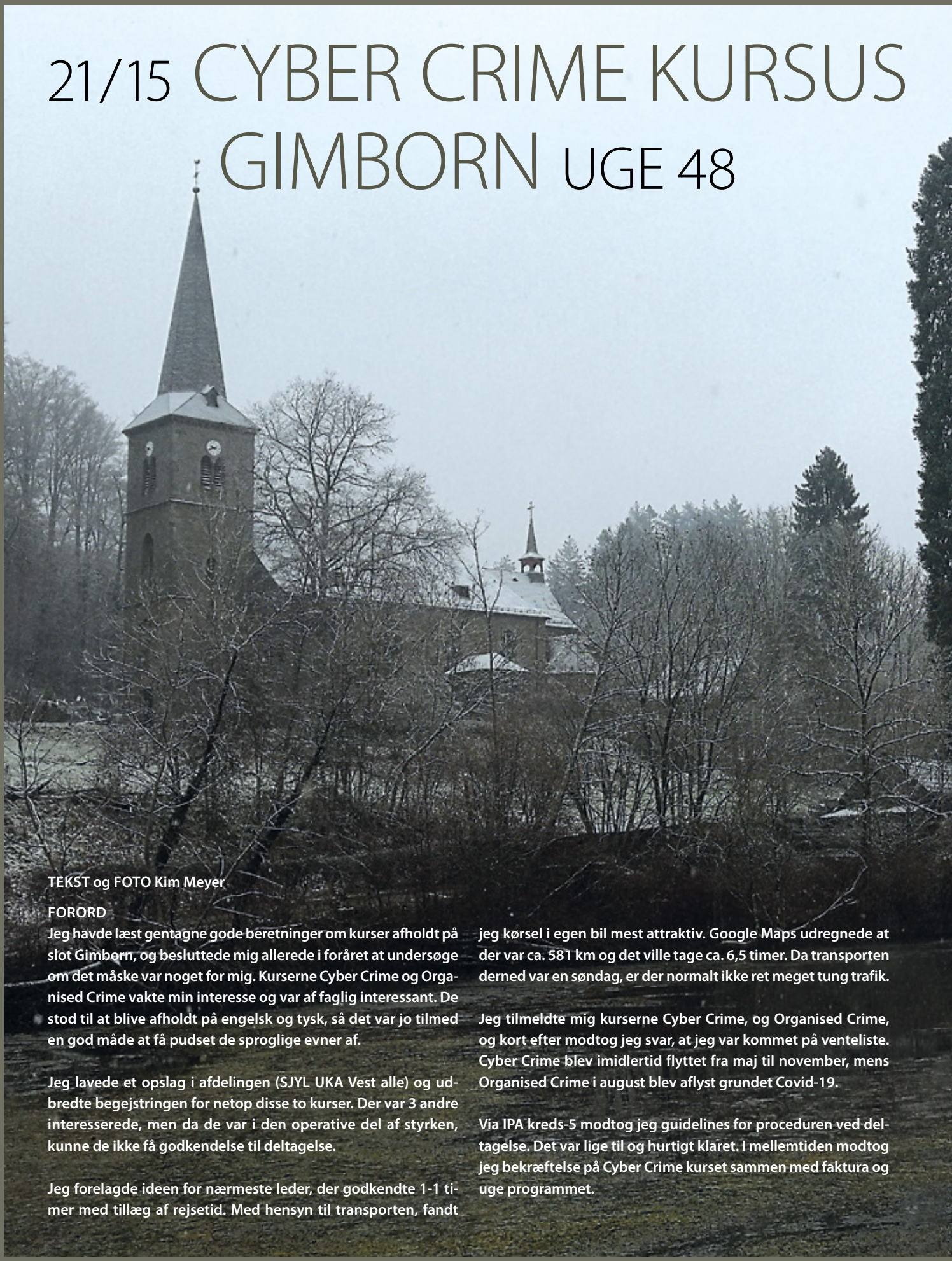
21/15 CYBER CRIME KURSUS GIMBORN UGE 48



TEKST og FOTO Kim Meyer

FORORD

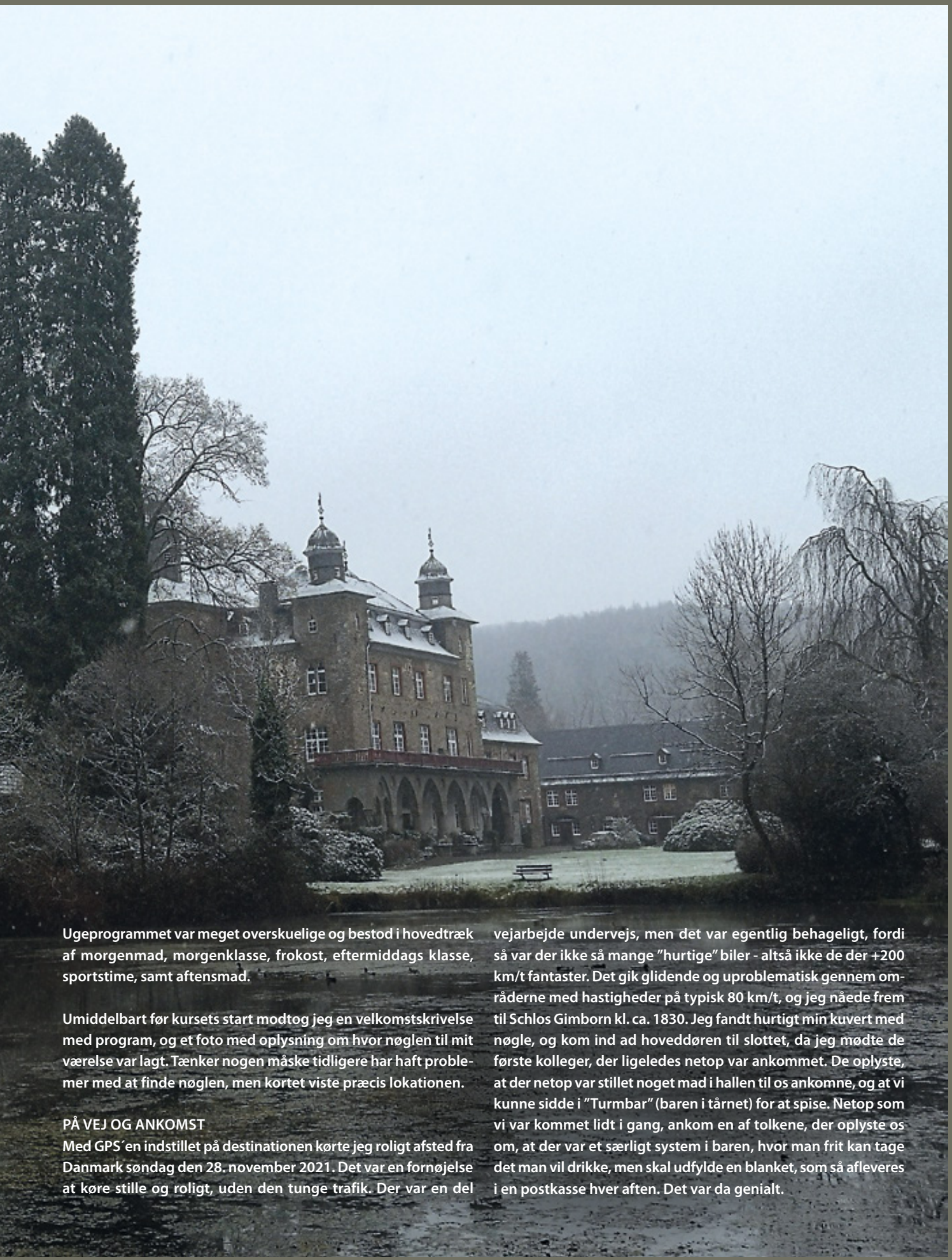
Jeg havde læst gentagne gode beretninger om kurser afholdt på slot Gimborn, og besluttede mig allerede i foråret at undersøge om det måske var noget for mig. Kurserne Cyber Crime og Organised Crime vakte min interesse og var af faglig interessant. De stod til at blive afholdt på engelsk og tysk, så det var jo tilmed en god måde at få pudset de sproglige evner af.

Jeg lavede et opslag i afdelingen (SJYL UKA Vest alle) og udbredte begejstringen for netop disse to kurser. Der var 3 andre interesserede, men da de var i den operative del af styrken, kunne de ikke få godkendelse til deltagelse.

Jeg forelagde ideen for nærmeste leder, der godkendte 1-1 timer med tillæg af rejsetid. Med hensyn til transporten, fandt jeg kørsel i egen bil mest attraktiv. Google Maps udregnede at der var ca. 581 km og det ville tage ca. 6,5 timer. Da transporten derned var en søndag, er der normalt ikke ret meget tung trafik.

Jeg tilmeldte mig kurserne Cyber Crime, og Organised Crime, og kort efter modtog jeg svar, at jeg var kommet på venteliste. Cyber Crime blev imidlertid flyttet fra maj til november, mens Organised Crime i august blev aflyst grundet Covid-19.

Via IPA kreds-5 modtog jeg guidelines for proceduren ved deltagelse. Det var lige til og hurtigt klaret. I mellemtiden modtog jeg bekræftelse på Cyber Crime kurset sammen med faktura og uge programmet.



Ugeprogrammet var meget overskuelige og bestod i hovedtræk af morgenmad, morgenklasse, frokost, eftermiddags klasse, sportstime, samt aftensmad.

Umiddelbart før kursets start modtog jeg en velkomstskrivelse med program, og et foto med oplysning om hvor nøglen til mit værelse var lagt. Tænker nogen måske tidligere har haft problemer med at finde nøglen, men kortet viste præcis lokationen.

PÅ VEJ OG ANKOMST

Med GPS´en indstillet på destinationen kørte jeg roligt afsted fra Danmark søndag den 28. november 2021. Det var en fornøjelse at køre stille og roligt, uden den tunge trafik. Der var en del vejarbejde undervejs, men det var egentlig behageligt, fordi så var der ikke så mange "hurtige" biler - altså ikke de der +200 km/t fantaster. Det gik glidende og uproblematisk gennem områderne med hastigheder på typisk 80 km/t, og jeg nåede frem til Schlos Gimborn kl. ca. 1830. Jeg fandt hurtigt min kuvert med nøgle, og kom ind ad hoveddøren til slottet, da jeg mødte de første kolleger, der ligeledes netop var ankommet. De oplyste, at der netop var stillet noget mad i hallen til os ankomne, og at vi kunne sidde i "Turmbar" (baren i tårnet) for at spise. Netop som vi var kommet lidt i gang, ankom en af tolkene, der oplyste os om, at der var et særligt system i baren, hvor man frit kan tage det man vil drikke, men skal udfylde en blanket, som så afleveres i en postkasse hver aften. Det var da genialt.

PROGRAMMET

Mandag

Velkomst og intro af Gimborn management, kursets leder, og gennemgang af uge programmet, samt en kort præsentation af deltagerne, hvor vi udvekslede erfaringer og forventninger til kurset. Grundet den særlige situation med Covid-19 var der installeret teknik til måling af lufttætheden, og at vi skulle lufte ud, og skulle vi gå nogen steder, var det med mundbind. Allerede i den første time røg der en alarm fra måleudstyret, hvorefter vi aftalte, at vi luftede ud hver halve time. Det var godt nok koldt, men en rigtig fornuftig beslutning.

Vi var deltagere Sverige, Ungarn, Malta, Estland, Sri Lanka, Schweiz, Danmark, samt 2 fra Japan og 22 fra Tyskland, plus kursusleder og 2 tolke i lokalet. Vi var jo alle mødt op med en frisk negativ PCR test, men det gav alligevel anledning til bekymring, idet deltagerne fra Japan og Sri Lanka jo ikke kom direkte hjemmefra, fordi de havde mellemlandet i flere lufthavne undervejs, og var ikke at regne som "helt clean" som vi andre. Der blev sørget for hurtig test til dem, og så kunne vi komme rigtig i gang.

Eftermiddagsprogrammet var online-class fordi underviseren fra Univ. of Portsmouth, UK, grundet Covid-19 ikke kunne risikere udrejse, for så skulle han i karantæne ved hjemkomst. Vi blev informeret om status på Cyber Crime Awareness, samt trends og udfordringer, så som fake news og propaganda, hacking via Cayla Dolls, som ingen af os før havde hørt om. En dukke der via Bluetooth kunne kommunikere eller spionere, fordi der var installeret kamera og mikrofon, og kunne styres udefra. Den var således en "uskyldig" dukke, som ingen regnede med kunne bruges til spionage. Men det var der adskillige beretninger på var sket.

Tirsdag

Online Sex offenders' behavior and impact on victims + Online Child Sexual Abuse – Policing, Investigation, Prevention and Management. Undervisningen blev holdt af Dr. Elena Martellozzo, der I 15 år havde lavet analyser for Scotland Yard. Emnet i sig selv er jo vældig interessant og lige nu meget oppe i tiden, hvis man skal sammenligne med de grooming sager vi netop lige har haft i Danmark, hvor unge piger enten presses til selvskade, gøre noget mod deres vilje, eller udveksler nøgenfotos osv., fordi de sidder i en klemme, som de ikke tør fortælle idet risikoen for den trussel som gerningsmanden har oplyst dem om, vil ødelægge deres liv. Det var et uhyggeligt tema især når vi ved at disse perverse magtsyge drenge/mænd findes globalt. Vi blev hurtigt enige om at netop dette tema kræver tæt internationalt samarbejde. Her vil jeg gerne henvise til en side som vi også i Danmark har gavn af at bruge: https://www.iwf.org.uk/

Hvis du har mod på at læse årsrapporten, er den her www.iwf.org.uk/about-us/who-we-are/annual-report/

Internet Watch Foundation (IWF) søger nettet igennem for materiale, og i 2020 fandt de 153.350 tilfælde, der kategoriseres som Child Sexual Abuse. Det er både webpages og ny-

hedsgrupper der gennemgås, og der er sket en stigning på 16 % i forhold til 2019, Det er skræmmende tal. Man kunne tænke sig, at Covid-19 situationen har lænket flere hjemme foran skærmen, og derved har der været længere skærmtid end normalt. Det har således givet gerningsmændene længere tid til at infiltrere og udfinde potentielle ofre.

Onsdag
Cybercrime investigation, Oberstaatsanwaltin Angela Komp, Center for Cybercrime, Nordrhein Westfalen, Køln. Gennemgang af det juridiske nødvendige for opstart og gennemførelse af rets- og strafforfølgelse, herunder div. kendelser, retshjælpsanmodninger til/fra udlandet. Her blev min viden om generel eller international retsplejelov opfrisket, og det er ganske omfangsrigt at lægge fundamentet til en international efterforskning.

The Darknet – Investigations, Cpi. Holger Martin, Bundeskriminalamt. Jeg blev så opslugt af emnet at jeg faktisk dårligt nåede at tage noter. Isbjergsoversigten illustrerer det som vi kender, og kaldes Surface Web. Det er ca. 4 % af det der findes på internettet. Siderne indekseres (får en overskrift eller titel) således at en browser som fx Google, Bing, Wikipedia, kan finde det.

Deep Web kan ikke søges direkte via en søgemaskine, men det er her man kan hacke virksomheders dokumenter, journaler, offentlige institutioner, databaser og log-on adgange, og indsætte en Malware, der gør at en virksomheds netværk kan overtages. Det skete faktisk også for danske Mærsk, der blev angrebet af NotPaytya, der kostede Mærsk 1,9 mia kroner. Spørgsmålet om det kan undgås er lidt irrelevant, for med mindre man er konstant vågen over for systemerne, vil der før eller siden være nogen der forsøger og endog bliver heldige med at overtage dit system.

Dark Web er ca. 6 % at indholdet på nettet, og er stedet hvor der føres private samtaler (man skal inviteres), forbudte sager (våben, narko, menneskehandel, børneporno) og krypterede sider. Her skal man have sin egen dynamiske VPN (Virtual Privat network) og en Onion router (TOR). Med TOR browseren kan man finde sider på det man ønsker at købe, men man har ingen garanti for hvem man handler med. Den mest kendte side for stoffer hed Silkroad og blev fornyligt lukket, men genopstår lige så hurtigt med nyt navn. Det er nærmest umuligt at lukke noget ned, fordi man i lukkede forum kan formidle i sit netværk, hvor man så kan købe det man ønsker. Børneporno er et lidt lukket territorie, og skulle man som myndighed forsøge sig adgang, vil man fx skulle kunne bytte børnepornografisk materiale, og det kan vi ikke som politimyndighed, da det jo er ulovligt at besidde eller distribuere, og for den sags skyld også at udstille en person igen og igen.

Aftenprogrammet var en tur til Køln, hvor en pensioneret kollega gav os en aldeles sjov og interessant byvandring til domkirken, rådhuset, julemarkedet og slutteligt til en bryggerirestaurant, hvor der var en særlig skik. Tjenerne var kvikke i replikken, og de kom konstant forbi med nye øl. Fidusen var at såfremt man ikke ønskede en ny øl, så skulle man sætte ølbrikken over glasset. De slog en blyantstreg for hver øl man havde fået. Det var lidt morsomt, for da jeg havde lyst til en dessert, ville jeg bestille kaffe dertil, hvorpå tjeneren noterede en bødestraf på 25 Euro på min ølbrik for ikke at drikke øl, men det var dog kun for sjov. Vi gik forbi flere julemarkeder, men ingen af os ønskede at gå derind grundet smitte risiko. Men det var flot på afstand,

Torsdag
Tools for investigators v/Nils Padeken, Task Force Cybecrime, Oldenburg.
Her blev vi introduceret for https://www.ripe.net/ som er en vigtig side hvis du skal finde en IP adresse, og hvis man skal vide noget fra udbyder, er port og tidsstemplet med tidszone særligt vigtigt. Det er således at man kan indhente data fra en PC i et firma netværk, hvis man kender port og tid. Det er faktisk temmelig fascinerende at tænke, at man fx i en virksomhed som Børsen, kan få adgang til at se det som en operatør har handlet eller indtastet på et givent tidspunkt. Andre rigtig gode sider:
www.virustotal.com - www.whois.net - www.gaijin.at

I sidstnævnte vil man kunne finde oplysninger om der forefindes en TOR exit note på din PC, og hvis man i forvejen har en Entry note (det du har kigget på) har man et godt udgangspunkt for at finde den nøjagtige vej for det man har søgt. Altså hvis man på en beslaglagt PC finder fx børneporno, vil det være muligt at finde hele netværket det har været på, fordi der på dark web mindst er 3 servere der leverer produktet. Man har en forespørgsel som går til første server, hvor forespørgslen får en entry note, der leverer videre til server 2, som ikke ved hvad indholdet er, men sender beskeden videre til server 3, der finder det man søger, og sender det retur med en exit note. Serveren i midten ved ikke hvad den har sendt videre, og det er kun entry og exit note der er vigtige.

Fredag
Jeg fik kontoret til at bestille en Covid-19 hurtig test i nærmeste lille by, således at jeg kunne rejse hjem til familien med negativt resultat. Ikke fordi nogen var smittet, men fordi jeg ville være sikker over for familien. Formiddagen blev brugt på evaluering og afrundende spørgsmål, hvorefter vi fik udleveret diplom for gennemførelse af kurset. Herefter frokost på slotskroen og så ellers afsted hjemad.

HJEMTUREN
GPS´en var igen indstillet på hurtigste vej hjem, og så var det ellers mod nord. Jeg lyttede til en lokalradio, der udsendte trafikmelding om en motorvejsbro, der var blevet lukket grundet risiko for sammenstyrtning, idet man havde fundet noget rust ved en laser undersøgelse. Det blev oplyst, at trafikken var nærmest kaotisk i de tilstødende byer omkring broen. Så uden at vide helt nøjagtigt hvor jeg var, besluttede jeg at holde ind på en rasteplads lige før jeg skulle på motorvejen. Og det var en god ide, for det var dæleme den strækning jeg skulle ind på. Der var 30 km kø, og kaos i byerne omkring, så jeg besluttede at køre 2. parallelvej udenom, således ind over Dortmund op til Ruhr distriktet ad landeveje. Det tog godt 3 timer længere, men jeg holdt ikke stille. Det tog 10,5 time at komme hjem.