Regeringens insättande av Försvarsmaktens cyberförsvarsförband i fred, kris och krig

Konstitutionella förutsättningar m.m.

Av jur.lic. MAGNUS SANDBU[1]

Cyberangrepp utmanar vår traditionella uppfattning om väpnade hot — när servrar slås ut, samhällsfunktioner lamslås och angriparen förblir anonym suddas gränsen mellan fred och väpnad konflikt ut. Hoten kommer utan förvarning och utan fysiskt våld, men kan ändå slå direkt mot rikets suveränitet och motståndskraft. I denna nya säkerhetspolitiska verklighet växer kravet på att snabbt kunna sätta in militär cyberförmåga — även i fredstid. Artikeln granskar de konstitutionella ramar som styr regeringens handlingsutrymme, med särskilt fokus på den rättsliga gråzon som hybridkrigföring och cyberangrepp kan medföra.

1 Inledning

Försvarsmaktens huvuduppgift är att försvara Sverige och allierade stater mot ett väpnat angrepp med utgångspunkt i det kollektiva försvaret inom Nato.[2] Försvarsmakten ska även hävda Sveriges territoriella integritet och kunna bidra till att hävda allierade staters territoriella integritet.[3] Uppgifterna får antas avse såväl land-, sjö- och luftterritorium, som cyberrymd.

Med svensk cyberrymd avses den virtuella rymd som uppstår vid användning av digital teknik som är fysiskt placerad inom svenskt territorium eller i övrigt faller in under svensk exklusiv jurisdiktion, exempelvis digital teknik på svenska ambassader och konsulat.

Denna artikel avser att belysa regeringens möjlighet att sätta in Försvarsmaktens cyberförsvarsförband vid cyberangrepp riktade mot svensk cyberrymd.

1.1 Det militära cyberförsvaret och cyberoperationer

Det militära cyberförsvaret omfattar den verksamhet som krävs för att i samtliga konfliktnivåer bl.a. kunna:[4]

- Avskräcka och förneka en motståndare att i eller genom cyberdomänen påverka det militära försvarets förmåga att mobilisera, möta ett väpnat angrepp, upprätthålla territoriell integritet…,

[1] Författaren är jur.lic. och har tidigare varit chef för Försvarsmaktens operativjuridiska sektion.
[2] 1 §, förordningen (2024:1333) med instruktion för Försvarsmakten.
[3] Ibid, 3 § andra stycket.
[4] Försvarsmaktens doktrinansats cyberförsvar kap. 2.1.

- förstärka skyddet av kritiska samhällsfunktioner som utgör beroenden för det militära försvaret,
- genom åtgärder i cyberdomänen bidra till att totalförsvaret som helhet är krigsavhållande,
- upptäcka och möta ett väpnat angrepp i eller genom cyberdomänen och
- genom offensiva cyberoperationer, enskilt eller tillsammans med andra, påverka en motståndares verksamhet i samtliga domäner.

Försvarsmakten är den myndighet som ska verka inom alla delar av dator- och nätverksoperationer samt vara dimensionerat mot de högre konfliktnivåerna.

Cyberoperationer delas in i defensiva cyberoperationer (DCO) och offensiva cyberoperationer (OCO).

Defensiva operationer kan genomföras både i Försvarsmaktens egna system och i system utanför myndigheten, samt delas in i fyra primära verksamheter; a) *sensoranalys* (SA), vilket innebär att loggar och larm för system eller sensorer korreleras och analyseras för att upptäcka antagonistisk verksamhet, b) *uppsökande verksamhet* (UV), vilket syftar till att upptäcka och hantera antagonistisk verksamhet i system där en antagonist kan ha tagit sig förbi en eller flera säkerhetsfunktioner utan att ha detekterats, c) *motåtgärder* (MÅ), vilket syftar till att förhindra, påverka eller avbryta en motståndares verksamhet i eller mot system och d) *incidenthantering* (IH), vilket syftar till att återställa tillförlitlig funktionalitet och utreda händelsekedjor i system efter att en händelse påverkat eller bedöms ha påverkat systemets tillgänglighet eller riktighet när händelsen bedöms ha antagonistiskt ursprung. I korthet innebär defensiva operationer att Försvarsmakten ska kunna övervaka skyddsvärda nätverk och digitala system, identifiera intrång, avbryta skadlig aktivitet samt återställa sådana nätverk och system. Övervakningen består främst i att nätverkens in- och utgående trafik övervakas, liksom trafiken i och mellan de digitala systemen inom nätverken.

I sammanhanget bör det uppmärksammas att defensiva operationer inte riktar sig mot den person som utför ett cyberangrepp, utan mot skadliga koder, överbelastningsattacker och intrångsförsök i de digitala system som hotas eller angrips.

Offensiva operationer delas upp i två kategorier; a) *cyberexploatering,* innebärandes inhämtning och andra förberedelser i cyberdomänen till stöd för underrättelseinhämtning och planering av cyberattacker samt b) c*yberattack,* innebärandes planerade aktiviteter som leder till önskade effekter. Effekterna syftar till att aktivt påverka motståndarens vilja och krigföringsförmåga.[5]

2 Regeringsformens betydelse vid cyberförsvar

Försvarsmakten är en statlig myndighet som lyder under regeringen. Regeringen kan därför disponera över Försvarsmakten i likhet med

[5] Ibid, kap. 4.1

andra statliga förvaltningsmyndigheter, med undantag för de begränsningar som följer av regeringsformen. Sådana begränsningar finns i 15 kap. RF.

Regeringens möjlighet att sätta in Försvarsmakten regleras bl.a. av regeringsformens 15 kap. 13 § (rikets försvar) och 16 § (insättande av väpnade styrkor). Bestämmelserna behandlar kompetensfördelningen mellan riksdag och regering när det gäller frågor som har att göra med rikets försvar och insättande av svenska väpnade styrkor i övrigt. De militära myndigheternas uppgifter och befogenheter regleras däremot inte i regeringsformen.[6]

2.1 15 kap. 13 § RF

En grundtanke i regeringsformen är att regeringen måste kunna disponera över Sveriges försvarsmakt till skydd för riket, samt att ett angrepp mot Sverige kan komma snabbt och överraskande och att insättandet av rikets försvarsmakt vid ett angrepp därför inte medger att frågan avvaktar riksdagens prövning.[7] Denna grundtanke gäller såväl vid ett väpnat angrepp mot riket som när främmande makt kränker svenskt territorium utan att ett väpnat angrepp föreligger. Regleringen innebär att grundlagen anger förutsättningarna för när regeringen på detta speciella område kan agera utan att ha stöd i lag och utan att först ha inhämtat riksdagens medgivande.[8]

15 kap. 13 § RF, inklusive rubrik, lyder:

> Rikets försvar
> 13 § Regeringen får sätta in rikets försvarsmakt i enlighet med internationell rätt för att möta ett väpnat angrepp mot riket eller för att hindra en kränkning av rikets territorium.
>
> Regeringen får uppdra åt försvarsmakten att använda våld i enlighet med internationell rätt för att hindra kränkning av rikets territorium i fred eller under krig mellan främmande stater.

2.1.1 Regeringens rätt att sätta in försvarsmakten

15 kap. 13 § första stycket RF anger när regeringen, utan riksdagens medverkan, får sätta in rikets försvarsmakt. Med försvarsmakten (med litet f) avses verksamheten att försvara riket. Uttrycket innefattar Försvarsmakten och andra försvarsmyndigheter som deltar i det väpnade försvaret av landet.[9] Bestämmelsen avser två typsituationer; a) insättande för att möta *ett väpnat angrepp mot riket*, och b) insättande i fredstid för att hindra *en kränkning av rikets territorium*.

Inledningsvis ska här behandlas regeringens möjlighet till insättande för att möta ett väpnat angrepp mot riket.

Med ”väpnat angrepp” åsyftas ett sådant väpnat angrepp som avses i

[6] SOU 2008:125, s. 508.
[7] Prop. 1973:90, s. 373.
[8] Infra not 6, 508.
[9] Se bl.a. prop. 1993/94:33. Se även supra not 17, s. 89.

FN-stadgans artikel 51,[10] och som ger en angripen stat rätt till individuellt och kollektivt självförsvar.[11]

Vad som utgör ett väpnat angrepp är inte definierat vare sig i svensk lag eller FN-stadgan. Det är regeringens sak att bedöma när ett fientligt angrepp nått sådan intensitet eller aktualitet att ett väpnat angrepp föreligger. Det anses också vara regeringens sak att under parlamentariskt ansvar ta ställning till angreppets karaktär och bestämma försvarsinsatsernas omfattning, samt tid och plats för dessa.[12]

I regeringsformens tidigare lydelse (10 kap. 9 § RF) tydliggjordes att regeringen fick sätta in rikets försvarsmakt eller del därav i strid för att möta ett väpnat angrepp mot riket.[13] I dess nya lydelse (15 kap. 13 § första stycket RF) togs uttrycket ”i strid” bort för att tydliggöra att andra medel än strid står till Försvarsmaktens förfogande.[14] I sin nuvarande lydelse och andemening får bestämmelsen anses avse insättande av försvarsmakten för såväl strid som andra former av militär vålds- och tvångsanvändning (militär maktutövning) som är nödvändig för rikets försvar. Cyberoperationer, såväl defensiva som offensiva, är exempel på medel för militär maktutövning.

Enligt regeringen kan ett cyberangrepp i vissa fall vara att betrakta som ett väpnat angrepp i FN-stadgans mening.[15] I sammanhanget bör det även noteras att regeringen anser att en rätt till självförsvar inte bara föreligger vid väpnade angrepp från stater, utan även vid terroristangrepp som är så storskaligt att det enligt artikel 51 i FN-stadgan är att betrakta som ett väpnat angrepp mot landet.[16] Som exempel bör kunna nämnas storskaliga cybersäkerhetsincidenter enligt NIS 2-direktivet, om angreppet samtidigt betraktas som terroristbrott enligt terroristbrottslagen (2022:666). Självförsvarsåtgärder kan då riktas mot stater som upplåtit sitt territorium till eller i övrigt stödjer terroristerna på ett sätt som gör att angreppet kan hänföras till staten ifråga.[17]

Ett cyberangrepp som är så pass storskaligt att det är jämförbart med ett konventionellt väpnat angrepp torde därför kunna betraktas som ett väpnat angrepp i regeringsformens mening, vare sig cyberangreppet utförs av statliga eller statsunderstödda aktörer, eller terrorister och andra icke-statliga aktörer.

Det bör dock noteras att 15 kap. 13 § första stycket RF inte medger att regeringen i förväg uppdrar till försvarsmakten att möta ett väpnat angrepp, vilket följer av att det är regeringen som under parlamentariskt ansvar ska fastställa om ett väpnat angrepp föreligger. Försvarsmaktens huvuduppgift att försvara Sverige och allierade stater mot ett

[10] Infra not 7, s. 373; supra not 14, s. 205 och 300.
[11] Jfr art. 2 (4) och art. 51, FN-stadgan.
[12] Infra not 7, s. 373; supra not 24, s. 189. Se även Erik Holmberg m.fl., *Grundlagarna*, Uppl 3:1, Norstedts Juridik AB, (2012), Stockholm, s. 637.
[13] Se tidigare lydelse av 10 kap. 9 § första stycket, regeringsformen.
[14] Prop. 2009/10:80, s. 300.
[15] Prop. 2020/21:30, s. 63, 151–152.
[16] Supra not 50, 11. Se även Ds 2022:24, s. 24.
[17] SOU 2016:64, s. 51.

väpnat angrepp är sålunda beroende av ett särskilt regeringsbeslut om insättande, oaktat vad som anges i 1 § förordningen (2024:1333) med instruktion för Försvarsmakten.

Nedan behandlas regeringens möjlighet till insättande för att hindra en kränkning av rikets territorium

Bestämmelsen om regeringens rätt att sätta in försvarsmakten för att hindra kränkningar av rikets territorium infördes i regeringsformen vid grundlagsreformen (2010), och medför ett uttryckligt stöd för regeringen att genom beslut i ett enskilt fall sätta in försvarsmakten för hävdande av Sveriges territorium.

Regeringens rättsliga förutsättningar att ”sätta in” försvarsmakten för att hindra en kränkning av rikets territorium är i princip desamma som förutsättningarna för regeringen att enligt 15 kap. 13 § andra stycket RF ”uppdra” åt försvarsmakten att använda våld i enlighet med internationell rätt för att hindra kränkning av rikets territorium i fred eller under krig mellan främmande stater, och kommenteras inte ytterligare här.

2.1.2 Fredstida uppdrag till försvarsmakten

Enligt 15 kap. 13 § andra stycket RF får regeringen uppdra åt försvarsmakten att använda våld i enlighet med internationell rätt för att hindra kränkning av rikets territorium i fred eller under krig mellan främmande stater. Bestämmelsen är en del av regeringens behörighet att nyttja försvarsmakten för ”rikets försvar”, även om bestämmelsen avser fredstida insatser.[18]

Bakgrunden till bestämmelsen är att ett väpnat angrepp mot riket kan föregås av eller inledas genom åtgärder som i ett första skede framstår som begränsade suveränitetskränkningar. Sådana begränsade suveränitetskränkningar, såväl i fred som under neutralitet, måste kunna mötas av försvarsmakten också när det inte är möjligt att invänta regeringens prövning av situationen. Regeringen kan därför, med stöd av regeringsformen, på förhand ”uppdra” till försvarsmakten att ingripa för att hindra kränkningar av territoriet.[19] Sådant uppdrag har också givits Försvarsmakten genom förordning (1982:756) om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet, m.m. (IKFN-förordning).

Grunden till bestämmelsen 15 kap. 13 § andra stycket RF lades i författningsutredningens betänkande (1963),[20] som ansåg att regeringen bör kunna ”bemyndiga krigsmakten att, i den utsträckning som internationell rätt och sedvänja medger, använda våld till värnande av neutraliteten”.[21] Den föreslagna texten ansågs dock vara för snäv.

[18] Se rubriken till 15 kap. 13 § regeringsformen.
[19] SOU 1963:17, s 478, infra not 6, s. 509–510, infra not 7, s. 371 och infra not 14, s. 300.
[20] Författningsutredningen, VI, Sveriges statsskick, del 2. Motiv, Förslag till regeringsform (1963), publicerad i SOU 1963:17.
[21] SOU 1963:17, s. 478.

Överbefälhavaren påpekade även att skrivningen inte motsvarade den då rådande ordningen enligt vilken försvarsmakten under vissa förhållanden redan ägde rätt att bruka våld under allmänt fredstillstånd,[22] se bl.a. 1967 års instruktion för krigsmakten vid hävdande av rikets oberoende under allmänt fredstillstånd samt under krig mellan främmande makter varunder Sverige är neutralt (IKFN).[23] Grundlagsberedningen (1966–1972) ansåg därför att regeringen skulle äga en uttrycklig rätt enligt regeringsformen att bemyndiga försvarsmakten att hävda rikets territorium såväl i fred som under neutralitet.[24]

Vad som utgör en kränkning av rikets territorium definieras inte av regeringsformen. Att hävda statens territorium och att värna landets neutralitet innefattar emellertid såväl ett skyddande av Sveriges geografiska gränser och fysiska sammansättning (*territoriell integritet*) som ett hävdande av Sveriges oberoende och självbestämmande, inklusive landets frihet att råda över sitt territorium och den verksamhet som ska få bedrivas där (*territoriell suveränitet*). Åtgärder som innebär kränkningar av Sveriges territoriella integritet och territoriella suveränitet är *suveränitetskränkningar*. Cyberangrepp, oavsett storlek och omfattning, som inom den svenska cyberrymden utgör kränkningar av svensk ”territoriell integritet” eller landets ”territoriella suveränitet”, kan därför anses falla in under lokutionen ”hindra kränkning av rikets territorium” i 15 kap. 13 § första och andra stycket RF.

De förhållanden som anges i förarbetena till 15 kap. 13 § andra stycket RF är i allt väsentligt kopplade till utländsk militär som begår våldshandlingar eller andra fysiska intrång på svenskt territorium. Att förarbetena (1963 och 1972) fokuserar på sådana militära handlingar ska ses i ljuset av de medel som stater förfogade över på 1960- och 1970-talen, och som förekom vid kränkningar andra staters territoriella överhöghet (suveränitet). Sedan 2000-talet utmanas staternas territoriella överhöghet inte bara av konventionella militära maktmedel, utan i allt ökande grad av obemannade vapensystem och cyberrelaterade intrång utförda av stater och statsunderstödda aktörer.

I likhet med vad som gäller vid insättande av försvarsmakten vid ett väpnat angrepp mot riket ankommer det på regeringen att under parlamentariskt ansvar även bedöma vilka handlingar som ska anses utgöra kränkningar av svenskt territorium, samt när försvarsmakten i sådana situationer bör sättas in till rikets försvar, liksom vilka insatser som ska vidtas m.m.[25]

Det kan i sammanhanget noteras att 15 kap. 13 § RF enligt sin ordalydelse inte tar sikte på vem som kränker svenskt territorium. Det centrala för bestämmelsen är att suveränitetskränkningar måste kunna bemötas och motåtgärder vidtas,[26] oberoende av vilken aktör som ligger

[22] SOU1965:34, s. 76.
[23] Generalordern d. 24 jan. 1967 nr 48/1967.
[24] SOU 1972:15, s. 28 och 189.
[25] Se bl.a. ibid, s. 189.
[26] Jfr SOU 2008:15, s. 509.

bakom kränkningen. Fokuset på att suveränitetskränkningar måste kunna bemötas i fredstid torde vara särskilt viktigt i samband med hybridhot, icke-linjär krigföring och antagonistiska cyberangrepp.[27]

Med hänsyn till att suveränitetskränkningar i form av väpnade angrepp kan utföras av såväl statliga som statsunderstödda aktörer, och terrorister,[28] torde regeringen med stöd av bestämmelsen även kunna uppdra till försvarsmakten att till rikets försvar ingripa mot sådana cyberangrepp som utgör begränsade suveränitetskränkningar emanerande från såväl statliga och statsunderstödda aktörer som terrorister och andra icke-statliga aktörer, även om angreppen inte är så pass storskaliga att de är jämförbara med ett konventionellt väpnat angrepp.

Regeringen har därför möjlighet, enligt 15 kap. 13 § andra stycket RF, att sätta in Försvarsmakten i fredstid för att möta, hindra och avbryta cyberincidenter som regeringen bedömer hotar den svenska ”territoriella integriteten” på cyberarenan eller som i övrigt utgör hot mot svensk ”territoriell suveränitet” (suveränitetskränkningar), oberoende av om angriparen är en statsaktör, statsunderstödd aktör eller annan antagonistisk aktör.

Insättande av försvarsmakten mot cyberangrepp, som inte bedöms utgöra begränsade suveränitetskränkningar eller väpnade angrepp, kan dock förutsätta riksdagens medgivande, se 15 kap. 16 § RF, se vidare nedan.

2.2 15 kap. 16 § RF

Bestämmelsen i 15 kap. 16 § RF infördes 2010.[29] Paragrafen motsvarar i allt väsentligt den tidigare bestämmelsen i 10 kap. 9 § första stycket andra meningen i 1974 års lydelse av regeringsformen,[30] med det undantaget att den tidigare bestämmelsen avsåg ”insättande i strid eller sändas till annat land”. Genom att uttrycket ”i strid” tagits bort innefattas även andra medel än strid,[31] exempelvis cyberoperationer. Bestämmelsen präglas av en strävan att ge riksdagen största möjliga inflytande över regeringens möjlighet att sätta in svenska väpnade styrkor för andra ändamål än rikets försvar.[32]

15 kap. 16 § RF, inklusive rubrik, lyder:

> Insättande av väpnade styrkor
> 16 § Regeringen får sända svenska väpnade styrkor till andra länder eller i övrigt sätta in sådana styrkor för att fullgöra en internationell förpliktelse som har godkänts av riksdagen.
>
> Svenska väpnade styrkor får i övrigt sändas till andra länder eller sättas in om
> 1. det är medgett i lag som anger förutsättningarna för åtgärden, eller

[27] Jfr infra not 15, s. 61 ff.
[28] Jfr bl.a. ibid, s. 63, 151–152, supra not 50, 11.
[29] Infra not 14, s. 301.
[30] Ibid.
[31] Ibid, s. 300.
[32] Infra not 7, s. 375.

2. riksdagen medger det i ett särskilt fall.

Bestämmelsen avser regeringens möjlighet att såväl ”sända” väpnade styrkor utomlands som regeringens möjlighet att ”sätta in” svenska väpnade styrkor i andra situationer än för rikets försvar.

Intresset för 15 kap. 16 § RF i denna artikel är begränsat till regeringens möjlighet att sätta in svenska väpnade styrkor enligt andra stycket ”för att agera och verka inom svenskt territorium”. Bestämmelsen har relevans i den utsträckning Försvarsmaktens cyberförsvarsförband sätts in vid cyberangrepp som inte utgör suveränitetskränkningar eller väpnat angrepp, och som därför inte omfattas av bestämmelsen i 15 kap. 13 § RF.

2.2.1 Konstitutionella krav vid icke-försvarsinsatser

När svensk militär ska sättas in i andra syften än att försvara Sverige, är det inte längre rikets ”försvarsmakt”, med den distinkta uppgiften att försvara Sverige, som tas i anspråk utan fokus ligger snarare på kapaciteteten att använda vapenmakt i annat militärt syfte.[33] 15 kap. 16 § andra stycket RF innebär att riksdagens medgivande erfordras om insättandet avser andra situationer än rikets försvar, exempelvis för att ingripa mot ren cyberbrottslighet. För att regeringen ska få sätta in väpnade styrkor i sådana situationer krävs enligt bestämmelsen att insättandet är medgivet i lag som anger förutsättningarna för åtgärden eller att riksdagen för ett särskilt fall medgivit åtgärden.

Enligt 1974 års lydelse krävdes riksdagens medverkan om en svensk väpnad styrka sattes in ”i strid” eller sändes till annat land för andra ändamål än rikets försvar. Efter grundlagsöversynen 2010 — och borttagandet av begränsningen till ”strid” — kan det dock finnas skäl att anta att militära enheter som ges uppdrag att använda andra former av våld- eller tvångsmedel än strid också kan komma att betraktas som en väpnad styrka i regeringsformens mening.[34]

Cyberförsvarsförband kan utgöra ”väpnade styrkor” i regeringsformens mening, särskilt när de ingår i och verkar som en del av de svenska stridskrafterna. Av bestämmelsen följer att dessa förband — om de anses utgör väpnade styrkor — inte får sättas in mot brottsliga cyberangrepp utan riksdagens medverkan enligt 15 kap. 16 § RF, såvida inte angreppen samtidigt bedöms utgöra suveränitetskränkningar.

Det kan dock ifrågasättas om cyberförsvarsförband som sätts in för att verka mot cyberangrepp utgör väpnade styrkor i regeringsformens mening. Det bör uppmärksammas att bestämmelsen i 15 kap. 16 § andra stycket RF inte avser att per automatik träffa alla militära förband och enheter som tillhör Försvarsmakten. Bestämmelsen har historiskt endast avsett de enheter som anses utgör ”svenska väpnade styrkor” i

[33] Infra not 17, s. 106.
[34] Jfr författningskommentaren som uppger att ändringarna mot tidigare lydelse endast är språkliga eller redaktionella, se prop. 2009/10:80, s. 301.

regeringsformens mening.[35]

Vad som enligt regeringsformen ska anses utgöra ”svenska väpnade styrkor” är inte klart fastlagt, utan är föremål för regeringens bedömning i det enskilda fallet.[36] Vikt har traditionellt lagts vid att styrkan är utrustad på sådant sätt att den anses som ”väpnad trupp” och att insättandet avser insättande i ”väpnad tjänst”.[37] Vid bedömningen av om en militär enhet är en väpnad styrka i regeringsformens mening har regeringen (2014) bl.a. utgått från att styrkan organiserats och utrustats för att kunna hantera situationer som går utöver självförsvar av den egna personen, exempelvis för att skydda annan person eller egendom.[38] Vad som här har avsetts är att den enhet som sätts in har en sådan militär förmåga att den med vapenmakt (jfr tidigare lydelse: strid) kan slå tillbaka mot en angripare.[39] Enligt regeringen (2019) anses en väpnad styrka i regeringsformens mening föreligga bl.a.[40]

> […] när den insatta militära personalen är utrustad och organiserad på ett sätt som innebär att den som en enhet har kapacitet att utföra väpnad strid, och detta även om styrkan inte har något mandat att använda vapenmakt utöver i självförsvar. Som utgångspunkt rör det sig därmed om en väpnad styrka när svensk militär personal — t.ex. beväpnade förband, bestyckade och bemannade örlogsfartyg, militära luftfartyg eller fordon, eller vapensystem med den personal som krävs för att hantera det — sätts in.

Enheter med militär personal som är utrustade med vapen endast för personligt självförsvar har tidigare inte ansetts vara en väpnad styrka i regeringsformens mening.[41] Som utgångspunkt är det numera inte heller en väpnad styrka om insättandet består av enskilda militärer, t.ex. militära experter eller stabsofficerare, som inte har stridsuppgifter och endast är beväpnade för personligt självförsvar.[42] Tillämpligheten av 15 kap. 16 § RF torde därför alltjämt vara baserad på att termen ”väpnad styrka” är kopplad till styrkans ”kapacitet att utföra väpnad strid”.

Det kan mot bakgrund härav ifrågasättas om ett insättande av cyberförsvarsförband alltid kan sägas utgöra ett insättande av en väpnad styrka i regeringsformens mening, exempelvis då dessa förband inte nyttjar sig av skjutvapen eller andra konventionella militära maktmedel för strid för att lösa sin uppgift, och särskilt om förbanden endast verkar genom att övervaka nätverk och digitala system, identifiera intrång, avbryta skadlig aktivitet i eller mot nätverk och digitala system samt återställa angripna nätverk och system (*defensivt cyberförsvar*), se ovan avsitt 1.1. Offensiva cyberoperationer i form av cyberexploatering är

[35] Ds 1999:2, s. 118.
[36] Se bl.a. prop. 2019/20:110, s. 23.
[37] Prop. 1992/93:77, s. 7–8.
[38] Prop. 2014/15:104, s. 9.
[39] Jfr infra not 14, s. 300. Se även infra not 17, s. 87.
[40] Prop. 2019/20:110, s. 23–24.
[41] Regeringsbeslut Fo91/50/6, 1991-01-10, Svenskt deltagande med fältsjukhus i Saudiarabien och 1990/91:KU30.
[42] Infra not 40, s. 24.

främst att jämföra med underrättelseverksamhet, vilken normalt inte kräver riksdagens medverkan.[43] Endast cyberattacker som syftar till att påverka motståndarens nätverk och digitala system torde kräva riksdagens medverkan enligt 15 kap. 16 § RF, om förbanden insätts mot cyberbrottslighet utan samband med en suveränitetskränkning.

Det bör i sammanhanget dock uppmärksammas att det sedan länge (1932) är en grundsats i Sverige att militärt tvång eller våld inte ska brukas mot den egna befolkningen eller andra civila,[44] även om en formell möjlighet att använda militär personal i polisiära ingripandesituationer fanns författningsreglerad fram till år 1969.[45] Enligt grundsatsen ska militär personal inte ges uppgifter som — utanför det traditionella militära verksamhetsområdet — tillåter utövande av våld eller tvång mot enskilda.[46] Statsmakternas syn på att väpnad trupp inte ska få sättas in mot den egna befolkningen eller andra civila har främst kommit till uttryck genom uttalanden som inte är rättsligt bindande, men som sedan lång tid har omfattats med så utbredd enighet att de ändå i stor utsträckning uppfattas som styrande.[47] Denna grundsats kommer också till uttryck i 7 § förordningen (2002:375) om Försvarsmaktens stöd till civil verksamhet, som anger att Försvarsmaktens personal inte får användas i situationer där det finns risk för att den kan komma att bruka tvång eller våld mot enskilda.

Grundsatsen har dock kommit att stå tillbaka i vissa situationer av särskilt allvarlig brottslighet (terroristbrott),[48] bl.a. vid införandet av lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning. Lagen anger uttryckligen att Försvarsmakten under vissa förutsättningar får lämna stöd till Polismyndigheten och Säkerhetspolisen vid terrorismbekämpning ”i form av insatser som kan innebära användning av våld eller tvång mot enskilda.”[49] I samband med införandet av lagen uttalade regeringen dock att det finns anledning att även fortsättningsvis vara restriktiv med användandet av Försvarsmakten vid polisiära ingripanden. Utgångspunkten bör alltså, liksom tidigare, vara att Försvarsmakten inte utför uppgifter som innebär användande av våld eller tvång mot den egna befolkningen,[50] om än med vissa restriktiva undantag.[51]

Det kan dock ifrågasättas om insättande av defensiva cyberförsvarsoperationer kan anses ha kapacitet att utföra väpnad strid eller utgör ett utövande av militär eller polisiär vålds- eller tvångsmakt mot befolk-

[43] Prop. 2006/07:63, s. 32. Se även SOU 1999:37, s. 204 f. Se dock även supra not 107, s. 32 f.
[44] Prop. 1995/96:12, s. 51. Se även prop. 1969:12, s. 4, och supra not 47, s. 59–64 och 129.
[45] Se prop. 1969:12.
[46] Prop. 1995/96:12, s. 51.
[47] SOU 2001:98, s. 129.
[48] Se 2–5 §§, lagen (2003:148) om straff för terroristbrott.
[49] 1 §, lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning.
[50] Prop. 2005/06:111, s. 17.
[51] Se även Justitieutskottets betänkande 2005/06:JuU17, s. 4 och 6 ff.

ningen eller enskilda (jfr ovan 1.1). Det finns skäl att anta att ett insättande av cyberförsvarsförband för defensiva cyberoperationer, dvs. för att övervaka skyddsvärda nätverk och digitala system, identifiera intrång, avbryta skadlig aktivitet samt återställa sådana nätverk och system, inte träffas av vare sig 15 kap. 16 § RF eller grundsatsen att militärt tvång eller våld inte ska brukas mot den egna befolkningen eller andra civila. Det följer av att defensiva operationer inte riktar sig mot den person som utför ett cyberangrepp, utan mot skadliga koder, överbelastningsattacker och intrångsförsök i de digitala system som hotas eller angrips. Bestämmelsen kommenteras därför inte ytterligare i denna artikel.

3 Vad innebär hänvisningen till internationell rätt i 15 kap. 13 § RF

Av 15 kap. 13 § RF framgår att insättandet av försvarsmakten, liksom försvarsmaktens våldsanvändning, vid rikets försvar ska ske i enlighet med internationell rätt. Bestämmelsen väcker dock frågor om vilka åtgärder som ska stå i överensstämmelse med internationell rätt, liksom vilken internationell rätt som avses.

3.1 Vilka åtgärder ska vara i enlighet med internationell rätt?

Vilka åtgärder vid rikets försvar som träffas av bestämmelsen i 15 kap. 13 § RF är oklart. Förutsättningen för regeringens möjlighet att sätta in försvarsmakten är dock att regeringen anser att såväl insättandet av försvarsmakten som försvarsmaktens våldsanvändning kommer att stå i överensstämmelse med internationell rätt, oavsett vilka uppgifter och befogenheter Försvarsmakten sedermera tilldelas.

De åtgärder som träffas av 15 kap. 13 § RF är inte alla de åtgärder som regeringen kan anse sig behöva vidta vid insättande av försvarsmakten i samband med ett väpnat angrepp på riket, eller för att hävda svenskt territorium i fred, utan är begränsat till sådana åtgärder som innefattar våld eller tvång mot motståndaren (*strid och annan våldsanvändning*).

Utanför tillämpningsområdet för 15 kap. 13 § RF faller sålunda beredskapsåtgärder som regeringen anser som nödvändiga för krigsansträngningarna i övrigt, exempelvis för förfogande av egendom eller för andra ändamål som bl.a. regleras av beredskapslagstiftningen.[52] Det samma gäller krigsadministrationens och krigsförvaltningens behov. Inte heller omfattar bestämmelsen politiska, diplomatiska och rättsliga åtgärder som vidtas i samband med krigföring eller vid ingripande mot suveränitetskränkningar i fredstid, exempelvis polisiära och rättsliga förfaranden.

I allt väsentligt är det således bara stridshandlingar och annan våldsanvändning (*militär maktutövning*) som utövas för rikets försvar som träffas av bestämmelsen i 15 kap. 13 § RF och som enligt bestämmelsen ska stå i överensstämmelse med internationell rätt.

[52] Se bl.a. 13 § förordningen (2015:1053) om totalförsvar och höjd beredskap.

3.2 Vilken internationell rätt avses i 15 kap. 13 § regeringsformen?

Huvudregeln är att domstolar och myndigheter, inklusive Försvarsmakten, ska iaktta och tillämpa den svenska rättsordningen sådan som denna framgår ur grundlagar samt andra lagar, förordningar, föreskrifter och andra rättsregler,[53] exempelvis EU-regler och svensk sedvanerätt.

Av 15 kap. 13 § RF följer dock att även internationell rätt ska iakttas vid rikets försvar. Internationell rätt utgör normalt inte en del av den svenska nationella rättsordningen, och internationella traktat måste därför införlivas i svensk rätt för att äga internrättslig giltighet.[54] Detta innebär att en traktat som Sverige tillträtt inte per automatik blir gällande internrättsligt, även om traktaten är rättsligt bindande för Sverige som nation. Domstolar och andra myndigheter, inklusive Försvarsmakten, kan därför inte direkt tillämpa traktatsbestämmelser såvida dessa inte tagits in i svensk författning. Den omständigheten att Sverige som stat har ratificerat en traktat, och gentemot andra fördragsslutande parter har åtagit sig att följa denna, medför emellertid att den svenska lagstiftaren har en skyldighet att se till att den interna svenska rätten stämmer överens med de internationella åtagandena.[55]

Det svenska förhållningssätt till folkrättsliga reglers tillämplighet i den nationella rättsordningen brukar benämnas *dualism*,[56] och innebär att folkrättsliga traktat normalt måste införlivas i svensk rätt genom en lagstiftningsakt varigenom det klargörs att ett visst traktat ska gälla som lag i Sverige (*inkorporering*) eller att traktatförpliktelserna inarbetas i befintlig eller i en särskild lagstiftning (*transformering*). En tredje metod innebär att riksdagen, i samband med att den lämnar sitt godkännande till att en traktat ratificeras, konstaterar att nationell rätt redan står i överenstämmelse med traktatförpliktelserna (*konstaterandet av normharmoni*). Vid denna typ av införlivning måste domstolar och myndigheter så lång möjligt eftersträvar en tolkning av befintliga nationella rättsregler så att dessa kommer att tolkas lojalt mot traktaten och dess anda, och så att svensk rätt därmed inte kommer i konflikt med traktatens bestämmelser (*fördragskonform tolkning*).[57]

I detta avseende medför de referenser till ”internationell rätt” som infördes i 15 kap. 13 § RF vid grundlagsöversynen 2010 vissa frågetecken, bl.a. med avseende på vilken internationell rätt som avses och om denna internationella rätt har införlivats i svensk rätt.

Själva grundlagstexten i 15 kap. 13 § RF anger att regeringen ”får sätta in rikets försvarsmakt i enlighet med internationell rätt” liksom ”får uppdra åt försvarsmakten att använda våld i enlighet med internationell rätt”. Vilken internationell rätt som avses framgår inte av ordalydelsen i bestämmelsen, men en viss indikation ges genom att

[53] Jfr infra not 7, s. 228.
[54] Prop. 1993/94:117, s. 32. Se även Ds 2007:5, s. 11 och Ds 2019:23, s. 58 ff.
[55] Prop. 2017/18:186, s. 60.
[56] Ehrenkrona, Carl Henrik, SvJT 2015 s. 781.
[57] Ds 2019:23, s. 61. Se även ibid, s. 781–782.

regeringens befogenhet i detta avseende är begränsat till att sätta in försvarsmakten för ”att möta väpnat angrepp” och ”hindra kränkning av rikets territorium”, dvs. *militär maktutövning*. Av författningskommentaren framgår att referensen till internationell rätt innebär att ”regleringen [om rikets försvar] knyts närmare till FN-stadgan och folkrätten. Därigenom begränsas möjligheten till våldsanvändning så att den alltid måste vara förenlig med folkrättens regler”.[58]

Den internationella rätt som berörs av 15 kap. 13 § RF torde därmed vara de internationella regler och regelsystem som syftar till att reglera statlig våldsanvändning såväl i fred, som kris och krig. Främst avses FN-stadgans bestämmelser om våldsförbud (art. 2 [4]) och rätten till individuellt och kollektivt självförsvar (art. 51), men även den internationella humanitära rättens och neutralitetsrättens bestämmelser (krigets lagar) samt bestämmelser om mänskliga rättigheter.

FN-stadgans regler om våldsanvändning och självförsvar har införlivats i svensk rätt genom konstaterande av normharmoni,[59] och svenska bestämmelser (såsom 15 kap. 13 § RF) ska därför av regeringen tolkas fördragskonformt med FN-stadgans bestämmelser.

Den internationella humanitära rätten (krigets lagar) har införlivats i svensk rätt genom att vissa bestämmelser har införlivats genom särskild lagstiftning (*transformering*),[60] och genom att andra materiella bestämmelser införlivats i svensk rätt genom konstaterande av normharmoni. 1907 års Haag-konventioner, om bl.a. lantkrig och neutralitet, antogs dock med stöd av 1809 års grundlag och anses vara automatiskt införlivade i svensk rätt.[61] Försvarsmaktens våldsanvändning ska därför vid ett insättande stå i överensstämmelse med de av krigets lagar som är bindande för Sverige.

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna har införlivats i svensk rätt genom inkorporering och ska gälla som lag i Sverige, se lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (1994 års lag). Konventionskomplexet ska vid tillämpning i svensk rätt — enligt principen om fördragskonform lagtolkning — så långt möjligt även tolkas så att tillämpningen står i överensstämmelse med den praxis som har utvecklats vid konventionsorganen, dvs. Europadomstolens praxis på området.[62] FN:s internationella konvention om medborgerliga och politiska rättigheter har införlivats genom konstaterande av

[58] Infra not 14, s. 300.
[59] Se bl.a. Utrikesutskottets betänkande nr 5 1946, s. 6 och prop. 1946:196, s. 15.
[60] Se bl.a. lagen (2014:406) om straff för vissa internationella brott; lagen (2014:812) om skydd för kännetecken i den internationella humanitära rätten. Se även prop. 1953:37, s. 36, prop. 1953:142, s. 13 ff., UU 1978/79:24, prop. 1978/79, s. 46 och prop. 2013/14:146, s. 56 ff.
[61] Jfr 12 §, 1809 års regeringsform, med ändringar bl.a. 1885 och 1909. Se även infra not 56, s. 781–782.
[62] Infra not 54, s. 12.

normharmoni.[63]

Det kan dock tänkas att Sverige, genom referensen till internationell rätt i 15 kap. 13 § RF, har intagit en monistisk hållning till internationell rätt inom detta specifika område, och att såväl regeringen som Försvarsmakten har att beakta samtliga de internationella regler som är bindande för Sverige vid våldsanvändning till rikets försvar, oavsett om dessa införlivats i svensk intern rätt eller ej.

4 Den internationella rättens inverkan på insatser för rikets försvar

4.1 Insats vid väpnat angrepp

4.1.1 Jus ad bellum

Regeringen får sätta in försvarsmakten vid ett väpnat angrepp i enlighet med internationell rätt (*jus ad bellum*) för att försvara riket.[64] Med ”väpnat angrepp” åsyftas ett sådant väpnat angrepp som avses i FN-stadgans art. 51,[65] och som ger en angripen stat rätt till individuellt och kollektivt självförsvar.[66]

Av art. 51 framgår att ingen bestämmelse i FN-stadgan inskränker den naturliga rätten till självförsvar i händelse av ett väpnat angrepp. Bestämmelsen innebär bl.a. att hot och våldshandlingar vid utövande av självförsvar får riktas mot den angripande statens territoriella integritet och politiska oberoende, och även får utövas på annat sätt som annars skulle anses oförenligt med Förenta nationernas ändamål.[67]

Vid ett väpnat angrepp mot Sverige kan regeringen sålunda med stöd av 15 kap. 13 § första stycket RF sätta in svensk militär trupp för att verka såväl i Sverige som inom motståndarens territorium. Självförsvarsåtgärderna måste dock vara proportionerliga, nödvändiga och riktade mot den stat som är ansvarig för angreppet.[68] Åtgärderna måste dessutom upphöra om och när säkerhetsrådet vidtagit nödvändiga åtgärder för upprätthållande av internationell fred och säkerhet.

Jus ad bellum-reglerna medför att det är folkrättsligt tillåtet att genomföra såväl defensiva som offensiva cyberoperationer inom eget och motståndarens territorium och cyberrymd.

4.1.2 Jus in bello

Referensen till ”internationell rätt” i 15 kap. 13 § första stycket RF tar, som tidigare konstaterats, sikte på folkrättens regler avseende staters rätt att gå i krig (*jus ad bellum*). Det är dock även underförstått att svensk trupp vid ett väpnat angrepp mot riket är skyldig att följa krigets lagar (*jus in bello*).[69]

Krigets lagar reglerar inte bara de krigförande styrkornas rätt att

[63] Prop. 1971:125, s. 25 ff.
[64] 15 kap. 13 § första stycket regeringsformen.
[65] Infra not 7, s 373; Infra not 14, s 205 och 300.
[66] Jfr art 2 (4) och art 51, FN-stadgan.
[67] Art 2 (4), FN-stadgan.
[68] Infra not 17, s 51.
[69] Infra not 14, s 205.

bruka våld vid strid (stridshandlingar). Krigets lagar ger även de krigförande styrkorna rätt att använda såväl civil som militär infrastruktur och egendom. Det gäller såväl egendom för själva krigföringen, exempelvis cyberinfrastruktur och uppkopplade datorer, servrar och annan IT-utrustning för utplacering av stridsmedel (skadlig kod m.m.), som för andra aktiviteter, exempelvis kartläggning, övervakning och kontroll av nätverk och nätaktiviteter, samt cyberexploatering som syftar till att förbereda eller underlätta stridshandlingar (*stridsrelaterad verksamhet*).[70] Krigets lagar medger sålunda att krigförande styrkor, med vissa humanitärrättsliga begränsningar, får använda datorer och servrar och den virtuella rymd och de programvaror m.m. (såväl civila som militära) som återfinns i sammankopplade IT-system för krigföringen, exempelvis som plattform för anfall och andra militära operationer i cybermiljön, när det är militärt befogat.

Ett försök att förklara folkrättens tillämplighet vid cyberkrigföring görs bl.a. i *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn-manualen).[71]

Vid krig och väpnad konflikt ska Sverige också iaktta och följa de mänskliga rättigheterna. Civilbefolkningens och enskildas rätt till liv, hälsa och skydd för den personliga integriteten liksom egendomsskydd regleras dock vid militära operationer under väpnade konflikter primärt av krigets lagar (den internationella humanitära rätten) i kraft av *lex specialis*, varvid krigföringsreglerna under en väpnad konflikt har företräde framför exempelvis mänskliga rättigheter vid åtgärder mot, eller genomförande av, cyberoperationer som har koppling till krigföringen (*belligerent nexus*).[72]

4.2 Insats vid begränsade suveränitetskränkningar (hävdande av territoriet)

Regeringen får enligt 15 kap. 13 § andra stycket RF uppdra till försvarsmakten att använda våld i enlighet med internationell rätt för att hindra kränkningar av rikets territorium i fredstid. Genom referensen till internationell rätt är avsikten även här att knyta insättandet av försvarsmakten närmare till bestämmelserna FN-stadgan och folkrätten,[73] varigenom möjligheten till våldsanvändning i fredstid alltid måste vara förenlig med folkrättens regler tillämpliga i fred (*fredens folkrätt*).[74] Bestämmelsen tar därtill uttryckligen sikte på att även Försvarsmaktens våldsanvändning ska vara i enlighet med internationell rätt.

[70] Se exempelvis art 35–67, TP I. Se även ICRC TP I Kommentar, 1875, 1936, 2161 och 2191. Se även Tallinn Manualen, regel 59, kommentar 13.
[71] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition, Cambridge University Press (2017).
[72] Prop. 2013/14:146, s. 43; Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ 8 July 1996, para. 25; Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Territories Palestinian Territory, ICJ 9 July 2004, para. 106; SOU 1984:56, s 56; SOU 2010:72, s. 275.
[73] Infra not 14, s. 205. Se även infra not 7, s. 373.
[74] Ibid, s. 300. Se även SOU 2010:72, s. 82 angående termerna ”fredens folkrätt” och ”konfliktpreventionens folkrätt”.

4.2.1 Rätten till våldsutövning vid suveränitetskränkningar

En kränkning av rikets territorium är inte att jämställa med ett väpnat angrepp och medför därför inte någon rätt till självförsvar enligt FN-stadgans art. 51. Vid insättande av rikets försvarsmakt för att hindra kränkningar av territoriet måste därför det internationella våldsförbudet (*jus contra bellum*), iakttas. Våldsförbudet återges i art. 2 (4) FN-stadgan, och lyder:

> Alla medlemmar skola i sina internationella förbindelser avhålla sig från hot om eller bruk av våld, vare sig riktat mot någon annan stats territoriella integritet eller politiska oberoende, eller på annat sätt oförenligt med Förenta nationernas ändamål.

Våldsförbudet hindrar dock inte användning av våld inom svenskt territorium mot en främmande stats aktörer, exempelvis statsfartyg, statsluftfartyg och militär personal, så länge bruket av våld är rimligt, nödvändigt och proportionerligt, samt inte sätter internationell fred och säkerhet i fara (*rätt till våldsutövning vid suveränitetskränkningar*).[75]

Inom ramen för fredens folkrätt har stater således rätt till ett visst, rimligt utövande av våld för att skydda statens gränser och territoriella integritet, liksom för att avvisa inkräktare och hindra olaga intrång och oönskade verksamheter. Denna rätt följer av allmän folkrätt och är en etablerad sedvanerättslig princip.[76]

Av regeringsformens bestämmelse följer sålunda att regeringens rätt — att i fredstid sätta in cyberförsvarsförband för att hindra en kränkning av svensk cyberrymd — inte får riktas mot en annan stats territorium eller politiska oberoende (suveränitet), och att cyberförsvaret ska vara rimligt, nödvändigt och proportionerligt, och inte får sätta internationell fred och säkerhet i fara.

Hävdandet av svensk cyberrymd i fredstid får därmed inte ske genom åtgärder som angriper eller skadar nätverk och digitala system belägna inom den kränkande staten eller andra staters territorium. Insättandet av cyberförsvarsförband ska därför vara begränsat till att agera och verka i Sverige, genom exempelvis defensiva som offensiva cyberförsvarsoperationer.

Rätten till våldsutövning vid suveränitetskränkningar ger dock även stater en viss rätt att ingripa mot våldshandlingar som utförs utanför statens territorium, men mot mål inom dess territorium eller mot statens fartyg eller luftfartyg på eller över fritt hav.[77] Som våldshandlingar riktade mot mål inom svenskt territorium torde bl.a. anses en främmande stats användning av medel för telekrigföring mot mål i Sverige, exempelvis om utländska statsfartyg eller statsluftfartyg som befinner

[75] Art. 1 (1) jämförd med art. 2(4), FN-stadgan. Se även infra not 40, s. 24.
[76] Infra not 17, s. 49.
[77] Se exv. 14 och 22 §§, förordningen (1982:756) om Försvarsmaktens ingripanden vid kränkningar av Sveriges territorium under fred och neutralitet, m.m. (IKFN-förordningen).

sig utanför svenskt territorium använder medel för telekrigföring för att störa ut eller blockera radarstationer eller elektroniska kommunikationssystem placerade inom svenskt territorium. Kränkningar av svensk cyberrymd som sker från fartyg eller luftfartyg som befinner sig på eller över internationellt vatten (fritt hav) kan därför bli föremål för cyberoperationer, även om effekten inträder utanför territoriet.

4.2.2 Regler om våldsanvändningen vid suveränitetskränkningar

Fredens folkrätt reglerar även *hur* våldsanvändning får utövas vid fredstida ingripanden mot suveränitetskränkningar (*regler om våldsanvändningen vid suveränitetskränkningar*).

Till skillnad från krigets lagar (*jus in bello*) är folkrättens regler om våldsanvändning vid suveränitetskränkningar i fred i huvudsak inte kodifierade och baseras främst på internationell sedvanerätt.

Våldshandlingarna ska primärt begränsas till de aktörer och den verksamhet som kränker statens territoriella suveränitet,[78] eller mot sådana vålds- eller tvångshandlingar som riktas mot statens fartyg och luftfartyg inom eller över internationellt vatten och fritt hav.[79] Det våld som tillgrips ska dock alltid anpassas till vad som bedöms nödvändigt för att förhindra att kränkningen genomförs och avbrytas då det avsedda syftet har uppnåtts.[80]

Enligt de sedvanerättsliga reglerna ska det våld som folkrättsligt tillåts vid ingripanden mot suveränitetskränkningar i fred vanligtvis föregås av varning,[81] men kan innefatta användande av nödvändigt våld i självförsvar[82] liksom användande av våld upp till och med dödligt våld för att avbryta suveränitetskränkningen.[83]

Vid hävdandet av sitt territorium i fredstid ska stater även ta hänsyn till andra staters rättigheter, exempelvis rätten till fri navigering och oskadlig genomfart. Till folkrättens regler om våldsanvändning vid suveränitetskränkningar får även anses höra regler om statsimmunitet och okränkbarhet, exempelvis till skydd för ambassad och konsulär verksamhet m.m., inklusive deras nätverk och digitala system.[84]

IKFN-förordningen och tillträdesförordningen (1992:118) ger uttryck för Sveriges tolkning av den tillämpliga internationella rätten.[85]

Vilka rättigheter som kan göras gällande inom cyberdomänen är i stor utsträckning oklar. Vid suveränitetskränkningar i fredstid är syftet med cyberoperationerna främst att övervaka och identifiera intrång,

[78] Se bl.a. 9–27 §§, ibid.
[79] Se bl.a. 14 § 3, och 22 § 3, ibid.
[80] 16 §, Försvarsmaktens föreskrifter (FFS 2013:3) om verkställighet av tillträdes- och IKFN-förordningen.
[81] 7 §, IKFN-förordningen. Se även ICJ, Reports, The Corfu Channel Case (Merits). 1949, s. 22.
[82] Se bl.a. 6 §, ibid.
[83] Se bl.a. 9, 13–15 och 22–23 §§, ibid.
[84] Se bl.a. art. 22, Wienkonventionen om diplomatiska förbindelser; art. 31, Wienkonventionen om konsulära förbindelser. Se även lagen (1976:661) om immunitet och privilegier i vissa fall.
[85] Infra not 40, s. 24.

samt avbryta skadlig aktivitet i eller mot nätverk och digitala system i Sverige, samt återställa angripna nätverk och system (*defensivt cyberförsvar*). Det torde dock inte finnas någon oklarhet om att sådana åtgärder i hävdandet av den egna statens cyberrymd är folkrättsligt tillåtna. Det är också klart att en angripen stat inom sin cyberrymd får genomföra cyberexploatering och cyberattacker (*offensivt cyberförsvar*) mot nätverk och digitala system belägna inom statens territorium.

I fredstid regleras den internationella rättens skydd av civila, exempelvis enskildas rätt till liv och hälsa, personlig integritet och egendomsskydd vid ingripanden mot suveränitetskränkningar, främst av allmänna och väl etablerade folkrättsliga principer, såsom ”*elementary considerations of humanity*”,[86] samt av folkrättens regler om skydd för de mänskliga rättigheterna.

Vad gäller skydd av civila vid våldsanvändning i samband med suveränitetskränkningar saknar fredens folkrätt regler motsvarande krigets lagar (den internationella humanitära rätten) som i kraft av *lex specialis* har företräde framför de mänskliga rättigheterna. Mänskliga rättigheter ska därför iakttas till skydd för civilbefolkningen och civila i den utsträckning rättighetsskyddet är tillämpligt.

5 Utgör 15 kap. 13 § RF tillräckligt lagstöd för att utföra cyberförsvarsoperationer?

Om de åtgärder som militära förband förväntas vidta vid defensivt respektive offensivt cyberförsvar kan medföra ett intrång i enskilda individers grundläggande fri- och rättigheter (se 2 kap. RF) eller i övrigt innebära ett ingrepp i individers personliga förhållanden (se 8 kap. RF) ska åtgärderna ha stöd i lag.[87] Detsamma gäller om de åtgärder som ska vidtas innebär ett intrång i den rättssfär som gällande lagstiftning avser att trygga, exempelvis genom bestämmelsen om dataintrång (4 kap. 9 c § BrB). Försvarsmaktens agerande ska i dessa situationer ha stöd i lag, exempelvis inom ramen för polislagens (1984:387) bestämmelser om laga befogenhet.[88] Lagstöd kan även vara nödvändigt om de åtgärder som ska vidtas inkräktar på det rättighetsskydd som följer av lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (1994 års lag), eller Europadomstolens praxis.

5.1 Rikets försvar

Av kap. 3 i denna artikel framgår att Försvarsmakten vid insatser för rikets försvar ska iaktta och följa internationell rätt, och att Försvarsmakten i detta avseende ska iaktta och följa den internationella humanitära rättens regler (*krigets lagar*) vid insatser under väpnat angrepp (väpnad konflikt), samt att Försvarsmakten ska iaktta och följa interna-

[86] ICJ, Reports, The Corfu Channel Case (Merits). 1949, s. 22.
[87] 2 kap. 20 § och 8 kap. 2 § 1, regeringsformen.
[88] Infra not 50, s. 11–12.

tionella regler om våldsanvändningen vid insatser mot suveränitetskränkningar i fredstid (*regler om våldsanvändningen vid suveränitetskränkningar*).

5.1.1 Situationen vid väpnat angrepp

Någon författningsreglering, exempelvis stöd i lag eller annan svensk författning, utöver bestämmelsen i 15 kap. 13 § RF har inte ansetts nödvändig för att Försvarsmakten ska få vidta folkrättsligt tillåtna åtgärder vid försvaret av riket vid ett väpnat angrepp.[89] Det finns heller inte någon närmare svensk författningsreglering av Försvarsmaktens våldsoch tvångsanvändning under väpnade konflikter.[90] Totalförsvarets folkrättsförordning innehåller dock vissa föreskrifter för svensk tolkning och tillämpning av krigets lagar,[91] se även Försvarsmaktens tillämpningsföreskrifter till förordningen.

Svensk rätt innehåller dessutom en oskriven ansvarsfrihetsgrund för den som vid väpnad strid agerar i enlighet med de folkrättsliga regler som gäller vid väpnad konflikt.[92] Regeringen har härvidlag, med avseende på ansvarsfrihet för handlingar under strid, uttalat att[93]

> I straffrättsligt hänseende är en väpnad styrkas rätt att bruka våld i samband med strid i princip oreglerad. Det ligger emellertid i sakens natur att det straffrättsliga regelsystemet inte är avsett att hindra en svensk väpnad styrka från att på vedertaget sätt lösa sin uppgift. Med hänsyn härtill får förutsättas att något straffrättsligt ansvar inte kan göras gällande för styrkans medlemmar såvitt avser sådan våldsutövning som kan anses motiverad från militär synpunkt och som står i överensstämmelse med folkrättens regler.

Vad som utgör otillåtna krigshandlingar enligt svensk rätt, och som kan omfattas av straffansvar, framgår av lagen (2014:406) om straff för vissa internationella brott.

Vid militära insatser inom cyberdomänen — under en väpnad konflikt — regleras således insatsernas tillåtlighet av bestämmelser i krigets lagar, och något ytterligare stöd i svensk rätt utöver att truppen satts in med stöd av 15 kap. 13 § RF, är inte nödvändigt.

2 och 8 kap. RF, liksom befintlig svensk lagstiftning som exempelvis skyddar personlig integritet, verksamhet eller egendom (inklusive datorer och nätverk mot intrång) m.m., är således inte avsedda att hindra den direkta krigföringen, såvida inte regleringen skulle vara särskilt avsedd för att just reglera stridshandlingar och andra åtgärder som vidtas för den direkta krigföringen. De folkrättsliga ”krigföringsreglerna” kan därför sägas ha företräde framför svensk rätt vid strids- och stridsrelaterade situationer.

[89] Infra not 14, s. 205.
[90] Infra not 17, s. 24.
[91] 1 §, Totalförsvarets folkrättsförordning (1990:12).
[92] N. Jareborg, *Straffrättens ansvarslära*, Iustus förlag, Uppsala (1994), s. 184. Ds JU 1984:6, s. 70 ff.
[93] Prop. 1995/96:113, s. 10 ff.

Effekterna av bestämmelsen i 15 kap. 13 § första stycket RF är dock begränsade till sådana åtgärder som innefattar våld eller tvång mot motståndaren (*strid och annan våldsanvändning*), dvs. åtgärder som är kopplade till den direkta krigföringen. Bestämmelsen avser inte att träffa alla åtgärder som regeringen eller Försvarsmaktens kan anse sig behöva vidta i samband med ett väpnat angrepp på riket. Försvarsmaktens cyberförsvarsförband måste därmed, med avseende på verksamhet som inte regleras av folkrättens ”krigföringsregler”, följa bestämmelser i svensk rätt vid ingripanden och andra åtgärder som saknar ett omedelbart samband med förberedelser eller genomförande av cyberkrigföring.

Något behov av ny eller ändrad författningsreglering föreligger därmed inte vad avser svenska cyberförsvarsförbands möjlighet att agera inom hela den ram som den internationella humanitära rätten (krigets lagar) medger.

5.1.2 Situationen vid hävdande av Sveriges territorium i fredstid

Enligt 15 kap. 13 § andra stycket RF får regeringen uppdra åt Försvarsmakten att använda våld i enlighet med internationell rätt för att hindra kränkning av rikets territorium i fred eller under krig mellan främmande stater. I likhet med vad som gäller vid insättande av Försvarsmakten för att möta ett väpnat angrepp är insättandet av Försvarsmakten för att hävda rikets territorium enligt 15 kap. 13 § andra stycket RF inte beroende av ytterligare stöd i lag eller annan svensk författning.

Bestämmelserna i 15 kap. 13 § RF återfanns tidigare i 10 kap. (om förhållandet till andra stater) i 1974 års regeringsform,[94] och anses främst avse insättande av Försvarsmakten mot en främmande stats militära enheter, om dessa kränker svenskt territorium. Med ”kränkning av rikets territorium i fred eller under krig mellan främmande stater” avses därför primärt kränkningar begångna av en främmande stat genom dess höghetshandlande (*acta jure imperii*) och bestämmelsen tar följaktligen främst sikte på kränkningar som utförs av främmande staters statsorgan och statsagenter i deras funktion av företrädare för eller utövare av statlig våldsmakt.

Bestämmelsen träffar även situationer när en suveränitetskränkning inte utgör ett klart uttryck för en stats höghetshandlande, dvs. även en kränkning som är isolerad och inte ingår i en större plan eller ens är centralt beordrad osv., liksom kränkningar som är orsakade av felorientering eller andra misstag.[95]

Vid ingripanden mot statliga eller statsunderstödda aktörer (statsagenter) i fredstid utgör de aktuella folkrättsliga bestämmelserna en specifik och självständig folkrättslig reglering (*sui generis*) av hur stater får använda våld och tvång inom sitt territorium.

[94] Infra not 7, s. 373 ff.
[95] Infra not 24, Bilaga 4, s. 354.

I detta avseende gäller exempelvis folkrättens skydd för mänskliga fri- och rättigheter inte i förhållande till en främmande stat och dess höghetshandlande (*acta jure imperii*), dvs. suveräna staters utövande av statlig makt, och följaktligen inte heller för främmande staters statsorgan och statsagenter i deras funktion av företrädare för eller utövare av statlig makt.[96] Folkrättens skydd för mänskliga fri- och rättigheter ska dock iakttas om ingripandet mot dem görs i deras egenskap av enskilda individer (privatpersoner), vilket inte är fallet vid suveränitetskränkningar.

Våldshandlingar och andra åtgärder mot statsaktörer och statsunderstödda aktörer i fredstid anses enligt svensk rätt dessutom kunna ske utan beaktande av kravet på lagstöd i 2 och 8 kap. RF, eftersom åtgärder mot statsaktörer inte rör inskränkningar i enskildas grundläggande fri- och rättigheter (2 kap.) eller riktas mot enskildas personliga förhållanden (8 kap.).[97] Motsvarande gäller vid intrång i rättighetsskyddet enligt 1994 års lag och Europadomstolens praxis. Jämför i detta avseende bl.a. IKFN-förordningens bestämmelser vid insatser mot främmande staters militära personal, statsfartyg och statsluftfartyg som har meddelats med stöd av 10 kap. 9 § tredje stycket 1974 år regeringsform (numera 15 kap. 13 § andra stycket RF).

Efter att Försvarsmakten ingripit och omhändertagit utländsk militär personal är det enligt IKFN-förordningen Polismyndighetens uppgift att besluta om vidare åtgärder.[98] Det är i viss uträckning oklart om Polismyndighetens åtgärder vid fortsatt omhändertagande regleras av 15 kap. 13 § andra stycket RF. En förutsättning torde dock vara att Polismyndigheten i så fall har satts in med stöd av bestämmelsen och (agerar) som en del av rikets ”försvarsmakt”.

En problematik som uppstår vid fredstida cyberhot och cyberangrepp är kopplat till svårigheten att härleda ett angrepp till utföraren (antagonisten) och att identifiera antagonisten som statsaktör eller icke-statsaktör under pågående insatser. Exempelvis är det inte alltid klart när cyberhot och angrepp emanerar från stater eller icke-statliga aktörer. Denna gråzon, som är kännetecknande för hybridkrigföring, understryker behovet av en tydlig rättslig styrning som klargör vilka typer av hot som berättigar insättande av militära cyberförsvarsförband i fredstid och vilka rättsliga regler som då ska gälla.

15 kap. 13 § andra stycket RF har i sin tidigare lydelse (10 kap. 9 § RF) ansetts innefatta kränkningar av svenskt territorium som utförts av icke-statliga aktörer, se bl.a. 28–35 §§, IKFN-förordningen. Försvarsmakten ges i dessa sammanhang främst uppgifter att bistå civila myndigheter med åtgärder som dessa myndigheter får vidta enligt svensk rätt. Bestämmelserna är därmed av mindre relevans för förståelsen av 15 kap. 13 § andra stycket RF, med undantag för 31 och 33 §§

[96] För dessa gäller, om tillämpligt i det enskilda fallet, exempelvis folkrättens regler om statsimmunitet och okränkbarhet.
[97] Se även infra not 47, s. 136.
[98] 10, 12 och 27 §§, IKFN-förordningen.

IKFN-förordningen.

Enligt 31 § IKFN-förordningen får Försvarsmakten förfölja, preja och föra handelsfartyg som inte lyder en prejningsorder eller en order om visitering in till svensk hamn. Ingripandet får göras först på begäran av den myndighet som begärt biträde med åtgärden, men utförs inte med stöd av åtgärder som den begärande myndigheten får vidta, utan med stöd av internationell rätt.[99] Av 33 § framgår att Försvarsmakten vid genomförande av åtgärder på begäran av annan myndighet får använda våld i självförsvar, men att våld får användas även i andra fall om det är oundgängligen nödvändigt med hänsyn till åtgärdens vikt och det krävs av den myndighet som har begärt åtgärden. Inte heller i detta fall utövas våld med stöd av befogenheter som den begärande myndigheten får vidta, utan efter medgivande av Försvarsmakten ytterst med stöd av 15 kap. 13 andra stycket RF. I betänkandet Stöd från Försvarsmakten (SOU 2001:98) anförs i detta sammanhang att ”det kan vara så att detta stadgande [nuvarande 15 kap. 13 § andra stycket RF] utgör lagstöd för utövning av tvång eller våld från Försvarsmaktens sida i de avseenden som anges i förordningen men endast om det rör sig om annat än normala fredstida företeelser som sjöfart och fiske eller om ingripandet ingår i hävdandet av territoriet eller sker mot utländska statsfartyg”.[100]

Om rätten till våldsanvändning i 31 och 33 § IKFN-förordningen inte grundas på 15 kap. 13 § andra stycket RF (tidigare 10 kap. 9 § tredje stycket RF) så krävs numera riksdagens medverkan enligt 15 kap. 16 § RF, och att Försvarsmaktens insättande i förevarande situationer regleras i lag eller särskilt riksdagsbeslut.[101] Enligt den tidigare lydelsen (10 kap. 9 § RF) erfordrades riksdagens medverkan dock endast om Försvarsmakten skulle sättas in i strid eller sändas till annat land.

Eftersom våldshandlingarna i 31 och 33 §§ IKFN-förordningen riktas mot personer inom svenskt territorium borde emellertid även 2 och 8 kap. RF ha uppmärksammats vid förordningens tillkomst, om lagstödet (grundlagsstödet i 10 kap. 9 §, nuvarande 15 kap. 13 § RF) för våldshandlingar mot enskilda hade ansetts otillräckligt. Så verkar dock inte ha varit fallet vid tidpunkten för IKFN-förordningens tillkomst.

Även om 15 kap. 13 § RF medger att Försvarsmakten sätts in mot icke-statsaktörer för att hävda svenskt territorium har denna möjlighet, vid sidan om vad som anges i IKFN-förordningen, inte nyttjats.[102] Regeringen har exempelvis vid insättande av Försvarsmakten mot terrorism (2006) inte använt sig av 10 kap. 9 § RF (nuvarande 15 kap. 13 § andra stycket RF), utan istället låtit riksdagen besluta om särskild lag för

[99] Se bl.a. art 25, Förenta nationernas havsrättskonvention Montego Bay den 10 december 1982 (Havsrättskonventionen).
[100] Infra not 47, s. 136.
[101] Se 15 kap. 16 § andra stycket, RF.
[102] Infra not 47, s. 96.

insättandet.[103] Regeringen anförde i sammanhanget att ”med hänsyn till bestämmelsen i 2 kap. 6 § RF som skyddar medborgarna mot påtvingade kroppsliga angrepp måste […] ett sådant regeringsbeslut utformas så att Försvarsmakten, om det blir aktuellt att använda våld mot enskilda, agerar med stöd av lag, exempelvis inom ramen för polislagens (1984:387) bestämmelser om laga befogenhet”.[104] Det av regeringen anförda torde visa att regeringen vid tidpunkten ansåg att grundlagsstödet i 10 kap. 9 § RF inte utgjorde ett tillräckligt lagstöd för insatser mot icke-statliga aktörer.

Motsvarande synsätt har använts i samband med införandet av lagen (2000:130) om försvarsunderrättelseverksamhet. Försvarsunderrättelseverksamheten avser att kartlägga yttre hot mot landet, och får endast avse utländska förhållanden.[105] Även om en lagreglering av försvarsunderrättelseverksamheten inte är obligatorisk, ansåg regeringen att en lagreglering markerar vikten av en väl fungerande underrättelseverksamhet som bedrivs utifrån i ett demokratiskt samhälle godtagbara grundprinciper.[106] Vid anpassning av försvarsunderrättelseverksamheten (2007) till tekniska förutsättningar, den rådande hotbilden och att hoten inte sällan utgår från icke-statliga aktörer,[107] innefattande IT-relaterade hot,[108] lades inte heller den dåvarande bestämmelsen i 10 kap. 9 § RF till grund för verksamhetens laglighet. Istället framhölls behovet av att iaktta bestämmelserna i 2 och 8 kap. RF samt den europeiska konventionen om mänskliga rättigheter,[109] bl.a. av integritetsskäl.[110]

Cyberoperationer som utförs för att hävda svensk cyberrymd i fredstid kan därför, med anledning av hur regeringen valt att tillämpa 15 kap. 13 § andra stycket RF, komma att behöva särskilt stöd i lag om operationerna innebär intrång i icke-statliga aktörers eller privatpersoners rättighetsskydd enligt 2 kap. RF eller medför intrång i dessas personliga förhållanden (8 kap. RF).

6 Behovet av lagstöd vid fredstida cyberförsvarsoperationer

Vid suveränitetskränkningar i fredstid är syftet med cyberoperationerna främst att övervaka och identifiera intrång i specifika skyddsvärda nätverk och digitala system, samt avbryta skadlig aktivitet i eller mot nätverk och digitala system i Sverige, samt återställa angripna nätverk och system (*defensivt cyberförsvar*). Övervakningen består främst i att nätverkens in- och utgående trafik övervakas, liksom övervakning av

[103] Se lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning.
[104] Infra not 50, s. 11–12.
[105] 1 §, lagen (2000:130) om försvarsunderrättelseverksamhet. Se även 1–2 a §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
[106] Prop. 1999/2000:25, s. 12.
[107] Prop. 2006/2007:63, s. 33.
[108] Ibid, s. 58 f.
[109] Ibid, s. 32 f.
[110] Ibid, s. 60 ff.

trafiken i och mellan digitala system inom ett nätverk. Det är alltså inte fråga om den mer omfattande och breda övervakning av nätverk som Försvarets radioanstalt (FRA) bedriver inom ramen för signalspaning.

För att genomföra defensiva cyberoperationer behöver Försvarsmakten emellertid tillgång till nätverk och digitala system som är utsatta för hot eller angrepp. Effektiva cyberoperationer förutsätter därutöver personal med kännedom om vilka informationssystem och vilken information som ska skyddas och på vilket sätt, liksom om arkitekturen och säkerhetsskyddet i aktuella digitala nät och system. Defensiva cyberoperationer förutsätter därför ofta ett nära samarbete mellan verksamhetsutövare och cyberförsvarsförbanden. Verksamhetsutövaren har kunskapen om arkitekturen och säkerhetsskyddet i aktuella digitala nät och system, liksom kännedom om vilka informationssystem och vilken information som ska skyddas, under det att den militära kompetensen bland annat bidrar med erfarenhet och kunskap om cyberhot, inklusive sårbarheter, tillvägagångssätt och aktörer, samt risker och hur dessa risker kan komma att förändras under höjd beredskap och väpnat angrepp. Den militära erfarenheten och kunskapen är särskilt viktig med avseende på de mest kvalificerade hoten och angreppen, där kända skydds- och motåtgärder för att neutralisera hotet eller angreppet är helt eller delvis verkningslösa. Defensiva cyberoperationer genomförs därför främst i nätverk och digitala system där verksamhetsägaren samtycker till insatsen och samverkar med cyberförsvarsförbanden. I detta avseende erfordras inte något särskilt lagstöd för att genomföra en cyberoperation, och regeringen kan sätta in Försvarsmakten med stöd av 15 kap. 13 § andra stycket RF. På begäran av verksamhetsutövaren kan Försvarsmakten i förevarande situation emellertid redan idag lämna stöd till verksamhetsutövaren enligt förordningen (2002:375) om Försvarsmaktens stöd till civil verksamhet.

Hävdandet av svensk cyberrymd i fredstid bör emellertid inte vara beroende av samtycke från verksamhetsutövare eller nätverksinnehavare, exempelvis när det är fråga om insatser i nätverk och digitala system som nyttjas i ett antagonistiskt syfte som kan få omfattande och allvarliga samhälleliga konsekvenser. Detta är särskilt relevant i dagens säkerhetsmiljö, där hybridkrigföring, ofta karakteriserad av en kombination av militära och icke-militära metoder, suddar ut gränserna mellan krig och fred. Hybridangrepp, inklusive cyberoperationer, kan bestå av allt från suveränitetskränkningar till ren cyberbrottslighet, exempelvis riktad mot samhällsviktig infrastruktur.

I dessa situationer kan även offensiva cyberoperationer behövas för att i vart fall omedelbart kunna stänga ner och isolera skadliga nätverk och digitala system temporärt. Även om bestämmelserna i 24 kap. BrB i viss grad skulle kunna tillämpas är detta varken tillräckligt eller tillfredsställande för upprätthållandet av svensk cyberrymd i fredstid, särskilt vid ingripanden mot hybridkrigföring och storskaliga cyberangrepp utförda av icke-statliga aktörer.

Lagstöd krävs dock i situationer när cyberförsvarsförbandens åtgärder saknar nödvändigt samtycke till att utföra cyberoperationer i aktuella nät och digitala system. Utan samtycke eller lagstöd skulle åtgärderna exempelvis kunna utgöra dataintrång enligt 4 kap. 9 c § BrB.

7 Sammanfattande iakttagelser

Regeringsformen utgör den centrala konstitutionella ramen för regeringens befogenheter att sätta in Försvarsmaktens cyberförsvarsförband. Bestämmelserna i 15 kap. 13 och 16 §§ RF bygger på insikten att regeringen måste ha en direkt möjlighet att fatta avgörande beslut till rikets försvar, men att riksdagen ska ha ett inflytande om väpnade styrkor sätts in för andra ändamål än rikets försvar, exempelvis för att hindra allvarligare cyberbrottslighet.

Regleringen (15 kap. 13 § första stycket RF) är till stor del oproblematiskt när ett angrepp mot svensk cyberrymd kan kopplas till ett väpnat angrepp mot riket, och krigets lagar ska tillämpas. Något behov av ny eller ändrad författningsreglering föreligger inte vad avser svenska cyberförsvarsförbands möjlighet att agera inom hela den ram som den internationella humanitära rätten (krigets lagar) medger.

I fredstid är situationen delvis annorlunda. Regeringen kan enligt 15 kap. 13 § andra stycket RF sätta in Försvarsmakten till rikets försvar för att agera mot kränkningar av svenskt territorium. Bestämmelsen har främst tillämpats vid insättande av Försvarsmakten mot utländska statsaktörer (militär personal och enheter). I praktiken har bestämmelsen emellertid inte använts för att sätta in Försvarsmakten mot icke-statliga aktörer som kränker svenskt territorium, även om bestämmelsen skulle medge det.

Möjligheten att redan i fredstid kunna sätta in Försvarsmakten mot icke-statliga aktörer som kränker svenskt territorium torde emellertid vara av särskild vikt i samband med exempelvis hybridhot, icke-linjär krigföring och allvarligare antagonistiska cyberangrepp. Vid hybrid- och cyberangrepp m.m. är aktörers identitet och handlingars karaktär och syfte ofta oklara. Det föreligger också betydande svårigheter att utreda om aktören är en statlig eller icke-statlig aktör, och om ingripanden är en polisiär eller militär uppgift. Det kan därmed uppstå rättsliga gråzoner vid insatser mot hybrid- och cyberangrepp.

Genom den nuvarande tillämpningen av 15 kap. 13 § RF ställs regeringen inför rättsliga utmaningar till följd av de gråzoner som kan uppstå, och som bl.a. kan fördröja tidskritiska och effektiva insatser mot hybrid- och cyberangrepp som utförs i övergången mellan fred och krig, eller för att testa den svenska försvarsförmågan. Gråzonsproblematiken innebär att den nuvarande regleringen kan vara otillräcklig vid cyberangrepp i fredstid, särskilt vid hybridhot där statliga och icke-statliga aktörer samverkar eller maskerar sin identitet. En tydligare och specifik lagreglering av Försvarsmaktens befogenheter vid cyberhot och angrepp skulle kunna minska denna rättsliga gråzon och säker-

ställa en effektiv respons utan att inskränka rättsstatens principer.

Regeringens förhållningssätt till 15 kap. 13 § RF, i situationer när icke-statliga aktörer kan påverkas, innebär sannolikt att regeringen vare sig kommer att besluta om insättande enligt 15 kap. 13 § första stycket RF eller uppdra till Försvarsmakten att ingripa mot hybridkrigföring utan att ett klart lagstöd för Försvarsmaktens åtgärder föreligger.

För att i möjligaste mån undanröja rättsliga oklarheter rörande möjligheten att sätta in Försvarsmakten bör övervägas att i lagform klargöra myndighetens befogenheter och ansvar, och möjliggöra ingripanden vid fredstida hybrid- och cyberangrepp som innebär kränkningar av svensk cyberrymd oberoende av aktörens status. En utgångspunkt för sådan lagstiftning kan exempelvis vara lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning.