9 TERRORISME

9.1 JIHADISTISCHE TERRORISTEN EN ANDERE RADICALEN

Jihadistische terroristen en andere radicalen gebruiken het internet in ruime mate. Voor contrastrategieën én beveiligingsvraagstukken in het kader van contraterrorisme is inzicht hierin van groot belang. Deze studie door het NCTb (Nationaal Coördinator Terrorismebestestrijding en Veiligheid) heeft daarin onderscheid gemaakt tussen het gebruik van het internet als doelwit en wapen (deel A) en internet als middel (deel B)

- **Internet als doelwit en wapen:**

  -> **internet als doelwit:**

  -> Hierin richten de terroristische activiteiten zich tegen (de infrastructuur van) het internet zelf. Daarbij kan gedacht worden aan onder andere knooppunten (computerparken), functionaliteiten en verbindingslijnen van het internet of de organisaties die diensten verlenen die cruciaal zijn voor het functioneren van het internet.

  -> **een aanval of aanslag tegen het internet kan verschillende vormen aannemen:**

  -> een cyberaanval door gebriukmaking van computers via het internet. Het internet is in dat geval zowel doelwit als wapen: het internet keert zich tegen zichzelf.

  -> een fysieke aanslag door gebruikmaking van conventionele wapens of door sabotageacties van binnen uit

  -> een elektromagnetische aanslag door het gebriuk van bijvoorbeeld elektromagnetische energiebronnen

  -> indirecte aanslagen of aanvallen bijvoorbeeld tegen de elektriciteitsvoorzieningen of koelvoorzieningen

  -> **internet als wapen:**

  -> aanslagen tegen fysieke doelen gepleegd via het internet

  -> overname van luchtverkeersystemen of besturingssystemen van vitale installaties in de chemische sector of de elektriciteitsvoorzieningen

  -> het gebruik van het ‘internet als doelwit en wapen’ is een regelmatig terugkerend thema in de berichtgeving

- De NCTb heeft een expertmeeting georganiseerd met vertegenwoordigers van de inlichtingendiensten, wetenschap, politie, overige overheidsdiensten en de telecom- en internetsector. In deze studie is vanuit uiteenlopende invalshoeken de dreiging beoordeeld

  -> **dit heeft geresulteerd in 3 conclusies:**

  1. **Cyberaanvallen door jihadisten en andere radicalen tegen het internet zijn niet waarschijnlijk:**

     -> wordt op dit moment niet waarschijnlijk geacht

     -> gelden als belangrijkste nadelen voor jihadisten, dat het uitschakelen van het internet ook de jihadistische infrastructuur op het internet treft en niet appeleert aan het martelaarschap

     -> een cyberaanval behoort ook niet echt tot de mogelijkheden, vooral als gevolg van de al genomen maatregelen hiertegen

     -> als we er 1 knnen verwachten, zal dat een kleinschalige aanval gedurende een beperkte tijd zijn of een geregiseerde combinatie van kleinschalige cyberaanvallen

  2. **Andersoortige aanslagen door jihadisten en andere radicalen tegen het internet zijn niet waarschijnlijk**

     -> een fysieke tegen het internet, wordt op dit moment evenmin waarschijnlijk geacht

     -> het nederlandse en belgische internet valt op deze wijze eigenlijk niet uit te schakelen

     -> jihadisten geven eerder de voorkeur aan een bomaanslag op een soft target in plaats van op een belangrijke internetlocatie

  3. **Cyberaanvallen via het internet zijn niet waarschijnlijk**

     -> de enigste aanvallen die hierin relevant zouden kunnen zijn, is de software voor procesbesturing (SCADA) waar diverse sectoren gebruik van maken.

     -> maar een dergelijke aanval vereist doorgaans veel (insider)kennis en is momenteel dus minder waarschijnlijk

     -> ook zijn klassieke aanvallen zoals bomaanslagen of zelfmoordaanslagen beter publicitair uit te buiten

     -> een combinatie van 1 of meer klassieke aanslagen met het internet als wapen lijken meer waarschijnlijk

- **Internet als middel:**

  Jihadisten en andere radicalen gebruiken het internet voor verschillende doeleinden en beschouwen het internet als een cruciaal middel voor de jihad. In een studie is gekeken naar de invloed op radicalisering, uitmondend in de volgende conclusies:

  1. **Propaganda via het internet draagt bij aan radicalisering:**

     -> propaganda vindt professioneel plaats, heeft een groot bereik en kent relatief weinig weerwoord.

     -> de propaganda blijft niet beperkt tot éénrichtingsverkeer: proberen actief de interactie aan te gaan met geïnteresseerden

     -> hier ontstaat een voedingsbodem voor verdere radicalisering.

     -> geldt zeker voor moslima's vanwege de aantrekkelijkheid van het internet

  2. **Informatie-inwinning via het internet draagt potentieel bij aan het plegen van terroristische activiteiten**

     -> onuitputtelijke bron van informatie

     -> vooral ontwikkelingen op het terrein van (real-time) sattelietbeelden, gecombineerd met een internetverbinding zoals in het geval van GoogleEarth

     -> hierdoor nemen mogelijkheden voor informatie-winning door jihadisten verder toe

  3. **Fondsenwerving via het internet door en voor jihadisten komt nog beperkt voor: verschuiving naar meer heimelijke fondsenwerving is te verwachten**

     -> in potentie bestaan vele mogelijkheden voor fondsenwerving door en voor jihadisten en er zijn enkele vb van bekend, maar komt in de praktijk nog weinig voor

     -> deze manier is immers zichtbaar en daardoor kwetsbaar voor overheidsingrijpen

     -> fondsenwerving via het internet zal eveneens kunnen toenemen als gevolg van nieuwe digitale en anonieme betalingsmiddelen

  4. **Internetgebruik resulteert in meer interactieve vormen van rekrutering die nog niet goed te duiden zijn evenals deelname aan de jihad en zelfontbranding**

     -> het voert te ver om hier te spreken van rekrutering

     -> er is wel een sterke interactieve vorm van rekrutering waarneembaar die gekoppeld is aan de interactieve manieren van propaganda te verspreiden

     -> kenmerkend is vooral dat potentiële strijders zich zelf willen aanmelden voor deelname aan de gewelddadige jihad (conscriptie)

5. **Gebruik van het internet voor trainingsdoeleinden werkt drempelverlagend voor het plegen van aanslagen**

   -> vooral voor 'home-grown'-terroristen kan het volop beschikbare trainingsmateriaal bijdragen om de intentie tot het plegen van terroristische aanslagen in daden om te zetten

   -> verspreiding van trainingsmateriaal via het internet door jihadisten draagt bovendien bij aan het snel verspreiden van het geleerde

6. **Jihadisten gebriuken het internet voor onderlinge communicatie en planning**

   -> er zijn voldoende aanwijzigingen dat jihadisten via het internet door onderling communiceren en terroristische activiteiten plannen

   -> maken gebruik van anonieme en afschermende communicatie

   -> naast voordelen voor jihadisten biedt dit internetgebriuk inlichtingen- en opsporingsinstanties de mogelijkheid tot ingrijpen

   -> jihadisten zijn zich hier wel van bewust

7. **Virtuele netwerken verhogen de slagkracht van de jihadistische beweging**

   -> hierdoor ontstaat een informele pool van bereidwilligen voor de jihad die in wisselende combinaties met elkaar of individueel geweldsactiviteiten kunnen ontplooien

   -> lokale en internationale elementen kunnen daardoor met elkaar verweven raken

8. **Internetgebruik ondersteunt het gehele proces van radicalisering**

   -> met behulp van het internet kan een potentiële jihadist processen doorlopen van ideologievorming, ideologieversterking en ideologische indoctrinatie

9. **Vanuit het perspectief van radicalisering gaat de grootste dreiging uit van propaganda via het internet in combinatie met de relatief grote groep jonge moslims die zoekende is**

   -> propaganda vindt professioneel plaats, heeft een groot bereik, is interactief en kent weinig weerwoord

   -> combineren we dat met het in potentie grote bereik bij kwetsbare jongeren, dan is duidelijk dat propaganda via het internet het meest bijdraagt aan radicalisering

10. **Vanuit het perspectief van terrorisme gaat de dreiging grotendeels uit van de (mogelijkheden tot) creatie van virtuele netwerken en het gebruik van het internet voor trainingsdoeleinden**

    -> virtuele netwerken verhogen vooral de slagkracht van de jihadistische beweging

    -> door het volop beschikbare trainingsmateriaal, zeker voor 'homegrown-terroristen', ertoe bijdragen dat de intentie tot het plegen van terroristische aanslagen wordt omgezet in daden

9.2 BESTAAT ER EEN KEUZE TUSSEN BEVEILIGING EN PRIVACY?

- **Terrorisme in cyberspace:**

  -> het dominante culturele thema uit het jaar 2017 op de overheidsagenda is de 'war on terror'

  -> dit komt door de verhoging van de terroristische aanvallen van ISIS/ISIL.

  -> dit heeft ervoor gezord dat de gelekte documenten van Edward Snowden over de illegaliteit van de veiligheidsprogramma's van de amerikaanse overheid op de achtergrond zijn geraakt

  -> de aanval in San Bernardino blijkt wat voor rol het internet, in het bijzonder de sociale media, speelt

      -> aanvaller had openlijk op social media gesproken over de jihad. Nationale veiligheidsinstellingen richten hun aandacht meer op surveillancevan social media en moedigen buurgers aan dit ook te doen

  -> op social media wordt gebriuk gemaakt van 'catfishing'. Een catfish is iemand die zich voordoet als iemand anders op facebook, om valse accounts te creëren.

      -> dit doen ze om jongeren te rekruteren voor ISIS

      -> overheid kan hierop inspelen door zelf valse accounts te maken om zo te leren hoe social media wordt gebriukt om nieuwe mensen te recruteren

  -> de cybersecurirty act of 2015 heeft een nieuwe bedrijfsstandaard gezet voor de samenwerking tussen publieke en private organisaties

  -> hackers-organisaties zoals anonymous hebben ook grote bijdragen geleverd tegen ISIS

      -> wat echter een probleem is van anonymous, is dat ze bv terroristiosche websites afsluiten, terwijl de overheid ook al vaak in die websites geïnfiltreerd is en dus geen data kan opslaan om verder onderzoek te doen

  -> maar niet alleen social media is een online platform voor terroristen. Ze hebben ook blogs, websites en social media profielen om terroristische idealen te promoten.

- **Privacy in cyberspace en mobile – wat was de invloed van Edward Snowden?**

  -> hij had kopieÊn gemaakt van geheime documenten en was deze van plan openbaar te maken.

  -> hij deed dat omdat hij vond dat de amerikaanse overheid zich schuldig maakte aan illegale surveillance-activiteiten

  -> hij vond dat het pbliek moest beslissen of deze programma's en beleid goed of slecht waren

  -> dit heeft ertoe geleid dat een belangrijk oorlogsprogramma in afghanistan moest stoppen om de veiligheid van de soldaten te garanderen

  -> daarnaast bleek uit een geopenbaard document dat de VS toegang had tot computers, audio surveillance, email en interne documenten van officials van de EU

  -> de overheid kreeg de e-mails en chat conversaties live te zien, wat leidde tot een grote vertrouwensbreuk van de maatschappei in internetproviders

  -> wat echter de grootste impact had, was de bulk data van telefoons waarmee de NSA de communicatie tussen miljoenen amerikanen kon volgen

  -> hierop is er een nieuwe wet gekomen waarbij het collecteren van bulk data verboden is. Maar de overheid heeft nog steeds de mogelijkheid om de data te gebruiken die van de telefoon providers komt

  -> ondanks het feit van openbaringen van Snowden een belangrijke bijdrage hebben geleverd aan de publieke perceptie van privacy, is het door toegenomen terrorisme van de overheidsagenda verdwenen

- Is de reguliering van privacy nog wel van belang?

  -> de afgelopen jaren worden gedomineerd door de groei van terroristische activiteiten, terwijl het lekken van data ook nog steeds een probleem is voor private en publieke organisaties

  -> de sony entertainment aanval is een door de staat gesponsorde vorm van cyber-oorlogsvoering

  -> deze aanval begon toen de woordvoerder van het ministerie van buitenlandse zaken van Noord-Korea de sony film 'the interview' als een 'daad van terrorisme' verklaarde, en beloofde genadeloos vergelding als een reactie op het uitbrengen van deze film

  -> ondanks deze waarschuwing besloot sony toch om verder te gaan met de film

  -> in november, verschenen er doodschedels op de schermen van de werknemers met een boodschap dat geheime gegevens zoden worden ontmaskerd

  -> meer dan een DDoS-aanval, een reeks van met elkaar verbonden virussen en malware stalen e-mails en docuumenten. Er werden vertrouwelijke materialen zoals scripts gepubliceerd en er werden harde schijven van de computer gewist.

-> deze aanval werd direct gevolgd door een directe aanval op de belangrijkste middelen van de amerikaanse overheid

-> een doorlopende reeks aanslagen lekten de administratie van de verenigde staten 'Office of Personnel Management' (OPM)

-> OPM staat in voor het rekruteren en screenen van potentiële werknemers voor de amerikaanse overheid

-> gegevens van hget personeel van 4.2 miljoen huidige en voormalige werknemers werden gestolen

-> hierin bevonden zich SOFI-nummers, arbeidsverleden, strafrechtelijke en financiële geschiedenis, vingerafdrukken, etc.

-> de overheid gelooft dat chinese hackers achter deze aanval zaten en dat de gegevens van al deze amerikanen nu bekend zijn bij de chinezen

-> een gevolg is dat de medewerkers van geheime inlichtingendiensten die in China zaten, ontmaskerd zoden worden.

- **CONCLUSIE:**

-> terwijl het internet de wereld dichter bij elkaar brengt, heeft het de afgelopen jaren bijgedragen aan een gevaarlijkere en dreigendere wereld

-> in plaats van verhoging van de privacy van burgers en het verantwoordelijk houden van regeringen voor het bespioneren van burgers, is er toegenomen aandacht voor de wereldwijde terreur en de grootste cyberaanvallen

-> de impact van Snowden ging verloren te midden van de fysieke aanvallen in Londen en San Bernandino

-> kortom de afgelopen jaren waren voor cybersecurity moeilijke jaren. Hopelijk wordt er gebouwd aan een transparanter en veerkrachtiger systeem voor de komende jaren