

MINISTERIE VAN DEFENSIE

MINISTRY OF DEFENCE

AIRCW Kaderadvies Cyber

AIRCW Framework Advice Cyber

Gevraagd besluit: instemming met het kaderadvies Cyber van de Adviescommissie Internationaal Recht en Conventioneel Wapengebruik.

Requested decision: consent to the framework advice on Cyber from the Advisory Committee on International Law and Conventional Weapons Use.

Met de toename van de inzetbaarheid van het Defensie Cybercommando en de mogelijkheid tot het uitvoeren van offensieve cyberoperaties, is de noodzaak ontstaan om cybermiddelen te onderwerpen aan de verplichte toets van nieuwe middelen en methoden van oorlogvoering. Het advies in bijlage is de uitkomst van deze toets.

With the increase in the deployability of the Defence Cyber Command and the ability to conduct offensive cyber operations, the need has arisen to subject cyber means to the mandatory test of new means and methods of warfare. The attached opinion is the outcome of this test.

Tot nu toe heeft de AIRCW alleen middelen getoetst en geen methoden, omdat methoden van oorlogvoering ofwel doctrine zijn (waarvoor een aparte procedure geldt via de Doctrinecommissie Krijgsmacht), ofwel ad-hoc besluiten zijn waarbij de commandant zijn militair jurist te velde kan raadplegen. Cybermiddelen laten zich echter naar hun aard niet goed toetsen via de gebruikelijke systematiek, zoals in het advies uitgebreid staat uitgelegd. Ook is er geen vergelijking mogelijk met de "artikel 36 toets" in andere landen in dit geval, omdat nog geen enkel land cybermiddelen heeft getoetst of althans geen uitkomsten van dergelijke toetsen bekend zijn gemaakt.

So far, the AIRCW has only tested means and not methods, because methods of warfare are either doctrine (which is subject to a separate procedure through the Doctrine Commission of the Armed Forces) or are ad-hoc decisions where the commander can consult his military lawyer in the field. Cyber means, however, by their very nature do not lend themselves well to review through the usual system, as explained in more detail in the opinion. There is also no comparison with the "Article 36 test" in other countries in this case, because no country has yet tested cyber means or at least no results of such tests have been made public.

Op basis van deze bevindingen is besloten cybermiddelen niet als zodanig, dus als "middelen" te toetsen, maar de inzet van die cybermiddelen als "methode" te toetsen. Deze benadering heelt echter ook tot gevolg dat het advies de vorm heelt gekregen van een kaderadvies in plaats van een middel-specifiek advies. Het advies geeft enkele algemene richtlijnen voor de inzet van cybermiddelen en wijst op de verplichting om voorafgaand aan de inzet specifiek advies in te winnen bij de juridisch adviseur van de commandant of bij DJZ. Ook wordt gewezen op de eis dat de inzet van cybermiddelen binnen het verstrekte (politieke) mandaat moet passen en dat desgewenst voorafgaand (specifiek) advies aan HDB kan worden gevraagd.

Based on these findings, it was decided not to test cyber means as such, i.e. as "means", but to test their deployment as a "method". However, this approach also results in the advice taking the form of a framework advice rather than a means-specific advice. The advice provides some general guidelines for the deployment of cyber means and points out the obligation to seek specific advice from the commander's legal advisor or DJZ [Directorate of Legal Affairs of the Ministry of Defence]. It also notes the requirement that the deployment of cyber means must fit within the (political) mandate provided and that prior (specific) advice may be sought from HDB [Main Directorate of Policy] if required.

Ik adviseer u in te stemmen met het advies.

I recommend agreeing with the advice.

Commandant der Strijdkrachten

Commander of the Armed Forces

TA Middendorp
Generaal

TA Middendorp
General

WERKGROEP INTERNATIONAAL RECHT EN CONVENTIONEEL WAPENGEBRUIK

Advies ter zake: Inzet van
Cybercapaciteiten en -middelen als
methode van oorlogvoering

Inleiding

Zoals hieronder nader zal worden uiteengezet, leveren cybercapaciteiten een nieuwe uitdaging op voor het toepassen van de verplichte toets van nieuwe middelen en methoden van oorlogvoering. In dit advies wordt eerst, om die uitdaging beter inzichtelijk te kunnen maken, de verplichting tot het toetsen van nieuwe middelen en methoden van oorlogvoering nader beschreven en uitgelegd. Daarna wordt het fenomeen "cybercapaciteiten" beschouwd in het licht van die verplichting. Tot slot wordt een kaderadvies gegeven ten aanzien van het gebruik van cybercapaciteiten in relatie tot het internationaal recht.

De verplichting tot toetsing van nieuwe middelen en methoden van oorlogvoering

Artikel 36 van het Eerste Aanvullende Protocol van 1977 bij de Verdragen van Genève van 1949 verplicht de Partijstaten om, kort gesteld, bij het ontwikkelen, verwerven of in gebruik nemen van nieuwe middelen en methoden van oorlogvoering, te beoordelen of het gebruik van die middelen of methoden in sommige of alle gevallen in strijd zou zijn met de verplichtingen van de betreffende Partijstaat onder het internationale recht.¹ Door het Internationale Comité van het Rode Kruis (International Committee of the Red Cross, ICRC), dat in de Verdragen en Protocolen van Genève onder andere is belast met het ondersteunen van de Partijstaten bij het toepassen van het humanitair oorlogsrecht, is deze bepaling van artikel 36 toegelicht in zowel de gezaghebbende

Unofficial translation

WORKING GROUP ON INTERNATIONAL LAW AND CONVENTIONAL WEAPONS USE

Opinion on: Deployment of Cyber
capabilities and means as a method of
warfare

Introduction

As will be detailed below, cyber capabilities present a new challenge to the application of the mandatory test of new means and methods of warfare. To better understand that challenge, this opinion first describes and explains in more detail the mandatory test of new means and methods of warfare. It then considers the phenomenon of "cyber capabilities" in the light of that obligation. Finally, framework advice is provided regarding the use of cyber capabilities in relation to international law.

The obligation to review new means and methods of warfare

Article 36 of the 1977 First Additional Protocol to the Geneva Conventions of 1949, in brief, obliges States Parties, when developing, acquiring or putting into use new means and methods of warfare, to assess whether the use of those means or methods would in some or all cases contravene the obligations of the State Party concerned under international law.¹ The International Committee of the Red Cross (ICRC), which is charged in the Geneva Conventions and Protocols, among other things, with assisting States Parties in the application of international humanitarian law (IHL), explains this provision of Article 36 both in the authoritative Commentary to the Protocols and in the Guide specifically focused

¹ De tekst van de bepaling luidt: Op een Hoge Verdragsluitende Partij rust bij de bestudering, ontwikkeling, aanschaf of invoering van een nieuw wapen, een nieuw middel of een nieuwe methode van oorlogvoering de verplichting, vast te stellen of het gebruik daarvan, in bepaalde of in alle omstandigheden, door dit Protocol of door enige andere regel van het ten aanzien van de Hoge Verdragsluitende Partij toepasselijke volkenrecht is verboden.

The text of the provision reads: In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

Commentary bij de Protocollen als in de Guide die specifiek is gericht op deze toetsverplichting. Uit deze toelichtingen op de verplichting vevat in artikel 36, zijn voor dit advies de volgende relevante elementen te identificeren.

Het element "nieuw" ziet nadrukkelijk op de vraag of het middel of de methode "nieuw" is voor de Partijstaat in kwestie. Ook als het middel of de methode al in gebruik is elders in de wereld, of al enige tijd bestaat, moet de toets zoals bedoeld in artikel 36 worden uitgevoerd. Daarbij kan in de praktijk wel de kanttkening worden geplaatst dat gebruik in andere landen waarvan bekend is dat die de toets zelf al hebben uitgevoerd en voor wie dezelfde internationaalrechtelijke verplichtingen gelden, in bepaalde gevallen het zelf uitvoeren van de toets tot een marginale toets kan reduceren of kan doen reduceren tot een (beperkte) verificatie van de door dat andere land uitgevoerde toets. Er moet dan echter wel sprake zijn van een redelijk vertrouwen dat de toets deugdelijk is uitgevoerd door het andere land in kwestie en het (beoogde) gebruik van het middel moet overeenkomen met het beoogde gebruik door het land dat het middel of de methode wil gaan toepassen. Hoewel deze benadering niet in lijn is met de adviezen van het ICRC, kunnen binnen de hierboven gestelde kaders en voorwaarden redenen van praktische en pragmatische aard bestaan om deze benadering met voorzichtigheid toe te passen. Zo heeft ook Nederland deze benadering enige tijd gehanteerd, tot aan de heroprichting van de AIRCW in 2007. Naast de hierboven bedoelde nieuwigheid, is een middel echter ook "nieuw" als het een modificatie betreft van reeds in gebruik zijnde middelen en de uitwerking van dat middel in relevante mate wijzigt als gevolg van de modificatie. Tot slot is een toets vereist als de inzetmodaliteiten van een middel significant wijzigen, zoals het gebruik van een antimaterieel middel voor antipersoneel inzet. Zie echter ook de opmerkingen hierna ten aanzien van het element "gebruik".

Wat betreft "middelen en methoden van oorlogvoering" heeft de AIRCW tot nu toe alleen adviezen uitgebracht ten aanzien van middelen van oorlogvoering. Daarbij is in de praktijk een benadering toegepast waarbij het begrip "middelen van oorlogvoering" wordt beschouwd als alle wapens en munitie omvattend. Daarbij worden als "wapens" beschouwd alle middelen waarmee wordt beoogd personen te doden of te verwonden of ten aanzien van personen dwang uit

on this review obligation. From these explanations of the obligation contained in Article 36, the following relevant elements can be identified for this Opinion.

The element "new" expressly refers to whether the means or method is "new" to the State Party in question. Even if the means or method is already in use elsewhere in the world, or has been in existence for some time, the test referred to in Article 36 should be carried out. In practice, however, the comment can be made that use in other countries that are known to have already performed the test themselves and to which the same international law obligations apply may, in certain cases, reduce the performance of the test itself to a marginal test or may reduce it to a (limited) verification of the test performed by that other country. However, there must then be reasonable confidence that the test has been properly carried out by the other country in question and the (intended) use of the means must correspond to the intended use by the country that intends to apply the means or method. While this approach is not in line with ICRC advice, within the frameworks and conditions set out above, there may be reasons of a practical and pragmatic nature to apply this approach with caution. Similarly, the Netherlands used this approach for some time, until the re-establishment of the AIRCW in 2007. However, in addition to the novelty referred to above, a means is also "new" if it is a modification of products already in use and the effect of that product changes to a relevant extent as a result of the modification. Finally, a test is required if the deployment modalities of a means change significantly, such as the use of an anti-material means for anti-personnel deployment. However, see also the comments below regarding the "use" element.

With regard to "means and methods of warfare", the AIRCW has so far only issued opinions with regard to means of warfare. In doing so, it has in practice applied an approach whereby the concept of "means of warfare" is considered to include all weapons and ammunition. "Weapons" include all means by which it is intended to kill, injure or coerce persons² as well as all means by which it is intended to destroy, damage or interfere with the functioning of the equipment of another³.

te oefenen² alsmede alle middelen waarmee wordt beoogd materieel van een ander³ te vernietigen of te beschadigen of de werking daarvan te (ver)hinderen. Als "munitie" worden tot slot beschouwd alle middelen die bedoeld zijn om verschoten te worden of die een explosieve lading bevatten.

Methoden van oorlogvoering zijn tot dusver niet door de AIRCW getoetst. Naast de observatie dat het een moeilijk definieerbaar begrip betreft, worden methoden van optreden van de krijgsmacht in het algemeen al voorzien van juridische toetsing. Bij ad-hoc beslissingen of keuzes tijdens de operationele inzet, beschikt de commandant over de mogelijkheid (en in veel gevallen ook de verplichting) om de militair jurist te velde (de "Legad" in het inzetgebied) te raadplegen. Meer structurele methoden van optreden vallen al snel onder het begrip "doctrine", waarvoor binnen de Nederlandse krijgsmacht speciale goedkeurings- en toetsingsprocedures gelden. In relevante gevallen wordt de Directie Juridische Zaken bij die procedures betrokken, net zoals die Directie wordt betrokken bij meer fundamentele of complexe vraagstukken ten aanzien van voorgenomen methoden van optreden tijdens (lopende) militaire operaties, zo nodig via het "24/7" piketsysteem. Het feit dat de AIRCW tot nu toe geen advies heeft uitgebracht ten aanzien van methoden van oorlogvoering is dan ook een pragmatisch gevolg van de bestaande procedures binnen Defensie en geen principiële keuze geweest.

Ten aanzien van "gebruik" geven de toelichtingen van het ICRC nadrukkelijk aan dat het hier het beoogde gebruik van het middel of de methode

Finally, "munition" includes any means intended to be fired or containing an explosive charge.

Methods of warfare have so far not been reviewed by the AIRCW. Besides the observation that it is a difficult concept to define, methods of the armed forces in general are already provided with legal review. For ad hoc decisions or choices during operational deployment, the commander has the option (and in many cases the obligation) to consult the military lawyer in the field (the "Legad" in the deployment area). More structural methods of action easily fall under the concept of "doctrine", which is subject to special approval and review procedures within the Dutch armed forces. In relevant cases, the Directorate of Legal Affairs is involved in those procedures, just as that Directorate is involved in more fundamental or complex issues regarding intended methods during (ongoing) military operations, if necessary through the "24/7" reach-back system. Therefore, the fact that the AIRCW has so far not issued an opinion regarding methods of warfare is a pragmatic consequence of the existing procedures within the Defence organisation and has not been a choice of principle.

Regarding "use", the ICRC's explanations explicitly indicate that this refers to the intended use of the means or method.

² Deze in de praktijk gegroeide werkdefinitie omvat dus ook alle minder-letale wapens, zoals de FN-303, die gebruikt worden in het kader van *crowd and riot control*. Ook als de FN-303 alleen wordt gebruikt om personen te markeren, is het ultieme doel daarvan het uitoefenen van (legitieme) dwang, waaronder rechtshandhaving.

This working definition, which has evolved in practice, thus includes all less-lethal weapons, such as the FN-303, used in the context of *crowd and riot control*. Even if the FN-303 is only used to mark individuals, its ultimate purpose is to exercise (legitimate) coercion, including law enforcement.

³ Deze neutrale term is bewust gekozen om onwenselijke beperking van de werkdefinitie te voorkomen. Dit ziet dus niet alleen op een vijand in een gewapend conflict of een als zodanig geïdentificeerde tegenstander in een confrontatie, maar op alle subjecten ten aanzien van wie de wapens worden toegepast. Anderzijds is hiermee bedoeld om gebruik tegen eigen middelen uit te sluiten, zoals het vernietigen van eigen materieel, voor zover dat het uitsluitend toegestane doel is van het middel in kwestie. Zie ook de opmerkingen hierna over misbruik.

This neutral term was deliberately chosen to avoid undesirable limitation of the working definition. Thus, it not only refers to an enemy in an armed conflict or an opponent identified as such in a confrontation, but to all subjects against whom weapons are applied. On the other hand, this is intended to exclude use against own means, such as the destruction of own equipment, insofar as that is the exclusively authorised purpose of the means in question. See also the comments below on abuse.

betreft. Al dan niet opzettelijk misbruik hoeft niet te worden meegewogen in de toets. Deze benadering is logisch, omdat in beginsel elk middel en elke methode misbruikt kan worden en daarmee strijdigheid met het recht kan opleveren, ook de middelen en methoden die normaliter in het geheel niet omstreden zijn. Daarnaast blijkt uit de praktijk dat de inventiviteit van personen die opzettelijk kwaad willen doen tamelijk onbegrensd is en kan van een toetsingsinstantie niet worden verwacht dezelfde inventieve benadering te moeten hanteren bij elke toetsing. Wel moet hierbij de kanttekening worden geplaatst dat evidente of zeer voor de hand liggende mogelijkheden tot misbruik die inherent zijn aan het middel, wel betrokken zouden moeten worden. Zo zal een instelbare laser die bedoeld is voor waarschuwing van personen- maar tevens instelbaar is op een intensiteit die permanente blindheid veroorzaakt, niet snel tot goedkeuring kunnen leiden.

Tot slot kan worden opgemerkt dat "het internationale recht" niet alleen het Eerste Aanvullende Protocol omvat, maar alle verplichtingen die op grond van het internationale recht van toepassing zijn op de Partijstaat. Dat omvat dus ook alle wapenbeheersings- of ontwapeningsverdragen en de mensenrechtenverplichtingen.

Cybermiddelen in relatie tot de toetsingsverplichting onder artikel 36

Op grond van bovenstaande uiteenzetting over de toetsingsverplichting onder artikel 36 van het Eerste Aanvullende Protocol en de eerder door de AICRW uitgebrachte adviezen over specifieke wapens en munitie kan worden opgemaakt dat de toets uitgaat van de gedragingen van de middelen en methoden van oorlogvoering en de effecten op de subjecten waartegen zij worden toegepast.⁴ Dit

⁴ Naast, uiteraard, de objectieve toets of het middel onder de definitie valt van een categoriaal verboden middel in daartoe bestemde specifieke verdragen en protocollen. Dergelijke verdragen en protocollen zijn echter in de regel gebaseerd op een eerdere beoordeling van de gedragingen en effecten van de middelen waarop zij zien. Daarnaast zij opgemerkt dat de AICRW ook een toetsingselement bevat aangaande gevaarlijke stoffen. Dat element is oorspronkelijk voortgekomen uit een motie van de Tweede Kamer inzake het gebruik van zware metalen in defensiemiddelen (waaronder munitie), en vormde daardoor feitelijk onderdeel van de politieke afwegingen ten aanzien van een middel, maar is in de praktijk uitgegroeid tot een beoordeling van alle gevaarlijke stoffen die een te toetsen middel bevat. Dit element is voor de onderhavige beoordeling van cybercapaciteiten echter niet relevant.

In addition, of course, to the objective test of whether the means falls within the definition of a categorically prohibited means in specific treaties and protocols intended for that purpose. However, such conventions and protocols are generally based on a previous assessment of the conduct and effects of the means to which they refer. In addition, it should be noted that the AICRW also contains a review element regarding hazardous substances. That element originally arose from a motion of the House of Representatives on the use of heavy metals in defence equipment (including ammunition), and was therefore effectively part of the political

Intentional or non-intentional misuse need not be considered in the test. This approach is logical because, in principle, any means and method can be abused and thus constitute a violation of the law, including means and methods that are normally not at all controversial. In addition, practice shows that the inventiveness of persons who deliberately want to do harm is fairly unlimited and a reviewing body cannot be expected to have to adopt the same inventive approach in every review. However, it should be noted that obvious or readily foreseeable possibilities for abuse inherent in the device should be included. For example, an adjustable laser that is intended for warning persons but is also adjustable to an intensity that causes permanent blindness will not be likely to lead to approval.

Finally, it may be noted that "international law" includes not only the First Additional Protocol, but all obligations applicable to the State Party under international law. This therefore includes any arms control or disarmament treaty and human rights obligations.

Cyber resources in relation to the review obligation under Article 36

Based on the above explanation of the review obligation under Article 36 of the First Additional Protocol and the earlier opinions issued by the AICRW on specific weapons and munitions, it can be seen that the review takes into account the conduct of the means and methods of warfare and the effects on the subjects against whom they are applied.⁴ This

toetsingssysteem veronderstelt dan ook wat betreft de middelen, dat deze aan bepaalde beproevingen of observaties kunnen worden blootgesteld en dat die beproevingen en observaties kunnen leiden tot replicerbare, empirische resultaten die beoordeeld kunnen worden. Die beoordeling gaat vervolgens uit van de fysieke, of kinetische, effecten van het middel op het subject en de afweging daarvan in relatie tot de verplichtingen onder het internationale recht.

Middelen worden in het kader van artikel 36, zoals ook door de AIRCW toegepast, beschouwd als wapens en munitie of andere meetbare of tastbare "subjecten" die als gevolg van hun fysieke kenmerken of uitwerkingen naar hun aard beoordeeld kunnen worden en zo nodig, afhankelijk daarvan, verboden zouden kunnen zijn. Cyber 'middelen' hebben dergelijke kenmerken echter niet en kunnen dus niet op die grondslag verboden zijn. Wel kunnen zij, afhankelijk van het soort en type cybermiddel, fysieke effecten teweeg brengen. Maar dat effect is het resultaat van een keten van interacties die uiteindelijk kunnen resulteren in een bepaald gedrag van een ander systeem waaruit fysieke gevolgen optreden. Dat verandert echter niet de observatie dat het cybermiddel zelf, als zodanig geen fysieke effecten tot gevolg heeft. Met het risico van overmatige simplificatie kan een vergelijking worden gemaakt met een schakelaar die een ziekenhuis met het stroomnet verbindt: de schakelaar is als zodanig niet relevant vanuit het perspectief van artikel 36, maar het moedwillig uitzetten van de stroom kan dat onder omstandigheden wel zijn als "methode van oorlogvoering". Wat betreft de cybermiddelen betekent dat, dat niet het cyber 'middel' (computerprogrammatuur) zelf, maar de methode of de manier waarop het wordt ingezet onder omstandigheden verboden kan zijn.⁵

system of review therefore assumes, with regard to the means, that they can be subjected to certain tests or observations and that those tests and observations can lead to replicable, empirical results that can be assessed. That assessment is then based on the physical, or kinetic, effects of the means on the subject and its consideration in relation to obligations under international law.

Means are considered under Article 36, as also applied by the AIRCW, as weapons and munitions or other measurable or tangible "subjects" that, as a result of their physical characteristics or effects, can be judged by their nature and could, if necessary, be prohibited, depending on it. Cyber 'means', however, have no such characteristics and therefore cannot be prohibited on that basis. They can, however, produce physical effects, depending on the kind and type of cyber means. But that effect is the result of a chain of interactions that may ultimately result in a determined behaviour of another system from which physical effects occur. However, that does not change the observation that the cyber agent itself, as such, does not result in physical effects. At the risk of oversimplification, a comparison can be made with a switch connecting a hospital to the power grid: the switch, as such, is not relevant from the perspective of Article 36, but deliberately turning off the power may be relevant under certain circumstances as a "method of warfare". As for cyber means, this means that it is not the cyber 'means' (computer software) itself, but the method or manner in which it is deployed that may be prohibited under the circumstances.⁵

considerations with regard to an agent, but in practice it has evolved into an assessment of all hazardous substances contained in an agent under review. However, this element is not relevant to the present assessment of cyber capabilities.

⁵ Hoewel in theorie ook zodanige cyber 'middelen' ontwikkeld zouden kunnen worden dat ze naar hun aard strijdig zijn met het oorlogsrecht (zoals software die specifiek gericht is op het uitschakelen van de stroomvoorziening in ziekenhuizen) is de ontwikkeling van dergelijke middelen vanwege de evidente strijdigheid met het oorlogsrecht niet verwachtbaar. Anderzijds zou het, ook als een dergelijk 'middel' niet als middel getoetst wordt maar aan de in dit advies gestelde voorwaarden getoetst wordt, niet tot een andere uitkomst leiden ten aanzien van de onverenigbaarheid met het oorlogsrecht.

Although in theory, cyber 'agents' could also be developed in such a way that they are by their nature contrary to the law of war (such as software specifically aimed at disabling the power supply in hospitals), the development of such agents is not expected due to the obvious conflict with IHL. On the other hand, even if such a 'means'

Het ontbreken van de hierboven genoemde kenmerken heeft ook tot gevolg dat het in de inleiding van dit deel van het advies beschreven toetsingssysteem niet op cybermiddelen als zodanig kan worden toegepast. Zo hebben middelen die zich bijvoorbeeld richten op de data van het subject(systeem) of de opslag, uitwisseling of verwerking van data, niet in alle gevallen fysieke gevolgen voor mensen en materieel. Voorbeelden van cybermiddelen zonder (direct) fysiek gevolg zijn cybermiddelen ter ondersteuning van inlichtingenactiviteiten, zoals het vergaren van inlichtingen of het misleiden van de tegenstander, en middelen die de toegang tot de eigen netwerken verhinderen of monitoren. Deze soort middelen zijn dan ook, voor zover zij inderdaad niet beoogd zijn om fysieke gevolgen te veroorzaken, niet toetsbaar op de wijze zoals hierboven omschreven.

Ook indien de inzet van cybermiddelen wel fysieke effecten beoogt,⁶ leveren deze middelen – evenals alle cybermiddelen – de complicatie op dat het middel als zodanig niet toetsbaar is op de wijze zoals hierboven omschreven. Het ‘middel’ bestaat immers uit computerprogrammatuur die op andere ICT-apparatuur of software een bepaalde – verwachte of voorspelbare – uitwerking heeft. Die uitwerking heeft vervolgens (al dan niet met andere tussenstappen) een beoogd fysiek gevolg

The absence of the aforementioned characteristics also means that the review system described in the introduction to this part of the opinion cannot be applied to cyber means as such. For example, means that focus on the data of the subject (system) or the storage, exchange or processing of data do not in all cases have physical consequences for people and equipment. Examples of cyber means without (direct) physical consequences are cyber means in support of intelligence activities, such as intelligence gathering or adversary deception, and means that prevent or monitor access to one's own networks. Therefore, to the extent that these types of means are indeed not intended to cause physical consequences, they are not reviewable in the manner described above.

Even if the deployment of cyber means is not intended to cause physical effects,⁶ these means – like all cyber means – pose the complication that the means as such are not testable in the manner described above. After all, the ‘means’ consists of computer software that has a certain – expected or predictable – effect on other ICT equipment or software. That effect then (with or without other intermediate steps) has an intended physical consequence

were not tested as a means but tested against the conditions set out in this opinion, it would not lead to a different outcome with regard to its incompatibility with IHL.

⁶ Voorbeelden van dergelijke middelen zijn cybermiddelen die specifiek tot doel hebben om bepaalde ICS (Industrial Control Systems) waaronder SCADA (Supervisory Control and Data Acquisition) systemen te beïnvloeden, zoals die van (vitale) infrastructuur. Naast de observatie dat ook ten aanzien van deze middelen beargumenteerd kan worden dat de effecten niet zozeer het gevolg zijn van het middel zelf maar van de methode (in dit geval het gerichte gebruik van het middel op specifieke ICS-systemen), leveren deze middelen – evenals alle cybermiddelen – de complicatie op dat het middel als zodanig niet toetsbaar is op de wijze zoals hierboven omschreven. Het middel bestaat immers uit computerprogrammatuur die op andere ICT-apparatuur of software een bepaalde uitwerking heeft. Die uitwerking heeft vervolgens (al dan niet met andere tussenstappen) een fysiek gevolg in de “tastbare wereld”. Ook al hebben bij deze soort cybermiddelen de fysieke effecten een meer directe relatie met het middel als zodanig, kan ook ten aanzien van deze middelen dan ook worden beargumenteerd dat de toets zich niet richt, c.q. moet richten, op het middel zelf, maar op de methode van oorlogvoering waarvan dit middel een (zonder twijfel fundamenteel of centraal) onderdeel vormt.

Examples of such means are cyber means specifically aimed at influencing certain ICS (Industrial Control Systems) including SCADA (Supervisory Control and Data Acquisition) systems, such as those of (vital) infrastructure. Besides the observation that also with regard to these means, it can be argued that the effects are not so much the result of the means itself but of the method (in this case, the targeted use of the means on specific ICS systems), these means – like all cyber means – pose the complication that the means as such are not testable in the way described above. After all, the means consists of computer software that has a certain effect on other ICT equipment or software. That effect then (with or without other intermediate steps) has a physical consequence in the “tangible world”. Even though in the case of these types of cyber means the physical effects have a more direct relationship to the means as such, it can therefore also be argued with regard to these means that the test does not focus, or should focus, on the means itself, but on the method of warfare of which this means forms a (no doubt fundamental or central) part.

in de "tastbare wereld". Het is dan ook niet mogelijk om de rechtstreekse fysieke gevolgen van het cybermiddel zelf te toetsen aan verenigbaarheid met het oorlogsrecht.⁷ De manier (methode) waarop cybermiddelen worden ingezet is echter wel toetsbaar aan verenigbaarheid met het oorlogsrecht.

Gelet op deze overwegingen moet geconcludeerd worden dat cyber 'middelen' geen "middelen of wapens" zijn in de tot nu toe gehanteerde invulling die onder andere het ICRC (en de AIRCW) aan "middelen" geeft in de zin van artikel 36.

Hierin schuilt, voor de onderhavige beoordeling, het onderscheid tussen het toetsen van een middel, waarbij de te beoordelen fysieke gevolgen en uitwerkingen rechtstreeks gekoppeld worden aan dat middel zelf, en het toetsen van een methode, waarbij niet de fysieke gevolgen van het middel zelf, maar de manier waarop het wordt ingezet, en de gevolgen daarvan, beoordeeld wordt.

Bovenstaande observaties ten aanzien van cybermiddelen en de beschrijving van de verplichte toets op basis van artikel 36 van het Eerste Aanvullende Protocol leveren de volgende conclusies op. Wat betreft het element "nieuw" vallen cybermiddelen en het gebruik daarvan onder de betekenis van dit element en dus onder de toetsingsverplichting. Daarbij zij opgemerkt dat de standpunten en uitspraken van de regering in politieke en maatschappelijke discussies in nationaal en internationaal verband, waaronder in het kader van de Verenigde Naties, inzake de juridische kaders van cyberoptreden en de rechtsstatelijke uitgangspunten ten aanzien van cyberspace een eigen, nationale toets onvermijdelijk maken. Ook al wordt in voorkomend geval mogelijk gebruik gemaakt van door andere landen ontwikkelde cybermiddelen, zal het (voorgenomen) gebruik daarvan door Nederland ook door Nederland zelf getoetst moeten worden.

Wat betreft het element "middelen en methoden van oorlogvoering" volgt uit de hierboven gestelde observaties dat de toets van het (voorgenomen) gebruik van cybermiddelen een toets van een

in the "tangible world". It is therefore not possible to test the direct physical effects of the cyber means itself for compatibility with IHL.⁷ However, the manner (method) in which cyber means are deployed is testable for compatibility with IHL.

Given these considerations, it must be concluded that cyber 'means' are not "means or weapons" in the interpretation used so far by the ICRC (and the AIRCW), among others, of "means" within the meaning of Article 36.

Herein lies, for the purposes of the present assessment, the distinction between testing a means, where the physical consequences and effects to be assessed are directly linked to that means itself, and testing a method, where not the physical consequences of the means itself, but the manner in which it is deployed, and its consequences, are assessed.

The above observations regarding cyber remedies and the description of the mandatory test under Article 36 of the First Additional Protocol yield the following conclusions. As regards the element "new", cyber means and their use fall within the meaning of this element and thus within the scope of the review obligation. It should be noted that the government's positions and statements in political and civil society discussions nationally and internationally, including within the framework of the United Nations, regarding the legal frameworks of cyber action and the principles of the rule of law in relation to cyberspace make its own, national test inevitable. Even though cyber means developed by other countries may be used where appropriate, their (intended) use by the Netherlands will also have to be tested by the Netherlands itself.

Regarding the "means and methods of warfare" element, it follows from the observations made above that the test of the (intended) use of cyber means is a test of a (intended) method of

⁷ Dit staat bovendien nog los van het feit dat een cybermiddel dat een ander systeem aan of uit kan zetten niet noodzakelijk relevant is in het kader van artikel 36, maar dat wel relevant kan zijn wat met dat middel aan of uit wordt gezet. Zie de vergelijking met de stroomnetschakelaar die hierboven werd gegeven.

Moreover, this is quite apart from the fact that a cyber means that can turn another system on or off is not necessarily relevant under Article 36, but what is turned on or off by that means may be relevant. See the comparison with the mains power switch given above.

(voorgenomen) methode van oorlogvoering betreft en niet van de middelen als zodanig. Dat betekent dat de toets zich richt op het beoogde effect van het optreden en een beoordeling van de rechtmatigheid van dat effect in de specifieke omstandigheden waarin het voorgenomen gebruik moet plaatsvinden. Dit aspect wordt hieronder in het advies nader besproken.

De elementen "gebruik" en "het internationale recht" hebben in deze context, zowel wat betreft het subject van deze toets als wat betreft het feit dat de toets zich richt op een methode in plaats van een middel van oorlogvoering, geen bijzondere of andere betekenis dan het geval was in eerdere adviezen van de AICW of dan hierboven in de uitleg van de toets is aangegeven. Wat betreft het recht zij slechts opgemerkt dat in het kader van de hierboven reeds genoemde uitlatingen en standpunten van de regering, de regering steeds het standpunt heeft ingenomen dat optreden in het cyberdomein onderworpen is aan dezelfde rechtskaders als optreden in het "tastbare" domein.

Advies

Hoewel het benaderen van het gebruik van cybermiddelen een toets zoals bedoeld in artikel 36 van het Eerste Aanvullende Protocol meer uitvoerbaar maakt dan een benadering waarbij de middelen centraal staan, wijkt het gebruik van cybermiddelen in zekere mate af van de (overige) methoden van oorlogvoering zoals normaliter bedoeld in het kader van deze toetsingsverplichting. Dergelijke methode-gerelateerde toetsen gaan immers uit van het specifieke effect of doel van de methode in kwestie, afgezet tegen de internationaalrechtelijke verplichtingen van de Partijstaat in kwestie. Het gebruik van cybermiddelen is echter een meer generieke methode van optreden, dat voor vele en sterk uiteenlopende doeleinden kan worden ingezet met evenveel en evenzo verschillende effecten. Dit heeft tot gevolg dat, evenals eerder het geval was bij het kaderadvies inzake klein kaliber munitie, dit advies alleen een algemeen kader bevat voor de rechtmatige toepassing van de, in dit geval, methode van oorlogvoering in kwestie. Bij daadwerkelijke voornemens tot inzet van deze methode van oorlogvoering zal dan ook een specifieke rechtmatigheidstoets moeten plaatsvinden. In tegenstelling tot voornoemd kaderadvies inzake klein kaliber munitie, en gelet op de hierboven beschreven specifieke

warfare and not of the means as such. This means that the test focuses on the intended effect of the action and an assessment of the legality of that effect in the specific circumstances in which the intended use is to take place. This aspect is discussed in more detail below in the opinion.

The elements "use" and "international law" have no particular or different meaning in this context, both in terms of the subject matter of this test and the fact that the test focuses on a method rather than a means of warfare, than has been the case in previous opinions of the AICW or than indicated above in the explanation of the test. In terms of law, it should only be noted that in the context of the government's statements and positions already mentioned above, the government has always taken the position that action in the cyber domain is subject to the same legal frameworks as action in the "tangible" domain.

Opinion

While the approach to the use of cyber means makes a test referred to in Article 36 of the First Additional Protocol more practicable than a means-centred approach, the use of cyber means differs to some extent from the (other) methods of warfare as normally envisaged under this test obligation. After all, such method-related tests are based on the specific effect or purpose of the method in question and evaluating that against the international law obligations of the State Party in question. However, the use of cyber means is a more generic method of action that can be used for many and widely different purposes with equally different effects. As a result, as was previously the case with the framework opinion on small calibre munitions, this opinion only provides a general framework for the lawful use of, in this case, the method of warfare in question. In case of actual intentions to use this method of warfare, a specific legality test will therefore have to be conducted. In contrast to the aforementioned framework advice on small-calibre ammunition, and given the specific characteristics of cyber means and their use described above, that case-specific test will in most cases not (be able to) be carried out by the AICW, but advice will have

eigenschappen van cybermiddelen en het gebruik daarvan, zal die casus- specifieke toets in de meeste gevallen niet uitgevoerd (kunnen) worden door de AIRCW maar zal advies moeten worden gevraagd aan ofwel de Legad van de commandant die deze methode van oorlogvoering wil gaan toepassen, ofwel de Directie Juridische Zaken. Deze conclusie wordt mede ingegeven door de observatie dat de voorgenomen inzet in veel gevallen onderworpen zal zijn aan een noodzaak tot snel handelen en een bepaalde mate van heimelijkheid of geheimhouding en in alle gevallen beoordeeld zal moeten worden aan de hand van de specifieke kaders, waaronder de toepasselijke juridische kaders, van de operatie of de (overige) militaire inzet in kwestie.

Hoewel geen voorgeschreven onderdeel van de toetsingsverplichting op grond van artikel 36 van het Eerste Aanvullende Protocol, betreft de AIRCW in elk advies ook politieke en beleidsaspecten in de beoordeling van het middel of de methode van oorlogvoering. Gelet op de hierboven genoemde afhankelijkheid van de uiteindelijke beoordeling van een daadwerkelijk voornemen tot gebruik van cybermiddelen van de specifieke context van dat voornemen, lenen politieke en beleidsaspecten zich niet voor opname in dit kaderadvies. Die aspecten liggen echter wel ten grondslag aan het algemene en algehele beleid van Defensie, en van de regering als geheel, ten aanzien van "cyber" als geheel, waaronder het element van offensieve inzet van cybermiddelen. Voor de beoordeling van specifieke voornemens tot inzet van cybermiddelen zij opgemerkt dat naast een Legad, veel commandanten ook over een politiek adviseur, de Polad, beschikken. Daarnaast vindt militair optreden altijd plaats met een vooraf bepaald politiek oogmerk, binnen door de politiek bepaalde randvoorwaarden en op basis van een door het politieke niveau gegeven opdracht en mandaat. Bij de besluitvorming omtrent de deelname aan, of uitvoering van, een militaire operatie of de inzet van militaire middelen, kan in voorkomend geval specifiek aandacht worden besteed aan het gebruik van cybermiddelen in die context. Tot slot is ook de Hoofddirectie Beleid benaderbaar, zoals hierboven al is opgemerkt ten aanzien van de Directie Juridische Zaken, en kan waar nodig worden geraadpleegd bij ad-hoc besluitvorming omtrent het beoogde gebruik van cybermiddelen.

to be sought from either the Legad of the commander intending to deploy this method of warfare, or the Directorate of Legal Affairs. This conclusion is partly prompted by the observation that in many cases the intended deployment will be subject to a need for swift action and a certain degree of stealth or secrecy, and in all cases will have to be assessed against the specific frameworks, including the applicable legal frameworks, of the operation or (other) military deployment in question.

Although not a prescribed part of the review obligation under Article 36 of the First Additional Protocol, the AIRCW also includes political and policy aspects in its assessment of the means or method of warfare in each opinion. Given the aforementioned dependence of the final assessment of an actual intention to use cyber means on the specific context of that intention, political and policy aspects do not lend themselves to inclusion in this framework opinion. However, those aspects do underpin the general and overall policy of the Defence organisation, and the government as a whole, on "cyber" as a whole, including the element of offensive deployment of cyber means. To assess specific intentions to deploy cyber means, it should be noted that in addition to a Legad, many commanders also have a political advisor, the Polad. In addition, military action always takes place with a predetermined political purpose, within politically determined preconditions and on the basis of an order and mandate given by the political level. When deciding on participation in, or execution of, a military operation or deployment of military means, the use of cyber means in that context may be specifically considered, where appropriate. Finally, the Main Directorate of Policy is also approachable, as already noted above in relation to the Directorate of Legal Affairs, and can be consulted where necessary in ad hoc decision-making regarding the intended use of cyber means.

Voor dit kaderadvies inzake de rechtmatigheid van het gebruik van cybermiddelen kunnen, met inachtneming van de hierboven beschreven observaties en conclusies, de volgende kaders worden vastgesteld:

1. Het gebruik van cybermiddelen moet als zodanig, maar ook wat betreft de voorgenomen of beoogde effecten en uitwerkingen van dat gebruik, passen binnen het mandaat en de opdracht van de inzet waarbinnen dat gebruik zal plaatsvinden.
2. Aan het specifieke gebruik van cybermiddelen gaat juridische advisering vooraf.
3. Op het gebruik van cybermiddelen zijn de regels van het internationale recht van toepassing. Deze regels worden in dit kaderadvies niet integraal weergegeven. De regels zoals opgenomen in de twee Tallinn Manuals zijn indicatief voor de toepasselijke rechtsregels voor het rechtmatig gebruik van cybermiddelen en kunnen door de Nederlandse krijgsmacht als uitgangspunt worden gehanteerd. De hierna genoemde regels gelden daarbij als algemene kaders en doen niet af aan, en zijn geen vervanging voor, de kaders zoals in voornoemde publicaties opgenomen.
 - A. Het gebruik van cybermiddelen mag geen inbreuk maken op de soevereiniteit van andere landen, tenzij daarvoor een volkenrechtelijke rechtsgrond aanwezig is.
 - B. Het gebruik van cybermiddelen mag geen schending opleveren van het non-interventie beginsel, tenzij daarvoor een volkenrechtelijke rechtsgrond aanwezig is.
 - C. Bij inzet buiten de context van een gewapend conflict moeten, behoudens en voor zover er sprake is van rechtmatige (wettelijke of volkenrechtelijke) uitzonderingen, bij het gebruik van cybermiddelen de verplichtingen op basis van de mensenrechtenverdragen worden nageleefd. Dit omvat onder andere het recht op leven, het recht op de persoonlijke levenssfeer en het recht op vrije meningsuiting.
 - D. Bij inzet in de context van een gewapend conflict moet bij het gebruik van cybermiddelen het humanitair oorlogsrecht worden nageleefd. Dit betekent onder andere dat:

For this framework opinion on the legality of the use of cyber means, taking into account the observations and conclusions described above, the following frameworks can be established:

1. The use of cyber means as such, but also the intended effects thereof, must fit within the mandate and remit of the deployment within which that use will take place.
2. The specific use of cyber means must be preceded by legal advice.
3. The use of cyber means is subject to the rules of international law. These rules are not reproduced in full in this framework advice. The rules as included in the two Tallinn Manuals are indicative of the applicable legal rules for the lawful use of cyber means and can be used by the Dutch armed forces as a starting point. The rules mentioned below are moreover to be considered as a general framework and do not detract from, nor replace, the framework as included in the aforementioned publications.
 - A. The use of cyber means should not infringe on the sovereignty of other countries, unless there is an international legal basis for doing so.
 - B. The use of cyber means should not violate the non-intervention principle, unless there is an international legal basis for doing so.
 - C. When deployed outside the context of an armed conflict, unless and to the extent there are legitimate (legal or international law) exceptions, the use of cyber means must comply with obligations under human rights treaties. These include the right to life, the right to privacy and the right to freedom of expression.
 - D. When deployed in the context of armed conflict, the use of cyber means must respect IHL. This means, inter alia, that:

- (i) De cybermiddelen richtbaar moeten zijn en uitsluitend gericht mogen worden op legitieme doelen;
- (ii) De verwachtbare nevenschade van het gebruik van de cybermiddelen niet buitensporig mag zijn in vergelijking met het concrete en directe militaire voordeel van dat gebruik.

- (i) Cyber means must be targetable and directed only at lawful targets;
- (ii) The expected collateral damage from the use of cyber means should not be excessive in relation to the concrete and direct military advantage anticipated from that use.

Geraadpleegde literatuur

Gill, T.D. en Fleck, D. [eds.], *The Handbook of the International Law of Military Operations*, 2nd Ed., Oxford, 2015

Henckaerts, J.M. en Doswald-Beck, L. [eds.], *Customary International Humanitarian Law, Volume I: Rules*, Cambridge/ICRC, 2005

ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, Genève, 2006 Sandoz, Y., Swinarski, C. en Zimmerman, B. [eds.], *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff/ICRC, 1987

Schmitt, M.N. [ed.], *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2014

Weller, M. [ed.], *The Oxford Handbook of the Use of Force in International Law*, Oxford, 2015

Literature consulted

Gill, T.D. and Fleck, D. [eds.], *The Handbook of the International Law of Military Operations*, 2nd Ed., Oxford, 2015

Henckaerts, J.M. and Doswald-Beck, L. [eds.], *Customary International Humanitarian Law, Volume I: Rules*, Cambridge/ICRC, 2005

ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, Geneva, 2006 Sandoz, Y., Swinarski, C. and Zimmerman, B. [eds.], *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff/ICRC, 1987

Schmitt, M.N. [ed.], *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2014

Weller, M. [ed.], *The Oxford Handbook of the Use of Force in International Law*, Oxford, 2015