Cyberförsvarsdagen 2018
Upptakt & Nuläge

Richard Oehme
Director
Cyber Security & Critical Infrastructure Protection

Findings from PwC's 2018 CEO Survey

Even though global economic volatility is no longer keeping CEOs up at night, they can't get complacent. If anything, they should take this opportunity, when growth prospects are good, to shore up other parts of their business that may be lagging behind. For example, US CEOs now rank cyber threats (63%), over-regulation (55%), terrorism (50%), and geopolitical uncertainty (50%) as their top concerns for 2018.

And while CEOs can't control over-regulation, terrorism, or geopolitical uncertainty, they certainly can put in place the safety protocols to protect against online hacks and cyberattacks.

Det sårbara samhället

Sverigebilden…

Myndigheten för samhällsskydd och beredskap

Detta är vad som varje dag ska fungera och ytterst kunna försvaras - och allt är digitaliserat…

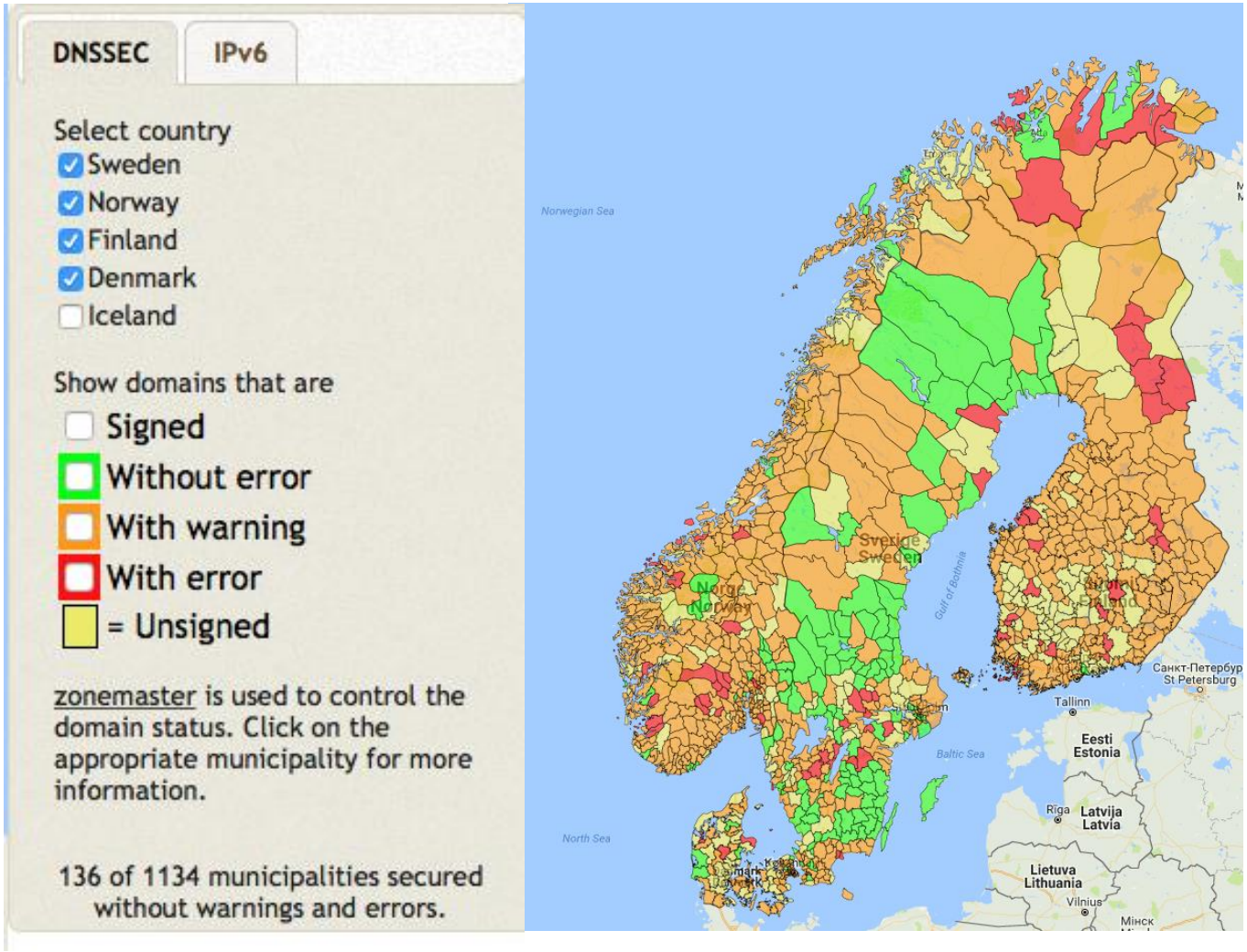
Sverige

10 053 061 inv.
(juni 2017)

- 20 landsting, varav 13 har regionstatus
- 290 kommuner
- 442 myndigheter, varav 238 statliga förvaltningsmyndigheter
- 4 militärdistrikt
- 7 polisregioner
- 45 flygplatser som möjliggör ca 367 000 landningar med ca. 36 miljoner passagerare
- Ca 1200 vårdcentraler och ca 90 sjukhus till ca 4 miljoner patienter och ca 13 miljoner vårdbesök
- 35 högskolor & universitet
- Ca. 1,6 miljarder påstigningar i kollektivtrafiken
- Ca. 1,58 miljoner .se-domäner
- 1 200 106 företag, 50% med minst 10 anställda använder molntjänster
- Ca 140 elbolag som möjliggör svenskarnas elförbrukning om 15MWh per invånare och år
- Ca 600 teleoperatörer som bl.a. tillhandahåller 13,5 miljoner internetabonnemang och 14,6 miljoner mobila teletjänster
- Ca 2400 finansbolag, 3 miljarder kortköp
- Ca 1750 vattenverk som förser varje invånare med 160 liter vatten per dygn, motsvarande ~587 miljarder liter per år
- 164 dagstidningar, 340 minuter mediekonsumtion per person och dag

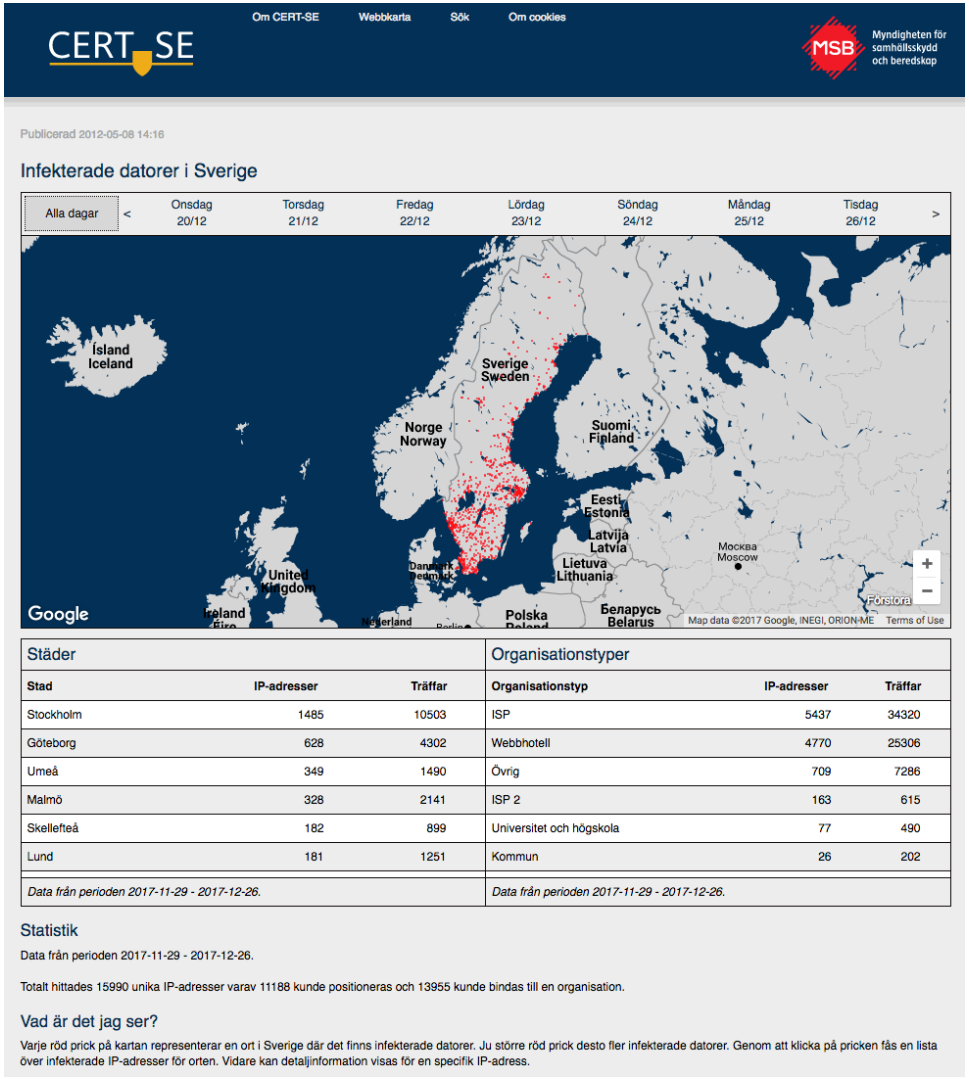
Källor: SKL, SCB [1], [2], [3], Trafikanalys [1], [2], [3], Socialstyrelsen, IIS [1], [2], Elskling.se, Energiföretagen, Hitta.se, Riksbanken, PTS, Svenskt vatten, Nordicom, Myndigheten för radio och tv

Sverigebilden – Exempel:
- Brister i DNSSEC hos kommuner



Källa: https://kommunermeddnssec.se/

Sverigebilden – Exempel:
- Infekterade datorer i Sverige - MSB/CERT-SE



CERT SE

Om CERT-SE Webbkarta Sök Om cookies

MSB Myndigheten för samhällsskydd och beredskap

Publicerad 2012-05-08 14:16

Infekterade datorer i Sverige

Alla dagar < Onsdag 20/12 Torsdag 21/12 Fredag 22/12 Lördag 23/12 Söndag 24/12 Måndag 25/12 Tisdag 26/12 >

Städer			Organisationstyper		
Stad	**IP-adresser**	**Träffar**	**Organisationstyp**	**IP-adresser**	**Träffar**
Stockholm	1485	10503	ISP	5437	34320
Göteborg	628	4302	Webbhotell	4770	25306
Umeå	349	1490	Övrig	709	7286
Malmö	328	2141	ISP 2	163	615
Skellefteå	182	899	Universitet och högskola	77	490
Lund	181	1251	Kommun	26	202
Data från perioden 2017-11-29 - 2017-12-26.			*Data från perioden 2017-11-29 - 2017-12-26.*		

Statistik

Data från perioden 2017-11-29 - 2017-12-26.

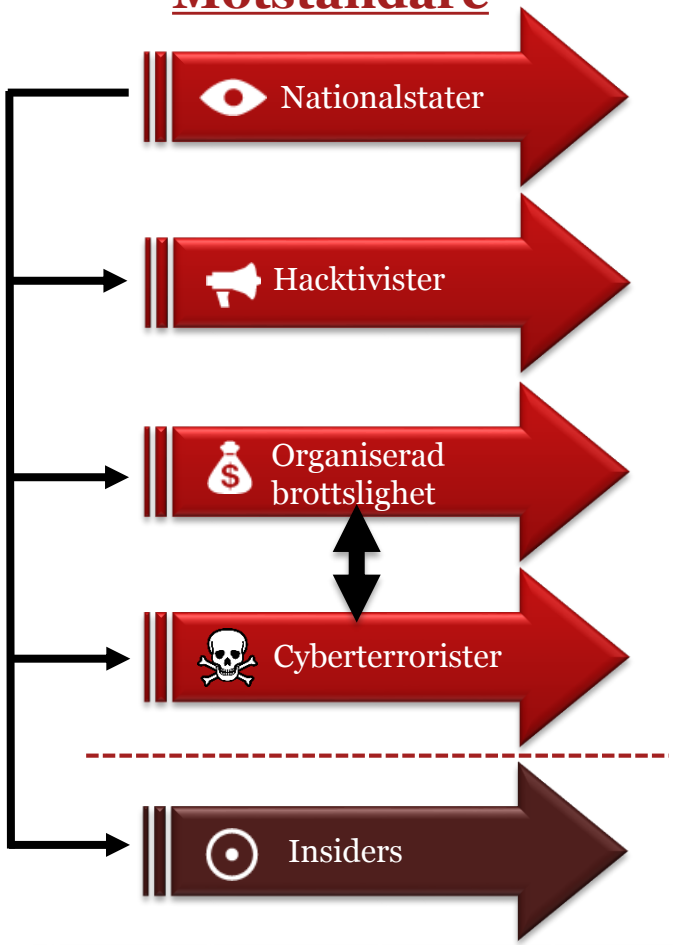
Totalt hittades 15990 unika IP-adresser varav 11188 kunde positioneras och 13955 kunde bindas till en organisation.

Vad är det jag ser?

Varje röd prick på kartan representerar en ort i Sverige där det finns infekterade datorer. Ju större röd prick desto fler infekterade datorer. Genom att klicka på pricken fås en lista över infekterade IP-adresser för orten. Vidare kan detaljinformation visas för en specifik IP-adress.

Antagonisterna och deras mål

Motståndare



Vad står på spel?

Exempel

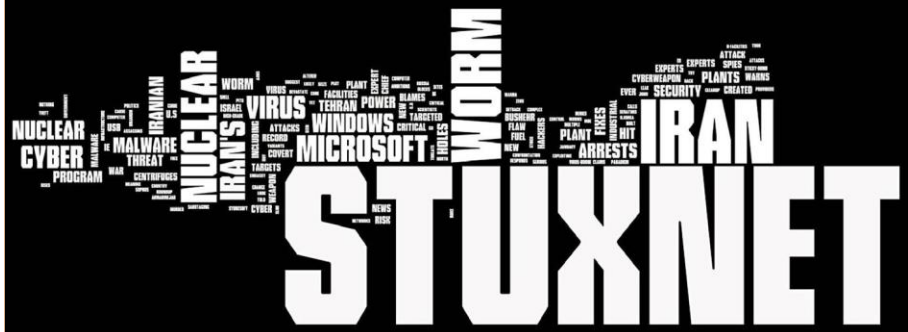
- Industriella informations- och styrsystem (SCADA)
- Tillväxt-teknologier
- Kreditkort/ finansmarknaden
- Avancerade material- och tillverkningsprocesser
- Energisystem
- Forskning och utveckling
- Hälso- och sjukvård, läkemedel och relaterad teknologi
- Information om affärsavtal
- Patientdata och övriga personuppgifter
- Informations- och kommunikations-teknologi

Antagonisterna utvecklar motiv, modus och mål beroende på den angripna orgaisationens produkter och tjänster.

Brytpunkten som alla tänker på…

Stuxnet

(Avsiktligt och mycket avancerat)



Riktad attack mot urananrikningsanläggning i Iran.

Genom att slumpmässigt ställa om hastigheten på ett antal centrifuger försenade angriparen irans program för anrikning av uran med två år…

Cloud Hopper – angrepp från Kina riktad till driftsleverantörer

ComputerSweden
FROM IDG

CSJOBB BRANSCH EVENT WHITEPAPERS NYHETSBREV

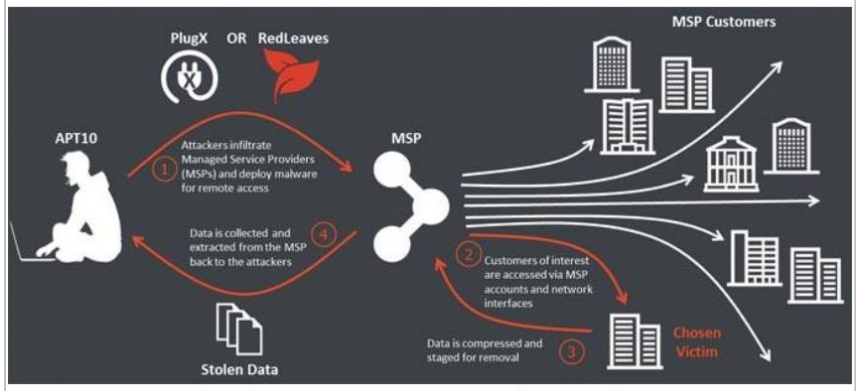
ANNONS

Av: Sophia Nilsson 2017-04-05 09:54

Kinesisk hackargrupp bakom massivt cyberangrepp mot svenska företag

Svenska företag har drabbats i ett omfattande internationellt cyberangrepp. Hackargruppen bakom, kinesiska APT10, har särskilt riktat in sig på driftleverantörer i ett flertal länder världen över.

Bakom rapporten står två företag i säkerhetsbranschen, brittiska försvarskoncernen BAE System och revisionsföretaget Pwc:s it-säkerhetsavdelning. Enligt deras granskning är anledningen till måltavlan främst underleverantörernas direkta tillgång till kundernas nätverk. Hackargruppen, som i säkerhetsvärlden kallas APT10, ska bland annat ha kommit över stora mängder interna dokument och data såsom immateriella tillgångar från de interna nätverk de kommit in i.



Så här har attackerna gått till enligt BAE System och Pwc:s it-säkerhetsavdelning.

Proliferation in cyberspace…

“ in 2013 you don’t need to know Assembly to generate undetected pieces of malware. You don’t need to utilize zero day vulnerabilities to infect tens of thousands of people on a daily basis. And in cases where you seek malicious innovation, coding malware for hire services are there to “take care”.”

Dancho Danchev, Webroot

Bygg ditt eget attackverktyg utan egentlig egen kunskap – klick för klick…

Steg 1.
- Generella val

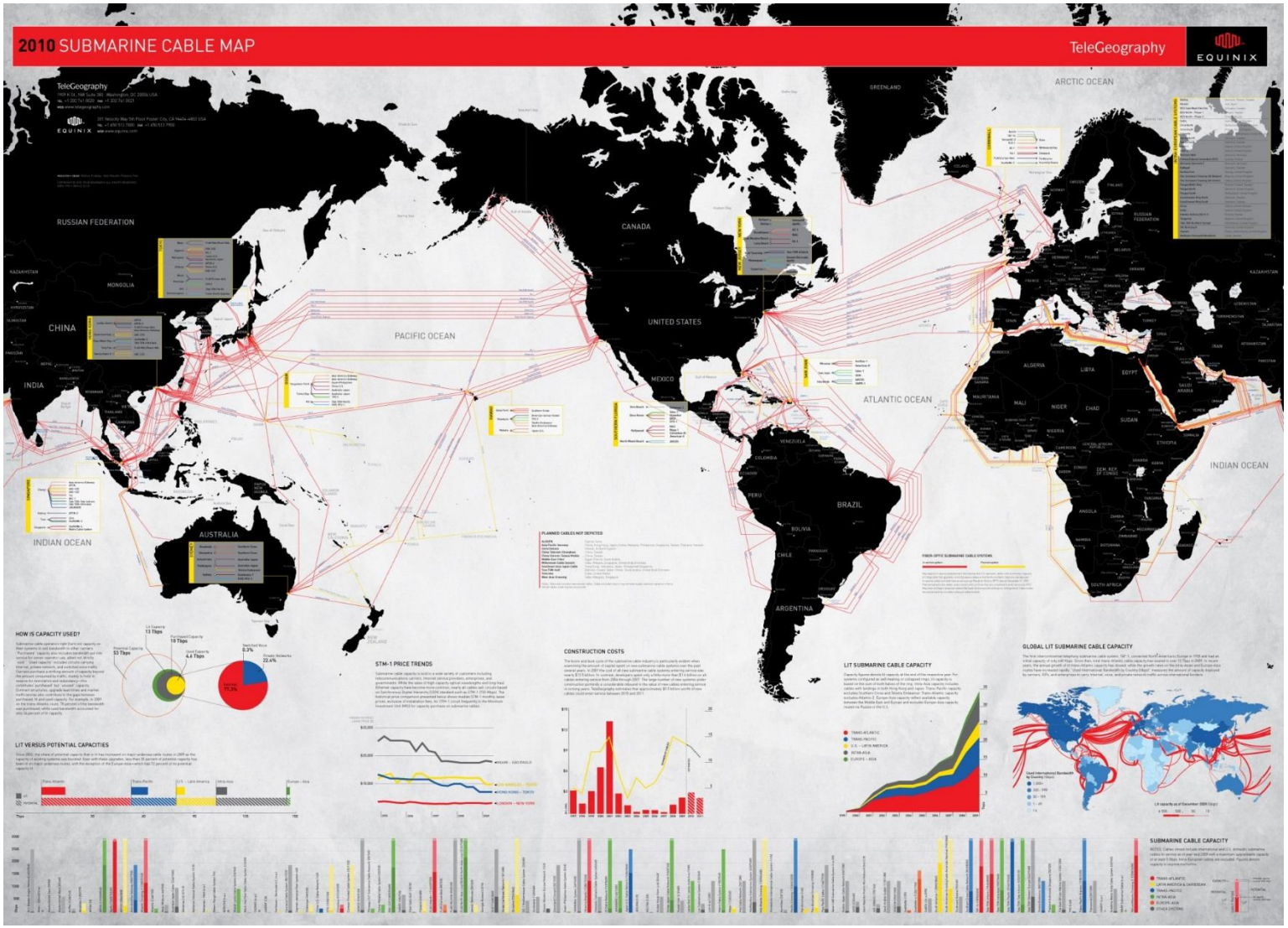
Steg 2.
- Val av spridningsfunktion

Steg 3.
- Inmatning av applikationsinformation

Steg 4.
- Andra val; exv. Typ av Ikon, radering, i autostart mappen

Steg 5.
- Leverans via e-post, USB etc.

Globala beroende



Kartan kommer från: Telegeography https://www.telegeography.com/

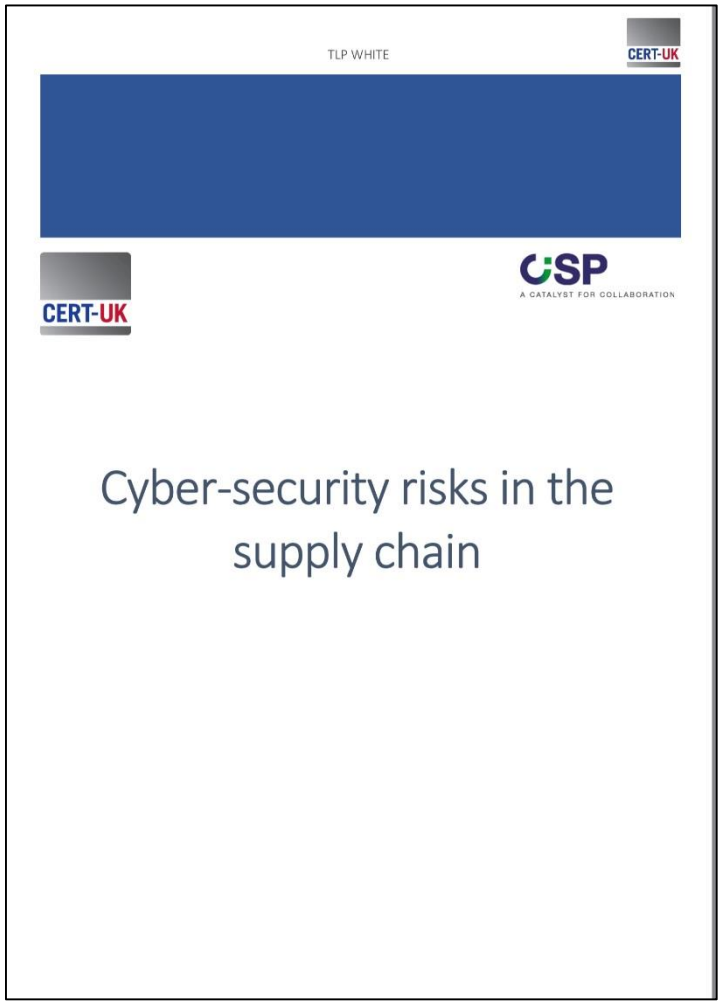
Globala beroende (forts.)

Cyber supply chain risks

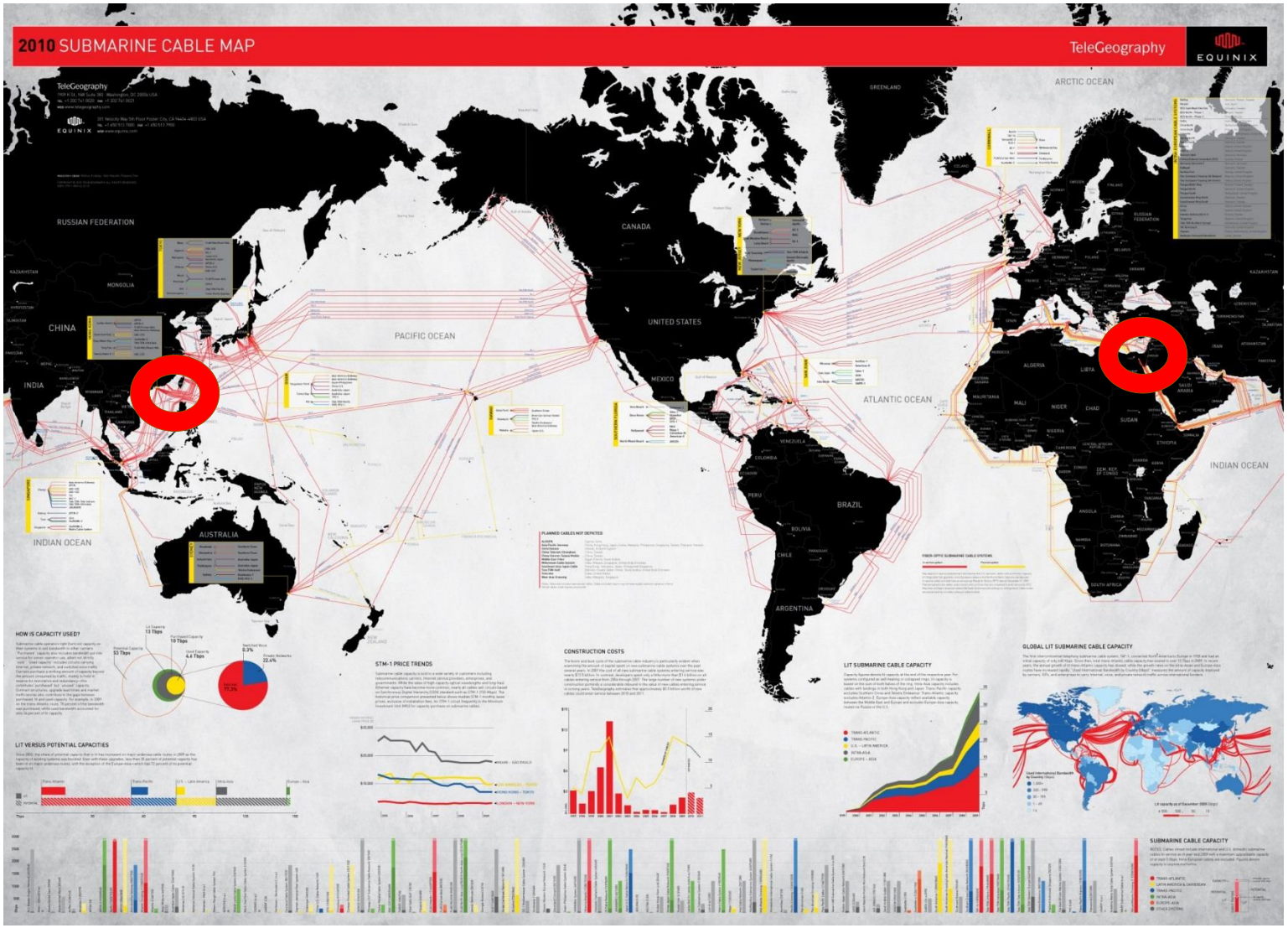
Globala oöverskådliga beroenden har skapats genom de senaste åren av accelererande digitalisering.

– Svenska företag och offentliga organisationer har inte i tillräcklig utsträckning analyserat de hot- och risker som uppstått på grund av detta.

– Antagonister kommer inrikta sig på de svagheter som finns i denna kedja…



Globala beroende (forts.)



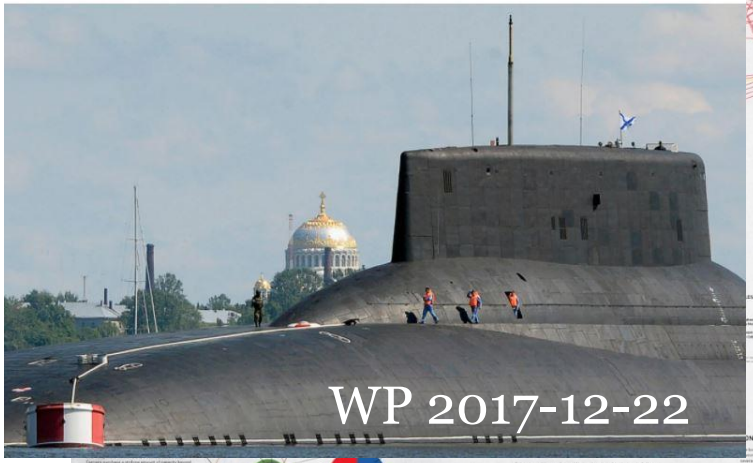
Kartan kommer från: Telegeography https://www.telegeography.com/

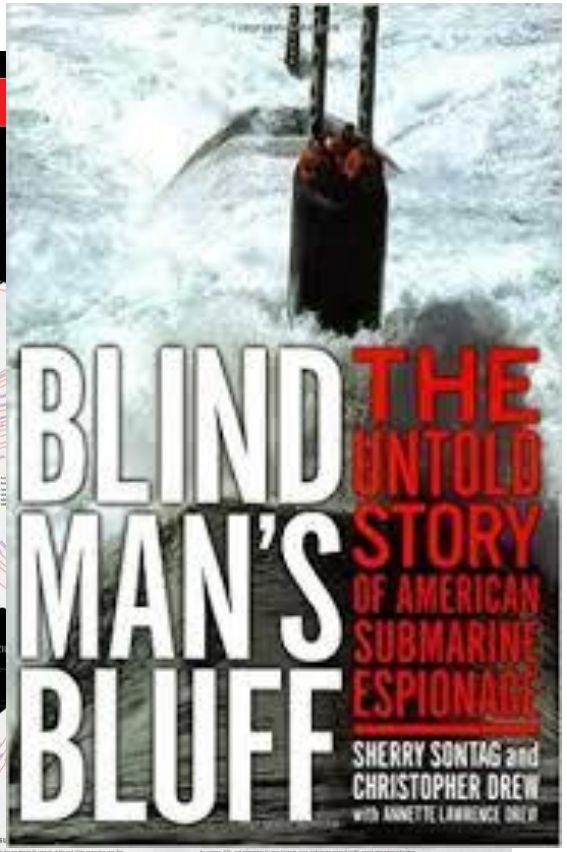
Globala beroende (forts.)

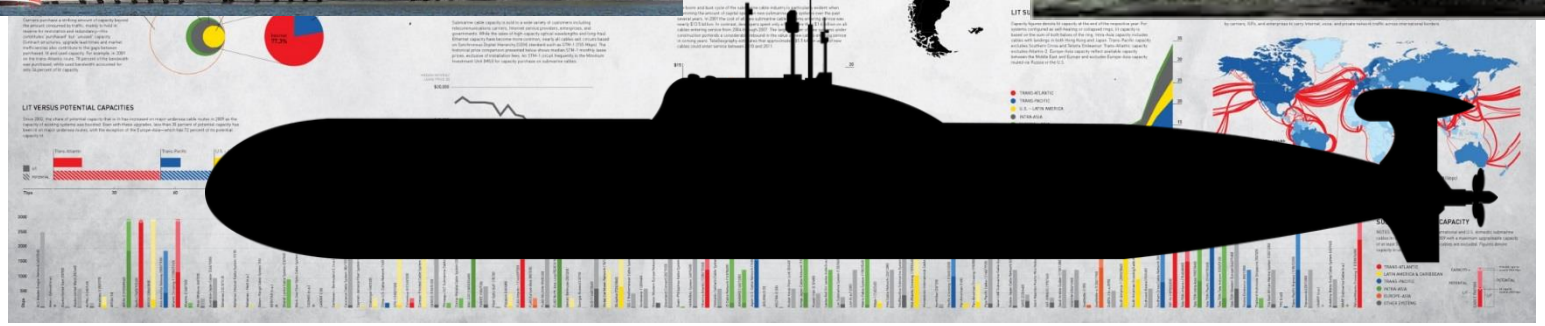
The Washington Post
Democracy Dies in Darkness

Europe

Russian submarines are prowling around vital undersea cables. It's making NATO nervous.

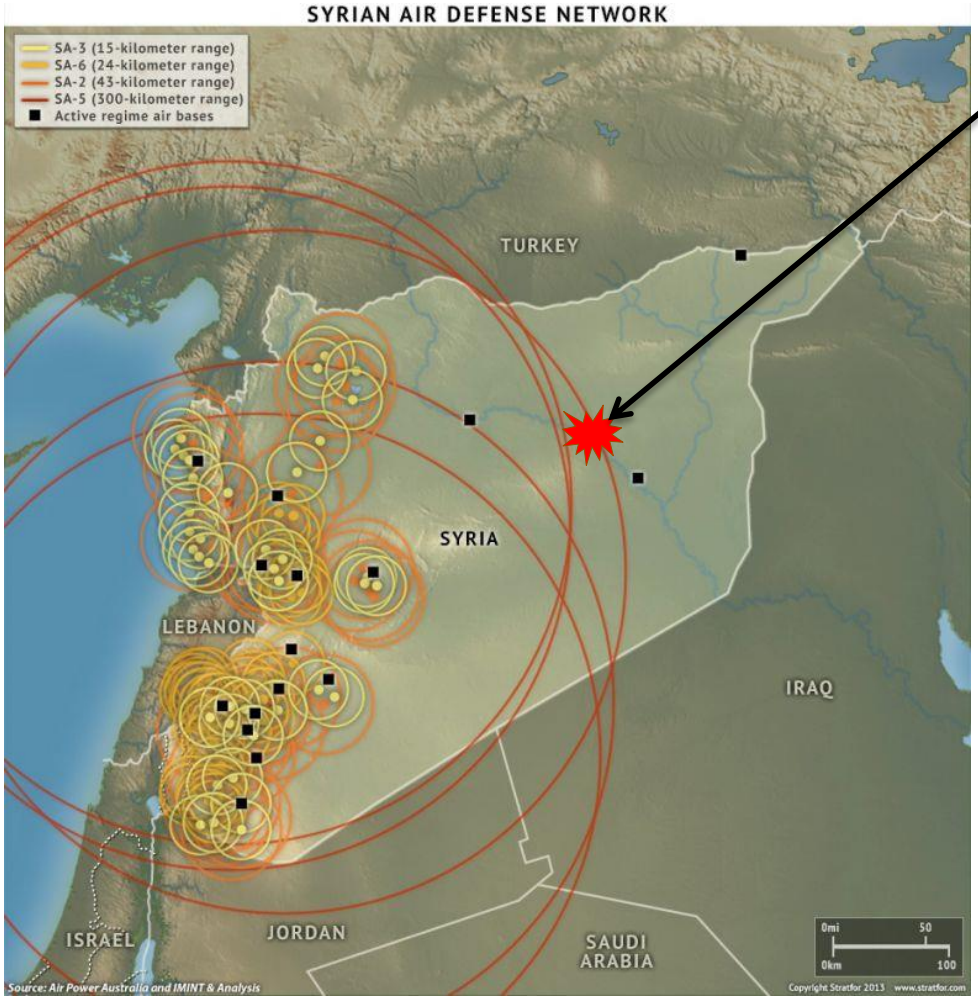




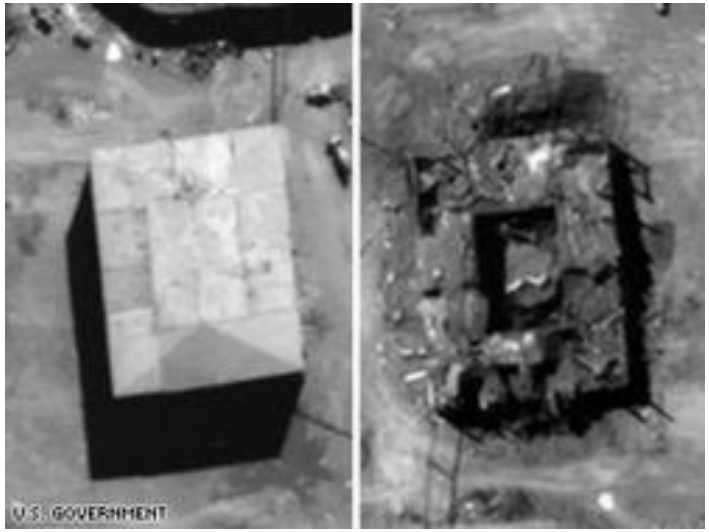


Kartan kommer från: Telegeography https://www.telegeography.com/

Operation Orchard – 6 september 2007 - Israel slår ut syriskt luftvärn…

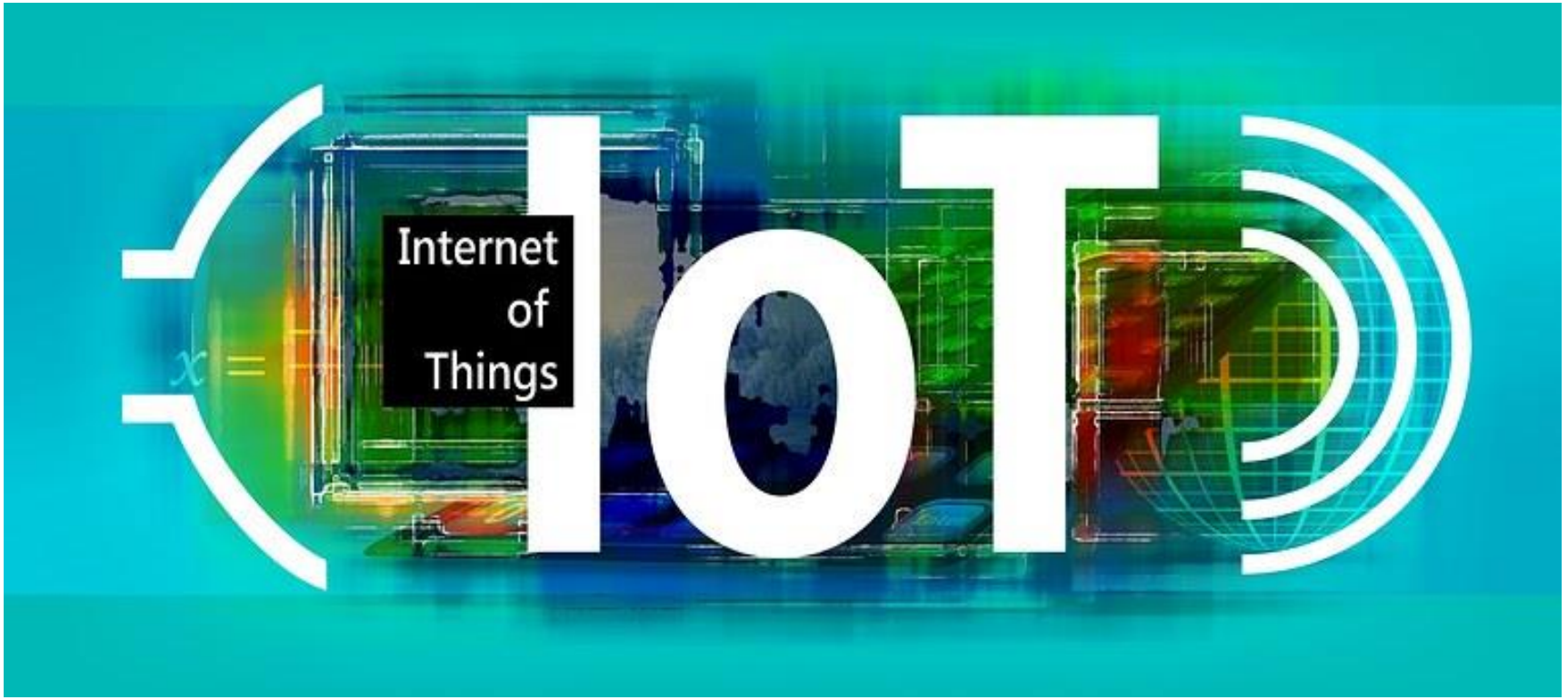


Al Kibar-anläggningen - Före och efter



Källa: Wikipedia

Och så har vi avslutningsvis…



www.pwc.se

Tack!

Richard Oehme
Director
Cyber Security & Critical Infrastructure Protection

Email: richard.oehme@pwc.com
Twitter: @RichardOehme
LinkedIn: www.linkedin.com/in/richard-oehme-a17445153

pwc