

Kleine catalogus van cyberrisico's [1, 2]

Cybercriminaliteit in enge zin

Het gebruik van informatiesystemen en computers niet alleen als middel, maar ook als doel. Bijvoorbeeld computers beschadigen, spamaanvallen, DDoS-aanvallen, virussen verspreiden.

Cybercriminaliteit in brede zin

Dit zijn alle strafbare activiteiten waarbij iemand een informatiesysteem of computer gebruikt. Denk aan diefstal en vervalsing van betaalpassen, oplichting, afpersing, kinderporno, racisme en belediging.

Georganiseerde cybercriminaliteit

Criminele netwerken die gebruik maken van IT, waarbij dat gebruik invloed heeft op hun criminele bedrijfsprocessen, maar meestal zonder enige ideologische achtergrond.

Dit kan theoretisch worden onderscheiden in: [3, 4]

- Traditionele georganiseerde criminaliteit, dat wil zeggen zaken zonder een sterke IT-component. Het gaat dan om gevallen van offline drugshandel, mensenhandel/-smokkel en andere (combinaties van) misdrijven;
- Traditionele georganiseerde criminaliteit met IT als belangrijk vernieuwend element in de modus operandi, zoals zaken van door IT gefaciliteerde drugshandel/-smokkel en een zaak waarin het witwassen van Bitcoins centraal staat.
- Georganiseerde low-tech cybercriminaliteit, waartoe skimming en phishing wordt gerekend bij de low-tech cybercriminaliteit; hierbij maken daders gebruik van contacten die ze hebben in het criminele milieu;
- Georganiseerde hightech cybercriminaliteit: zaken als banking malware; kernleden van het criminele samenwerkingsverband de benodigde technische expertise verschaffen door het gebruik van forums.

Cyberterrorisme

Terroristische activiteiten die digitaal worden uitgevoerd, met (enige) ideologische achtergrond. Bijvoorbeeld het beschadigen of uitschakelen van belangrijke informatienetwerken via internet.

Cyberspionage

Het binnendringen van digitale systemen voor het verkrijgen van vertrouwelijke informatie, vaak strategisch, economisch of militair van aard, veelal door staten of (staats)bedrijven.

Cyberoorlog/cyberwar(fare)

Digitale (genetwerkte) technieken die gebruikt worden om de systemen van staten of organisaties aan te vallen. Vaak met een militair of strategisch doel.

Referenties

[1, 2] Verder ontwikkeld en geïnspireerd op:

Gaycken, S. (2015) *Cybersecurity – Kleiner Katalog der Cyberrisiken*. In: Jäger, T. (eds) (2015) *Handbuch Sicherheitsgefahren. Globale Gesellschaft und internationale Beziehungen*, Wiesbaden Springer, p. 230 en

het Cyberveilig Nederland i.s.m. Cybersecurity Alliantie (2021). *Cybersecurity Woordenboek : van cybersecurity naar Nederlands*, 3e druk

[3] Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R., & Roks, R. (2018). *Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit*. (Cahier; Vol. 2018, No. 8). WODC.

[4] Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R., & Roks, R. (2018). Criminele geldstromen en ICT: over innovatieve werkwijzen, oude zekerheden en nieuwe flessenhalzen. WODC: *Justitiële Verkenningen* 44(5), 23-39.