Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

Mijn Cyber Rijbewijs

VAN KENNIS, VIA INZICHT, NAAR GEDRAG!

Een lessenreeks over digitale weerbaarheid voor

GROEP 7 EN 8

Via een film maakt jouw klas kennis met middelbare scholieren die voor straf online moeten nablijven. De jongeren begrijpen niet waarom. Wat is er aan de hand? De film gaat over een digitaal misdrijf dat heeft plaatsgevonden en waar de jongeren een rol in spelen. Maar hoe zit het precies? Hoe heeft het zo ver kunnen komen? Jouw klas gaat op zoek naar het 'hoe' en het 'waarom'.

In de les werk je naast kennisoverdracht aan het verwerven van inzicht in het handelen in een digitale omgeving.

- De leerlingen ervaren hoe de kenmerken van de digitale wereld een rol spelen in hun keuzes.
- Ze leren dat iemand onbedoeld dader kan worden en dat omstanders niet altijd onschuldig zijn.
- En ze leren wat hun eigen handelingsperspectief is in dit soort situaties.

Met Mijn Cyberrijbewijs vergroot je de digitale weerbaarheid, werk je aan digitale geletterdheid en aan burgerschapsdoelen.

In deze handleiding vind je uitleg over het proces in jouw klas en hoe je dat kan begeleiden.

Voorbereiding en benodigdheden

Elke les duurt 90 minuten en heeft een voorbereiding van ongeveer 20 minuten. Al het uit te printen materiaal staat op **www.mijncyberrijbewijs.nl**

1. Lees de lerarenhandleiding.
2. Neem de slides van het digibord en het bijbehorende filmmateriaal door.

Indien nog niet gedaan:

3. Print de A3 poster voor in de klas (kleur, een per klas)
4. Print de persoonlijke poster (kleur, een per leerling)
5. Print de informatiebrief voor de ouders en/of verzorgers en bijhorende praatplaat (kleur, een per leerling)

Tijdens de les wordt de klas in drie of zes (gelijke) groepen gesplitst. Elke groep bekijkt een ander filmfragment. Vragen over dit fragment worden beantwoord op de bij het fragment behorende lesbrief.

6. Zet voor elke groep een device (tablet, chromebook of computer) klaar. Idealiter in een aparte ruimte.
7. Print voor iedere groep een van de drie lesbrieven. (Kleur, een van de drie opties per groep)

Tip! Leg voor elke leerling een eigen map of insteekhoesje klaar. Hierin kunnen de materialen en notities met inzichten worden bewaard.

De opbouw

Mijn Cyberrijbewijs bestaat uit vijf lessen met ieder een ander onderwerp. Het volgen van de hele reeks zorgt voor het grootste leerresultaat. Mijn Cyberrijbewijs is zo ingericht dat je ook een of een aantal lessen kan geven.

Online Hatespeech

Online Fraude

Doxing

Hacking

Sexting

Uitreiking Certificaat

Voorbereiding per les:
20 minuten

Duur van een les:
90 minuten

De lessenreeks wordt afgesloten met het uitreiken van het Mijn Cyberrijbewijs certificaat. De certificaten zijn te downloaden via de website **www.mijncyberrijbewijs.nl**

Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

Mijn Cyber Rijbewijs

VAN KENNIS, VIA INZICHT, NAAR GEDRAG!

Een lessenreeks over digitale weerbaarheid voor

GROEP 7 EN 8

Vier stappen

De opzet van Mijn Cyberrijbewijs is geïnspireerd op het socratisch gesprek. Een zorgvuldig gesprek waarin je leert je oordeel uit te stellen en je leert je te verplaatsen in anderen. Vanuit verschillende perspectieven kom je samen tot nieuwe kennis. Elke les bestaat uit vier verschillende stappen. Elke stap kenmerkt zich door een vraag.

Stap 1: Wat is er gebeurd?

Stap 2: Wat vinden de hoofdpersonen?

Stap 3: Hoe kon dit gebeuren?

Stap 4: Hoe voorkomen we dat het (opnieuw) gebeurt?

Per stap krijgen de leerlingen meer informatie en verplaatsen ze zich nog beter in de verschillende hoofdpersonen. Samen komen jullie tot inzichten om de vraag bij stap 4 te beantwoorden.

Meer weten? Op de website www.mijncyberrijbewijs.nl vind je:

- Al het lesmateriaal van Mijn Cyberrijbewijs
- De informatiebrief en praatplaat voor ouders en/of verzorgers
- Achtergrondinformatie over Mijn Cyberrijbewijs
- Aanvullend lesmateriaal over digitale weerbaarheid

Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

MIJN CYBER RIJBEWIJS

OMG HACKING

Inleiding onderwerp

Deze les gaat over *hacking*. Ter voorbereiding staat op de komende twee pagina's informatie over dit thema gebundeld.

De informatie is opgedeeld in

- Algemene kennis.
- Uitleg over de achterliggende online mechanismen.
- Handelingsperspectief voor daders, slachtoffers en omstanders.
- Plekken waar je experts kunt vinden en hulp kunt krijgen.

Je kunt deze informatie gebruiken voor:

- Het toelichten van het onderwerp in jouw klas.
- Het begeleiden van de gesprekken die in jouw klas zullen ontstaan.
- Begeleiding en ondersteuning die nodig kan zijn als leerlingen persoonlijke verhalen delen in jouw klas.

Algemene kennis

Wat is het?

- Hacken is als iemand binnendringt in andermans computer, telefoon of ander mobiel device. Het is strafbaar als dit gebeurt zonder toestemming van de eigenaar. Het doel van de hacker is bijvoorbeeld het overnemen van de computer om gegevens te stelen, onbruikbaar te maken of aan te passen.
- Hackers proberen toegang tot computers te krijgen door:
  - Het raden of achterhalen van iemands inloggegevens.
  - Iemand te dwingen zijn gegevens te delen (door bedreiging of chantage).
  - Phishing (lokmailtjes). Phishing is een vorm van social engineering. Social engineering is het kraken van de zwakste schakel in een computersysteem, de mens. Hierbij horen technieken als misleiden, overtuigen gegevens te delen of valse nieuwsgierigheid.
  - Het gebruiken van inloggegevens die zijn buitgemaakt bij andere gehackte websites.

Hacken gebeurt om verschillende redenen:

- Commerciële motieven (hackers verdienen geld met het binnendringen in computersystemen). Wanneer dit systeem vervolgens ook gegijzeld wordt (versleuteld door de hacker) noemen we dat ransomware. De hackers vragen losgeld om het systeem weer vrij te geven.
- Politieke of idealistische motieven.
- Als dienstverlening: het testen van systemen. Dat noemen we ethical hacking en gebeurt met toestemming.
- Als experiment om te te zien of het lukt, dit zijn relatief kleine hacks.
- Met een persoonlijk doel (cijfers op school aanpassen).

Voorbeelden:

- **Erik gaf zijn school vrij**
- **Hacken met toestemming van een bedrijf om diens website sterker te maken.**

Hoe komt het?

- Daders hacken vaak uit nieuwsgierigheid, ze willen weten hoe systemen in elkaar zitten.
- Ze onderzoeken de mogelijkheden van technologie.
- Ze testen kun skills.

Wat doet het?

Maatschappelijk effect

- Het vertrouwen in systemen, organisaties en overheden neemt af. Onbekende personen kunnen in systemen inbreken, je gegevens zijn in deze systemen of bij deze instanties niet veilig.
- Mensen zien hackers als een soort van nieuwe piraten die er met hun acties voor zorgen dat het internet veiliger wordt. Ze dwingen bedrijven hun data beter te beveiligen en helpen daar soms zelfs mee.

Effect op dader

- Daders zijn trots op hoe slim en handig ze zijn.
- Ze zijn tevreden met de waardering die ze krijgen.
- Ze raken gesterkt in hun ethische en/of politieke overtuigingen.

Effect op slachtoffer (persoon)

- Slachtoffers zijn bang en vertrouwen hun computer niet meer. Ze hebben een gevoel van onveiligheid.
- Ze zijn verontwaardigd over het onrecht dat ze is aangedaan.
- Ze schamen zich.
- Ze verliezen data en/of geld.
- Systemen moeten vaak opnieuw worden opgebouwd, dit kost veel geld.

Effect op slachtoffer (organisatie)

- Gevoel van onmacht in het voorkomen van dit soort problemen.
- Irritatie vanwege de gedwongen onderbreking van lopende processen.
- Een bedrijf dat, of organisatie die gehackt is loopt vaak financiële- en reputatieschade op.
- Ze verliezen data en/of geld.
- Systemen moeten vaak opnieuw worden opgebouwd, dit kost veel geld.

Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

MIJN CYBER RIJBEWIJS

Inleiding onderwerp

HACKING

Achterliggende online mechanismen

Het ervaren en/of doorzien van de mechanismen die hacking verergeren:

- **Verbindingen en netwerken:** Steeds meer systemen zijn verbonden met het internet en daarmee via het internet toegankelijk. Daarbij zijn deze systemen nog niet allemaal even goed beveiligd. Dit maakt dat er veel kansen zijn voor hackers. De gelegenheid schept de dief.
- **Virtuele realiteit:** Het gaat om een anonieme hacker die een systeem aanvalt. Dat er persoonlijke of zakelijke gevolgen zijn in de offline wereld is niet meteen duidelijk.
- **Wanorde:** Hacken is een nieuw soort criminaliteit, er is nog geen heldere maatschappelijke opvatting. Hacken veroorzaakt wanorde en komt voort uit het ontbreken van regulering.

Handelingsperspectief

Voorkomen dat je dader wordt:

- Weet dat hacken strafbaar is.
- Weet dat je hack-vaardigheden ongestraft kunt inzetten en ontwikkelen, bijvoorbeeld via organisaties die fouten in ICT-systemen ontdekken. Zij melden dit dan bij de eigenaar van het systeem zodat criminelen daar geen misbruik van kunnen maken.
- Doe mee met **hackathons**; via georganiseerde wedstrijden kun je je hack-vaardigheden verder ontwikkelen.

Handelingsperspectief vanuit de rol van slachtoffer:

Voorkom dat je gehackt wordt:

- Stel goede wachtwoorden in.
- Zorg dat je regelmatig je software update.
- Stel een twee staps verificatie in.

Ná een hack:

- Doe aangifte bij de politie.
- Vraag hulp aan een expert.
- Schakel familie, vrienden of andere mensen die je vertrouwt in voor steun en hulp.
- Leg de hack vast: maak er foto's van, schrijf op wat er gebeurt of gebeurde.
- Sluit je accounts en wijzig je wachtwoorden.
- Rapporteer de hack bij de beheerder van het systeem of social media platform.

Handelingsperspectief vanuit de rol van omstander (bij een jonge dader):

- Ken je een (potentiele) hacker? (H)erken dat talent en help diegene met interessante lessen en uitdagingen.
- Laat positieve rolmodellen zien.
- Laat zien dat er interessante opleidingen en banen zijn voor hackers.

Experts en hulp

Veilig internetten website
www.veiliginternetten.nl
Een website voor vragen en problemen rondom veilig internetten. Praktische tips en hulp vind je hier.

Kindertelefoon
www.kindertelefoon.nl tel: **0800-0432**
Je mag elke dag over **ALLES** bellen of chatten met één van de goed getrainde vrijwilligers. Bellen is gratis en anoniem. Ook weet de kindertelefoon welke organisatie of instantie jou het beste kan helpen als dat nodig is.

Politie
www.politie.nl tel: **0900-8844**
Wanneer je hacken ervaart of herkent doe dan zo snel mogelijk aangifte bij de politie.

Meer weten?
Op **www.mijncyberrijbewijs.nl** vind je meer lesmateriaal over dit onderwerp.



Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

MIJN CYBER RIJBEWIJS

Slides

HACKING

Stap 0: Introductie online hate-speech

Tijdsduur: **10** minuten

Inleiding
In deze fase vertel je jouw klas wat jullie gaan doen.

- Waar gaat het over?
- Hoe ziet de activiteit eruit?
- Hoe lang zijn jullie bezig?



Onderwerp
Deze les gaat over hacken. Hacken is het zonder toestemming inbreken in (computer) systemen.

Voorbeelden van hacking zijn het inbreken in een bedrijfssysteem, of in iemands game account.
Offline voorbeeld hacking: inbreken in iemand zijn huis.



Film
Laat de bijbehorende start-film zien en toon deze eventueel een tweede keer.



Gesprek over eigen ervaringen
Naar aanleiding van de film ga je in op eigen ervaringen van de leerlingen.

Zorg dat leerlingen kunnen delen, maar houd ook je proces in de gaten. Werk met uitgestelde aandacht:

- Dat doe je bijvoorbeeld door een leerling die iets wil delen de beurt te geven, maar (nog) niet te reageren. (Je komt er dan later op terug.)
- Of je vraagt leerlingen dat wat ze willen zeggen op te schrijven en aan het einde van de les te delen.

Stap 1: Wat is er gebeurd?

Tijdsduur: **10** minuten

Vraag 1: Wat is hier gebeurd?

In deze fase vormen de leerlingen een beeld over wat er is gebeurd. Bespreek de vragen op de slide en probeer ze alle drie te beantwoorden.





Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

MIJN CYBER RIJBEWIJS

WTF

Slides

HACKING

Stap 2: Wat vinden de hoofdpersonen?

Tijdsduur: **20** minuten

Vraag 2: Wat vinden de hoofdpersonen?

In deze fase onderzoeken de leerlingen de gebeurtenis door in de huid van de hoofdpersonen te kruipen.

Verdeel de klas in drie groepen.

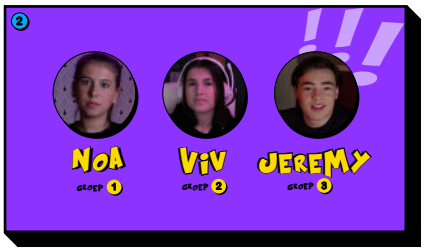
Er zijn 3 films, verdeel de films over de drie groepen.
De groepen bekijken alleen hun eigen film! Zorg dat er tussen de groepen niets uitgewisseld wordt.

De groepjes maken aantekeningen op de lesbrief van hun hoofdpersoon. Leg uit hoe ze dat aanpakken:

- Beantwoord de drie vragen.
- Formuleer een oordeel over je hoofdpersoon.

Geef aan hoeveel tijd ze hebben: 20 minuten.
Geef aan dat de link van hun filmpje te vinden is op de lesbrief.

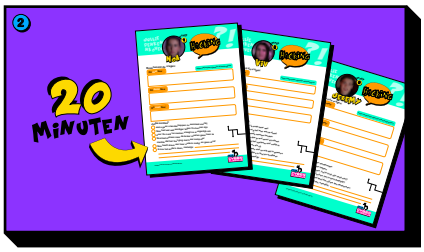




Perspectieven bekijken

Tijdsduur: **20** minuten

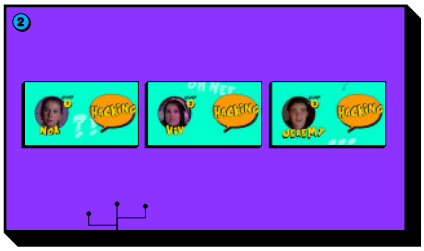
Laat de films één voor één aan de hele klas zien en laat de groepjes na 'hun' film aan het woord.
Laat het groepje, aan de hand van hun lesbrief, vertellen over hun hoofdpersoon.



Begeleid het gesprek:

Is jouw klas het eens met het oordeel?
De klas komt erachter dat de waarheid niet altijd zo helder is als het lijkt. Praat met jouw klas over deze inzichten.

- Hoe is het om maar één hoofdpersoon en zijn of haar ervaring mee te kijken?
- Wat verandert er als je de verhalen van de anderen hoofd-personen hebt gezien?
- Wat denken jullie nu over de gebeurtenis in relatie tot de rollen van de hoofdpersonen?



Afloop bekijken

Tijdsduur: **4** minuten

Hoe liep het af? Jouw klas bekijkt de eindfilm waarin dat duidelijk wordt.



Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

MIJN CYBER RIJBEWIJS

HACKING

Slides

Stap 3: Hoe kon dit gebeuren?

Tijdsduur: **15** minuten

De leerlingen stemmen op stellingen over hacking. Door na te denken over deze stellingen krijgen ze inzicht in de mechanismen die te maken hebben met dit onderwerp. Je kunt zelf bepalen hoeveel stellingen je in de klas wilt behandelen.

Bespreek de stellingen een voor een met elkaar, waarom zijn leerlingen het ermee eens of oneens? Hieronder vind je bij sommige stellingen aanvullende vragen.



Stelling	Aanvullende vragen
Iemand had Noa moeten steunen.	Denk je dat Viv de gevolgen inzag? Hoe komt het dat ze de gevolgen verkeerd had ingeschat?
Voor zoiets bel je toch niet de politie? Is het strafbaar dan?	Wanneer zou je een hack wel aangeven bij de politie? Wanneer niet?
Online de cijfers veranderen was wel echt een stap te ver, dan breng je mensen in de problemen.	Waarom is dit erger dan de spreekbeurt aanpassen? Het effect in de offline wereld is veel heftiger dan online lijkt.
Ze moeten dat online cijfersysteem gewoon beter beveiligen, best goed dat Viv dat duidelijk heeft gemaakt.	Had ze dit op een andere manier kunnen doen?



Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

MIJN CYBER RIJBEWIJS

HACKING

Slides

Stap 4: Hoe voorkomen we dat dit gebeurt?

Tijdsduur: **20** minuten

Als hacking plaatsvindt, spelen oorzaken en omstandigheden een rol. Met de volgende slides worden aan de hand van vragen een aantal van deze oorzaken en omstandigheden besproken.

Vraag de leerlingen oplossingen te bedenken.
- Wat is er nodig om de oorzaak weg te nemen?
- Wat moet er veranderen zodat dit niet meer gebeurt.

Laat ze voor zichzelf antwoord geven (opschrijven) en bespreek de antwoorden daarna met de klas.

Vul indien nodig aan met het handelingsperspectief:
- Deel kennis: hacken is strafbaar (ook als het 'voor de grap' is).
- Hulp vragen (aan volwassenen of experts).
- Hulp geven (aan slachtoffer en dader)
- Aangifte doen.
- (H)erken het talent van de hacker en stuur hem/haar een positieve richting op.

Individuele opdracht:
- Laat de leerlingen op hun persoonlijke poster een inzicht naar aanleiding van deze les opschrijven.
- Een aantal hulpvragen hierbij zijn: Waar ga je op letten? Wat vind je belangrijk? Hoe wil je samen werken? Wat doe je als het jou overkomt?
- Geef aan dat de leerlingen de persoonlijke poster goed moeten bewaren.

Groepsopdracht:
- Formuleer met de klas een afspraak naar aanleiding van deze les. Hoe voorkomen jullie dat hacking in deze klas gebeurt?
- Schrijf deze afspraak op de klassikale Mijn Cyberrijbewijs poster.
- Vraag een aantal leerlingen wat zij op hun persoonlijke poster hebben geschreven.

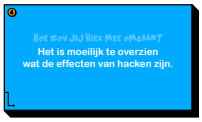


















Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.

Dit document is gedownload door () op November 2, 2026.
Mag alleen gekopieerd worden voor gebruik binnen de school van 'gebruiker'. Zie ook de abonnementsvoorwaarden van Leapo.

MIJN CYBER RIJBEWIJS

Slides

HACKING

Afronding

Tijdsduur: **5** minuten

Thuis

Maak de koppeling met de thuis-, leefomgeving van de leerlingen, je kan de leerlingen bijvoorbeeld vragen:

- Vraag of er iemand wel eens gehacked is.

Deel, indien nog niet gedaan, de informatiebrief en praatplaat uit aan de leerlingen en geef aan dat ze deze aan hun ouders en/of verzorgers mogen geven.

Vraag tenslotte of alles gezegd is, zijn er nog kinderen die iets kwijt willen?

Deel als nodig nog een keer de opties voor hulp.

Rond de les af







Kindertelefoon: 0800-0432

Veilig internetten website: www.veiliginternetten.nl

Politie: 0900-8844 www.politie.nl

Meer weten? Op de website www.mijncyberrijbewijs.nl vind je:

- Al het lesmateriaal van Mijn Cyberrijbewijs
- De informatiebrief en praatplaat voor ouders en/of verzorgers
- Achtergrondinformatie over Mijn Cyberrijbewijs
- Aanvullend lesmateriaal over digitale weerbaarheid

Een initiatief van het ministerie van Justitie en Veiligheid. Ontwikkeld door FutureNL © 2022 Je mag het materiaal gebruiken, kopiëren en verspreiden, mits het in originele staat is en met naamsvermelding. Wil je het veranderen of erop voortbouwen? Neem dan even contact met ons op. Creative Commons licence: CC BY-NC-ND 4.0.