

«Du har blitt hacket av Gaza Hacker Team»

Siden 2000 har flere palestinske angrep blitt utført mot israelsk kyberinfrastruktur, inkludert børsen i Tel Aviv, flere israelske myndigheter og bedrifters nettsider.¹ Står vi overfor en ny form for palestinsk motstandskamp?

Av Erik Skare, master i arabisk ved Universitetet i Oslo.

23. OKTOBER 2012: DET ISRAELSK POLITIET finner ut at alle datamaskinene deres har blitt infiltrert med spionware og blitt kompromittert. Det verste er likevel at det har tatt dem en hel uke å oppdage det, og trojaneren har spredd seg til andre israelske departementer. Det ender med at politiet må ta ned alle sine servere, kutte internettforbindelsen og forby bruken av minnepenner. Forbudet varer en hel uke.² I februar 2014 skjer det igjen når hackerne bryter seg inn i Siviladministrasjonen for Judea og Samaria, myndighetsorganet som behandler alle administrative saker i område A på Vestbredden.³ Begge angrepene blir koblet til den palestinske hacker-gruppa Gaza Hacker Team.⁴

Betyr det at vi er vitner til en ny form for palestinsk motstandskamp hvor hacking er blitt nok et middel for å presse okkupasjonsmakten? For å svare på dette er det nødvendig å finne ut hvem Gaza Hacker Team faktisk er, hva de står for og hva de gjør. Denne artikkelen er basert på intervjuer gjort med gruppa fra september 2014 til april 2015 og et internt dokument – en form for «prinsippprogram» –

som ble oversendt artikkelforfatteren. Det gir oss tilgang til informasjon som aldri har blitt publisert andre steder. Likevel, før vi kan konkludere hvorvidt hacking kan regnes som et middel i motstandskampen, må vi først gjøre rede for hva politisk hacking, *hacktivisme*, faktisk er. Når vi forstår hva begrepet innebærer, kan vi bevege oss videre til å analysere Gaza Hacker Team og hva dette fenomenet kan ha å si for en palestinsk motstandskamp med midler i – potensiell – utvikling.

Hvordan forstår vi hacktivisme?

Da Internett dukket opp, ble det hevdet at dette verktøyet ville føre til en demokratisering av, og fri flyt av, kommunikasjon. For de største optimistene var Internett ensbetydende med slutten på utbytting, fattigdom, militarisme, korrupsjon og tyranni. En av datidens teknologioptimister, Al Gore, beskrev for eksempel «informasjonsmotorveiene» som «en metafor for selve demokratiet».⁵ Likevel, som blant annet professor i kommunikasjon ved Universitetet i Illinois, Robert McChesney, har påpekt, har Internett siden begynnelsen av

1990-tallet blitt lagt under logikken til kommersialisering og profitt, og det demokratiske potensialet man forespeilet har ikke utviklet seg slik en håpet på.⁶ Bakgrunnen er viktig fordi hacktivism, sammenslåingen av de to ordene «hacking» og «aktivisme», ble skapt og formet i skjæringspunktet mellom Internettets demokratiske potensial og dagens situasjon. Et eksempel er da den første kommersielle e-posten ble sendt ut til alle Usenet-brukere i 1994 og avsenderens e-post ble så overflommet av sinte svar at den rett og slett gikk ned.⁷ Forestillingen blant Usenet-brukerne da – som førte til denne digitale aksjonsformen i protest mot kommersielle e-poster – var at kommersialisme og internettdemokrati ikke skulle (eller kunne) forenes.

Artikkelen tar dermed utgangspunkt i «hacktivism» som: «[e]kteskapet mellom politisk aktivisme og hacking [hvor] hacktivism kombinerer den sivile ulydighetens transgressive politikk med teknologiene og teknikkene til hackere».⁸ Hacktivismen kan ta flere former hvor de mest vanlige er såkalte «defacements» (en endring av det visuelle uttrykket på en nettside) eller DDoS-angrep (*Distributed Denial-of-Service attack*: å overflomme en server med så mye informasjon at den går ned for en begrenset periode). Det er først og fremst disse formene for hacktivism denne artikkelen bruker som eksempler.

Dette må ikke forveksles med begreper som *kyberterrorisme* eller *kybervandalisme* som gjør lite annet enn å infantiliserer hackerne – hvor ugagn tilsynelatende er det eneste målet. Om vi begrenser oss til disse definisjonene vil vi miste muligheten til å se på hackere som sosiale og politiske aktører. Sandor Vegh, med sin doktorgradsavhandling om Internettets påvirkning på demokratiet, poengterer at begrepsbruken gitt ovenfor tvert imot vil føre til at sosialt og politisk progressive blir presset

enda mer ut i periferien hvor Internett i utgangspunktet er deres eneste mulighet til å bli hørt.⁹ Akkurat som det finnes aksjonsformer i den fysiske sfæren, som sitt-ned-demonstrasjoner hvor målet er å hindre tilgang til visse områder, eller graffiti hvor en politisk melding kan uttrykkes, kan DDoS-angrep sammenlignes med å hindre tilgang til visse sfærer, om enn digitalt, mens det å endre det visuelle uttrykket på en nettside for å gi en beskjed kan sammenlignes med graffiti. På samme måte som at ikke all graffiti regnes som politisk, ved at det begrenser seg til hærverk, vil «defacements» som ikke har noe annet formål enn å «tagge» en nettside falle utenfor definisjonen av hacktivism.

Det er nettopp dette «ekteskapet» mellom aktivisme og hacking som vi har sett flere ganger i Israel/Palestina. Blant annet med den saudiarabiske hackeren Oxomar som i 2012 hacket og publiserte kredittkortinformasjonen til tusenvis av israelere.¹⁰ Samtidig kalte han alle muslimske hackere til å delta i hans elektroniske kamp mot Israel.¹¹ Tilsynelatende åpnet det øynene opp for det palestinske politiske etablissementet. Sami Abu Zuhri, talsperson for Hamas, understrekte at disse angrepene åpnet «et nytt område for motstandskampen mot israelske forbrytelser».¹²

Hvem er egentlig Gaza Hacker Team?

Lite har blitt skrevet om gruppa, og i akademisk sammenheng er materialet så godt som ikke-eksisterende. Selv om gruppa ble grunnlagt i 2007, er det vanskelig å finne de store angrepene og innbruddene dette året.¹³ Den 13. februar 2008 klarte de å ta ned nettsiden til det israelske partiet Kadima. Fire år senere, i 2012, hadde gruppa klart å få nyhetsoppslag i Israel og internasjonalt med flere hackede nettsider.¹⁴

Når det gjelder den organisatoriske

ERIK SKARE

strukturen til Gaza Hacker Team, er det en tydelig tredelt hierarkisk inndeling:

Lederskapet (al-Qiyada) som består av tre palestinske ungdommer i Gaza: mr.leon, Casper og Claw.

Teamet (al-Fariq) som utgjør hele Gaza Hacker Team og som lederskapet er ansvarlig for. Medlemmene er palestinere i tillegg til flere hackere fra andre arabiske land, særlig Algerie, Egypt, Marokko og Saudi-Arabia.

Grupper (al-Majmu'at) som spesialiserer seg på sine respektive felt som for eksempel hacking av e-poster, servere med mer Gruppenes samlede kunnskap samles i teamet på nivå 2.

mr.leon gjorde det klart at de ikke hadde noen interesse av å samarbeide med andre: «Vi tilhører ikke noen bevegelse... Vi er ungdom fra Gaza».¹⁵ Dette innebar at de verken fikk noen støtte fra noe politisk parti, gruppe eller bevegelse, og de hadde heller ingen interesse av å innlede noen form for samarbeid. Da jeg diskuterte hvordan dette kunne være tilfelle med en venn som var Fatah-medlem og som hadde vært involvert i palestinsk politikk siden ungdommen, men uten noen form for tilknytning til hacker-gruppa, beskrev han uttalen som taktisk orientert.¹⁶ At de ikke hadde bånd til noen politisk bevegelse, var aldri et uttrykk for noen form for apolitisk virksomhet, men heller noe som i større grad ville fristille dem ideologisk, og stille dem utenfor faren for å fremmedgjøre palestinere som hadde en annen politisk overbevisning.

Det bør for øvrig bemerkes at de tradisjonelle politiske partiene, og deres organiserte makthierarkis fremmedgjøring av palestinsk ungdom, kan spille en rolle for den palestinske hacktivistgruppas lyst til å samarbeide med dem. Jacob Høigilt, ved PRIO, viser til lignende tendenser under den første intifadaen da lokale grasrotbevegelsene, ledet av unge palestinske voksne, «erstattet den

paralyserte politiske eliten».¹⁷ Dermed sagt er det åpenbare forskjeller på situasjonen i dag og perioden 1987-1993, men det kan legges grunnlaget for en analyse som ser på palestinsk hacktivism som en uavhengig faktor som transcenderer oppfatningen av palestinske politiske partier (inkludert deres væpnede brigader) som de eneste agentene for frigjøring av landet.

Når en går gjennom oversikten over de hackede nettsidene av Gaza Hacker Team og hva som publiseres der, er mye av det som går igjen en retorikk hvor de presenterer seg selv som elektroniske jihadister. Gaza Hacker Teams fokus er med andre ord på den *religiøse* istedenfor den mer sekulære «muqawama» (motstand). Dette kommer fram i dokumentet deres, «ihda' li-sha'b al-falastini: injazat fariq qarasinat Ghazza» («Gave til det palestinske folket: Gaza Hacker Teams bragder»), blant annet i deres første kapittel «Hvordan være en elektronisk jihadist». På flere av de hackede nettsidene blir beskjedene deres videre introdusert med «bismillah rabb al-mujahidin wa-l-shuhada'» («I guds navn, jihadistene og martyrenes herre») – en uttrykksform som deles av grupperinger tradisjonelt knyttet til salafi-jihadisme.¹⁸ Videre er det ikke Israel som utpekes som mål, men jødiske og sionistiske nettsider, samt nettsider til sjiaer, sufister, ibadister, vantro og ateister for å nevne noen. Dette kommer kun i tillegg til nettsider som inneholder sang, musikk, gambling, hekseri, astrologi og pornografi.¹⁹ Med andre ord er formen i dokumentet tydelig forenlig med en salafistisk tolkning av sunniislam. Samtidig slås det fast at elektronisk jihad skal spre den «korrekte versjonen» av islam som plasserer gruppa i den salafi-jihadistiske folden.²⁰

Derfor kom det ikke som noen overraskelse da mr.leon, som samtlige intervjuer ble gjort med, uttalte: «Vi regner oss selv som en del av den væpnede palestinske motstands-

kampen».²¹ Dette kommer også til uttrykk i måten de velger å representere seg selv på forumet deres. Et eksempel er hvordan en per august 2015 på forumet deres blir møtt av et bilde av to bevæpnede, maskerte menn.²²

Jeg vil likevel argumentere for at til tross for at Gaza Hacker Team forsøker å etablere et jihadist-salafistisk narrativ rundt seg selv som elektroniske jihadister, så er målene og



*Israelerne skal føle på den samme
usikkerheten for hvor og når neste
angrep skal skje.*



kravene deres i høyeste grad nasjonalistiske. Et eksempel er da gruppa hacket israelske nettsider hvor innholdet ble byttet ut med koranvers og Gud som jihadistenes og martyrenes herre. Likevel ble hackingen i utgangspunktet gjennomført for å protestere mot krenkelsen av islamske helligdommer i Palestina.²³ Andre eksempler er hackinger med den samme religiøs-politiske språkdrakten, men hvor målet har vært å protestere mot drapet på 'Arafat Jaradat i et israelsk fengsel 2013,²⁴ solidaritet og protest mot behandlingen av palestinske sultestreikende fanger (og da særlig i solidaritet med med Khadr 'Adnan og Samir 'Issawi)²⁵ eller mot operasjon «Pillar of Defense» i Gaza.²⁶

De palestinske hacktivistenes mål

Til nå har det altså blitt slått fast at Gaza Hacker Team presenterer seg selv som elektroniske jihadister, og aksjonene er en del av det de betegner som jihad. Slik de ser det selv, er de en fortsettelse av den væpnede motstandskampen. På den andre siden har de åpenbart nasjonalistiske krav med fokus på frigjøring av

Palestina når de aksjonerer. Så hvordan skal dette bli oppnådd? I forordet av dokumentet deres blir viktigheten av moderne, elektronisk krigføring, og at muslimer deltar i den, fremhevet.²⁷ Dette blir hovedsaklig begrunnet på tre plan: økonomisk og psykologisk krigføring, samt informasjonskrig.

Det første argumentet til Gaza Hacker Team for å gjennomføre angrep mot den israelske kyberinfrastrukturen, er at det vil påføre okkupasjonsstaten store økonomiske skader.²⁸ Tankegangen deres er at hver gang en israelsk nettside blir hacket, vil det ikke bare koste store ressurser for å få nettsiden til å fungere igjen, de må også hele tiden tette igjen smutthull som kan utnyttes. Det vil naturligvis være problematisk for bedrifter, for eksempel banker, å ha et system som blir tatt ned i tide og utide. Om en bedrift får et rykte på seg for å være upålitelig – i en tid hvor det meste av handel har blitt digitalisert – vil de fleste velge et annet sted å handle eller oppbevare pengene sine.

Om det ikke er umulig, så er det svært vanskelig å si sikkert hvor mye et enkeltangrep koster i kroner og øre for hver enkel bedrift, men det er eksempler på faktiske skader hacktivistene har påført Israel. I februar 2013 klarte en ukjent gruppe med hacktivistene å stenge en tunnel i Haifa to dager på rad da de hacket sikkerhetskameraene i tunnelen. Det første angrepet varte ikke lenger enn tjue minutter, mens det andre varte i over åtte timer. Sammenlagt regner man med at det kostet Israel hundretusenvis av dollar.²⁹

Det andre målet som ble fremhevet, var det psykologiske aspektet av hackingen hvor Gaza Hacker Team uttalte: «Den [elektroniske jihad] dreper moralen til fienden, skader sinnet hans og terroriserer dens folk og soldater».³⁰ Gaza Hacker Team begrunnet ikke påstanden nærmere, men den psykologiske

ERIK SKARE

krigføringen har i hovedsak som mål å skape et brudd i normaliteten for israeleres dagligliv ved å skape usikkerhet og uforutsigbarhet, som utgjør kjernen i angrepene. Israelere vet enkelt og greit aldri når en nettside blir tatt ned eller om det første som møter dem når de skal logge seg inn på bankkontoen er bilder av døde barn og kvinner i Gaza. Denne formen for aksjoner, hvor målet er å brutalt trekke israelere ut av normaltilstanden, er derimot ikke begrenset til hacking, men er også, som Naser Abufarha påpeker i sin forskning på palestinske selvmordsbombere, nært knyttet opp mot mimetisk vold: Å mime den samme volden og bruddet med normaliteten som palestinerne blir påtvunget gjennom okkupasjonen.³¹ Israelerne skal føle på den samme usikkerheten for hvor og når neste angrep skal skje.

Gaza Hacker Team er en ny form for motstandskamp som har blitt muliggjort av den teknologiske utviklingen.

Et konkret eksempel på en slik aksjon mot Israel, som riktignok ikke ble gjennomført av Gaza Hacker Team, hvor feilinformasjon brukes som en del av det psykologiske spillet: Under den siste eskaleringen i Gaza, sommeren 2014, publiserte den engelske Twitter-kontoen til den israelske hæren:

«#ADVARSEL: Mulig atomlekkasje i regionen etter at 2 raketter har truffet Dimona atom-anlegg».³²

Noen timer senere, da IDF hadde fått tilbake kontrollen over kontoen, ble det gjort klart at den hadde blitt hacket av Syrian Electronic Army, og at det ikke var grunn til bekymring.

Til slutt var Gaza Hacker Teams siste argument at angrepene nødvendigvis inne-

holdt et aspekt av informasjonskrig hvor de visuelle endringene av nettsidene (med lyd, bilder og tekst) bidro til å gi israelerne en flik av den virkeligheten som Gaza Hacker Team opplevde i Gaza. Det bør for eksempel nevnes at mr.leon påpekte hvordan hjemmene til medlemmene hadde blitt bombet sommeren 2014.³³

Så langt har jeg forsøkt å gjøre rede for hva hacktivism er, og hva det ikke er, hvem Gaza Hacker Team er, hva de gjør og hva målsettingen deres er. Spørsmålet som vi står igjen med: Står vi overfor en ny form for motstandskamp? Hackerne i Gaza Hacker Team ser til slutt på seg selv som en fortsettelse av den væpnede palestinske motstandskampen, men er det så enkelt?

Motstand i den digitale og fysiske sfæren

Siden den britiske, og senere den sionistiske koloniseringen av Palestina, har det blitt brukt flerfoldige midler for å gjenvinne landets suverenitet, og den palestinske motstandskampen går så langt tilbake som slutten av 1800-tallet.³⁴ Siden da har det blitt dokumentert hvordan palestinerne har gjennomført boikott, generalstreiker, graffiti i tillegg til væpnede aksjoner for å nevne noe.³⁵ Målet har ikke bare vært å presse okkupasjonsmakten til å gi makten tilbake til palestinerne, men også å bevisstgjøre omverdenen på det som skjer:

«Det finnes ikke noe palestinsk folk ... De eksisterte ikke», uttalte Golda Meir.³⁶ Dermed så palestinerne det som nødvendig å vise at de eksisterte og at de var et folk med et land å vinne tilbake. Det er kun innenfor dette rammeverket at man kan forstå én av aksjonsformene – flykapringene – som ble gjen-

Gaza Hacker Team ser på seg selv som en fortsettelse av den væpnede palestinske motstandskampen.



ERIK SKARE

nomført av grupper som PFLP på 1970-tallet. Som George Habash uttalte: «Å kapre et fly har mer effekt enn å drepe hundre israelske soldater» og «I tiår har verdensopinionen verken vært med eller mot palestinerne. Den har simpelthen ignorert oss. Nå snakker de i det minste om oss».³⁷

Behovet for å tiltrekke seg verdens oppmerksomhet har derimot ikke vært begrenset til flykapringer. I Darweish og Rigbys dokumentasjon av den palestinske folkelige og ikke-voldelige motstandskampen i dag, er for eksempel ett av de uttrykte målene for landsbykomiteene å belyse okkupasjonen for det internasjonale samfunnet gjennom organiseringen av fredagsdemonstrasjoner.³⁸ Dermed er likheten med den palestinske hacktivismen slående om vi bruker en annen palestinsk hacker-gruppe, KDMS Team, som eksempel på at målet er å vise resten av verden at Palestina eksisterer og at det er okkupert. KDMS Team hacket aldri israelske, men kun vestlige sider som WhatsApp og Bitdefender, og beskjedene de la igjen er illustrerende: «Det er på jorda et land kalt Palestina. Det har blitt stjålet av sionistene. Vet du om det?»³⁹ Og som KDMS Team selv uttalte da jeg intervjuet dem: «Vi hacker internasjonale nettsider for å gi en beskjed til verden».⁴⁰ Videre har aktivistene ved fredagsdemonstrasjonene, jamfør Darweish og Rigby, satt seg som mål å øke kostnadene ved okkupasjonen til et nivå som er utålelig – på samme vis som Gaza Hacker Team argumenterer for i sitt dokument.⁴¹

Videre eksisterer det fellestrekk mellom den palestinske hacktivismen og den ikke-voldelige folkelige motstanden når vi sammenligner hacktivistenes aktiviteter med sitt-ned-demonstrasjonene gjennomført i den palestinske fysiske sfæren: 16. oktober 2012 blokkerte en gruppe palestinere rute 443, hovedruten mellom Jerusalem og Tel Aviv. I

tretti minutter klarte aktivistene å stoppe trafikken helt til det israelske politiet fjernet dem. Aktivistene klarte å hindre tilgang til en offentlig sfære (veien mellom Jerusalem og Tel Aviv) for en begrenset periode, og dette kan dermed, som argumentert, sammenlignes med DDoS-angrepene som hindrer tilgang i den digitale sfæren. En av organisatorene for sitt-ned-demonstrasjonen uttalte at så lenge palestinerne led under okkupasjonen, ville heller ikke israelsk dagligliv fortsette som vanlig.⁴² Å mime den israelske volden og bryte normaliteten i det israelske dagliglivet er med andre ord et fellestrekk ved et vidt spekter av palestinske aksjoner fra sitt-ned-demonstrasjoner i den fysiske sfæren til DDoS-angrep i den digitale – til tross for at midlene som brukes er kvalitativt ulike.

Om en velger å ikke se på den palestinske motstandsbegnelsen som historisk abstrakt, men heller som flerfoldige midler gitt spesifikke historiske forhold, vil vi dermed se at hacktivismen *a priori* faller inn under begrepet:

~
*Palestinsk hacktivismen er et middel
for å utfordre okkupasjonen i
den digitale sfæren.*



Palestinsk hacktivismen som et middel for å utfordre okkupasjonen i den digitale sfæren – som et ledd i å bevisstgjøre omverdenen og tiltrekke seg dens oppmerksomhet, bryte normaliteten og påvirke okkupasjonsøkonomien negativt. Den jobber for å forstyrre okkupasjonen med et mål om å endre den politisk-sosiale situasjonen på bakken i det okkuperte Palestina.

Videre kan *defacements* av nettsider sammenlignes med politisk graffiti – noe som er

relevant siden det først og fremst er denne aksjonsformen som er blitt brukt som eksempel i denne artikkelen. Bruken av graffiti er ikke tilfeldig, og er ikke bare brukt som et kommunikasjonsmiddel, men har også blitt dokumentert som en inngripen i det etablerte maktforholdet mellom okkupant og okkupert.⁴³ Slutningen om at graffiti er en direkte inngripen er dermed passende med *defacements* hvor hackerne bevisst trenger seg inn på et fremmed område for å markere seg. Denne formen for aksjon er derfor også en historisk prosess hvor aksjonistene omformer seg fra passive til aktive subjekter for egen frigjøring. Denne omformingsprosessen – enten det er graffiti eller *defacements* – er blitt beskrevet (om enn i annen kontekst) av Franz Fanon om den afrikanske koloniserte som forsøker å oppheve sin eksistens som *den svarte* for å gjenskape seg selv som negasjonen, *mennesket*, i abstrakt form: «Avkoloniseringen er den ekte skapelsen av nye menn. [...] ‘Tingen’ som har blitt kolonisert blir menneske gjennom den samme prosessen som den frigjør seg i».⁴⁴ Dette er fortsatt relevant den dag i dag for den palestinske motstandskampen.

Konklusjonen så langt vil derfor være at hacktivismen til Gaza Hacker Team er en ny form for motstandskamp som har blitt muliggjort av den teknologiske utviklingen. De to formene for hacktivismen nevnt over har samtidig klare paralleller til den folkelige, ikke-voldelige motstanden hvor blant annet blokkering av tilgang til digitale sfærer føyer seg inn i palestinsk historie med sivil ulydighet.

Islamsk Jihad og Gaza Hacker Team

Finnes det da palestinsk politisk hacking som kan defineres som væpnet? Ja, men ikke hos Gaza Hacker Team. Det er derimot en annen gruppe som jeg vil argumentere faller inn

under denne definisjonen: palestinsk Islamsk Jihad. Informasjonen i følgende del har kommet etter intervjuer med gruppas hovedrepresentant på Vestbredden.

Vi vet at palestinsk Islamsk Jihad har hackere i al-Quds-brigaden. Allerede i 2008 skrev for eksempel nyhetsbyrået for MØNA, Menassat, at Islamsk Jihad nylig hadde utviklet en elektronisk brigade som hadde hacket flere israelske nettsider.⁴⁵ Dette ble bekreftet av Islamsk Jihad-representanten jeg intervjuet.⁴⁶ Han hadde derimot en rettelse: Den politiske avgjørelsen i Islamsk Jihads lederskap om å integrere en elektronisk del i al-Quds-brigaden hadde blitt tatt allerede i 1999 da arbeidet begynte for å holde tritt med okkupasjonens teknologiske utvikling.⁴⁷ De første stegene hadde blitt tatt for å «akselerere okkupasjonens slutt» og de hadde «en spesialisert enhet som var en del av al-Quds-brigaden som tilhørte den militære jighaden. Det er en enhet som tar del i den politiske jighaden i tillegg til sivile enheter som utøver arbeidet deres i Gaza».⁴⁸ Hovedoppgavene til brigaden var likevel ikke å ta ned så mange israelske nettsider som mulig. Heller oppsummerte hovedrepresentanten for Islamsk Jihad det viktigste arbeidet i følgende punkter:

- å hindre elektroniske angrep fra Israel
- å hindre spionasje og overvåking
- å spre den palestinske saken til resten av verden og media

Med andre ord bryter disse virkemidlene med Gaza Hacker Teams påstand om at hacktivismen først og fremst er et offensivt verktøy. Heller fremhevet han at den elektroniske enheten var nødvendig for å få den væpnede brigaden til å jobbe mer effektivt og trygt – blant annet ved å spore og overvåke israelske soldater samt å forstyrre (*jamming*) kommunikasjonslinjene deres. Likevel, det er fortsatt eksempler på at Islamsk Jihads cyberbrigade ikke

ERIK SKARE

er begrenset til ren defensiv virksomhet. Hovedrepresentanten nevnte som eksempel aksjonen hvor 20 000 israelske soldater mottok sms-er fra Islamsk Jihad: «Gaza vil bli deres soldaters gravplass og Tel Aviv vil bli et flammehav». Det bør påpekes at 20 000 er et særdeles høyt antall. Han refererte sannsynligvis til hackingen av det israelske telefonsystemet hvor antall israelske soldater som mottok meldingen var «begrenset» til fem tusen stykker i det Islamsk Jihad betegnet som «Nervekrigen».⁴⁹ Hackingens virkemidler passer dermed videre inn i det som Julie Peteet ved Universitet i Louisville skriver om steinkasting, en annen tradisjonell form for motstand i de okkuperte områdene. Hun beskriver det som et «[k]ommunikasjons-, angreps- og forsvarsvåpen», jamfør hackingens målsetting.⁵⁰

Er det dermed mulig å analysere Gaza Hacker Team sine aksjonsformer som en væpnet form for motstandskamp i lys av at de er mer offensive enn de midlene som hovedrepresentanten for Islamsk Jihad har beskrevet? Som argumentert er det ikke tilfellet. Tvert imot, Islamsk Jihad sine elektroniske brigader er en fortsettelse av den væpnede motstandskampen, mens Gaza Hacker Team utøver en «folkelig», ikke-voldelig form for motstandskamp. Hvis DDoS-angrep og *defacement* er en væpnet form for motstandskamp, vil ikke det nødvendigvis implisere at sitt-ned-demonstrasjoner og graffiti innebærer en militarisering av den fysiske sfæren? Aktivister og demonstranter vil av åpenbare grunner benekte dette. Det samme gjelder lekkasje av informasjon som kan sammenlignes med Edward Snowdens lekkasjer fra NSA. Selvsagt, det er fortsatt en debatt om Snowdens aksjoner var legitime eller ikke, men det vil være unødvendig å påpeke at det ikke er snakk om en militarisering av det offentlige rom.

Islamsk Jihad og Hamas sine hackergrupper er derimot en fortsettelse av den væpnede motstandskampen, men med andre midler ved at de opererer innenfor rammeverket av væpnede brigader. De hacker ikke for hackingen eller berømmelsens skyld, men fungerer heller som en utvidelse av en allerede eksisterende væpnet kamp hvor de hacker for å lette arbeidet til soldatene i gruppa i form av å gi informasjon, kryptere egen infrastruktur, forstyrre telefonlinjer med mer. Ronald J. Deibert, professor ved University of Toronto, beskriver for eksempel militariseringen av internett som den eksplisitt *militære* bruken av den, og skiller skarpt mellom politisk motivert hacking gjort av hacktivist og det amerikanske militærets bruk av hackere, trojanere, virus, ormer og teknikker for

❧

Å identifisere de ulike strømningene som eksisterer blant de palestinske hackerne er nødvendig om vi skal forstå fenomenet.

❧

«kyberpropaganda».⁵¹ Slik sett bør hackerne i Islamsk Jihad regnes inn under sistnevnte.

Med andre ord vil Gaza Hacker Team være aktivister i tradisjonell form – om enn i den digitale sfæren – mens hackerne i Islamsk Jihad er kyberkrigere som er en del av en pågående og sammenhengende militær krigføring i stadig utvikling. Gaza Hacker Team er ikke profesjonelle hackere, men gjør det ut fra sin politiske overbevisning, på fritiden, etter egen opplæring, og i en mye mindre skala enn for eksempel Islamsk Jihad. Selve ordet hacktivism kommer som sagt av «hacking» og «aktivisme», og dermed kan vi, ut fra en snever lesing, ekskludere Islamsk Jihad og al-Qudsbrigaden fra denne definisjonen ettersom den

ikke er aktivistisk i sin natur. Med andre ord kan ikke hacktivism regnes som en katalysator av den militariseringen av internett som vi ser i dag.

Den elektroniske motstandskampen er her Forskningen på Gaza Hacker Team, Islamsk Jihad og de andre palestinske hackerne viser oss at den elektroniske motstandskampens natur er mer mangslungen enn det som ellers blir lagt til grunn i diskusjoner rundt fenomenet. Intervjuene med Gaza Hacker Team har gitt innblikk i deres syn på hvem de er, hva de gjør og hvorfor. Videre har jeg sammenlignet gruppa med den elektroniske enheten i Islamsk Jihads al-Quds-brigade for å avgjøre om vi står overfor en ny form for palestinsk motstandskamp og om den arter seg væpnet eller folkelig.

Å identifisere de ulike strømningene som eksisterer blant de palestinske hackerne er nødvendig om vi skal forstå fenomenet. I likhet med den tradisjonelle motstandskampen, slik den har artet seg forskjellig innad den i palestinske befolkningen og dens grupperinger – avhengig av tid og kontekst – er de elektroniske gruppene ingen monolittisk enhet, verken i sine strategier, virkemidler, mål eller former. Å identifisere de forskjellige strømningene vil forebygge mot fordummende begreper som kyberterrorisme som ikke gir oss noen dypere forståelse av fenomenet. Tvert om er hacktivistene et symptom på utviklingen av den palestinske motstandskampen i den digitale æraen, og deres grupper er like ulike som tilfellet var for noen tiår siden da midlene ikke var digitale, men fysiske.

Til tross for at det er vanskelig å datere den eksakte dagen for når kyberkrigen mot Israel begynte, er det overveiende sannsynlig at den begynte, og utviklet seg, rundt tusenårsskiftet.⁵² Den kan regnes lav-intensiv gjennom

den første delen av tiåret, før den eskalerte rundt den arabiske våren med flere aksjoner mot Israel – både nasjonale og internasjonale. Det er ingenting som tyder på at denne formen for motstand vil avta i en tid hvor større deler av aktivisme og krigføring overføres til den digitale sfæren. Det vil være trygt å si at vi ikke har sett det siste til de palestinske hackerne.

• f •

1. Jeg vil takke Olav Skare, Charlotte Lysa, redaktør for Babylon, Kristian Takvam Kindt, og to anonyme fagfeller for svært nyttige kommentarer til artikkelen.
2. «How Israeli Police Computers were hacked: The inside story», Shamah, David, 28. oktober 2013 <http://www.timesofisrael.com/how-israeli-police-computers-were-hacked-the-inside-story/> (27.08.2015) og «Operation Molerats: Middle East Cyber Attacks Using Poison Ivy», Haq, Thoufique, Moran, Ned & Villeneuve, Nart, 23. august 2013 <https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html> (14.09.2015)
3. «Xtreme Rat bites Israeli government sites, yet again» Shamah, David, 12. februar 2014 <http://www.timesofisrael.com/xtreme-rat-bites-israeli-government-sites-yet-again/> (27.08.2015)
4. «Operation Molerats: Middle East Cyber Attacks Using Poison Ivy», Haq, Thoufique & Moran, Ned, 23. august 2013 [https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html%20%20\(27.08.2015\)](https://www.fireeye.com/blog/threat-research/2013/08/operation-molerats-middle-east-cyber-attacks-using-poison-ivy.html%20%20(27.08.2015))
5. Sitert i: Thornton, Alinda L.: «Does the internet create democracy?» i *Equid Novi: African Journalism Studies*, vol. 22, nr. 2, s. 128
6. McChesney, Robert: *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*. New York, London: The New Press, 2013, s. 97
7. Ibid: s. 102
8. Samuel, Alexandra Whitney: *Hacktivism and the Future of Political Participation*. Doktorgradsavhandling, Massachusetts: Harvard University Cambridge, 2004, s. 1
9. Vegh, Sandor: «Hacktivism or Cyberterrorists? The Changing Media Discourse on Hacking», i *First Monday*, vol. 7, nr. 7
10. «al-hakkir 'Oxomar' yanshur mazidan min battaqaat al-i' timan al-israiliyya» («Hackeren «Oxomar» publiserer flere israelske kredittkort») al-Iqtisadiyya 12. januar 2012 http://www.aleqt.com/2012/01/12/article_615664.html (27.08.2014)
11. Ibid. «Ad'u al-hakkirz al-'arab al-muslimin li-al-tawahhud didd Israil wa al-indimam li-hadhihi al-harb kama ad'u al-hakkirz al-atrak alladin yakhtaraqun al-'adid min al-mawaqi' al-iliktruniyya yawmiyyan» (Oversettelse: «Jeg oppfordrer alle muslimske og arabiske hackere til å forene seg mot Israel og bli med i denne krigen såvel som alle tyrkiske hackere som angriper nettsidene daglig»)

ERIK SKARE

12. «al-hakkir 'ala khatt al-muwajih wa "Hamas" tad'uila "jihad iiliktruni" didd Isra'il» («Hackere ved frontlinjen og Hamas oppfordrer til "elektronisk jihad" mot Israel») Security & Defense Arabia 18. januar 2012 http://sdarabia.com/preview_news.php?id=25005&cat=6 (27.08.2015)
13. Intervju med forfatteren, mr. Leon, på e-post, 10. mars 2015
14. Se for eksempel, «Arab hackers leave 'message to all Jews' on Chief Rabbinate's website" Ben Zion, Ilan, 23. september 2012 www.timesofisrael.com/hackers-leave-message-to-jews-on-rabbinate-website/ (05.10.2015) og «Hackers Assault Tel Aviv Stock Exchange, El Al Websites" Ferziger, Jonathan & Odenheimer, Alisa, 16. januar 2012 <http://www.bloomberg.com/news/articles/2012-01-16/hackers-assault-tel-aviv-stock-exchange-el-al-airlines-websites> (05.10.2015)
15. Intervju med forfatteren, mr. Leon på e-post, 10. september 2014
16. Anonymisert, personlig kommunikasjon, 27. september 2014
17. Høigilt, Jacob: «The Palestinian Spring That Was Not: The Youth and Political Activism in the Occupied Palestinian Territories» i Arab Studies Quarterly, vol. 35, nr. 4, s. 346
18. «Defacement of hasamba.co.il» Zone-h, 25. august 2012 <http://zone-h.org/mirror/id/18255985> (29.09.2014)
19. Gaza Hacker Team: *Ihda' li-al-sha'b al-falastini: Injazat Fariq Qarasinat Ghazza* (Gave til det palestinske folket: Gaza Hacker Teams bragder) (i.d.) internt dokument, s. 8
20. Ibid: s. 6
21. Intervju med forfatteren, mr. Leon på e-post, 15. september 2014
22. Gaza Hacker Teams forum: <http://www.gaza-hacker.cc>
23. «Defacement of hasamba.co.il» Zone-h, 25. august 2012 <http://zone-h.org/mirror/id/18255985> (29.09.2014)
24. «Defacement of mamtakim4u.co.il» Zone-h, 25. februar 2013 <http://zone-h.org/mirror/id/19395494> (29.09.2014)
25. «Defacement of asia-construction.co.il» Zone-h, 14. mai 2012 <http://zone-h.org/mirror/id/17900790> (29.09.2014)
26. «Defacement of your-smile.co.il» Zone-h, 17. november 2012 <http://zone-h.org/mirror/id/18608836> (29.09.2014)
27. Ibid: s. 5
28. Ibid: s. 6
29. «Hackers Shut Down a Tunnel Road in Israel» Ohlheiser, Abby, 27. oktober 2013 <http://www.thewire.com/global/2013/10/hackers-shut-down-tunnel-road-israel/70983/> (14.09.2015)
30. Ibid: s. 7
31. Abufarha, Naser: *The Making of a Human Bomb. An Ethnography of Palestinian Resistance*. Durham, London: Duke University Press, 2009, s. 158
32. «Israel Army's Twitter account hacked, posts 'incorrect' tweets» Kerr, Dara, 03. juli 2014 <http://www.cnet.com/news/israel-armys-twitter-account-hacked-posts-incorrect-tweets/> (27.08.2015)
33. Intervju med forfatteren, mr. Leon på e-post, 11. september 2014

«DU HAR BLITT HACKET AV GAZA HACKER TEAM»

34. Se for eksempel Khalidi, Rashid: *Palestinian Identity: The Construction of Modern National Consciousness*. New York: Columbia University Press, 1997, s. 24
35. Se for eksempel Kimmering, Baruch & Migdal, Joel S.: *The Palestinian People: A History*. Cambridge, London: Harvard University Press
36. Siter i: Schindler, Colin: *A History of Modern Israel*. New York: Cambridge University Press, 2008, s. 153
37. Siter i: Ubayasiri, Kasun: «Virtual hostage dramas and real politics», i *Ejournalist*, vol. 4, nr. 2, s. 4.
38. Darweish, Marwan & Rigby, Andrew: *Popular Protest in Palestine: The Uncertain Future of Unarmed Resistance*. London: Pluto Press, 2015, s. 75
39. «Defacement of bitdefender.com» Zone-h, 12. oktober 2013 <http://www.zone-h.org/mirror/id/20965099> (12.12.2014)
40. Intervju med forfatteren, mr. KDMS-Team på e-post, 21. desember 2014
41. Darweish, Marwan & Rigby, Andrew: *Popular Protest in Palestine: The Uncertain Future of Unarmed Resistance*. London: Pluto Press, 2015, s. 82
42. Ibid: s. 159
43. Peteet, Julie: «The Writing on the Walls: The Graffiti of the Intifada», i *Cultural Anthropology*, vol. 11, nr. 2, s. 140
44. Fanon, Frantz: *The Wretched of the Earth*. London: Penguin Books, 2001, s. 28
45. «Islamic Jihad's cyber-war brigades» al-Madhoun, Ola, 17. juni 2008 <http://www.menassat.com/?q=en/news-articles/3966-islamic-jihad-s-cyber-war-brigades> (28.08.2015)
46. Intervju med forfatteren, Vestbredden, 16. november 2014
47. Intervju med forfatteren, Vestbredden, 16. november 2014
48. «Iran Top Backer of Palestinian Islamic Jihad» Ayyoub, Abeer, 9. januar 2013 <http://www.al-monitor.com/pulse/originals/2013/01/palestinian-islamic-jihad.html> (28.08.2015)
49. «REPORT: Jihadi Hackers Email Israel's Military 'Tel Aviv Will Be A Ball Of Fire'» Ingersoll, Geoffrey, 19. november 2012 <http://www.businessinsider.com/islamic-hackers-email-israel-military-2012-11> (14.09.2015)
50. Peteet, Julie: «The Writing on the Walls: The Graffiti of the Intifada», i *Cultural Anthropology*, vol. 11, nr. 2, s. 139
51. Deibert, Ronald J. «Black Code: Censorship, Surveillance, and the Militarization of Cyberspace», i *Millennium. Journal of International Studies*, vol. 32, nr. 3, s. 517-518
52. Allen, Patrick D. & Demchack, Chris C.: «The Palestinian-Israeli Cyberwar», i *Military Review*, vol. 83, nr. 2, s. 52