Säkerhetspolitik i informationssamhället

av Ulrik Franke

Résumé

Information and communications technology (ICT) has had a profound impact on our society. But how does ICT influence international relations, diplomacy and armed conflict? This article sheds light on this question from several perspectives. A closer look at the "Twitter revolutions" of the Arab Spring reveals ICT to be a double-edged sword: it does indeed enable new kinds of communication, but it also creates new opportunities for monitoring and censorship. Further, the article examines how Internet policy– domestic and foreign – in countries like China and Russia is fuelled by a desire for stability, but concludes that the results may be illusory. Developments in government Internet control are also investigated, and trends are identified. For instance, primitive content filtering is increasingly being replaced by competition for attention, where governments sometimes exert leverage of intelligence assets and sophisticated so-called sock puppetry on social networks. Addressing cyber war, it is argued that state actors' use of cyber-attacks differs importantly from everyday cyber-crime. In particular, on the international strategic level, the advantage of the attacker over the defender may not be as great as is often supposed. The article is concluded with some reflections about research challenges and the interplay between policy and research.

DET ÄR INGEN överdrift att säga att informations- och kommunikationstekniken har ändrat vårt samhälle i grunden. Idag använder vi internet för att arbeta, betala räkningar, umgås och roa oss på ett sätt som var otänkbart för bara tio år sedan. Det vi kallar informationssamhället är här för att stanna, men konsekvenserna för säkerhetspolitik och internationella relationer är ännu oklara. En iakttagelse som man kan göra redan idag är att teknikutvecklingen får beslutsfattare att agera – världens länder stiftar lagar, verkar diplomatiskt och ser över sina militära förmågor. Men hur påverkar informationstekniken framtidens politiska beslutsfattande, diplomati och väpnade konflikter? Här behövs mer forskning.

Användningen av sociala media under den så kallade arabiska våren har blivit något av en ikon för teknikens förmåga att påverka skeenden i samhället. Bilden av modiga aktivister som använde Twitter, Facebook och YouTube för att avslöja förtryck och mobilisera motståndet mot auktoritära regimer spred sig som en löpeld världen över. Det är emellertid en oerhört förenklad bild. Det är sant att kommunikation via internet skapar nya arenor för umgänge, där det är lättare att nå ut till många människor. Men det är också sant att dessa arenor skapar nya möjligheter för övervakning, censur och åsiktskontroll. Informationssamhällets svärd kan vara tveeggat.

Den som kan sprida ett budskap via Twitter har potential att långt snabbare nå långt fler än den som är hänvisad till dörrknackning eller ryktesspridning – och kan göra det mycket billigare än den som an-

vänder dagstidningar eller TV. På det viset kan gamla informationsmonopol utmanas. Framförallt i samhällen där censuren ligger tung över traditionella medier får nya kommunikationsarenor stor potential – så länge censuren inte utvidgas snabbt nog. Vissa har entusiastiskt framkastat hypotesen att aktivisterna sannolikt är snabbare än censorerna och tenderar att ligga steget före.[1] Andra konstaterar mer lakoniskt att modern teknik kan tjäna såväl demokrater som autokrater.[2] Det är ingen slump, menar forskare som Hussain & Howard, att despoterna i länder som Tunisien och Egypten sveptes bort, medan de satt kvar i Saudiarabien, Bahrain och Förenade Arabemiraten. De sistnämnda länderna hade investerat i mer sofistikerade system för övervakning och censur.[3]

Det finns också mer historiskt betingade skäl att ifrågasätta informations- och kommunikationsteknikens frälsarroll. När demonstranter 1919 fyllde Kairos gator var det tryckta tidningar snarare än Facebook som levererade eggande budskap.[4] Tekniken är varken en nödvändig eller en tillräcklig faktor för att sätta igång en revolution. I tryckpressens barndom var det ingen hejd på tilltron till det tryckta ordets förmåga att skapa välfungerande direktdemokrati. Den franska revolutionen föddes i en sådan intellektuell miljö – men de revolutionärer som överlevde giljotinen fick se Napoleon återinföra censuren och etablera statsmonopol på tryckpressar.[5]

Informationen lever sitt eget liv

Icke desto mindre är det tydligt att internetuppkopplingar och sociala medier kom att spela en viktig roll i det mediala ekosystemet.[6] Bilder och berättelser som spreds via internet nådde den internationella nyhetsrapporteringen och påverkade i sig händelseutvecklingen.[7] Sociala och traditionella media samspelade i en ny sorts offentlighet som bidrog till att väcka omvärldens sympatier. Facebook och Twitter gjorde inte nödvändigtvis något nytt i sak – medier och kändisar som lord Byron väckte Västeuropas solidaritet med den grekiska frigörelsen från det osmanska imperiet på 1820-talet – men fiberkommunikation är onekligen snabbare än hästdroskor och brevduvor. Tajming kan vara nog så viktig i en globaliserad värld.

Den kanske mest intressanta aspekten av den arabiska våren är därför hur händelser får sitt eget liv. Oavsett i vilken utsträckning som demonstranterna på Tahrir-torget hade lockats dit via internet så var själva ryktet om detta nog för att Mubarak skulle ta beslutet att försöka stänga ner landets uppkopplingar. Det räddade honom inte – vissa argumenterar till och med för att det påskyndade hans fall, genom att ge en enande och koordinerande signal till hela befolkningen om vem som var fienden.[8] Och oavsett vad som faktiskt orsakade Mubaraks fall så fick den ikoniska internetaktivisten sitt eget liv. Omvärlden, exempelvis amerikanska State Department och svenska UD, började lova stöd till internetaktivister i form av programvaror, pengar och utbildningar. Och oavsett vilken effekt sådana insatser i sin tur faktiskt får – eller kan tänkas komma få i framtiden – så fick bilden av ett internet flödande av subversiv information som kan välta stater över ända sitt eget liv. I september 2011 skrev Ryssland, Kina, Tadzjikistan och Uzbekistan ett brev till FN:s generalsekreterare med en uppmaning till världens alla länder om att göra gemensam sak för att förhindra spridningen av information som underminerar stabiliten i andra länder.[9] Blotta föreställningen om ”Twitter-revolutioner” får kon-

sekvenser, oavsett om vetenskapssamhället är överens om att begreppet är både överförenklat och överilat.[10]

Den illusoriska stabiliteten

Just stabiliteten – och rädslan för att den ska gå om intet – är centrala för hur ett land som Kina förhåller sig till internet. Censuren är delegerad – outsourcad, med modernt språkbruk – till tidningar, nyhetsbyråer, telekombolag och andra. Det är inte så att kritik mot systemet inte förekommer – men bara vissa sorters kritik tillåts.[11] Fokus hos censorerna är snarast att förhindra varje form av mobilisering.[12] Folk i rörelse – av vilket skäl som helst – är synbarligen mer skrämmande än folk med åsikter. Den senaste åtgärden är att förbjuda ryktesspridning på internet, under hot om upp till tre års fängelsestraff. Som rykte kan vad som helst räknas, om det vidarebefordras mer än 500 gånger.[13] Det är en ödets ironi att det välregisserade kinesiska medielandskapet, alla ansträngningar till trots, är närmast unikt i sin sårbarhet för rykten.[14] Kanske gör censorerna i själva verket stabiliteten en otjänst?

Forskarna Nassim Nicholas Taleb och Mark Blyth har hävdat att den som snabbt försöker hejda varje tecken på avvikelse – må det vara oliktänkande i diktaturer eller fluktuerande börskurser – ofta bara skapar en *illusion* av stabilitet. Under ytan bubblar osäkerheten fortfarande och förr eller senare slår den över i omvälvningar som får mycket större konsekvenser än om man hade låtit systemet ha sin gång.[15] Taleb och Blyth tillämpar resonemanget på både finanskrisen och den arabiska våren. Om de har rätt så är den kinesiska internetcensuren kontraproduktiv ur ett stabilitetsperspektiv.

Taleb och Blyth föreslår ingen särskild mekanism som minskar stabiliteten, men argumentet går att förstå intuitivt: i ett samhälle där bara utvald och noga selekterad information normalt får spridas är det svårt att förutsäga konsekvenserna av avvikande budskap.[16] När Gorbatjov tillät diskussion om bristerna i det sovjetiska systemet släppte han loss en flodvåg av kritik som till slut välte systemet över ända. Det är svårt att tänka sig något liknande i ett land som Sverige, där samhällskritik av alla möjliga sorter är en del av det normala offentliga samtalet. Kritiska böcker om kungen har ingen omstörtande potential i Sverige – men ingen kan sia om vad som skulle ske om motsvarande budskap om Kim Jong-Un skulle få spridning i Nordkorea. En observation från psykologisk forskning talar också för den tanken: ungdomar som utsätts för reklam lär sig att förhålla sig kritiskt och tar den inte för sann[17] – men reaktionen hos den som aldrig har stött på reklam är mycket mer svårförutsägbar. Så blir rädslan för rykten närmast en självuppfyllande profetia.

Att helt stoppa information är dock inte det enda som står på agendan. Forskarna Deibert och Rohozinski, som bland annat noggrant har studerat situationen i före detta Sovjetunionen, menar att den mest primitiva innehållsfiltreringen – vad de kallar första generationens internetkontroll – håller på att bli förlegad. Istället för att konsekvent ta bort oönskat innehåll satsar stater i allt högre grad på att skapa en juridisk miljö av gummiparagrafer där oönskat innehåll kan filtreras bort vid behov. Den ryska ”svartlistningslagen” från 2012 och hotet om fem miljoner rubel i böter för förtal kan exemplifiera den strategin – vars effekt till inte så liten del kan antas bestå i självcensur. Sådan andra generationens internetkontroll inrymmer dessutom möjlig-

heten att dolt sätta press på internetleverantörer eller andra att skapa tillfälliga tekniska fel som omöjliggör åtkomst till visst innehåll vid strategiskt valda tidpunkter. Sådana åtgärder är mycket svårare att detektera och leda i bevis än statiska listor på förbjudna ord och fraser.[18]

Samma subtilitet återfinns i tredje generationens internetkontroll, där statsmakten inte i första hand satsar på att blockera information – som Mubarak – utan tar upp kampen om det kommunikativa rummet. Den svenske forskaren Johan Lagerkvist har kallat den kinesiska strategin i det avseendet för *ideotainment*: den kommunistiska enpartistaten ska göras cool och hipp bland unga, med hjälp av snygga bilder och ljud i väldesignade appar. Censuren säljs in med associationer till hygien och behovet av renhållning.[19] Det är något helt annat än att stänga av internet när demonstranterna blir besvärande många på torget.

En huvudroll i tredje generationens internetkontroll kan spelas av vilseledning av olika slag. Vilseledning på internet är i sig inget nytt. Vanliga dagstidningar har skrivit om svenska företag som säljer ”likes” på Facebook till hugade spekulanter. Så kan man vässa sitt varumärke, oavsett om det är personligt eller kommersiellt. Statsaktörer kan emellertid sätta extra kraft bakom sådana ansträngningar. I både USA[20] och Ryssland[21] har grävande journalister avslöjat upphandlingar där federala myndigheter velat köpa system för att etablera och styra kvalificerade falska identiteter på sociala nätverk – så kallade strumpdockor (*sock puppets*). En enda operatör kan styra ett dussin sådana falska personas, var och en komplett med trovärdiga namn och bakgrundsuppgifter. Tekniska lösningar med så kallade virtuella privata nätverk får det att verka som om identiteten befinner sig på önskad plats i världen. Den här sortens teknik ökar räckvidden för statsaktörers möjligheter att påverka. Censur och internetfiltrering har svårt att nå utanför det egna landet. Tävlan om den digitala uppmärksamheten och falska identiteter på sociala nätverk har global räckvidd.

En föränderlig spelplan

Staters påverkansoperationer går dock inte att till fullo förstå bara genom att titta på internet. En bra begreppsmodell är DIME – en engelsk förkortning som utläses diplomati, information, militär och ekonomi. Stater har förmåga att agera i alla dessa fyra dimensioner för att påverka varandra – och det är när de kombineras på ett genomtänkt sätt som effekten blir som störst.

Den kombinationen är emellertid inte alltid så enkel. Det har påtalats att flera av de mest uppmärksammade exemplen på vad som skulle kunna kallas informationskrigföring inte har levererat önskade resultat. Om cyberattackerna på Estland 2007 var ett ryskt försök till påverkan så lyckades man i det korta perspektivet väcka mycket uppmärksamhet. Men den beryktade bronsstatyn flyttades, och Estlands strategiska västorientering påverkades inte. Om Stuxnet var ett amerikanskt eller israeliskt försök att påverka Irans kärnvapenprogram, så lyckades man skapa tekniskt huvudbry på kort sikt. Men på längre strategisk sikt är det oklart om Irans förmåga och vilja att genomföra sitt kärnvapenprogram alls påverkades.[22]

De här exemplen illustrerar att staters strategiska – ibland militära – användning av informationsoperationer och cyberattacker på avgörande punkter skiljer sig från den cyberbrottslighet som plågar det moderna samhället. Cyberbrottslighet är i huvudsak ekonomiskt driven. Därför har brottslingarna lyxen att vara opportu-

nister – de väljer de mål som verkar lättast. Internet svämmar över av datorer med sårbarheter för vilka det finns uppdateringar, men vilkas ägare inte har installerat dem.[23] Den virtuelle bankrånaren har all anledning att försöka få in en trojan på någon av dessa, istället för att ödsla tid på mer uppdaterade datorer. Även slarviga datorägare betalar sannolikt räkningarna på internet. Det är inte konstigare än att inbrottstjuven helst väljer det olarmade huset. Den statsaktör som har strategiska mål att uppnå har inte samma lyx. Målvalen begränsas av de effekter man vill uppnå och av synkroniseringen i alla fyra DIME-dimensionerna. Råkar det utsedda målet ändra på sitt beteende eller uppdatera bort en viktig sårbarhet så är man tillbaka på ruta ett.

Därför måste tvärsäkra uttalanden om att anfallaren har alla fördelar och försvararen alla nackdelar i cyberrymden nyanseras. Det är sant, som det ofta sägs, att det är nästintill omöjligt att täppa till alla säkerhetshål, såväl tekniskt som organisatoriskt, och att det gör försvararens uppgift överväldigande. Men det är också sant att den som attackerar med ett bestämt syfte i åtanke inte kan välja vilket säkerhetshål som helst – den beryktade svagaste länken – och ändå vara säker på att uppnå önskad effekt. Konfigurationen måste stämma, angreppskoden måste justeras för hand, övervakningssystem måste undvikas – och alltihop måste passa ihop med den överordnade planen. Även om IT-angrepp är lätta att genomföra för opportunister så kan de vara nog så svåra att utnyttja för en stat som vill uppnå strategiska mål.

En annan viktig insikt om den globala informationsmiljön är att den ser olika ut i olika delar av världen. I Afrika som helhet har ungefär 70 % av befolkningen tillgång till en mobiltelefon, men medan mobilbetalningar och sms med aktuella världsmarknadspriser revolutionerar tillvaron för bönder i Kenya, har bara 25 % tillgång till mobiltelefon i grannlandet Etiopien. Och med en internetpenetration på 2,5 % gör man sig en intellektuell otjänst om man okritiskt analyserar etiopisk politik med samma verktyg som rysk, kinesisk eller svensk. Radio, TV och utbredd analfabetism måste tas med i beräkningen. Etiopien har Afrikas sista stora statsmonopol på telekommunikation, och den nyligen slutna överenskommelsen med de kinesiska bolagen Huawei och ZTE om 3G- och 4G-utbyggnad kommer inte att ändra på det. Den auktoritära regimen ser monopolet som ett medel för att behålla makten.[24]

Spelplanen kan dock ändras snabbt. 2010 hade 0,6 % av befolkningen i Nigeria mobilt bredband – 2011 var de 10 %.[25] Utjämningen sker inte bara mellan världens länder utan också mellan stater och icke-statliga aktörer. Framsteg inom distribuerade beräkningar och så kallade molntjänster gör att beräknings- och lagringskapacitet som för några år sedan var förbehållen myndigheter som NSA eller FRA snart blir tillgängliga även för driftiga icke-statliga aktörer. Den mindre nogräknade behöver inte nöja sig med Amazon Web Services, utan kan stjäla beräkningskraft via så kallade botnät – världsomspännande nätverk av infekterade datorer som utan ägarnas vetskap kontrolleras av någon annan.

Spelplanens utseende avgörs också av hur världens länder väljer att se på säkerhetspolitiken i informationssamhället. Här har en del uppseendeväckande konflikter utspelats på sistone. Konfliktlinjerna mellan å ena sidan USA och EU och å den andra Ryssland och Kina blev tydliga på ITU-mötet i Dubai i slutet av 2012. De sistnämnda förordade en modell där internet skulle ställas under ITU-kontroll – vilket

de förstnämnda såg som ett sätt att utöka möjligheterna till censur och statlig styrning. I spåren av Snowden-avslöjandena under 2013 är det oklart i vilken mån den demokratiska världen förmår upprätthålla bilden av sitt moraliska övertag. Kina utmålar ofta och gärna USA som hycklare. Situationen kompliceras ytterligare av att samspelet mellan teknik, politik och juridik är så komplext.

Finns det alls förutsättningar för världens länder att enas? Forskarna Ryan, Ryan och Tikk har påpekat att man kan dra lärdomar av analogier till befintliga internationella avtal och fördrag. Alla avtal måste exempelvis inte vara fullständigt bindande – flygtrafikledning rymmer både obligatoriska och rågivande instruktioner. Inte heller måste alla problem lösas på en och samma gång – Antarktisfördraget från 1961 vare sig erkänner eller bestrider de territoriella anspråk som vissa stater har gjort. Samtidigt måste hänsyn tas till informationssamhällets unika egenskaper: Även om de så kallade routing-protokoll som styr internettrafiken är skapade av människan så är de tämligen oförutsägbara. Snarare är det som med satellitbanor – den celesta mekaniken kräver att satelliter får passera ovanför länder utan att ta hänsyn till gränser. Skulle man ställa krav på gränskontroller och explicita tillstånd att passera i ettdera fallet så skulle både rymdfarten och internet som vi känner det omöjliggöras.[26]

Karta, verklighet och beslutsfattare

Fördragen för oss åter till frågan om informationssamhällets konsekvenser för säkerhetspolitik och internationella relationer. Till del bestäms utvecklingen av framsteg på teknikområdet. Men beslutsfattares perceptioner är minst lika viktiga. Mubaraks nedstängning av internet och de rysk-kinesiska FN-initiativen om begränsningar av digitala informationsflöden speglar en föreställning om internets farliga och destabiliserande roll. Den föreställningen måste inte vara sann för att få effekt. På samma sätt spelar det roll om diplomater och statsmän ser säkerheten i informationssamhället som ett nollsummespel eller tror på *win-win*-situationer. Sådana föreställningar styrs bland annat av forskningsläget. Vilka perspektiv och metoder vi väljer för att studera säkerhetspolitik i informationssamhället spelar roll – långt utanför vetenskapssamhället.

Några frågeställningar är särskilt angelägna att undersöka noggrannare, inte minst för ett land som Sverige, där frågorna om informationstekniken länge har stått högt på den politiska och diplomatiska agendan. Hur fattas beslut i cyberkonflikter? Det finns mycket skrivet om antivirusprogram och brandväggar, men mycket mindre om mänskligt beslutsfattande. Vilka är förutsättningarna för konventioner om cybernedrustning? Det talas ibland om digital kapprustning, men ingen vet egentligen om vare sig avskräckning eller förtroendeskapande åtgärder fungerar. Hur ser krigets lagar ut i cyberkontext? Uppfattningarna går isär om förutsättningarna för distinktion, proportionalitet, attribution och så vidare. Hur kommer makten att fördelas mellan statliga och icke-statliga aktörer? Stater vill upprätthålla sin westfaliska suveränitet, men de har allt mindre inflytande på teknikutvecklingen. Hur ska politiska och militära beslutsfattare få en effektiv och ändamålsenlig lägesbild av vad som sker i cybermiljön?

Världens länder kan agera i alla DIME-dimensionerna, men samordningen är svår och ställer höga krav på både teknik och

metod. Än finns det många spännande frågor som söker sina svar.

Författaren är tekn dr, verksam vid Totalförsvarets forskningsinstitut (FOI) och major i reserven vid Högkvarteret, Insatsstaben.

Noter

1. Alqudsi-ghabra, Taghreed: "Creative use of social media in the revolutions of Tunisia, Egypt & Libya", *International Journal of Interdisciplinary Social Sciences*, vol 6 nr 6 2012, s 147–158.
2. Diamond, Larry: "Liberation technology", *Journal of Democracy*, vol 21 nr 3 2010, s 69–83.
3. Muzammil M Hussain och Philip N Howard: "Democracy's Fourth Wave? Information Technologies and the Fuzzy Causes of the Arab Spring", mars 2012. Tillgänglig via SSRN: *http://ssrn.com/abstract=2029711*.
4. Anderson, Lisa: "Demystifying the Arab spring: parsing the differences between Tunisia, Egypt, and Libya", *Foreign Affairs*, vol 90 2011, s 2–7.
5. Dartnell, Michael: "Insurgency online: Elements for a theory of anti-government internet communications", *Small Wars & Insurgencies*, vol 10 nr 3 1999, s 116–135.
6. Gonzalez-Quijano, Yves: "The Arab riots in digital transition times. Myths and Realities", *Nueva Sociedad: democracia y politica en America Latina*, 2011, s 110–121.
7. Nanabhay, Mohamed och Farmanfarmaian, Roxane: "From spectacle to spectacular: How physical space, social media and mainstream broadcast amplified the public sphere in Egypt's 'Revolution'", *The Journal of North African Studies*, vol 16 nr 4 2011, s 573–603.
8. Hassanpour, Navid: "Media disruption exacerbates revolutionary unrest: Evidence from Mubarak's natural experiment", *APSA 2011 Annual Meeting Paper*, 2011.
9. Baodong, Li; Churkin, Vitaly; Aslov, Sirodjidin och Askarov, Murad: Brev daterat den 12 september 2011 från de permanenta representanterna för Kina, Ryska federationen, Tadzjikistan och Uzbekistan till Förenta nationerna, ställt till generalsekreteraren. Generalförsamlingens diarienummer A/66/359.
10. Cottle, Simon: "Media and the Arab uprisings of 2011: Research notes", *Journalism*, vol 12 nr 5 2011, s 647–659.
11. Lagerkvist, Johan och Sundqvist, Gustav: "Loyal Dissent in the Chinese Blogosphere: Sina Weibo Discourse on the Chinese Communist Party", *Studies in Media and Communication*, vol 1 nr 1 2013, s 140-149.
12. King, Gary; Pan, Jennifer och Roberts, Molly: How censorship in China allows government criticism but silences collective expression, i *APSA 2012 Annual Meeting Paper*, 2012.
13. Reuters, "China threatens tough punishment for online rumor spreading", *http://www.reuters.com/article/2013/09/09/us-china-internet-idUSBRE9880CQ20130909*, 2013-09-09, (2013-10-18).
14. Ma, Ringo: "Spread of SARS and war-related rumors through new media in China", *Communication Quarterly*, vol 56 nr 4 2008, s 376–391.
15. Taleb, Nassim Nicholas och Blyth, Mark: "The black swan of Cairo", *Foreign Affairs*, vol 90 nr 3 2011, s 33–39.
16. Franke, Ulrik: "Disconnecting digital networks: A moral appraisal", *International Review of Information Ethics*, vol 18 2012, s 23-29.

17. Boush, David M.; Friestad, Marian och Rose, Gregory M.: "Adolescent Skepticism toward TV Advertising and Knowledge of Advertiser Tactics", *Journal of Consumer Research*, vol 21 nr 1 1994, s 165-175.
18. Deibert, Ronald och Rohozinski, Rafal. "Control and subversion in Russian cyberspace" i Deibert, Ronald; Palfrey, John; Rohozinski, Rafal och Zittrain, Jonathan (red): *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, s 15–34, MIT Press, Cambridge, MA 2010.
19. Lagerkvist, Johan: "Internet Ideotainment in the PRC: national responses to cultural globalization", *Journal of Contemporary China,* vol 17 nr 54 2008, s 121-140.
20. Fielding, Nick och Cobain, Ian: "Revealed: US spy operation that manipulates social media", *The Guardian*, 2011-03-17, *http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks*, (2013-01-18).
21. Barabanov, Ilja; Safronov, Ivan och Tjernenko, Jelena: "Razvedka botom" [Underrättelsetjänst med en bot], *Kommersant*, 2012-08-27, *http://www.kommersant.ru/doc/2009256*, (2012-11-07).
22. Iasiello, Emilio: "Cyber attack: A dull tool to shape foreign policy", *5th International Conference on Cyber Conflict (CyCon 2013)*, 2013, IEEE, s 451–468.
23. Shahzad, Muhammad; Zubair Shafiq, Muhammad och Liu, Alex X: "A large scale exploratory analysis of software vulnerability life cycles", *34th International Conference on Software Engineering (ICSE), 2012,* IEEE, s 771-781.
24. "Telecoms in Ethiopia: Out of reach", *The Economist*, 2013-08-24, s 32.
25. 'The World Telecommunication/ICT Indicators database online', International Telecommunications Union, 16 upplagan, 2012.
26. Ryan, Julie J.C.H.; Ryan, Daniel J. och Tikk, Eneken: "Cybersecurity regulation: Using analogies to develop frameworks for regulation" i Tikk, Eneken och Talihärm, Anna-Maria (red): *International Cyber Security Legal & Policy Proceedings*, Cooperative Cyber Defence Centre of Excellence (CCD COE), Tallinn 2010, s 76–99.