LONGREAD

Cybersäkerhet:
Hög tid för cyberutvecklingsmål

Rene Summer är *Director Government and Industry Relations* på Ericsson och ordförande för ICC:s internationella *Working Group on Cybersecurity*, som följer och deltar i FN:s arbete på cybersäkerhetsområdet.

Digitaliseringen har medfört såväl stora ekonomiska möjligheter som ökad tillgång till och integrering av marknader runtom i världen. Med den ökade digitaliseringen följer samtidigt ett ökat hot för intrång och andra kriminella aktiviteter i cyberrymden som slår hårt mot såväl näringslivet som offentliga aktörer. Hur kan denna ökade hotbild hanteras och vad är näringslivets roll?

Cyberattacker är ett växande globalt problem, som hämmar ekonomisk tillväxt och medför betydande förluster av arbetstillfällen inom alla ekonomier. Uppskattningsvis går 60 procent av de småföretag som utsätts för en cyberattack i konkurs. I en rapport publicerad av EU-kommissionens *Joint Research Centre (JRC)* från 2020 framgår det att den totala kostnaden för de som drabbas av cyberbrottslighet har ökat markant. År 2015 uppskattades kostnaden till 2 700 miljarder euro. År 2020 hade samma siffra ökat till 5 500 miljarder och om trenden håller i sig kan vi förvänta oss ytterligare en dubblering till 11 000 miljarder euro år 2030. Det är en summa som motsvarar Tysklands, Frankrikes och Japans sammanlagda BNP 2021.

Till viss del drivs utvecklingen av kriminella element, men oroväckande nog är cyberkriminella inte de enda aktörer som företag och andra måste försvara sig mot. Det finns även ett ökande antal stater som investerar i och arbetar med destabiliserande aktiviteter i cyberrymden. Stater ser och betraktar i allt högre grad teknologi och cyberrymden som ett område för geopolitiskt maktspel, och antalet stater med förmåga och vilja att genomföra sofistikerade cyberattacker har blivit betydligt fler.

De senaste årens ständigt ökande intensitet och frekvens av cyberattacker av såväl kriminella som statliga aktörer har inte bara visat deras förödande konsekvenser, utan har även genererat en oönskad normalisering av situationen. Näringslivet tvingas vänja sig vid allt fler attacker. Denna trend måste brytas, men det kräver en samordnad policystrategi som möjliggör konkreta åtgärder och leder till påtagliga resultat. Det är en av målsättningarna för ICC:s arbete på området. I vår internationella *Working Group on Cybersecurity* samlar vi ledande experter från vårt globala nätverk för att ge näringslivet en röst i frågan, öka insikterna om de utmaningar som företagen står inför på området och

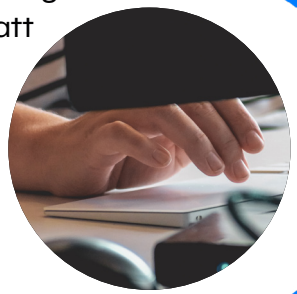
driva på för åtgärder på global nivå för att bryta den negativa trenden.
Även om många utmaningar kvarstår har betydande ansträngningar redan gjorts för att stärka motståndskraften i den digitala infrastrukturen, bland annat genom branschregleringar och investeringar i cybersäkerhet för att stärka upp säkerheten. Reglering har varit nödvändigt och kommer att fortsätta utvecklas, men det i sig själv räcker inte. Att endast fokusera på defensiva åtgärder kan i bästa fall begränsa skadan men gör väldigt lite för att bryta trenden av tilltagande cyberattacker. Det gör heller inget för att förändra normaliseringen av detta ständigt växande hot.

Näringslivet tvingas vänja sig vid allt fler attacker. Denna trend måste brytas, men det kräver en samordnad policystrategi som möjliggör konkreta åtgärder och leder till påtagliga resultat.

Det räcker inte att enbart stärka cybermotståndskraften i den privata sektorn – det behövs dessutom en långsiktigt hållbar och bredare lösning. En anledning är den stora mängden och den ökade frekvensen av cyberhot. Av ett slumpmässigt antal cyberattacker, säg en miljon om dagen, som ett stort företag rutinmässigt utsätts för, behöver företaget skydda sig framgångsrikt varje enskild gång. För angriparen räcker det däremot att lyckas bara en enda gång. En ständigt ökad frekvens av attacker missgynnar försvararen. En annan anledning är skillnaden i kostnadseffektivitet för angriparen i jämförelse med den som försöker skydda sig. För en hypotetisk summa, till exempel tio miljoner kronor, kan ett företag bara marginellt förbättra sitt försvar. Angriparen kan för samma summa däremot införskaffa sig en mängd offensiva verktyg utan att ha någon specialiserad kunskap eller förmåga att nyttja dem. Utöver dessa asymmetrier som missgynnar de som angrips, har vi statsaktörer, s.k. APT (*Advanced Persistent Threat* på engelska), som besitter både betydande resurser, kapacitet och motivation.

Men att defensiva förmågor som syftar till att stärka den privata sektorns cyberresiliens inte räcker till innebär inte att vi måste vända oss allena till offensivt cyberförsvar. Det pågår förvisso en diskussion om staters "lagliga" eller "legitima" offensiva cyberaktioner, men de ligger bortom gränsen för ett laglydigt civilsamhälle och näringsliv. Det finns dock ett tredje sätt som väsentligt kan bidra till en förbättring.

Det tredje tillvägagångsättet går ut på att göra cyberattacker mindre attraktiva för angriparna att utföra. Angriparnas avkastning är en avvägning mellan kostnad och nytta, och denna avvägning behöver ändras genom att markant höja kostnaderna för attacker genom att öka sannolikheten för att angriparen upptäcks, fångas och tvingas möta konsekvenserna av sina olagliga handlingar. Här spelar staters agerande för att höja kostnaden för att bedriva cyberbrottslighet en avgörande roll.



Lyckligtvis betyder det tredje tillvägagångsättet inte att vi behöver börja från noll. Viktiga grunder har lagts under senare år. År 2015 enades man inom FN:s Group

of *Governmental Experts on Information Security (GGE)* om elva normer för ett ansvarsfullt statligt agerande i cyberrymden. Det var det första steget mot ett gemensamt ramverk för cybersäkerhet. Sedan dess har normerna vidareutvecklats i flera processer inom FN-systemet, bland annat inom den första s.k. *Open-ended Working Group on Security of and in the Use of Information and Communications Technologies* (OEWG). Arbetet i OEWG kulminerade 2021 i en rapport som bekräftar medlemsländernas stöd för tillämpligheten av internationell lag i cyberrymden och för de elva GGE-normerna för statligt ansvarsfullt agerande. Därför är frågan inte längre *om* det finns gällande lagar och normer på området, utan *hur* de skall implementeras.

ICC är mån om att fortsätta vara en aktiv intressent för att stödja detta implementeringsarbete, som är nästa nödvändiga steg för att leverera påtagliga resultat och stävja den negativa utvecklingen. I dagsläget finns ingen konsensus bland FN:s medlemsländer om vilka tekniska, rättsliga och politiska ramar som behövs för att kunna tillämpa internationell lag och GGE-normerna. För att underlätta implementeringen av dem behövs ett gemensamt genomföranderamverk. Därför har vi från ICC:s sida lanserat konceptet *Cyber Development Goals* (CDG). Konceptet hämtar inspiration från FN:s *Sustainable Development Goals* (SDG) och syftar till att definiera de nödvändiga tekniska, rättsliga och politiska ramarna samt de kapacitetsbyggande åtgärder som behövs för implementering på nationell nivå och för att inspirera till kollektiva åtgärder globalt. Det kan exempelvis röra sig om utvecklandet av nationella cybersäkerhetsstrategier, inrättandet av samarbetsmekanismer för att myndigheter och näringsliv gemensamt ska kunna upptäcka och hantera incidenter och att få till stånd den lagstiftning som behövs för att effektivt bekämpa cyberbrottslighet.

Läs mer om ICC:s prioriteringar på cybersäkerhetsområdet i arbetsgruppens policypapper:

ICC Policy Primer on Cybersecurity

ICC Cybersecurity Issue Brief #1

ICC Cybersecurity Issue Brief #2: Implementing norms and rules for responsible state behaviour in cyberspace and enhancing cooperation to counter cybercrime

För ICC:s arbetsgrupp blir nästa steg att med hjälp av inspel från vårt globala nätverk vidareutveckla konceptet CDG till ett konkret ramverk och med det som grund fortsätta företräda näringslivets intressen i FN:s arbete. Betydelsen av gemensamma cyberutvecklingsmål för en stabil och uthållig utveckling inom cyberrymden är stor inte minst för en fortsatt framgångsrik digitalisering. Men helt centralt är att cyberutvecklingsmålen kan bidra till att bryta både den negativa trenden av ökade cyberattacker och den normaliseringen som finns kring den hotbild som företagen står inför.

– Rene Summer, Ericsson

Vill du veta mer om ICC:s arbete inom cybersäkerhet och hur du kan engagera dig i utvecklandet av Cyber Development Goals? Kontakta vår policykoordinator Alfred Ram på alfred.ram@icc.se