# Øvelsesplanlegger

Pakke 1 øving 1

## «*Sosial manipulering*»

Utgave 1 .0

## Innholdsfortegnelse

# 1 Innledning

## 1.1 Bakgrunn og formål

Anlegg og installasjoner i petroleumssektoren skal ha beredskapsplaner for håndtering av uønskede hendelser. Næringen har scenarioer som kan knyttes til IKT-hendelser men Havindustritilsynet (Havtil) har i tilsyn sett at det knapt trenes innen IKT-sikkerhet for de industrielle kontroll- og sikkerhetssystemene. Derfor har Havtil fått utarbeidet et sett med trenings- og øvelsesscenarioer. Dette øvelses-opplegget ble utarbeidet av Proactima med Netsecurity som partner. Opplegget er videre bearbeidet av Havtil.

Aktivitetsforskriften § 23 beskriver at «det utføres nødvendig trening og nødvendige øvelser, slik at personellet til enhver tid er i stand til å håndtere operasjonelle forstyrrelser og fare- og ulykkessituasjoner på en effektiv måte». Samme formulering finnes også i teknisk og operasjonell forskrift § 52. Det er altså samme krav til trening og øvelser for anleggene på land som det er til innretningene på sokkelen.

Når vi trener, øker vi personlige ferdigheter og kunnskaper. Øvelser tester samhandling og beredskapsevne, avdekke styrker og svakheter, samt forbereder ledelsen på å håndtere ulike kriser.

## 1.2 Oppbygging av veilederen

Øvelsesplanleggeren inneholder scenarioer, og det er foreslått hvilke funksjoner som er aktuelle å inkludere i øvelsen. Scenarioene kan benyttes som trening, table top eller spilløvelse.

Veilederen har i del 3 ekstra informasjon til forberedelse og gjennomføring så som:

- et mulig hendelsesforløp i forkant av startpunkt
- sekvensskjema for hendelsen
- relevant fagstoff

# 2 Scenario

Scenariet for denne veilederen er at trusselaktør benytter sosial manipulering for å få tilgang inn i virksomheten for videre å kunne gjennomføre målrettede aktiviteter mot SAS-nettverket og de industrielle kontrollsystemene.

## 2.1 Oversikt scenarioer

I denne veilederen er det skissert hvordan en trusselaktør får fotfeste via sosial manipulering og kompromitterer kontrollsystemer på innretningen.
De neste punktene beskriver de videre stegene for å håndtere det målrettede cyberangrepet.

*Tabell 1 - Oversikt over hvem som kan trenes/øves i de ulike modulene*

| Oppgave | Tittel | SAS/IACS-ansvarlig | Lokal driftsledelse | System-ansvarlig drift | IKT-avdeling |
|---|---|---|---|---|---|
| **2.2** | Innledende forhold - Uregelmessigheter i SAS | x | x | x | x |
| **2.3** | Eskalering | | | x | x |
| **2.4** | Skadeomfang | | | x | x |
| **2.5** | Skadebegrensning | x | x | x | x |
| **2.6** | Gjenoppretning | | | x | x |

## 2.2 Innledende forhold – Uregelmessigheter i SAS

Det oppdages det en mindre uregelmessighet i et av kontrollsystemene. Dette blir rapportert til systemansvarlig drift, som klassifiserer dette som en tilfeldig hendelse. Tilsvarende hendelser gjentar seg, og det blir etter hvert oppdaget en feil på en sentral enhet. Det blir besluttet at den aktuelle enheten må byttes. En stund etter at den aktuelle enheten er byttet, er uregelmessighetene tilbake igjen.

### 2.2.1 Veiledende spørsmål

**SAS/IACS-ansvarlig**

- Hvordan håndteres uregelmessigheter i kontrollsystemene?
- Hvordan foregår varsling/informasjonsflyt?

**Lokal driftsledelse**

- Hva anses som normale uregelmessigheter i kontrollsystemene?

**Systemansvarlig drift**

- Hva anses som normale uregelmessigheter i kontrollsystemene?
- Hvem har ansvaret i en slik situasjon?

### 2.2.2 Leverandørdialog

I dialog med leverandør kommer det fram at det er rapportert tilsvarende hendelsesmønster fra anlegg med svake skiller mellom kontor- og industrinettverkene.

**SAS/IACS-ansvarlig**

- Hvilke svekkelser kan oppstå i skillet mellom kontor- og kontrollnettverkene?
  - PC med tilgang til begge nett?
  - Flyttbare medier?
  - Andre forhold?
- Hvordan beskytter rutinene for bruk av jobb-PC mot sosial manipulering? (bruk av privat e-post, nedlastning av vedlegg, installasjon av programvare, tilkobling med eksterne medier etc.)
  - Er rutinene godt nok dokumentert og fulgt opp?
  - Ble rutinene fulgt i tiden forut for uregelmessighetene i kontrollsystemene?

**Lokal driftsledelse**

- Hvordan beskytter rutinene for bruk av jobb-PC mot sosial manipulering? (bruk av privat e-post, nedlastning av vedlegg, installasjon av programvare, tilkobling med eksterne medier etc.)
  - Er rutinene godt nok dokumentert og fulgt opp?

**Systemansvarlig drift / IKT-avdeling**

- Hvilke muligheter har det vært for svekkelser i skillet mellom kontor- og industrinettverkene?
  - PC med tilgang begge nett?
  - Flyttbare medier?
- Hvilke systemlogger kan bistå i å identifisere slike forhold?
- Hvordan beskytter rutinene for bruk av jobb-PC mot sosial manipulering?

### 2.2.3 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Hvordan avdekke at et avvik skyldes skadevare?
- Hvordan kan organisasjonen øke motstandsdyktigheten mot sosial manipulering?

## 2.3 Eskalering

IKT-avdelingen utfører analyse av engineeringsstasjonen. Etter reinstallering settes den tilbake i kontrollnettet. Det viser seg at systemet fortsetter å oppføre seg unormalt.

### 2.3.1 Veiledende spørsmål

**Systemansvarlig drift /IKT-avdeling**

- Hvordan reinstallerer vi engineeringsstasjonen?
- Hvordan kan angrepet fortsette etter at engineeringsstasjonen er reinstallert?
- Kan skadevaren ha spredd seg til andre maskiner?
    - Hvem og hvordan brukes ressurser for å identifisere dette?
    - Hvilken støtte fra leverandører er det behov for?
- Hvem har ansvar i en slik situasjon?
- Hvem skal varsles?

### 2.3.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Det viser seg at alle servere har samme passord, og det benyttes bare en bruker og denne er lokal administrator. Dette har ført til at skadevaren har spredd seg til andre maskiner i samme nettverk.

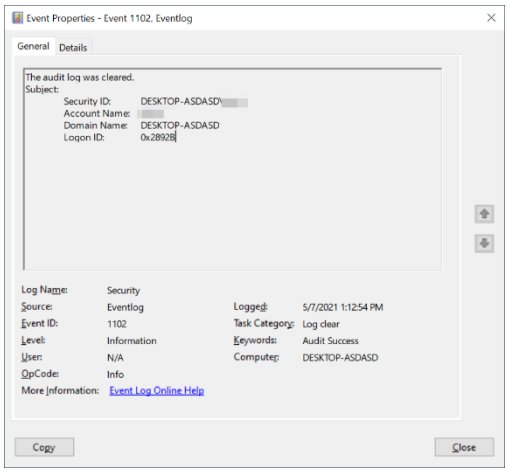
## 2.4 Skadeomfang

Ettersom det viste seg at den ondsinnete programvaren mest sannsynlig har spredd seg til flere servere i nettverket, må alle disse analyseres for å kartlegge hva skadevaren gjør. Bildet illustrerer en mulig event-log. Event-log viser seg å være lik på andre maskiner.

### 2.4.1 Veiledende spørsmål

**IKT-avdeling**

- Hva gjør skadevaren?
- Opererer skadevaren automatisk, eller er dette en bakdør?
- Er det mulig å innhente indikatorer fra nettverket som viser tegn til kartlegging av tjenester eller spredning?
- Hvordan kan servere renses?
- Hvilke tekniske indikasjoner har skadevaren?
- Vil en rens/reinstallering av servere fjerne alle spor av skadevaren?
- Har skadevaren forårsaket skade på kontrollsystemer?




### 2.4.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Det viser seg at skadevaren gjør endringer på servere som kjører Windows, og sender kommandoer som gjør at funksjoner i kontrollsystemet låser seg.

## 2.5 Skadebegrensning

Alle servere som virker til å ha fått installert skadevaren blir isolert vekk fra nettverket, og det blir satt opp som en midlertidig løsning for å se om kontrollsystemene vil fungere normalt i denne situasjonen.

### 2.5.1 Veiledende spørsmål

**SAS/IACS-ansvarlig**

- Hvordan verifiseres at kontrollsystemene fungerer som normalt?
- Hvordan verifiseres konfigurasjon til kontrollsystemene?
- Hvordan kontrollere integritet til kontrollsystemene?

**Lokal driftsledelse**

- Hvordan verifiseres at kontrollsystemene fungerer som normalt?
- Er det beredskapstiltak som må iverksette?

**Systemansvarlig drift / IKT avdeling**

- Finnes det skadebegrensende tiltak som bør iverksettes?

### 2.5.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Skadevaren er fjernet, men det er fremdeles uregelmessigheter i kontrollsystemene.
- Skadebegrensningen dekker ikke alle infiserte servere på grunn av manglende deteksjon.
    - Hvordan finner vi de siste maskinene?

## 2.6 Gjenoppretting

Alle infiserte servere ble til slutt identifisert og lokalisert. Systemene blir reinstallert fra backup.

### 2.6.1 Veiledende spørsmål

**Systemansvarlig drift land/ IKT avdeling**

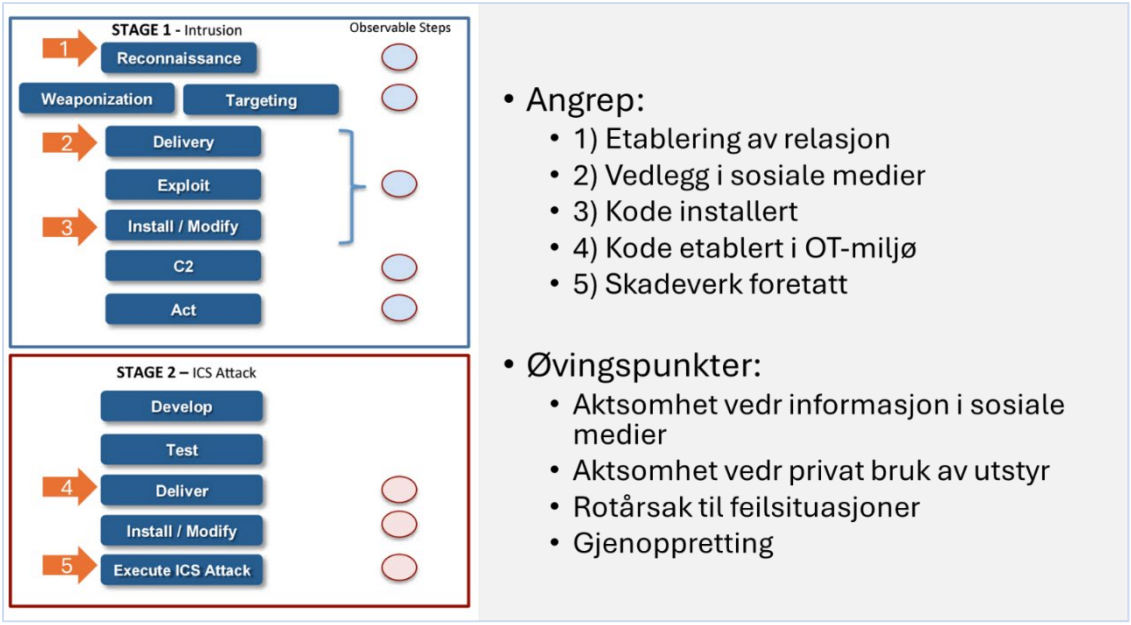
- Bør det gjøres endringer i rutiner for reinstallasjon, slik at ikke samme situasjon kan skje igjen?
- Når var siste back-up gjennomført?
- Har vi mulighet til å gjenopprette systemene fra før aktør kom inn?
- Hva vil det bety for oss dersom det er tapt informasjon mellom siste back-up og tidspunkt for gjenoppretning (teknisk og operasjonelt)?
    - Dersom tapt informasjon, hvilke typer informasjon er tapt?
    - Hva betyr dette for sikker drift og bruk av systemet?

### 2.6.2 Oppfølgingspunkter, avhengig av utfall på diskusjon og beslutninger

- Det viser seg at det er en feil i rutine som blir brukt for å reinstallere servere. Hvordan gå frem for å rette dette?
- Hvordan involveres leverandører?
- Bør man vurdere om det skal utføres en sikkerhetstest i ettertid, for å avdekke om det er andre sårbarheter som kan utnyttes av trusselaktører?
- Er det laget en indikatorliste som kan benyttes i håndtering av lignende hendelser?
- Hvordan sikre at læring fra denne hendelsen blir videreført i hele organisasjonen?
- Hvordan kan selskapets policy om informasjon i sosiale medier tydeliggjøres?

# 3 Ekstra informasjon til forberedelse og gjennomføring

Dette kapittelet inneholder bakgrunns-informasjon om målrettet cyberangrep mot industrielle IKT-systemer. Digitale angrep følger ofte faste mønster, på engelsk kalt kill chain. Figuren viser hvilke steg som er med i denne øvelsen og hvilke øvingspunkter som er innarbeidet i veilederen.




## 3.1 Innledning til hendelse

Ola Normann er ansatt i en nøkkelposisjon med tilgang til de industrielle IKT-systemene. LinkedIn-profilen hans reflekterer denne stillingen og lister opp hans utdanning, kurs og erfaring. Ola Normann har også en Facebook-profil til privat bruk, hvor noe informasjon er tilgjengelig for alle, og ytterligere informasjon er tilgjengelig for venner. Trusselaktøren har målrettet søkt i sosiale medier etter personer i tekniske nøkkelstillinger, og opprettet en Facebook-profil med tilsvarende interesser som Ola Normann.

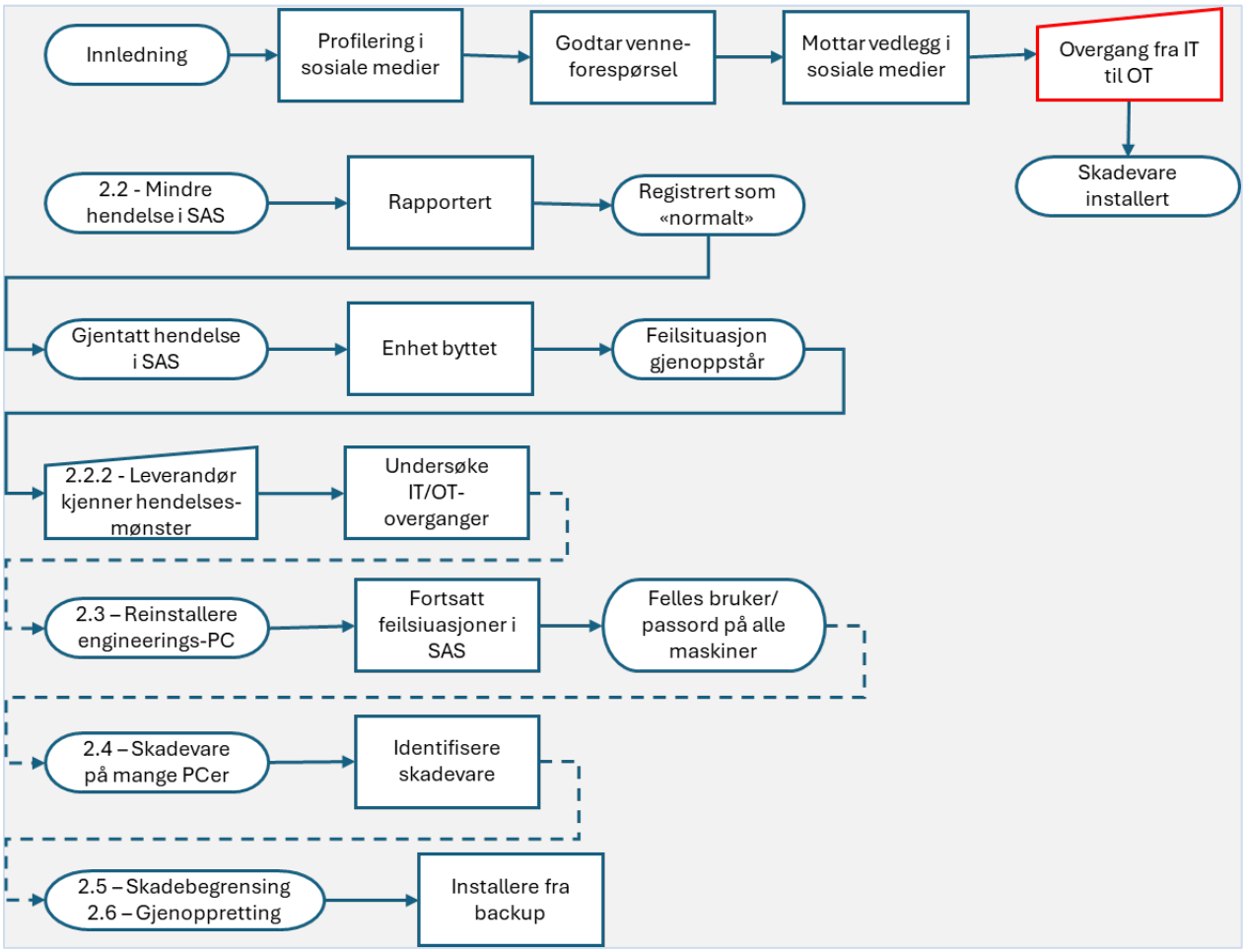
For en tid tilbake mottok Ola Normann en venneforespørsel med innledende tekst om at de møttes på en konsert i Oslo året før. Venneforespørsel ble akseptert. Aktøren og Ola Normann holder kontakt over lengre tid, hvor de deler sine interesser. En dag mens Ola Normann er på arbeid, mottar han en Facebook-melding fra aktøren med vedlegget «Konsertbilletter.pdf». Ola Normann åpner vedlegget på sin jobb-PC uten å merke noe spesielt, men aktøren oppnår fotfeste i nettverket.

## 3.2 Hendelse

En trusselaktør oppnår fotfeste via sosial manipulering. Aktøren har utført rekognosering gjennom sosiale medier og stillingsannonser. Angrepet innledes ved sosial manipulering av eksponert personell.

Aktøren oppretter kommunikasjon via en skjult kanal i en ukjent åpning i nettverket. Aktøren utfører videre interne angrep mot spesifikke mål, i kombinasjon med automatisk spredning av skadevare.

I utarbeidelsen av øvingen er det tatt utgangspunkt i følgende forløp:




Hendelsesforløpet tar utgangspunkt i en trusselaktør som opererer på det svarte markedet og leverer tjenester i form av en «leiesoldat»-virksomhet, også kjent som «Hacker for hire». Via anonymiserte forbindelser kan personer ta kontakt for å bestille angrep mot spesifikke mål og ønsker.

Trusselaktøren bruker velprøvde angrepsteknikker som sosial manipulering og kjente sårbarheter. Sårbarheter blir ofte identifisert via forskjellige sårbarhetsskannere. Menneskelige mål blir valgt via sosiale medieprofiler, basert på hvem målet jobber for, og

hva målet jobber som. Sosial manipulering i forbindelse med denne aktøren er som oftest målrettede operasjoner, som kan ta fra dager til måneder å gjennomføre.
Kjennetegnene for denne aktøren er terror og sabotasje av industrielle kontrollsystemer, som kan skape store konsekvenser både for økonomi, helse, miljø og sikkerhet.

### 3.2.1 Egenskaper ved skadevaren

- «Polymorphic»-orm med egenskaper som en tidsbombe.
- Etablerer fotfeste på systemet som skadevaren kjøres på, pakker ut angrepskode, og sletter installasjonsfilen.
- Oppretter bakdør til det infiserte systemet som aktøren kan benytte seg av, blant annet for manuell utnyttelse og angrep lokalt, eller mot tilgjengelige nettverk.
- Sprer seg selv over nettverk ved gjenbruk av passord to dager etter installering.
- Benytter seg av kjente/ukjente sårbarheter mot en rekke kontrollsystemer.
- Utfører destruktive funksjoner, som endringer i innstillinger etter 29 dager (kryptering av data, slette firmware, nullstille konfigurasjonene e.l.).

## 3.3 Læring

Gjennomgang av rutiner, forbedring av systemer for å sikre mot nye angrep etc.

- Hvordan involveres deltakerne i sluttrapporten fra øvelsen?

**SAS/IACS-ansvarlig**

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?
- Hvordan sikrer en læring til alle skift?
- Hvilke kompetansebehov ble avdekket?

**Lokal driftsledelse**

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?
- Hvordan sikrer en læring til alle skift?

**Systemansvarlig drift / IKT avdeling**

- Er ansvar og roller tilstrekkelig beskrevet?
- Hvordan støtter definerte rutiner håndteringen av hendelsen?
- Ble rutinene fulgt? Hvilke endringer bør gjøres?

## 3.4 Aktuell litteratur

Telenor har laget et hefte om cybertrusler.[1] Der diskuteres også hvordan sosial manipulering foregår. Det er ofte menn over 50 år som lar seg lure av spesielt e-post svindel. Falske profiler i sosiale medier med mange kontakter og sammenfallende interesser kan fremstå troverdige.


Det kan være at trusselaktøren har noen av dine venner på sin kontaktliste. Når du blir invitert, vil bekjentskaper gi trygghet slik at du aksepterer invitasjonen siden dere har «felles bekjente».

I desember 2015 utførte hacker-gruppen Sandworm et angrep mot el-forsyningen i deler av Ukraina. Dette angrepet er diskutert i ulike sammen-henger, bl.a. i artikkelen som dette abstraktet er hentet fra.[2]

**Analysis of Ukraine power grid cyber-attack 2015**

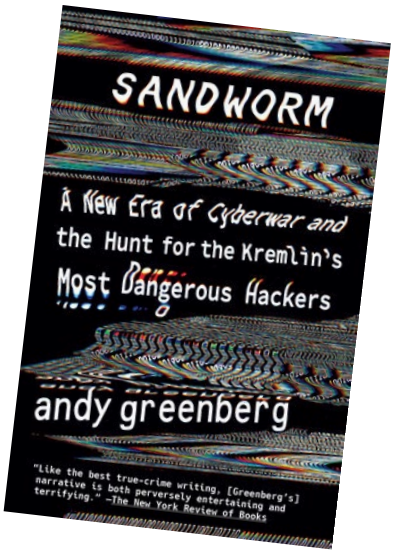
**Abstract**
In December 2015, a regional electricity distribution company in Ukraine reported service outages to its customers. The outages were due to a cyber-attack on the company's computers systems and SCADA systems. Seven 110 kV and 23,335 kV substations were disconnected for many hours. Later reports suggested that additional portions of the electricity distribution grid were impacted and forced the operators to switch to manual mode.

The Ukraine power grid attack of 2015 is perhaps one of the most notable cyberattacks in the ICS industry. Over a period of six months, the attackers were successfully able to launch a series of sophisticated attacks that completely disabled the power system of Ukrainian power companies. The paper discusses the sequence of attacks that led to the final failure of the Ukraine power grid. Further it will highlight the details of each attack steps taken by the attacker. This attack vector can serve as the footprint of the potential threats an organisation might face in the event of a similar attack to the organisation.

I rapporten «Analysis of the Cyber Attack on the Ukrainian Power Grid" utgitt av SANS i 2016, finnes ytterligere informasjon om hendelsen.[3]

[1] https://www.telenor.no/binaries/bedrift/blogg/sikkerhet/sosial-manipulasjon/CTA%20cybertrusler.jpg
[2] https://doi.org/10.30574/wjaets.2024.11.1.0024
[3] SANS-and-Electricity-Information-Sharing-and.pdf (gwu.edu)

Journalisten Andy Greenberg har skrevet en bok om hvordan Sandworm arbeider.[4] Financial Times omtaler boken på følgende måte: *The true story of the most devastating act of cyberwarfare in history and the desperate hunt to identify and track the elite Russian agents behind it: "[A] chilling account of a Kremlin-led cyberattack, a new front in global conflict".*




[4] ISBN 9780525564638