Voorwoord

Afgelopen maand gingen tienduizenden Europeanen de straat om te protesteren tegen het ACTA-verdrag, het Anti-Counterfeiting Trade Agreement dat een wereldwijde standaard moet zetten voor handhaving van intellectuele eigendomsrechten. De protesten zijn gericht tegen een onderdeel van het verdrag, de bestrijding van 'digitale piraterij': het gratis downloaden op internet van films en muziek waarop auteursrechten rusten. Nadat tal van ngo's zoals Bits of Freedom en Amnesty International zich al tegen het verdrag hadden gekeerd wegens de veronderstelde schending van burgerrechten, kregen ook politici zo hun bedenkingen. In navolging van enkele Oost-Europese landen trok Duitsland zijn steun voor het verdrag in, terwijl de Nederlandse Tweede Kamer zich in een motie keerde tegen ratificatie van het verdrag op dit moment. Eurocommissaris voor Justitie en Mensenrechten Viviane Reding verklaarde dat de bescherming van copyrights nooit een rechtvaardiging kan zijn voor de beperking van de vrijheid van meningsuiting of de vrijheid van informatie. Mensen afsluiten van internet wegens schending van auteursrechten is geen optie en zou nooit onderdeel mogen uitmaken van het EU-recht, aldus Reding. Zij wil dat het Europese Hof van Justitie een onderzoek instelt om na te gaan of het ACTA-verdrag fundamentele burgerrechten schendt.

De verwikkelingen rond het verdrag laten zien dat er een hevige strijd gaande is over welke regels gelden in cyberspace, ofwel op het internet. Naast de bescherming van commerciële belangen schuren ook maatregelen om een veilig internet te creëren vaak dicht aan tegen schending van de persoonlijke levenssfeer. En ruimere bevoegdheden voor politie en Justitie voor digitale opsporing – hoe gewenst ook – hebben vaak hetzelfde effect. Ook in het virtuele domein leidt het streven naar veiligheid tot een situatie waarin menig burger zich helemaal niet veilig voelt bij het idee dat al zijn communicatie en bewegingen op het internet kunnen worden nagetrokken.

De bovengenoemde actuele ontwikkelingen rond 'digitale piraterij' worden in een van de artikelen in dit themanummer nader geanalyseerd. Daarnaast is er aandacht voor cybercrimewetgeving, voor de vorderingen van de politie bij de bestrijding van cybercrime en voor fraude met identiteit en internettransacties. Het lekken van

geheimen in cyberspace komt eveneens aan bod, waarbij wordt teruggeblikt op de WikiLeaks-affaire. Voorts is er een artikel gewijd aan het fenomeen cyberwar.
In het openingsartikel van Koops staat de vraag centraal of het strafrecht met zijn traditionele nationale oriëntatie opgewassen is tegen allerlei snel veranderende vormen van cybercrime. De auteur gaat in op de dynamiek tussen Europese en nationale cybercrime-wetgeving, daarbij focussend op de Nederlandse initiatieven op dit terrein. De dynamiek bestaat hieruit dat de Europese regels minimumstandaarden hanteren voor de belangrijkste kwesties, waarbij veel ruimte is voor de lidstaten om de geformuleerde standaarden te interpreteren en zelf wetgeving te maken op punten waarover de Europese regels zwijgen. Tot nu toe heeft dit volgens de auteur goed gewerkt. Maar als cybercrime doorgaat zich te ontwikkelen tot grootschalige georganiseerde misdaad, zou het nodig kunnen zijn om de Europese kaders meer gewicht en sturing te geven.
Hoe de bestaande wetgeving inzake cybercrime door de Nederlandse politie wordt gehandhaafd, komt aan bod in de bijdrage van Stol, Leukfeldt en Klap. Zij stellen de vraag welke voortgang de politie in de afgelopen jaren heeft geboekt op dit terrein. Hoewel er is geïnvesteerd in proefprojecten, de rekrutering van digitale experts en de integratie van digitale aspecten in training en educatie, kan de politie nog nauwelijks bogen op concrete successen in de strijd tegen cybercrime. Bovendien heeft de politie soms moeite te bepalen welke bevoegdheden zij precies heeft bij de opsporing van cybercrime, zo wordt duidelijk uit het betoog.
Wat er gebeurt als de 'cybercops' er niet in slagen serieus tegenspel te bieden tegen criminele dreigingen op het internet, beschrijft Prins. Hij stelt dat particuliere cyberbewakers die leemte zullen vullen, vooral omdat er voor het bedrijfsleven grote belangen op het spel staan. Wijzend op situaties die zich al in de Verenigde Staten hebben voorgedaan waarschuwt de auteur dat deze particuliere bewakers de neiging hebben wettelijke voorschriften – bijvoorbeeld inzake privacy – nogal losjes te interpreteren. Net zoals de veiligheid op straat een primaire overheidstaak is, zo geldt dat ook voor de veiligheid op internet, zo meent hij. De auteur inventariseert de verschillende typen dreigingen evenals de actoren daarachter en bespreekt de reactie van overheden daarop. Na een analyse van de belangrijkste obstakels bij de opsporing van cybercriminelen doet

hij enkele aanbevelingen voor een meer effectieve overheidsstrategie tegen cybercrime.
Cyberwar is misschien wel de meest tot de verbeelding sprekende dreiging op internet, en is tegelijkertijd het meest omstreden. Volgens verschillende deskundigen is de cyberwardreiging niet meer dan een hype opgeklopt door commerciële webbeveiligers. Lodder en Boer gaan kort in op dit debat. Hoewel de actuele dreiging van cyberoorlog discutabel is, staat vast dat het onderwerp binnen de politiek, het leger en internationale bondgenootschappen zeer veel aandacht krijgt, zo stellen zij. De auteurs concentreren zich op de vraag of het internationaal recht, in het bijzonder het oorlogsrecht, is toegesneden op cyberwar. Zij onderscheiden daarbij cyberwar, -misdaad, -spionage en -terrorisme. Na een bespreking van verschillende historische cyberincidenten wordt nagegaan welke rechtsgebieden relevant zijn bij deze verschillende incidenten.
Bedreiging van cyberveiligheid komt echter niet alleen van buiten, zo stelt Maat in zijn artikel, maar ook van binnenuit organisaties. Door de digitalisering is informatie mobieler geworden dan ooit. Enorme hoeveelheden al dan niet gevoelige informatie kunnen op een simpele usb-stick worden meegenomen, terwijl interne netwerken van organisaties en bedrijven kwetsbaar blijken te zijn voor hackers. De auteur gaat in op verschillende gevallen van het lekken van geheimen in cyberspace, zoals de WikiLeaks-affaire, om de kwetsbaarheid van de huidige informatiemaatschappij te illustreren. Vervolgens bespreekt hij de ontwikkelingen rond 'Het Nieuwe Werken' en het daaraan gepaard gaande gebruik van nieuwe technologie. Met enkele voorbeelden laat de auteur zien hoe organisaties de cyberveiligheid kunnen vergroten door medewerkers slimme, technologisch geavanceerde oplossingen te bieden.
Vervolgens verleggen we de aandacht naar enkele vormen van cybercrime, te beginnen bij een webactiviteit die vooralsnog is toegestaan, maar de vraag is: hoelang nog? Het gratis downloaden van film en muziek waarop auteursrechten rusten zou volgens een recent wetsontwerp van de staatssecretaris van Veiligheid en Justitie Fred Teeven moeten worden verboden. Leeuw bespreekt de voors en tegens van een downloadverbod tegen de achtergrond van recente ontwikkelingen rond 'digitale piraterij'. Daarbij betrekt hij resultaten van empirisch onderzoek naar de gevolgen van illegaal

downloaden op de betrokken industrieën. Ten slotte gaat de auteur in op de rol van auteursrechten in een digitale omgeving.
Daarna is er aandacht voor identiteitsfraude en slachtofferschap. Van Wilsem bespreekt de belangrijkste resultaten van internationaal en Nederlands onderzoek naar dit fenomeen. Daarbij gaat hij in op de vraag hoe omvangrijk digitale id-fraude is, wat de risicofactoren zijn, de schade en de nasleep voor de slachtoffers. De auteur doet voorts enkele suggesties voor vervolgonderzoek.
Het laatste artikel van dit themanummer is gewijd aan fraude samenhangend met de verkoop van goederen en diensten via internet. Het is een vorm van fraude die als gevolg van de groei van websites als Marktplaats, flink is toegenomen in de afgelopen jaren. Leukfeldt en Stol stellen de vraag of er met internetfraude een nieuw type dader is opgestaan. Daartoe vergelijken zij internetfraudeurs met klassieke fraudeurs. De belangrijkste conclusie luidt dat de twee groepen, gelet op factoren als sociaaleconomische klasse, sociale binding, werkloosheid en dergelijke erg op elkaar lijken. Het enige verschil is dat internetfraudeurs gemiddeld jonger zijn.

Marit Scheepmaker