012)

marts 2012 af den øverste leder, ayatollah Ali Khamenei[23], og rådet har kompetence til at fastlægge bindende policies og retningslinjer for Irans ageren i cyberspace. En anden central myndighed er Cyberspace Defense Command, der er underlagt Irans civile forsvarsorganisation. Cyberkommandoen er således en del af de iranske væbnede styrkers generalstab og har til opgave at beskytte kritisk infrastruktur mod cyberangreb.[24] MAHER-centeret[25], som er underlagt det iranske ministerium for kommunikation og teknologi, er en anden defensiv myndighed, der skal identificere og imødegå cyberangreb. Irans cyberpoliti, FETA[26], blev oprettet i maj 2011[27] og bekæmper almindelig cyberkriminalitet i Iran. Cyberpolitiet er imidlertid også bemyndiget til at efterforske landsskadelige aktiviteter.[28]

Det er fælles for myndighederne, at de ifølge det iranske styre alene har en defensiv natur og dermed blot skal opretholde cybersikkerheden i Iran og beskytte landet mod cyberangreb. På trods af myndighedernes angivelige defensive karakter kan det dog ikke udelukkes, at de selvsamme myndigheder kan virke som selvstændige angrebsplatforme eller indgå som støtteelementer i offensive cyberoperationer.[29]

De mange forskellige myndigheder gør det desuden vanskeligt for en modstander med et enkelt angreb at sætte Irans cyberforsvar ud af kraft. Det tyder således på, at Iran, når det gælder landets cyberkapabiliteter, følger princippet i den defensive militære doktrin, som Irans civile forsvarsorganisation offentliggjorde i februar 2014, hvor den centrale grundtanke er at undgå at samle militære kapabiliteter ét sted.[30]

Revolutionsgarden: cyberkrig og blød krig

Revolutionsgarden har siden den iranske republik blev grundlagt i 1979 været et vigtigt instrument til at beskytte Iran mod trusler i og uden for landets grænser. Revolutionsgarden spiller ligeledes en central rolle i forbindelse med Irans aktiviteter i cyberspace, hvor garden på internettet bekæmper den politiske opposition. Det sker blandt andet gennem overvågning af internettet og ved at lægge såkaldte antirevolutionære og zionistiske hjemmesider ned.

(23) "Iran paper discusses composition of 'Supreme Council of Cyberspace'", BBC Monitoring Middle East (Qods website) (19. marts 2012)

(24) Gabi Siboni og Sami Kronenfeld, "Iran and Cyberspace Warfare, Military and Strategic Affairs", vol. 4, no. 3 (december 2012)

(25) "Maher" er det farsiske ord for at være dygtig, og akronymet står for "Computer Emergency Response Team Coordination Centre"

(26) FETA er et farsisk akronym for "Information Production and Exchange Cyberspace"

(27) "Tehran cyber police officially launched", BBC Monitoring Middle East (30. januar 2013)

(28) "Iran official speaks on 'cyber threats' to Islamic Republic", BBC Monitoring Trans Caucasus Unit (Fars News Agency website) (18. maj 2014)

(29) Den norske efterretningstjenestes vurdering for 2014, "Fokus", http://forsvaret.no/om-forsvaret/fakta-om-forsvaret/publikasjoner/Documents/Fokus-2014.pdf

(30) "Iran develops new defensive doctrine to 'confront US'", BBC Monitoring Middle East (Tasnim News Agency) (24. februar 2014)

I september 2009 fik Revolutionsgarden aktiemajoriteten i Irans telekommunikationsselskab.[31] Det giver garden kontrol med Irans telefonnet og med internetudbydere og dermed mulighed for at indsamle oplysninger om den politiske opposition. På baggrund af overvågningen af internettet anholder Revolutionsgarden bloggere og andre personer, der på internettet ytrer sig kritisk om regimet.[32]

Den tidligere talsmand for den øverste leder, Hojjat ol-Eslam Mojtaba Zonnur, har udtalt, at Revolutionsgarden også hacker udenlandske hjemmesider med indhold, der er kritisk over for Iran.[33] Revolutionsgarden har oprettet et særligt center, der skal efterforske organiseret kriminalitet (Organized Crime Investigation Centre).[34] Centerets primære opgave er at overvåge hjemmesider, blogs og e-mailkorrespondance for at identificere regimekritisk indhold.

Revolutionsgarden har over hele Iran forskellige cyberenheder, som ifølge gardens egne oplysninger overvåger internettet, skriver blogs og gennemfører kulturelle og sociale aktiviteter.[35] Den første cyberenhed blev etableret i 2010 med et rapporteret budget på 76 millioner amerikanske dollars.[36] I 2012 oprettede Revolutionsgarden en cyberdivision i Teheran, der skal beskytte Iran mod trusler i cyberspace.[37]

Revolutionsgardens overvågning af og kontrol med den iranske del af internettet udgør ikke i sig selv en trussel mod andre staters it-sikkerhed. Det er imidlertid sandsynligt, at overvågningen og bekæmpelsen af landets interne opposition giver Revolutionsgarden teknisk viden og kendskab til internettet, som kan anvendes i forbindelse med offensive handlinger mod udlandet.

Forbereder cyberkrig

Revolutionsgarden har et generelt fokus på asymmetrisk krigsførelse[38], og cyberkrigsførelse er et relativt billigt og effektivt middel, der kan anvendes mod en militært stærkere part.[39] En ledende general har proklameret, at Revolutionsgarden

(31) Daniel Baldion, "Iran and the emergence of information and communications technology: the evolutions of revolution?", vol. 68, issue 1, 2014

(32) "Iran guards arrest cyber activists with links to foreigners", BBC Monitoring Middle East (3. december 2013)

(33) "Former aide to Iran leader outlines Guards intelligence, political activities", BBC Monitoring Middle East (3. marts 2014)

(34) "Iran changes structure of Revolutionary Guard's cyber defence command", BBC Monitoring Middle East (ISNA website) (22. februar 2012)

(35) "Iran commander denies hacking US intelligence systems", BBC Monitoring Middle East (16. oktober 2012)

(36) Matthew Poletti, "Iran Joins the Cyberwarfare Age", Military Periscope Special Reports, (26. juli 2013)

(37) "Iran Guards Corps to set up cyber division – commander", BBC Monitoring Middle East (16. oktober 2012)

(38) Jane's World Armies, "Iran" (10. marts 2014)

(39) "Iran is now a global cyber power, general says", Islamic Republic of Iran Broadcasting (4. februar 2013)

råder over verdens fjerdestørste cyberhær.[40] Garden tæller ca. 125.000 soldater, og det er derfor ikke usandsynligt, at et stort antal gardister gør tjeneste som professionelle cyberkrigere.

Revolutionsgarden afholder forskellige typer af øvelser, der omfatter både selvstændige cyberøvelser[41] og øvelser, hvor cyberenheder træner sammen med gardens konventionelle styrker. I februar 2013 afholdt garden en større øvelse med titlen Great Prophet 8, der blandt andet havde til formål at afprøve gardens defensive cyberkapabiliteter.[42] Ifølge en talsmand for Revolutionsgarden lykkedes det under øvelsen for gardens cyberkrigere at overtage kontrollen af en efterligning af en fjendtlig drone.[43] Iran har tidligere påstået at have erobret en amerikansk overvågningsdrone, der befandt sig i iransk luftrum, ved at hacke sig ind i dens kontrolsystemer.[44]

Revolutionsgarden menes at råde over avancerede kapaciteter til elektronisk krigsførelse.[45] Den førnævnte øvelse med at kontrollere droner vidner om, at garden arbejder på at kombinere elementer fra cyberkrigsførelse med traditionel elektronisk krigsførelse. Det er således muligt, at Revolutionsgarden i en militær konflikt kan være i stand til at udføre bredspektrede elektroniske angreb mod en modstanders tekniske udstyr såvel som vitale it-systemer.

Konventionelle styrker opruster

Irans konventionelle væbnede styrker (Artesh) opruster ligeledes med hensyn til cyberkapabiliteter, og den strategisk vigtige flåde er en central aktør. I december 2012 afholdt flåden en øvelse, hvor en defensiv cybergruppe skulle forhindre en anden gruppe i at trænge ind i flådens it-netværk for at skaffe sig informationer og sprede computervirus. Flåden har desuden afholdt en konference, hvor et af temaerne var cyberangreb til søs. Den iranske hær afholder cyberøvelser sammen med Revolutionsgarden, hvilket skal styrke interoperabiliteten.

(40) "Commander says Iran has fourth biggest cyber army in the world", BBC Monitoring Middle East (2. februar 2013)

(41) "Iranian Army Preparing for 8 Wargames", Islamic Republic of Iran Broadcasting (31. januar 2014)

(42) "Drones, cyber defense feature in Iranian Revolutionary Guards' drill", Jerusalem Post (24. februar 2013)

(43) "Iran's IRGC cyber-warriors take control of mock enemy's spy drone", Press TV (24. februar 2013)

(44) "Iran's IRGC cyber-warriors take control of mock enemy's spy drone", Press TV (24. februar 2013)

(45) Gabi Siboni og Sami Kronenfeld, "Iran and Cyberspace Warfare, Military and Strategic Affairs", vol. 4, no. 3 (december 2012)

Militær spionage

Revolutionsgarden udgør en aktiv komponent i Irans efterretningsmiljø og råder over sit eget efterretningsdirektorat med ca. 2.000 efterretningsofficerer.[46] Der er indikationer på, at Revolutionsgarden udfører cyberspionage for at indsamle oplysninger om andre nationers militære forhold.

I september 2012 annoncerede Revolutionsgarden, at en cyberenhed havde skaffet sig adgang til højt klassificerede data hos en af sine fjender.[47] Året efter - i september 2013 - blev den amerikanske flådes uklassificerede it-system kompromitteret, og det lykkedes hackere at skaffe sig adgang til e-mails og dokumenter. Ifølge unavngivne kilder hos de amerikanske myndigheder stod iranske hackere på vegne af styret i Teheran bag kompromitteringen.[48]

Det er dog ikke bevist, at Iran står bag kompromitteringen af den amerikanske flådes it-netværk, men det er sandsynligt, at andre nationers militære it-systemer udgør et hovedmål for Revolutionsgardens cyberspionage, og at garden forsøger at plante såkaldte bagdøre, som kan anvendes senere i en krise eller konflikt til at forstyrre eller ødelægge systemerne. Det er desuden sandsynligt, at Revolutionsgarden efterretningsmæssigt forbereder den fremtidige kampplads i cyberspace ved at finde svagheder i sine modstanderes it-systemer, som kan udnyttes under en væbnet konflikt.

Der har været spekulationer om, at de paramilitære elitetropper, Al-Quds-styrken, der er underlagt Revolutionsgardens efterretningsdirektorat[49], har udført cyberangreb mod en række amerikanske banker.[50] Al-Quds-styrken er ansvarlig for at udføre hemmelige operationer i udlandet, hvor styrken blandt andet støtter lokale oprørsgrupper med våben og træning.[51] Der foreligger umiddelbart ingen tilgængelige oplysninger, der tyder på, at Al-Quds-styrken råder over egne cyberkapabiliteter, og det virker ikke sandsynligt, at det er tilfældet, at den taktiske enhed selvstændigt skulle råde over kapabiliteter til at udføre cyberangreb. Det er imidlertid tænkeligt, at Quds-styrken, som arbejder tæt sammen med den iranske efterretningstjeneste, har til opgave at identificere og rekruttere hackere i udlandet.

---

(46) Jane's Sentinel Security Assessment – "The Gulf States, Security and Foreign Forces", Iran (29. januar 2014)

(47) "Commander says Iran gained access to enemy's secret intelligence", BBC Monitoring Middle East (Fars News Agency website) (30. september 2012)

(48) "U.S. Says Iran Hacked Navy Computers", The Wall Street Journal (27. september 2013) http://online.wsj.com/news/articles/SB10001424052702304526204579101602356751772

(49) Jane's Sentinel Security Assessment – "The Gulf States, Security and Foreign Forces", Iran (29. januar 2014)

(50) "Lieberman Theorizes Iran's Quds Force behind Recent Cyberattacks on Bank of America, JP Morgan Chase", CNS News (27. september 2012) http://cnsnews.com/news/article/lieberman-theorizes-iran-s-quds-force-behind-recent-cyberattacks-bank-america-jp-morgan#sthash.VorE3bSM.dpuf

(51) Mark Sexton, "Qods Force: Iranian Unit Tied to U.S. Plot", The Counter Terrorist, (februar/marts 2012)

Den iranske efterretningstjeneste

Der er sparsomme oplysninger om den iranske indenrigs- og udenrigsefterretningstjenestes (MOIS')[52] aktiviteter i cyberspace. MOIS er et af de mægtigste ministerier i den iranske regering, og Hassan Rohani har fremhævet, at MOIS' væsentligste rolle er at imødegå cyberangreb.[53] Forhenværende chef for MOIS Heydar Moslehi har udtalt, at efterretningstjenesten er aktiv i cyberforsvaret af Iran, og at tjenesten har afværget cyberangreb mod landet. I april 2012 placerede det amerikanske finansministerium MOIS på sin sanktionsliste, idet tjenesten havde støttet den syriske efterretningstjeneste med træning, udstyr og værktøjer til at overvåge internettet og de sociale medier i Syrien.[54] Støtten til Syrien indikerer, at MOIS råder over egne cyberkapabiliteter.

En af MOIS' primære opgaver er at overvåge og bekæmpe dissidenter i og uden for Iran, som udgør en trussel mod det iranske styre.[55] MOIS har navnlig fokus på den iranske oppositionsgruppe Mujahedin-e Khalq og dens politiske gren Det Nationale Modstandsråd.[56] Det er sandsynligt, at også eksiliranere og iranske dissidenter i Danmark kan blive udsat for MOIS' cyberspionage.

MOIS spionerer desuden mod andre lande med henblik på at indsamle informationer om politiske, økonomiske og videnskabelige forhold.[57] Heydar Moslehi annoncerede i august 2011, at iranske efterretningsstyrker havde infiltreret fjendtlige it-netværk.[58] Revolutionsgardens efterretningsdirektorat er forpligtiget til at støtte MOIS i indsamlingen af oplysninger, men snitfladerne mellem de to organisationer er uklare.[59] Der foregår givetvis et tæt samarbejde og en tæt koordination mellem Revolutionsgarden og MOIS om spionage mod dissidenter i og uden for Iran.

MOIS er desuden involveret i at sprede falske informationer, og tjenesten har en selvstændig afdeling til psykologiske krigsførelse mod regeringens modstandere.[60] Udbredelsen af propaganda og falske informationer udgør en vigtig del af det iranske styres cyberstrategi. Det har været rapporteret, at Iran har oprettet falske blogs og

(52) MOIS er den engelske forkortelse for "Ministry of Information and Security", som på farsi hedder "Vezarat e Ettela" at Va Amniat e Keshvar" (VEVAK)

(53) "Pres. Rouhani underlines vital role of Cyber security", Islamic Republic of Iran Broadcasting (6. februar 2014)

(54) "Fact sheet: New Executive Order Targeting Human Rights Abuses via Information Technology", States News Service (23. april 2012)

(55) "Iran's Ministry of Intelligence And Security: A Profile", The Library of Congress (december 2012)

(56) "Verfassungsschutzbericht 2013", Bundesamt für Verfassungsschutz, 2013

(57) "Iran's Ministry of Intelligence And Security: A Profile", The Library of Congress (december 2012)

(58) "Iran Intelligence Ministry fully prepared to repel cyber attacks", BBC Monitoring Middle East (27. august 2011)

(59) "Iran's Ministry of Intelligence And Security: A Profile", The Library of Congress (december 2012)

(60) "Iran's Ministry of Intelligence And Security: A Profile", The Library of Congress (december 2012)

Facebook-konti med henblik på at sprede falske rygter om iranske journalister i eksil.[61] Det kan således tænkes, at MOIS anvender internettet og sociale medier til at sprede falske informationer, der har til formål at påvirke såvel den iranske befolkning som befolkningsgrupper og beslutningstagere uden for Iran.

Kina støtter med aflytningsudstyr

Ifølge det franske efterretningstidsskrift Intelligence Online indgik MOIS ved årsskiftet 2012/13 en aftale med Folkets Befrielseshær (PLA) om at udvikle lytteposter og uddanne iranske teleingeniører i aflytningsteknologi. Aftalen blev indgået med det 12. kontor i PLA's tredje departement, der er ansvarligt for elektronisk indhentning af informationer. Samme departement står bag omfattende cyberspionage mod industrielle og politiske mål i Vesten. Selv om det specifikke samarbejde ikke angik udviklingen af Irans cyberkapabiliteter, er det sandsynligt, at Kina – som er storimportør af iransk olie – ligeledes har støttet iranske myndigheder med forskellige typer af it-teknologi, som kan anvendes til cyberspionage og monitorering af internettet. En afhopper fra den syriske efterretningstjeneste berettede i november 2012 til den tyrkiske avis Today's Zaman, at Kina ligeledes har støttet det syriske styre med overvågning- og aflytningsudstyr.

Derudover har MOIS til opgave at støtte militante organisationer og terrorister i udlandet.[62] Ifølge det amerikanske finansministerium har MOIS angivelig deltaget i flere hackingprojekter sammen med den militante islamitiske gruppe Hizbollah.[63] Der er ikke offentliggjort detaljerede oplysninger om projekterne, men Hizbollah er mistænkt for at være involveret i cyberangrebet mod Saudi-Arabiens nationale olieselskab Saudi Aramco.[64] I juni 2013 udtalte den israelske premierminister, Benjamin Netanyahu, at Iran har anvendt både Hizbollah og den palæstinensiske gruppe Hamas til at udføre cyberangreb mod Israel.[65] Hizbollah og Hamas er ikke de eneste ikke-statslige aktører, som opererer på vegne af og støttes af Iran. En række forhold tyder på, at Iran benytter sig af private hackere og andre ikke-statslige aktører til at udføre skadelige handlinger i cyberspace.

(61) "Iran uses fake blogs in smear campaign against journalists in exile", The Guardian (24. januar 2013)
(62) "Iran's Ministry of Intelligence And Security: A Profile", The Library of Congress (december 2012)
(63) "Treasury Designates Iranian Ministry of Intelligence and Security for Human Rights Abuses and Support for Terrorism", Targeted News Service (16. februar 2012)
(64) Gabi Siboni og Sami Kronenfeld, "Iran and Cyberspace Warfare, Military and Strategic Affairs", vol. 4, no. 3 (december 2012)
(65) "Israel PM says sharp rise in cyber attacks from Iran", Agence France-Press (9. juni 2013)

Hackere som stedfortrædere

Iran er berygtet for at benytte sig af forskellige stedfortrædere til at udføre terrorhandlinger og andre skadelige aktiviteter i udlandet på vegne af den iranske stat.[66] Der er flere indikationer på, at Iran også i cyberspace benytter sig af private hackere til at udføre forskellige former for operationer. Lederen af Irans civile forsvarsorganisation, Gholamreza Jalali, har udtalt, at Iran byder hackere velkomne, der er villige til at arbejde for den islamiske republik[67]. Hojjat ol-Eslam Mojtaba Zonnur har ligeledes udtalt sig positivt om individer og organisationer, som støtter Revolutionsgardens bløde krig i cyberspace.[68]

Iran har en ung og veluddannet befolkning, hvilket giver iranske myndigheder gode muligheder for at rekruttere it-kyndige personer fra landets tekniske universiteter. Iran har flere uddannelsesinstitutioner inden for avanceret teknologi, og Imam Hossein-universitetet i Teheran har et institut for elektronisk krigsførelse og cyberforsvar.[69]

En iransk hackergruppe ved navn Ashiyane Digital Security Team (herefter Ashiyane) har i en årrække taget ansvaret for at have hacket et stort antal udenlandske hjemmesider. Hackergruppen er sat i forbindelse med Revolutionsgarden, men relationen er ikke dokumenteret.[70] Ashiyane har tilsyneladende også rettet sine cyberaktiviteter mod Frederiksberg Skoles hjemmeside, der blev lagt ned i august 2008.[71] Det fremgik af hjemmesidens computerkode, at Ashiyane havde lagt hjemmesiden ned som en protest mod fornærmelser af muslimer. Det virker dog mere sandsynligt, at hackere har fundet og udnyttet en svaghed i Frederiksberg Skoles hjemmeside, end at Revolutionsgarden har udpeget siden som et mål for Ashiyanes aktiviteter.

Også hackergruppen Iranian Cyber Army har skaffet sig adgang til en række udenlandske hjemmesider og ændret indholdet. I februar 2011 tog gruppen ansvaret for angreb mod nyhedssiden Voice of America, og i samme måned udtalte den øverste leders talsmand i Revolutionsgarden, Ali Saeedi Shahroudi, at Iranian Cyber Army arbejder på vegne af Revolutionsgarden.[72]

(66) Nathaniel F. Manni, "Iran's Proxies: State Sponsored Terrorism in the Middle East", Global Security Studies, Vol. 3, Issue 3, 2013

(67) "Iran says it welcomes hackers who work for Islamic republic", Radio Free Europe (7. marts 2011)

(68) "Former aide to Iran leader outlines Guards intelligence, political activities", BBC Monitoring Middle East (3. marts 2014)

(69) "Iran to hold national cyber defence conference in May", BBC Monitoring Middle East (Mashreq new website) (7. april 2014)

(70) House Homeland Security Subcommittee on Counterterrorism and Intelligence and Cybersecurity, Infrastructure
Protection, and Security Technologies Hearing, "Iranian Cyber Threat to the U.S. Homeland"; testimony by
Frank J. Cilluffo, director, Homeland Security Policy Institute, The George Washington University Congressional (26. april 2012)

(71) "Iranske hackere slår til mod Frederiksberg Skole", Sjællandske Slagelse (11. august 2008)

(72) "Iran militia claims credit for VOA cyber strike", The Washington Times (23. februar 2011)

Revolutionsgardens paramilitære basij-milits, der efter sigende tæller en million mand, er også aktiv i cyberspace, hvor militsens medlemmer deltager i den bløde krig mod såkaldt negativ vestlig indflydelse i Iran.[73] Sikkerhedsekspert og tidligere særlig rådgiver under præsident George W. Bush Frank J. Cilluffo udtalte ved en kongreshøring i april 2012, at militsen udgør en betydelig del af arbejdsstyrken i forbindelse med Irans cyberoperationer.[74] Militsens cyberhær overvåger blandt andet oppositionens hjemmesider og skriver blogindlæg. I marts 2011 udtalte militsens næstkommanderende, Ali Fazli, at den har mobiliseret en magtfuld cyberhær, der skal imødegå fjendtlige cyberangreb. Cyberhæren består af eksperter, professorer og studenter, som vil angribe fjendens hjemmesider.[75] Militsen uddanner desuden skoleelever i at jage og tvangslande overvågningsdroner.[76]

Iran kan ved at benytte sig af private stedfortrædere sløre forbindelsen mellem den iranske stat og dens offensive aktiviteter i cyberspace, og på den måde kan styret undgå at blive gjort politisk og juridisk ansvarlig for handlingerne.[77] Irans samarbejde med private hackere og terrorgrupper indebærer desuden en risiko for, at disse aktører tilegner sig viden og hackersoftware, der kan anvendes til at udføre cyberangreb, og som kan spredes til andre ikke-statslige aktører.

Cyberangreb og cyberspionage mod udlandet

Iran er mistænkt for at udføre både cyberangreb og cyberspionage mod it-systemer i andre lande. Der er dog endnu ikke offentliggjort beviser, der entydigt dokumenterer, at det iranske styre står bag fjendtlige aktiviteter i cyberspace. Mistanken mod Iran bygger således i høj grad på indicier og *cui bono*-betragtninger snarere end egentlige håndfaste beviser. Det kan da heller ikke afvises, at andre stater eller ikke-statslige aktører bevidst misbruger iransk it-infrastruktur til at udføre fjendtlige aktiviteter for derved at kaste mistanken på Iran.

Ifølge AIVD har Iran i de seneste år haft et stort fokus på at udføre skadelige cyberaktiviteter i udlandet.[78] AIVD har således konstateret, at hollandsk it-infrastruktur er blevet anvendt til at udføre hackerangreb mod udenlandske hjemmesider, der er kritiske over for det iranske regime.[79] Angrebene kunne spores tilbage til Iran,

(73) "Iran Guards Corps commander announces formation of 'Basij Cyber Army'", BBC Monitoring Middle East (Iranian Sobh-e Sadeq website) (3. november 2012)

(74) "U.S. seen as Iran 'cyber-army' target; Specialists to testify about threat", The Washington Times (26. april 2012)

(75) "Iran cyber forces to attack enemy websites – commander", BBC Monitoring World Media (15. marts 2011)

(76) "Iran to teach schoolchildren to hunt drones", The Scotsman (19. august 2013)

(77) "Efterretningsmæssig risikovurdering 2013 - en aktuel vurdering af forhold i udlandet af betydning for Danmarks sikkerhed", Forsvarets Efterretningstjeneste 2013

(78) "Cyber Security Assessment Netherlands", National Cyber Security Center (juni 2013)

(79) I begyndelsen af 2012 blev regeringshjemmesider i Aserbajdsjan udsat for defacementangreb, hvor iranske hackere angiveligt ændrede hjemmesidernes indhold

og AIVD vurderer, at den iranske regering står bag angrebene.[80] AIVD estimerer, at Iran har moderate cyberkapabiliteter, men at landet arbejder på at udvikle sine kapaciteter.

I 2011 lykkedes det hackere at trænge ind i it-systemet i det hollandske selskab DigiNotar, der producerede sikkerhedscertifikater for blandt andet Google. En række tekniske spor pegede på, at kompromitteringen skete med base i Iran.[81] Der er mistanke om, at angrebet blev udført på vegne af iranske myndigheder, der ville kunne bruge certifikaterne til at overvåge borgeres krypterede kommunikation på Googles servere.

I august 2012 annoncerede Saudi Aramco, at selskabets it-systemer var blevet udsat for et cyberangreb[82]. Angrebet blev udført med den såkaldte Shamoon-virus, der satte omtrent 30.000 af selskabets pc'er ud af drift. Kort tid efter angrebet på Saudi Aramco blev Qatars naturgasselskab udsat for et lignende angreb. Saudi Aramco var nødt til at genoprette sit it-system, men selskabernes olie- og gasproduktion blev ikke berørt af angrebene. En hackergruppe med navnet Retfærdighedens Skærende Sværd tog ansvaret for angrebet, men Iran er blevet beskyldt for at stå bag.[83]

I september 2012 blev en række banker i USA udsat for overbelastningsangreb, der fortsatte ind i 2013. En gruppe ved navn Izz ad-Din al-Qassam Cyber Fighters tog ansvaret for angrebene som en protest mod den kontroversielle film *Innocence of Muslims*. Som en konsekvens af angrebene kunne bankkunder i kortere perioder ikke få adgang til deres onlinekonti. Formanden for Senatets sikkerhedsudvalg, Joe Lieberman, beskyldte Iran for at stå bag angrebene som hævn over USA's politiske og økonomiske sanktioner mod landet.[84] Ifølge Thomas Lund-Sørensen, chef i Center for Cybersikkerhed under Forsvarets Efterretningstjeneste, er der indikationer på, at danske computere og servere har været brugt som angrebsplatform mod de amerikanske banker.[85]

I 2012 spredte den såkaldte Mahdi-virus sig via e-mails med inficerede vedhæftede filer. Virussen havde tilsyneladende to formål: dels at spionere mod individer, selskaber og organisationer i Iran, dels at spionerer mod mål uden for Iran - navnlig Israel.[86] AIVD vurderer på baggrund af målene for Mahdi-virussen, at den iranske regering sandsynligvis har været involveret.[87] I maj 2014 offentliggjorde den amerikanske selskab iSIGHT Partners en rapport, der hævder, at iranske hackere igennem tre

(80) "Cyber Security Assessment Netherlands", National Cyber Security Center (juni 2013)
(81) "DigiNotar Certificate Authority breach 'Operation Black Tulip'", Foxit (5. september 2011)
(82) Christopher Bronk og Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco", Survival: Global Politics and Strategy, 55:2, 81-96, 2013
(83) Christopher Bronk og Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco", Survival: Global Politics and Strategy, 55:2, 81-96, 2013
(84) "Wells Fargo believed to be victim of cyber-attack over Innocence of Muslims", The Guardian (26. september 2012)
(85) "Staternes digitale slagmark", Jyllands-Posten, (6. juli 2013)
(86) "Cyber Security Assessment Netherlands", National Cyber Security Center (juni 2013)
(87) "Cyber Security Assessment Netherlands", National Cyber Security Center (juni 2013)

år har udført cyberspionage mod et stort antal embedsmænd i USA og højtstående officerer i det amerikanske forsvar.[88] Ifølge rapporten har hackerne skaffet sig adgang til fortrolige oplysninger ved at oprette falske profiler på sociale medier for derigennem at skabe forbindelse til deres målpersoner. Rapporten fremlægger ikke egentlige beviser på, at Iran står bag spionagen, men derimod flere indicier, der peger mod Iran.

I 2014 afdækkede Verfassungsschutz i den tyske delstat Bayern cyberspionage mod en række tyske og internationale selskaber, der kunne føres tilbage til Iran.[89] Cyberspionagekampagnen var blandt andet rettet mod selskaber inden for forsvars-, og luftfartsindustrien, hvor hackerne havde udvist interesse for informationer om fremstilling af raketter, helikoptere, satellitter og droner.[90] Iran er underlagt omfattende økonomiske sanktioner og eksport kontrol. Det er derfor sandsynligt, at Iran bruger cyberspionage til at skaffe sig adgang til militærteknologi og anden teknologisk knowhow.

Iran mistænkes for at stå bag en række attentater og konventionelle angreb mod mål i Vesten såsom bombningen af et jødisk center i Buenos Aires i 1994[91]. Det anses på den baggrund for meget sandsynligt, at Iran ligeledes udnytter cyberspace til at gennemføre angreb som led i landets asymmetriske krig mod sine fjender. Angrebene mod både Saudi Aramco og de amerikanske banker blev gennemført, kort tid efter at det iranske energiministerium ifølge iranske myndigheder blev udsat for et cyberangreb i april 2012. Det er således muligt, at der var tale om gengældelsesangreb udført af private hackere på vegne af det iranske styre. Det er desuden tænkeligt, at angrebene havde til formål at afprøve landets offensive cyberkapabiliteter.

Konklusion

Iran har inden for de seneste år udviklet og styrket sine cyberkapabiliteter, og landet har i dag både evne, vilje og kapabiliteter til at udføre såvel cyberangreb som spionage via internettet. Udviklingen er blandt andet blevet fremskyndet af, at landet har været udsat for flere cyberangreb. Dertil kommer, at den iranske ledelse ønsker at kunne kontrollere og overvåge internettet i Iran. Det er meget sandsynligt, at Iran har skiftet fra primært at forsvare sig mod angreb i cyberspace til at indtage en mere offensiv rolle, hvor landet udfører offensive operationer mod andre nationer.

(88) "Iranian hackers are targeting U.S. officials through social networks, report says", The Washington Post (29. maj 2014) http://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html

(89) "Cyber-Attacken; Spione aus dem Iran greifen deutsche Firmen an, Welt Online (13. november 2014)

(90) "Iranische Cyber-Attacke auf deutsche Unternehmen", Bilanz (6. november 2014) http://www.bilanz-magazin.de/ideen/iranische-cyber-attacke-auf-deutsche-unternehmen/

(91) "Intelligence for Terror" The Counter Terrorist, Vol. 5, Issue 3, 54-67 (juli 2013)

Det er endvidere sandsynligt, at Iran i stigende grad vil udføre cyberspionage mod mål i Vesten for at skaffe sig teknologisk knowhow.

Det er dog ikke sandsynligt, at Iran på nuværende tidspunkt har kapabiliteter til at udføre omfattende cyberangreb, der kan ødelægge it- og teleinfrastruktur eller anrette fysisk skade på tilknyttet infrastruktur såsom industrielle systemer.[92] Iran har derimod kapabiliteter til at forårsage kortvarige forstyrrelser af og sabotage mod it-systemer og hjemmesider.

Irans hovedfjender i cyberspace er - ligesom i den analoge verden -hovedsagelig USA og Israel. Ifølge det amerikanske efterretningsorgan National Intelligences årsrapport fra 2014 er Iran en utilregnelig aktør, der kan anvende cyberspionage og cyberangreb til at provokere eller destabilisere USA og dets allierede.[93] Spørgsmålet er, om Danmark, som USA's nære allierede, har en særlig risiko for at blive udsat for cyberangreb fra Iran.

Danmark og Iran har længe haft gode bilaterale relationer, hvilket udenrigsminister Martin Lidegaards besøg hos den iranske udenrigsminister, Mohammad Javad Zarif, i september 2014 bekræftede. Der er således ikke umiddelbart grundlag for at tro, at Iran vil gennemføre et uventet cyberangreb mod Danmark. Der er heller ikke grund til at tro, at Iran vil rette cyberangreb mod Danmark, i tilfælde af at dansk it-infrastruktur udnyttes som led i angreb mod Iran. Stuxnet-angrebet blev eksempelvis gennemført ved brug af en kommando- og kontrolserver, der befandt sig i Danmark, hvilket så vidt vides ikke medførte repressalier fra iransk side.[94]

Forsvarets Efterretningstjeneste skriver i sin risikovurdering for 2013, at det ikke er sandsynligt, at Danmark vil blive udsat for et stort og ødelæggende cyberangreb inden for de kommende ti år. Den vurdering gentages i den seneste risikovurdering for 2014.[95] Chefen for Forsvarets Efterretningstjeneste, Thomas Ahrenkiel, udtalte i november 2013, at vurderingen kan ændre sig, hvis Danmark eksempelvis engagerer sig aktivt i en koalition mod en stat, der har kapabiliteter til et cyberangreb.[96] Det må på den baggrund anses for sandsynligt, at Danmark kan blive genstand for iranske cyberangreb i tilfælde af eventuel dansk deltagelse i en væbnet konflikt med Iran.

Den største trussel mod Danmarks nationale it-sikkerhed synes dog primært at være private iranske hackergrupper, der lejlighedsvist og lidt tilfældigt hacker danske hjemmesider eller udnytter dansk it-infrastruktur som angrebsplatform mod andre lande. Der er desuden risiko for, at danske selskaber inden for primært forsvarsindustrien kan blive udsat for iransk cyberspionage.

(92) Gabi Siboni og Sami Kronefeld, "Developments in Iranian Cyber Warfare, 2013-2014", Military and Strategic Affairs, vol. 6, nr. 2 (august 2014) http://www.inss.org.il/index.aspx?id=4538&articleid=6809

(93) US Intelligence Community Worldwide Threat Assessment (29. januar 2014)

(94) "A Declaration of Cyber-War", Vanity Fair (april 2011)

(95) "Efterretningsmæssig Risikovurdering 2014", Forsvarets Efterretningstjeneste

(96) "FE-chef frikender USA for spionage", Berlingske (13. november 2013)