

**SCHEMER
OORLOG**

SCHEMER OORLOG

Kolonel
ROGER HOUSEN



**We zijn slecht voorbereid op cyberaanvallen, drones,
desinformatie en sabotage - wat nu?**

INHOUD

9

VOORWOORD

15

HOOFDSTUK I

Een dag in de toekomst – Uitgangssituatie

25

HOOFDSTUK II

Schemeroorlog als een systeem

35

HOOFDSTUK III

Wanneer de waarheid verduisterd wordt

63

HOOFDSTUK IV

Wanneer de stroom uitvalt

83

HOOFDSTUK V

Wanneer je kopieermachine een wapen wordt

105

HOOFDSTUK VI

Wanneer de overheid tot stilstand
komt... net zoals je auto

139

HOOFDSTUK VII

Wanneer de schemeroorlog verder escaleert

167

HOOFDSTUK VIII

Wanneer België de militaire crisistijd uitroept

203

HOOFDSTUK IX

Een dag in de toekomst: onze tegenstanders te
slim af zijn om de schaduwoorlog te winnen

VOORWOORD

De oorlog waar dit boek over gaat, is anders dan het type oorlog waar wij spontaan aan denken, namelijk de ‘conventionele’ of ‘klassieke’ krijgsverrichtingen die gebaseerd zijn op beelden van de Tweede Wereldoorlog met schietende tanks, bombarderende vliegtuigen en elkaar op zee bekampende oorlogsschepen. Dit is het westerse model van gewapende conflicten, de ‘kinetische’ strijd: vuurkracht is koning – en liefst dan nog met grote precisie – en de overwinning op het slagveld is alles.

Maar we krijgen een compleet andere krachtmeting wanneer onze tegenstanders zich realiseren dat ze een dergelijke klassieke oorlog niet kunnen winnen en een andere weg naar de zege gaan bewandelen.

Dan krijg je een oorlog die je nauwelijks hoort en amper ziet, want hij wordt gevoerd zonder kanongebulder, wapengekletter en loopgraven. Het is een schemeroorlog. Hij wordt gevoerd in het gebied tussen vrede en oorlog en bestaat uit talloze kleine en op het eerste gezicht losstaande incidenten, maar die uiteindelijk hetzelfde doel hebben als elke andere oorlog, met name: de tegenstander de eigen wil opleggen.

De bedenker van die schemeroorlog zit in het Kremlin. Om zijn Europese burens onderdanig te maken, gebruikt hij alle methoden die hij bij de KGB, de geheime dienst van de voormalige Sovjet-Unie, heeft geleerd, waaronder sabotage, cyberincidenten, spionage en moord. Het gaat erom een gevoel van onzekerheid te zaaien, verwarring te stichten, onenigheid te zaaien of een figuur uit het spel te halen en een andere persoon in een sleutelpositie te hijsen.

Aan het begin van de schemeroorlog staat geen formele oorlogsverklaring. De aanvaller is al lang geleden met zijn strijd begonnen, terwijl de aangevallen partij zich nog in vrede waant. Deze laatste ziet misschien de afzonderlijke prikjes, maar voegt ze niet samen tot een totaalbeeld. België en zijn Europese bondgenoten bevinden zich precies in deze situatie. Grote delen van hun bevolking hebben nog geen idee hoe uitgebreid en verstrekkend de aanval op hun land is.

Deze aanval treft ons land en zijn Europese partners bovendien in een tijd van grote onzekerheid. De Verenigde Staten dreigen namelijk

weg te vallen als garant voor hun veiligheid. Sinds de eerste verkiezing van Donald Trump in 2016, maar zeker sinds zijn herverkiezing in 2024, komt het woord ‘het Westen’ zelfs bij doorgewinterde transatlantici niet meer zo gemakkelijk over de lippen als voorheen. President Trump zaait namelijk niet alleen twijfel over de loyaliteit van Amerika aan zijn bondgenoten in de NAVO, hij sympathiseert ook openlijk met autocraten en kopieert hun methoden. Zijn aanvallen op de instellingen van de Amerikaanse democratie volgen een patroon dat ook te zien was bij Victor Orban en doorlopend toegepast wordt door andere rechts-populisten in Europa. De Russische president Vladimir Poetin heeft al deze ontwikkelingen met alle macht bevorderd.

De heerser in het Kremlin is slechts een van de verschillende autocraten die met veel doorzettingsvermogen werken aan het doorbreken van de door westerse democratieën gedomineerde wereldorde. Een andere is de Chinese leider Xi Jinping, die zijn alliantie met Poetin wel bijzonder tastbaar maakte op 22 maart 2023. Na een driedaags staatsbezoek aan Moskou daalde de Chinese president toen samen met Vladimir Poetin de trappen van het Kremlin af. Beneden bij de deur zei Xi Jinping nog enkele woorden tegen Poetin: ‘Er zijn nu veranderingen gaande zoals we die in honderd jaar niet hebben gezien’, aldus Xi. ‘En we brengen deze verandering samen tot stand.’ Schemeroorlog is daarvoor hun belangrijkste instrument.

Zowel Europa als de VS hebben de neiging om de acties van hun tegenstrevers verkeerd te interpreteren, omdat ze die door een oude bril bekijken. Ze begrijpen de motieven van Rusland en China vaak verkeerd, evenals hun doelstellingen en de gevolgen op lange termijn. Dat gebeurt vooral omdat deze landen datgene ondermijnen en verzwakken wat het Westen als zijn sterke punten beschouwt: open samenlevingen, militaire innovatie, dominantie van technologie op aarde en in de ruimte en langdurig leiderschap in mondiale instellingen.

In *Schemeroorlog* ontwikkelen we een scenario dat gebaseerd is op de escalatie van de dreiging van een gewapend conflict in Europa. De situatieschetsen met de verschillende incidenten en hun verloop zijn deels gebaseerd op echte gebeurtenissen en deels op draaiboeken van zogenaamde *war games* — computersimulaties van ernstige gebeurtenissen — en *table top*-oefeningen waarbij gefingeerde noodsituaties en crises bediscussieerd en geëvalueerd worden. In het algemeen

zijn ze fictief, overdreven en zullen ze waarschijnlijk niet in deze vorm plaatsvinden. Ze zijn gecondenseerd en moeten worden gezien als een kettingreactie van gebeurtenissen.

Centraal in onze veronderstelde situaties staan niet strategische of militaire overwegingen, maar vooral de gevolgen voor ons dagelijks leven, de samenleving, de vrijheid, de veiligheid en de democratie. Wat gebeurt er in België en in onze buurlanden als de aanvallen met niet-militaire middelen – cyberaanvallen, sabotage van essentiële voorzieningen, desinformatiecampagnes, verdachte dronevluchten – sterk toenemen en een gewapend conflict in Europa steeds waarschijnlijker wordt? Hoe robuust zijn onze noodvoorzieningen? Wat presteren onze overheden en veiligheidsdiensten in een scenario waarin kritieke infrastructuur – elektriciteit, water of telecommunicatie – uitvallen? Hoe kan de informatiebeveiliging worden gewaarborgd wanneer gerichte desinformatie en cyberaanvallen het vertrouwen in overheidsinstellingen ondermijnen?

Onze vrijheid moet worden begrepen, beschermd en in geval van nood ook verdedigd, niet alleen door strijdkrachten en veiligheidsdiensten, maar door alle burgers. Raketaanvallen of bombardementen op West-Europa zijn de komende jaren erg onwaarschijnlijk, net als een klassieke oorlog met tanks, pantserwagens en kanonnen. Rusland is daar op korte termijn militair niet toe in staat; het heeft minimaal vijf jaar na het einde van de oorlog in Oekraïne nodig om zijn krijgsmacht weer op te bouwen en zijn samenleving en economie opnieuw in staat te stellen om een nieuwe oorlog te voeren. En China zal Europa militair niet aanvallen.

Nochtans kan er ondertussen en op basis van de beschreven dreigingsscenario's wel grote schade bij ons en onze buurlanden aangericht worden.

Wij zijn daarop, om het cru te zeggen, onvoldoende voorbereid. We hebben talrijke mensen bij overheidsinstanties, in de politiek, bij organisaties en bedrijven gezien die nadenken over noodsituaties, zich inzetten en werken aan passende voorzorgsmaatregelen – of het nu gaat om klimaatverandering, een technische fout of een geopolitieke crisis. Ook het sterke vrijwilligerswerk in dit land en de daarmee samenhangende maatschappelijke solidariteit vormen een belangrijke bouwsteen van de veerkracht van de hele samenleving.

VOORWOORD

Maar daartegenover hebben de talloze incidenten en agressies van de voorbije jaren in Europa duidelijk gemaakt dat meer investeringen nodig zijn in de bescherming van de bevolking en de vitale diensten van ons land. Dat behoort tot de centrale uitdagingen waaraan de politiek, het bedrijfsleven en de samenleving de komende jaren meer dan ooit het hoofd moeten bieden.

Met dit boek willen we politieke besluitvormingsprocessen, maatschappelijke reacties en infrastructurele uitdagingen schetsen om ruimte te creëren voor reflectie en de voorbereiding te bevorderen. *Schemeroorlog* maakt geen aanspraak op volledigheid. Er zijn maatregelen en acties die we niet hebben voorzien, processen die door deskundigen zeer verschillend worden beoordeeld, regelgeving die nog in opmaak is of zaken die de lezers misschien nog te binnen schieten.

Ons boek is niet bedoeld om van jullie preppers te maken; we willen geen paniek zaaien, maar de discussie over maatschappelijke veerkracht objectiveren. Wij zijn van mening dat voorbereiding op een noodsituatie of crisis – of die nu het gevolg is van milieu-incidenten, oorlogen of geopolitieke omstandigheden – dit juist kan helpen voorkomen.

We willen informeren, sensibiliseren en motiveren. Want een veerkrachtige democratie leeft van een geïnformeerde en handelingsbekwame samenleving. In geval van nood worden het incasserings- en herstelvermogen van een land niet alleen bepaald in de politieke en militaire commandocentra, maar ook in het dagelijks leven van zijn burgers: in het functioneren van de veiligheidsdiensten en de noodhulp, in de toegang tot betrouwbare informatie, in het vertrouwen in het optreden van de staat en in de psychologische weerbaarheid van de mensen. Veerkracht is daarbij een uiting van democratische volwassenheid en rationeel handelen.

Met *Schemeroorlog* willen we aanzetten tot discussie, afweging en actie. Het is een uitnodiging om na te denken over noodsituaties – zodat we vandaag kunnen praten over wat morgen mogelijk zou kunnen zijn. En zodat we als samenleving de kracht ontwikkelen om ook in een crisis vrij, democratisch en handelingsbekwaam te blijven. Want voorbereiding op crises begint met verbeeldingskracht – en met de bereidheid om vragen te stellen en antwoorden te zoeken.

HOOFDSTUK I

EEN DAG IN DE TOEKOMST
– UITGANGSSITUATIE

Een novembermaand in de toekomst

Het is nog vroeg in de ochtend. Het allerheiligenverlof is net achter de rug en in de Europese hoofdsteden verloopt het leven zoals gewoonlijk. Maar in het NAVO-hoofdkwartier en in de commandocentra in Parijs, Londen en Berlijn heerst onrust. Ook in de Wetstraat 16 brandt al de hele nacht het licht; al urenlang lopen er onheilspellende berichten binnen. Europa stevent af op een nieuwe crisis: inlichtingendiensten observeren met name omvangrijke troepenbewegingen in Wit-Rusland en de Russische enclave Kaliningrad. De leiders in Moskou en Minsk sussen en wijzen kwaadwillige intenties af. Zij spreken van een ‘grote oefening’. Maar specialisten waarschuwen: de schaal van de manoeuvres is enorm en ze lijken verdacht veel op de massale troepenverplaatsingen rond de jaarwisseling van 2021 naar 2022, in de aanloop naar de Russische inval in Oekraïne.

Twee vragen liggen op ieders lippen in de Europese politieke en militaire operatiecentra: zal de Russische president het bevel geven om een NAVO-land binnen te vallen, en zo ja, wat wil hij dan bereiken? Op verzoek van de Baltische Staten en Polen start de NAVO het consultatiemechanisme overeenkomstig artikel 4 van het Noord-Atlantisch Verdrag. Dit stelt dat de lidstaten onderling overleg plegen wanneer de territoriale integriteit of veiligheid van een van hen bedreigd wordt.

De Belgische regering roept de Nationale Veiligheidsraad bijeen, die de reacties op urgente veiligheidssituaties in of voor het land coördineert. Hij wordt voorgezeten door de eerste minister en bestaat uit de vicepremiers, de ministers van Justitie, Binnenlandse Zaken en Buitenlandse Zaken en Defensie, en de chefs van de verschillende Belgische veiligheidsdiensten. Naast de beslissingen die achter gesloten deuren genomen worden, wil de premier dat de overheid naar buiten toe daadkrachtig overkomt.

De meeste Europese landen brengen hun legers in verhoogde paraatheid. De Belgische krijgsmacht plaatst onder meer logistieke en genie-troepen, belast met de verbetering van de weginfrastructuur, op een

hoger gereedheidsniveau, zodat zij in geval van een escalatie snel ondersteuning kunnen bieden aan andere overheidsdiensten.

Het Kremlin zoekt contact met de Verenigde Staten. De Russische president verzekert zijn Amerikaanse ambtsgenoot dat zijn land geen enkele agressieve bedoeling heeft. Washington van zijn kant wil te allen prijze vermijden in een nieuwe oorlog in Europa te worden meegezogen. Slechts na meerdere uitdrukkelijke Europese smeebedes laat het Witte Huis de aanvankelijke terughoudendheid enigszins varen en krijgt het Pentagon het bevel 2.000 bijkomende soldaten via luchtmachtbases in Duitsland en Polen naar Europa te sturen.

De NAVO verhoogt de paraatheidsstatus van haar snelle reactiemacht VJTF (Very High Readiness Joint Task Force) en verplaatst extra verkenningsvliegtuigen en AWACS-radartoestellen naar de oostflank van Europa. Een Belgisch fregat wordt naar de Oostzee gestuurd, terwijl onze luchtmacht samen met die van andere West-Europese landen een versterkte aanwezigheid laat zien boven de Baltische landen. Verschillende incidenten met Russische en westerse gevechtsvliegtuigen leiden tot een gespannen sfeer.

Via sociale netwerken en anonieme berichtenkanalen duiken nu desinformatiecampagnes op die gericht zijn op het zaaien van wantrouwen tegenover de Europese landen en hun leiders. Ze worden vergaande incompetentie, gebrek aan aandacht voor de échte problemen van de burgers en grotesk wokisme verweten. Ook de Belgische regering is een continu doelwit van valse en misleidende informatie. Zo worden er doelbewust deepfakes van politici verspreid om het wantrouwen te versterken.

Daarnaast zijn er onophoudelijk berichten over zogenaamd oprukkende Russische militaire formaties en een algemene mobilisatie en aanstaande evacuaties in Duitsland, Polen, Estland, Letland en Litouwen. Ze worden weliswaar als onjuist geïdentificeerd, maar verspreiden zich wel razendsnel. De verklaringen van de Belgische regering dat de legerdienst niet opnieuw zal ingevoerd worden en dat reservisten voornamelijk niet opgeroepen zullen worden, doen de ongerustheid

bij de bevolking niet afnemen. Integendeel, onder meer in Brussel, Luik en Antwerpen vinden er demonstraties plaats tegen de vermeende provocerende houding van het Noord-Atlantisch Bondgenootschap.

Tijdens de koude herfstsdagen van midden november worden Parijs en Berlijn opgeschrikt door ongewoon gewelddadige straatprotesten. Ook Brussel wordt overspoeld door geweld. De manifestanten breken ramen, beschadigen geparkeerde auto's, gooien met stenen en brandflessen en belagen de ordediensten. Langs de centrale lanen en in de wijken nabij de Grote Markt en het Luxemburgplein in Brussel heerst complete chaos. De politie heeft alle moeite om de orde te herstellen en kan de menigte niet onder controle krijgen. De agitatoren sporen medebetogers aan om nog meer schade te veroorzaken: ietwat verderop, in de richting van de Wetstraat, worden een tramstel en twee stadsbussen compleet vernield en wordt er brand gesticht in twee kantoorgebouwen. Een poging van een groepje keetschoppers om de gebouwen van de openbare omroep aan de Reyerslaan binnen te dringen, kan maar ternauwernood verhinderd worden.

Piiiiieeeepp! In de Montoyerstraat grijpen enkele honderden demonstranten plots naar hun hoofd. Ze worden 'overvallen' door een keiharde, snerpande piep – een enorme schrille geluidsgolf. 'Plotseling voelde het alsof mijn hoofd van binnenuit explodeerde', vertelt een betrokkene. Met de handen op de oren maken de manifestanten zich uit de voeten; ze zijn woedend op de ordediensten. Maar die zijn compleet verrast. Enkele politiemensen merken al snel een soort rechthoekige speaker op in een open raam van een hotelkamer op het derde verdiep. Bij controle blijkt deze de dag voordien geboekt door een veertiger met een vals Servisch paspoort. De speaker blijkt een LRAD te zijn, een long-range acoustic device, een geluidswapen zoals de Servische ordediensten bij protesten in Belgrado hebben gebruikt.

Het geweld escaleert de volgende uren en nacht: bijna 200 mensen raken gewond, sommigen zelfs zeer ernstig, en er valt één dode. Meer dan 1.000 betogers worden gearresteerd en 20 politieagenten moeten met verwondingen afgevoerd worden. De relschoppers scanderen 'Stop het imperialisme van Donald Trump', 'Geen Amerikaanse militairen

meer op Europese bodem' en 'Weg met de NAVO'. De straatrellen zijn van een schaal die België nog nooit gezien heeft.

Agenten van de Veiligheid van de Staat herkennen tussen de opruiers medewerkers van verenigingen en organisaties die door het Pravfond, het Russische diasporafonds, financieel gesteund worden. Het fonds is gelinkt aan het Russische ministerie van Buitenlandse Zaken en staat sinds juni 2023 op de Europese sanctielijst. Het Pravfond heeft bovendien banden met de SVR, de Russische buitenlandse inlichtingendienst, en ondersteunt in het Westen Russischtalige media die de boodschappen van het Kremlin uitdragen. Weinigen geloven nog dat de rellen spontaan zijn. Al snel vermoeden de veiligheidsdiensten dat ze georkestreerd zijn door Moskou.

Naarmate de uren verstrijken en de verwarring toeneemt, blijkt het geweld op straat slechts één front te zijn van een bredere aanval. In stilte, in cyberspace, voert een onzichtbaar leger een ander offensief. De eerste aanwijzingen zijn verwarrend. De cyberaanval ontvouwt zich in golven van ogenschijnlijk onschuldige online interacties.

Het doelwit? De commentaarsecties van een Vlaamse en een Brusselse krant die overspoeld worden. De voorgaande dagen kregen de krantenartikelen zo'n acht- tot negenduizend anonieme reacties per dag. Plots zijn er meer dan 10.000 in 10 minuten. Naast het ongekende tempo valt een vreemde uniformiteit op in de reacties die binnenkomen. Op de redactievloer identificeert en telt men een handvol identieke berichten die duizenden keren worden herhaald. Het is duidelijk dat dit het werk is van computerbots en niet van echte lezers. Er is een variatie van ongeveer dertig verschillende berichten over het uiteenvallen van de NAVO en de corruptie van de westerse regeringen die telkens herhaald worden, zo snel dat er geen mensen achter kunnen zitten.

Zowel het tempo als de omvang van de aanval nemen snel toe. Binnen een uur stijgt het aantal reacties op de website van de kranten opnieuw met een factor 10, tot 100.000 in 10 minuten. De aanval op beide websites wordt gevolgd door de bestorming van sites in de particuliere en publieke sector.

In het Nationaal Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken ziet men dat alle nieuwsportalen offline zijn. Onmiddellijk daarna wordt gemeld dat enkele banken offline zijn en even later ook de meeste websites van de overheid. Het noodnummer 112 is niet langer bereikbaar. In de ziekenhuizen van Hasselt, Mons en Brugge zijn de IT-systemen zwaar verstoord en worden de meeste medische activiteiten opgeschort. In het belangrijkste seinhuis van ons land in Berchem, het grootste verkeerscentrum voor treinen in België, gaan de beeldschermen op zwart. Heel het treinverkeer tussen de Nederlandse grens en Brussel en in de haven van Antwerpen komt tot stilstand.

Dit is een gecoördineerde aanval vanuit het buitenland. 'Het is duidelijk dat het geen slecht weer is', zegt iemand in het Crisiscentrum. 'Het zijn slechte mensen daarbuiten.' De Belgen zijn plotseling van de buitenwereld afgesneden – zonder toegang tot nieuws- of overheidswebsites en dus zonder informatie over wat er aan de hand was. België is het doelwit van een DDoS-aanval (Distributed Denial of Service), met name een digitale aanval waarbij websites, servers of online diensten overspoeld worden met een enorme hoeveelheid nepverkeer, afkomstig van duizenden geïnfecteerde apparaten (de 'botnets'), om die te overladen en onbereikbaar te maken.

Defensie ziet geen inbreuken op het Belgische luchtruim of grondgebied en bij de andere NAVO-lidstaten wordt er evenmin een schending van de territoriale integriteit vastgesteld. Het patrouillevaartuig Pollux van de Belgische marine merkt wel een 200 meter lange olietanker op die door de Belgische Exclusieve Economische Zone vaart, het deel van de internationale wateren waar België voor verantwoordelijk is. Het schip behoort tot de Russische schaduwvloot – de oude olietankers waarmee Moskou de westerse sancties op energie-export omzeilt. De schaduwvloot wordt ook gebruikt om andere illegale activiteiten uit te voeren. Zo bestaat er bij de westerse veiligheidsdiensten het sterke vermoeden dat een aantal drones die in het najaar van 2025 West-Europa teisterden, afkomstig waren van schepen van de schaduwvloot.

Britse en Duitse veiligheidsdiensten melden bovendien dat de werking van het Europese satellietnetwerk IntelSat ernstig verstoord is, vermoedelijk als gevolg van acties van nabij vliegende Russische satellieten. IntelSat wordt niet alleen gebruikt voor satelliettelevisie, maar ook voor een deel van de militaire communicatie van Europese legers en voor het overbrengen van gevoelige overheidscommunicatie.

Hoewel er geen verdere menselijke slachtoffers en bijkomende materiële schade zijn, is een groot deel van de bevolking bang en gedestabiliseerd. Dit is een aanval op de psychologie van een aantal NAVO-lidstaten en hun bevolking, met als doel: verwarring stichten, verdeeldheid zaaien, angst veroorzaken en twijfel opwekken over het politieke leiderschap. Omdat de overheden worstelen om de bevolking te kalmeren vanwege de lamgelegde communicatie-infrastructuur, beginnen mensen zich af te vragen of hun regering nog wel de touwtjes in handen heeft.

De dagen nadien vinden in Duitsland, Polen, Tsjechië en Finland gecoördineerde sabotageacties plaats op spoorlijnen, seinhuizen, zendmasten, cruciale wegenknooppunten, waterzuiveringsinstallaties en elektriciteitsleidingen. Na een hevige explosie en brand van een vrachtwagen geladen met kunstmeststof is de Elbetunnel in Hamburg niet langer bruikbaar. Een binnenschip botst dezelfde dag tegen een betonnen pijler van de spoorwegbrug over de Oder nabij de Duitse stad Frankfurt (Oder), waardoor de voornaamste spoorwegverbinding met Polen niet langer bruikbaar is. Zowel de chauffeur van de vrachtwagen als de binnenschipper blijken na de incidenten spoorloos.

De Europese veiligheidsdiensten spreken van de mogelijkheid van ‘slappende cellen’ of geïnfiltreerde speciale eenheden (‘Spetsnaz-achtig’, naar het voorbeeld van de speciale eenheden van het Russische leger) die actief zijn geworden in het kader van een uitgebreider hybride aanvalsplan. In Polen, Finland en de Baltische staten wordt de bescherming van kritieke infrastructuur door het leger versterkt.

Ook in België neemt de volgende dagen het aantal incidenten toe: een hooggeplaatste manager van wapenproducent FN Herstal ontsnapt

ternauwernood aan een aanslag; er worden drones gesignaleerd boven Brussels Airport en de vliegbasis van Kleine-Brogel; op het productie-terrein van John Cockerill Defense nabij Luik vindt een grote explosie plaats; een belangrijke haventerminalbeheerder wordt getroffen door een cyberaanval, waardoor hun terminals in de haven van Antwerpen zo goed als stilliggen; en een van de dikke onderzeese stroomkabels waarlangs windenergie vanaf de negen Belgische windmolenparken in de Noordzee naar het vasteland wordt getransporteerd, wordt zwaar beschadigd. Vermoed wordt dat het Russische vrachtschip dat nabij de Thorntonbank voer hiermee te maken heeft. Aandachtige constructiewerkers vinden bovendien een verborgen opslagplaats met een tiental kilogram explosieven aan het begin van de oostelijke havenstrekdam van Zeebrugge, nabij de lng-aardgasterminal. Het is onduidelijk wie ze heeft aangelegd. Zelfs officiële instanties spreken nu van ‘gecoördineerde incidenten’.

Het blijft voorlopig evenwel onduidelijk of het gaat om de voorbereiding van een conventionele aanval op een of meerdere landen of om een escalatiestrategie om Europa te destabiliseren en te chanteren. De Belgische regering en de secretaris-generaal van de NAVO spreken in ieder geval van een ‘ongekende schemeroorlog zoals Europa die nog nooit heeft meegemaakt’. De Baltische staten en Polen brengen hun troepen in staat van paraatheid. De Belgische Nationale Veiligheidsraad overweegt om de crisistoestand af te kondigen.

HOOFDSTUK II

SCHEMEROORLOG
ALS EEN SYSTEEM

Een dag in het verleden: op 24 februari 2022 valt Rusland Oekraïne binnen

Vrede in Europa verandert van een betrouwbare vanzelfsprekendheid in een toenemende onzekerheid. De voorbije jaren verslechterde de situatie in het Midden-Oosten: een vreselijke oorlog ontvlamde in Gaza, er vond een wederzijdse raketaanval plaats tussen Israël en Iran, Tel Aviv hakte de kop van de Hezbollah-slang in Libanon af en ook de VS voerden samen met Israël een oorlog uit tegen Teheran. Washington deinsde er bovendien niet voor terug om NAVO-bondgenoten af te dreigen over Groenland en om een staatshoofd te ontvoeren uit de Venezolaanse hoofdstad. Hoewel het einde van de vijandelijkheden tussen Rusland en Oekraïne tot de mogelijkheden behoort, is een duurzame vrede tussen beide landen niet voor morgen. En evenmin voor overmorgen.

Doorgesneden kabels. Verstoorde luchtvaart. Brandstichting. Sabotage. Moord. Infiltratie. Spionage. Desinformatie. Beïnvloeding. Cyberaanvallen. Operaties die bedoeld zijn om een tegenstander af te leiden, te verwarren en te verzwakken en zijn samenleving te ontwrichten. Terwijl Oekraïne blijft lijden onder golf na golf van bombardementen en een steeds verdergaande bezetting van zijn oostelijke en zuidelijke grondgebied, wordt Europa als geheel blootgesteld aan een aanhoudende strijd van een andere aard: een schemeroorlog.

In de periode tussen het begin van de Russische invasie in Oekraïne en 31 december 2025 hebben er in Europa 124 agressieve daden plaatsgevonden met niet-militaire middelen, waarvan Moskou onweerlegbaar als opdrachtgever aangeduid kan worden. Dit is maar het tipje van de ijsberg: we kunnen er namelijk met zekerheid van uitgaan dat er een veelvoud van dit soort aanvallen heeft plaatsgevonden, alleen was de link met Rusland niet onomstotelijk vast te stellen. Dit is de strijd die Rusland op systematische wijze tegen ons voert in de ruimte tussen vrede en oorlog.

In deze schemerzone voert Rusland een soort van geopolitieke guerrillastrijd. Die vloeit voort uit het besef dat het niet kan concurreren met de NAVO – zelfs niet met de ‘Europese NAVO’ – in een direct, conventioneel militair conflict. Vandaar dat het Kremlin tegen het Westen een andere strategie hanteert en een ander soort oorlog voert. De nieuwe aanpak is ontwikkeld om te profiteren van de zwakke plekken en besluiteloosheid van het Westen – het gevolg van onze open samenlevingen die afhankelijk zijn van een vrij verkeer van goederen, mensen, diensten en informatie en van een constellatie van op wetten gebaseerde democratiën, waarbij zekere spelregels gerespecteerd moeten worden. Maar de Russische aanpak is tegelijk een weerspiegeling van een diepere ideologische en institutionele logica, een neostalinistisch dreigingsmodel dat oorlogvoering als continu en alomtegenwoordig beschouwt, binnenlandse en buitenlandse dreigingen met elkaar versmelt en alles en iedereen als een potentieel doelwit beschouwt. Met andere woorden, oorlog als een systeem.

Deze guerrillastrijd in de geopolitieke arena omvat asymmetrische tactieken: in plaats van conventionele militaire macht te gebruiken, maakt Rusland gebruik van ontkenbare geheime acties, politieke misleiding, economische druk, propaganda en spionage om tegenstanders te ondermijnen. Daarnaast hanteert Rusland de ‘Great Game’-benadering, naar analogie met het negentiende-eeuwse Great Game, het conflict tussen het Britse en het Russische rijk om politieke, economische en militaire invloed over Centraal-Azië. In deze werkwijze worden conflicten niet gewonnen door regelrechte militaire superioriteit, maar door vijanden te dwingen volgens de regels van Moskou te spelen.

Verder ‘wapent’ het Kremlin alles: de grenzen tussen misdaad en oorlog, publiek en privé, en soldaat en burger vervagen. Allerhande niet-militaire middelen worden een wapen: cyberaanvallen, desinformatie, het manipuleren van energievoorzieningen, vluchtelingen crises, criminaliteit, internationale regelgeving, cultuur, politici en politieke partijen, democratische processen, technologie, kritieke infrastructuur, media en zelfs religie en religieuze spanningen. Alles wordt ingezet tegen allen.

Het is naïef om aan te nemen dat het Westen deze schemeroorlog zal winnen met dezelfde formule die het tijdens de Koude Oorlog gebruikt heeft. Destijds verenigde het Westen de vrijmarkteconomie, de populaire cultuur en de democratische politiek in één pakket: parlementen, investeringsbanken en popmuziek smolten samen om het politiebureau, de planeconomie en het sociaal realisme te verslaan. Maar het nieuwe Rusland (en het nieuwe China) heeft die formule aan flarden gescheurd: de Russische populaire cultuur is verwesterd; mensen rijden in BMW’s, spelen op de aandelenmarkt en luisteren naar Taylor Swift, terwijl ze tegelijkertijd antiwesterse retoriek toejuichen en de ondergang van Amerika vieren.

De ruimte tussen oorlog en vrede is niet leeg, maar is een landschap vol politieke, diplomatieke en economische concurrentie en competitie in de veiligheids- en informatiedomeinen. Als we dat niet erkennen, loopt ons veiligheidsbeleid het risico te worden gereduceerd tot een louter reactieve aanpak, met de nadruk op het tactisch gebruik van het militaire instrument. En omdat onze tegenstanders de westerse militaire macht niet rechtstreeks kunnen evenaren, is het juist in deze ruimte – het strijdtoneel van perceptie, dwang, cyberaanvallen, sabotage en wreedheden – waar ze het liefst opereren.

De tragedie van ons onvermogen – of onze onwil – om de mentaliteit en de mechanismen te ontwikkelen om de competitie aan te gaan in die ruimte tussen oorlog en vrede, betekent dat we onze opties beperken en uiteindelijk onze toevlucht nemen tot het militaire instrument.

Vrede bestaat niet in een staat van inertie. Ze moet actief en consequent worden gehandhaafd door alle instrumenten van het veiligheidsbeleid aan te wenden: diplomatiek, economisch, informatieel en militair.

Schemeroorlog: de strijd in het niemandsland tussen vrede en klassieke oorlog

De Pruisische oorlogstheoreticus Carl von Clausewitz (1780-1832) stelde ooit terecht dat ‘elk tijdperk zijn eigen soort oorlog kent’. Schemeroorlog is de oorlog van onze tijd.

In de hedendaagse veiligheidsomgeving geldt dat hoe meer technologie het mogelijk maakt om de status quo uit te dagen, hoe minder grootschalig geweld op een slagveld nodig is. Daardoor wordt de wereld minder voorspelbaar en wordt het ingewikkelder om nieuwe dreigingen af te schrikken of een alliantie tegen nieuwe gevaren te vormen.

Schemeroorlog is de strijd tussen staten of groepen die plaatsvindt buiten het slagveld, in het ‘niemandsland’ tussen vrede en oorlog. Hij wordt gevoerd met agressieve acties onder de drempel van een gewapend conflict – dus zonder gebruik van strijdkrachten en zonder daadwerkelijke gevechten tussen legers – met het oog op het verzwakken, ontwrichten en van binnenuit ondermijnen en polariseren van samenlevingen, het beïnvloeden van hun politieke besluitvorming en het creëren van onrust en angst. Schemeroorlog handelt dus niet over het fysiek binnenvallen, bezetten of beschieten van land.

In de schemeroorlog worden de materiële, economische, politieke en sociale kwetsbaarheden van onze samenlevingen aangevallen, zowel met fysieke middelen (bijvoorbeeld sabotage, brandstichting, moorden), niet-fysieke middelen (bijvoorbeeld desinformatie, propaganda, manipulatie, culturele beïnvloeding, manipulatie van verkiezingen, het lamleggen van internationale instellingen en het negeren van internationale regels, misbruiken van juridische procedures, het gebruiken van bevriende politici, corruptie) als met een combinatie van beide methodes (bijvoorbeeld cyberaanvallen).

Onze zwakke punten zijn legio. De meeste westerse landen importeren een groot deel van hun levensmiddelen en andere dagelijkse benodigdheden en detailhandelaars werken steeds meer volgens het just-in-timemodel, waardoor de voorraden tot een minimum worden beperkt en de kosten dus dalen. Maar een dergelijke commerciële efficiëntie brengt kwetsbaarheden met zich mee. Het hacken van de IT-systemen van voedselbedrijven kan snel tot lege winkelrekken leiden. Kritieke nationale infrastructuur is op haar beurt in veel gevallen niet

langer in handen van de overheid, maar van particuliere bedrijven, die soms zelfs in het buitenland gevestigd zijn. En zelfs al zijn ze nog in overheidshanden, dan worden ze meestal slechts rudimentair bewaakt. Wanneer de tegenpartij het elektriciteitsnet of de transportnetwerken hackt, kan ze snel steden en landen lamleggen. Langere verstoringen kunnen verwoestende cumulatieve schade veroorzaken.

Bij een gerichte aanval op de cruciale schakels van ons stroomnet én de hoogspanningslijnen die ons met het buitenland verbinden, komen onmiddellijk miljoenen mensen zonder stroom te zitten, iets wat pas na meerdere weken volledig verholpen zou zijn. De elektriciteitsvoorziening is de achilleshiel van hoogontwikkelde economieën, kwetsbaarder dan ziekenhuizen of de voedselvoorziening.

Iedereen vindt het logisch dat we de kerncentrales van Doel en Tihange goed beschermen tegen aanslagen, maar ze zijn als doelwit relatief oninteressant. De inspanning om vele meters beton en staal op te blazen staat niet in verhouding tot de schade aan de elektriciteitsproductie, al zal die wel lang voelbaar zijn. Daarentegen laat de oorlog in Oekraïne zien hoe groot de gevolgen zijn als de elektriciteitsdistributie wordt aangevallen. Een raket op een hoogspanningsstation heeft gevolgen voor de wijde omgeving. Bij een tekort aan reserveonderdelen en gekwalificeerd personeel kan herstel tijdrovend zijn.

Schemeroorlog verschilt van hybride oorlog in de zin dat hybride oorlog traditionele, conventionele oorlogvoering op een slagveld combineert met andere agressieve daden met niet-militaire middelen, uitgevoerd door niet-militaire uitvoerders tegen dezelfde tegenstander(s) buiten het eigenlijke gevechtsgebied. Rusland voert bijgevolg op dit moment geen hybride oorlog tegen een Europees land.

Een schemeroorlog is een echte oorlog in de optiek van Clausewitz, met name een voortzetting van de politiek – oftewel: het nastreven van politieke doeleinden met andere middelen.

Westerse landen hebben niet alleen moeite om schemeroorlog als zodanig te herkennen, maar ook om die te begrijpen. De leer van de rechtvaardige oorlog en het grote respect voor het volkenrecht zijn namelijk diep in de westerse intellectuele geschiedenis geworteld, en die gaan uit van een redelijk duidelijk onderscheid tussen een staat van oorlog en een staat van vrede. Hoewel Clausewitz al wist dat oorlog een ‘ware kameleon’ is en ook de zogenaamd klassieke oorlogen in

het Westen bij kritische beschouwing veel minder klassiek waren dan aangenomen, blijven wij naar dergelijke binaire denkpatronen neigen.

Onze tegenstanders denken daarentegen niet in dergelijke categorieën. Zij voelen zich op hun gemak wanneer de categorieën vervagen en in beweging komen. En hoe verder je naar het oosten gaat, hoe sterker die tendens in het militair-strategisch denken verankerd is. China en Rusland hebben een ‘meer holistisch’ begrip van conflicten. Deze landen, maar ook Noord-Korea en terroristische groeperingen zoals IS, maken zelfs gebruik van het stereotiepe denken in het Westen door hun aanvallen doelbewust te richten op raakvlakken of gebieden met gedeelde of onduidelijke verantwoordelijkheden.

België en West-Europa als doelwit

In de schemeroorlog vormen België en zijn nabije burens belangrijke doelwitten voor de autoritaire regimes in Rusland en China. Dat komt in de eerste plaats door hun positie als doorvoerland in het geval van een grootschalig militair conflict aan Europa's oostgrens en de aanwezige vitale maritieme infrastructuur in de Noordzee en Oostzee. In de Noordzee bijvoorbeeld liggen belangrijke internetkabels, gasleidingen en windmolenparken die van cruciaal belang zijn voor het functioneren van België en het aangrenzende buitenland. Antwerpen en Zeebrugge zijn belangrijke ‘aanlegsteigers’ voor de militaire bevoorradingen uit de Verenigde Staten en het Verenigd Koninkrijk.

Brussel is de vestigingsplaats van het hoofdkwartier van de NAVO en van de voornaamste EU-instellingen en kent, samen met Washington D.C., de grootste diplomatieke vertegenwoordiging van de hele wereld. Verder zijn er belangrijke internationale instellingen in of nabij onze hoofdstad gehuisvest, zoals Euroclear (de financiële dienstverlener gespecialiseerd in de afwikkeling van effectentransacties) en SWIFT (het wereldwijde communicatienetwerk voor financiële instellingen), evenals de hoofdzetels van grote ondernemingen. Het is bijgevolg een belangrijk doelwit voor spionage, beïnvloedingsoperaties, offensieve cyberprogramma's en laagdrempelige digitale sabotage- en verstoringsaanvallen.

West-Europa is eveneens een belangrijke logistieke en transporthub. Het drukke spoorwegennet, de drukbezochte luchthavens, de

tallose sluizen en de uitgebreide communicatie-infrastructuur vormen risicovolle verbindingen. Ze zijn essentieel in het vervoer van mensen, diensten, goederen en data, waardoor sabotage of cyberaanvallen verwoestende gevolgen kunnen hebben. Hetzelfde geldt voor de belangrijke aanwezigheid van de chemische en farma-industrie in deze regio.

De financiële sector is een reëel doelwit en banksystemen zijn kwetsbaar. Deze kwetsbaarheid wordt versterkt doordat de financiële infrastructuur in Europa genetwerkt is en bestaat uit vele digitale verbindingen, elektriciteitsleveringen en de vitale infrastructuur voor grote datastromen en datacentra. Ook klassiekere aanvallen zoals het afsluiten van stroomtoevoer, telefonie of elektriciteit op regionaal niveau vormen bedreigingen voor de telecom- en financiële sector.

België en zijn buurlanden bezitten verder een robuuste kennissector. Het is een domein waar beïnvloeding, diefstal van intellectuele eigendom en ongewenste overdracht van technologie kunnen plaatsvinden, waardoor kennis kan wegvloeien naar vijandelijke mogendheden.

De West-Europese landen vormen samen de derde economie ter wereld. Voor China zijn ze daarom niet alleen een belangrijke handelspartner en afzetmarkt, maar door hun marktleiderschap op een aantal technische gebieden zijn ze tegelijk een belangrijk doelwit voor spionage. Rusland van zijn kant blijft – ondanks alle sancties en maatregelen om Europa los te koppelen van de Russische olie en het Russisch gas – toch een vooraanstaande energieleverancier en kan op die manier invloed blijven uitoefenen op de Europese besluitvorming.

Tegelijk heeft België's oostelijke buur, Duitsland, met 3 tot 4 miljoen Russischsprekende inwoners een aanzienlijke bevolkingsgroep die een bijzonder doelwit is voor Russische propaganda. Natuurlijk is deze groep, waartoe Russische Duitsers, Joodse vluchtelingen en ook immigranten uit vele andere staten van de voormalige Sovjet-Unie behoren, zeer divers en bestaat die zeker niet voornamelijk uit sympathisanten van het regime van Poetin. Maar delen van deze groep zijn kwetsbaar voor Russische propaganda en daardoor kunnen sommige personen als actoren worden gerekruteerd voor activiteiten in de schemerzone in West-Europa.

HOOFDSTUK III

WANNEER DE WAARHEID
VERDUISTERD WORDT