

In een snel veranderende wereld waar de oorlogsdoctrines van onze tegenstanders alle registers bestrijken, is defensie niet langer enkel een opdracht voor de krijgsmacht. Op het eerste gezicht zou men kunnen stellen dat het gebruik van niet-militaire middelen op zich niets nieuws is: reeds in de vijfde eeuw voor Christus gaf Sun Tzu¹ de voorkeur aan aanvallen op domeinen waar de tegenstander het meest kwetsbaar is.

De *new generation warfare*, zoals die door Rusland beoefend wordt, vormt desalniettemin een heuse paradigmaverschuiving. Het verschil schuilt in de vectoren waar gebruik van gemaakt wordt, die sectoren viseren of instrumentaliseren die op hun beurt voortkomen uit technologische innovatie en nog niet allemaal structureel geïntegreerd zijn in onze defensieplannen. De sabotage van kritieke onderzeese infrastructuren, *denial-of-service*-cyberaanvallen die zowel onze openbare diensten als onze luchthavens en ziekenhuizen raken, het rekruteren van criminele onderaannemers via het *dark web*² of het gecoördineerde gebruik van informatie- en digitale middelen om onze democratieën te doen wankelen, alsook om de percepties en emoties van bepaalde doelgroepen te beïnvloeden.

Om het hoofd te bieden aan deze paradigmaverschuiving is het onontbeerlijk en dringend om het concept van defensie *an sich* te herzien en uit te breiden naar activiteiten waar de strijdkrachten niet noodzakelijk de eerste verdedigingslijn vormen. Aangezien ‘defensie’ zich niet langer beperkt tot ‘Defensie’, moet het concept ook uitgebreid worden naar ‘weerbaarheid’, dat kan opgevat worden als een gedeelde verantwoordelijkheid van de Staat, de economische wereld en de maatschappij in brede zin. Volgens een definitie die breed gedeeld en opgepikt wordt door de NAVO en de Europese Unie slaat ‘weerbaarheid’ op de capaciteit om aanvallen te voorkomen, de schok ervan op te vangen, de schade aan vitale functies te beperken en snel opnieuw een aanvaardbare werking in te voeren van het openbare leven en zijn ondersteunende infrastructuren^{3,4}.

¹ Sun Tzu, *De kunst van het oorlogvoeren*, vertaald door Samuel B. Griffith (s-Hertogenbosch: Librero, 2010).

² Het *dark web* verwijst naar netwerken en diensten die alleen toegankelijk zijn via specifieke software of configuraties, die een relatieve anonimiteit bieden en gebruikt worden om illegale inhoud te hosten.

³ NATO, Resilience Committee, civil preparedness and article 3, [Resilience, civil preparedness and Article 3 | NATO Topic](#).

⁴ Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten, <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2557>.

Volgens deze logica, waarbij defensie wordt uitgebreid naar weerbaarheid, moet de gecoördineerde actie van alle actoren gepland worden en bekend zijn bij de bevolking. Weerbaarheid moet absoluut het voorwerp uitmaken van oefeningen om erover te waken dat de maatregelen op het vlak van preventie, actie en recuperatie goed functioneren wanneer zich een aanval voordoet. Noord-Europese landen zoals Finland en Zweden zijn in dat opzicht concrete voorbeelden van de complementariteit tussen militaire en civiele defensie. De Zweedse *Totalförsvar* – of ‘totale defensie’ – definieert specifieke taken en kent deze toe aan overheidsinstanties, ondernemingen, gemeenschappen en iedere burger tussen 16 en 70 jaar oud, om de continuïteit van de vitale functies van het land te vrijwaren. De uitvoering van weerbaarheidsplannen wordt toevertrouwd aan het Agentschap voor Civiele Bescherming, dat tevens de oefeningen inzake crisisbeheer coördineert in samenwerking met de strijdkrachten. In België moet de Nationale Veiligheidsstrategie, die werd gepubliceerd in december 2021 en momenteel wordt herzien, de samenwerking tussen de verschillende beleidsniveaus, alsook tussen Defensie en de andere veiligheidsdiensten, op elkaar afstemmen.

Op sommige gebieden is de noodzaak om civiele en militaire middelen te integreren vanzelfsprekend. De medische en ziekenhuiscapaciteiten moeten opnieuw worden geëvalueerd om in staat te zijn te reageren op scenario’s van hoge-intensiteitsconflicten. Tijdens de Koude Oorlog beschikten onze legers over zorginfrastructuren die waren berekend op een massale toestroom van gewonden. Net als de andere onderdelen van onze strijdkrachten zijn deze capaciteiten progressief afgebouwd, ten voordele van een grotere rol voor de civiele sector. In een context van herbewapening en een toenemende kwetsbaarheid van de Europese bevolking hangt weerbaarheid echter ook af van de garantie dat de zorgstelsels, in geval van een grote crisis, kunnen functioneren op een geïntegreerde manier, ongeacht of deze crisis militairen, burgers of beide tegelijk treft. Naast de logistieke aspecten van de opvang van gewonden moet ook specifieke kennis en *knowhow* worden gedeeld op het gebied van gevechtstraumatologie, rampengeneeskunde en de gelijktijdige behandeling van een groot aantal gewonden. Een dergelijke aanpak, die volledig binnen defensie in de breedste zin van het woord past, vereist gemeenschappelijke protocollen, gezamenlijke oefeningen en een duidelijk bestuurskader over militaire autoriteiten, volksgezondheid en ziekenhuizen heen.

Hoewel gezondheidszorg duidelijk behoort tot de eerstelijnsbehoeften op het gebied van weerbaarheid zijn andere domeinen – zoals energiezekerheid, de beveiliging van communicatiemiddelen, de voedsel- en drinkwatervoorziening – net zo belangrijk. Het is dan ook noodzakelijk dat militairen en burgers informatie en kennis met elkaar delen.

Deze samenwerking moet of mag zich echter niet beperken tot crisisbeheer. In een tijdperk dat de toegang tot nieuwe technologische hulpmiddelen ervoor zorgt dat de snelheid waarmee nieuwe kennis verworven wordt exponentieel toeneemt, is het noodzakelijk om professionele en technische raakvlakken te creëren tussen militaire en civiele beroepen. Naast eenvoudige samenwerkingsmechanismen moet men een ware osmose bewerkstelligen tussen de kennis uit de civiele en militaire milieus. Hoewel innovatie vroeger vaak voortkwam uit een militaire behoefte en vervolgens zijn weg vond naar civiele toepassingen, vloeien nieuwe technologieën de laatste jaren massaal voort uit de burgerlijke commerciële sector: sensoren, artificiële intelligentie, robotica, communicatie, beeldvorming, biotech. Om een militaire operationele superioriteit te behouden, is het van belang dat er een goed begrip is van deze nieuwe domeinen, zodanig dat civiele componenten die zijn aangepast aan de behoeften en omstandigheden van militairen snel geïntegreerd kunnen worden in wapensystemen.

Ten slotte zijn er domeinen die voortvloeien uit baanbrekende innovaties en waar de respectievelijke verantwoordelijkheden en samenwerkingsmodellen nog grotendeels bepaald moeten worden. De *new generation warfare* is de cognitieve sfeer binnengedrongen; die laatste ontsnapt nog vaak aan de traditionele analysekaders wanneer geprobeerd wordt om de mechanismen te begrijpen waarmee onze tegenstanders de gedachtegang van onze samenlevingen manipuleren. Omdat deze aanvallen zich vaak vermengen en verward worden met ons democratische debat, zijn ze moeilijk te identificeren. De aanvallen doen een beroep op sociale psychologie en technologieën zoals artificiële intelligentie of *microtargeting*. Het doel is om op lange termijn het vertrouwen van bepaalde groepen burgers in hun instellingen te ondermijnen of om het mediadebat over gevoelige onderwerpen te beïnvloeden. De ervaringen van landen in de frontlinie, die dus het eerste doelwit zijn van zo'n cognitieve oorlogsvoering, pleiten voor de ontwikkeling van een

flexibele en geloofwaardige informatiehygiëne die de samenleving kan beschermen tegen dergelijke slinkse aanvallen. De Europese maatregelen ter bestrijding van desinformatie en de inspanningen van geallieerde expertisecentra bieden een nuttig kader voor het uitwisselen van *good practices*. Het veldwerk kan echter enkel worden gedaan op het niveau van de overheidsstructuren.

Deze voorbeelden tonen aan hoezeer de term ‘totale defensie’, gekozen door Zweden om zijn weerbaarheidsplan te beschrijven, relevant is. Als het gaat om het plannen van operaties, het inzetten van troepen om een crisissituatie het hoofd te bieden of het organiseren van oefeningen om zich daarop voor te bereiden, bevinden militairen zich in hun comfortzone. Het zit in hun DNA om voorbereid te zijn en zich aan te passen aan buitengewone omstandigheden. Nadenken over nationale weerbaarheid omvat echter steeds meer domeinen waar militairen afhankelijk zijn van de kennis en expertise van hun burgercollega’s. De symbiose tussen de verschillende domeinen kan niet uitgevoerd worden door enkel de horizontale som te maken van expertise en vaardigheden. Wat samenwerking, integratie of fusie gemeenschappelijk hebben, is het feit dat kennis en informatie gedeeld moeten worden. Zelfs bij aspecten zoals cognitieve oorlogsvoering moeten militairen en burgers samen narratieve verdedigingslinies en communicatiestrategieën uitwerken om zich te bewapenen en weerstand te bieden aan de slinkse en subversieve aanvallen van onze tegenstanders.

‘Totale defensie’ zijn dus de twee woorden bij uitstek die ons moeten leiden wanneer we denken aan onze veiligheid van morgen.

Kapitein-ter-zee Kurt Engelen

Dans un monde en rapide évolution où les doctrines de guerre de nos adversaires s'étendent à tous les registres, la défense a cessé d'être une mission pour les seules forces armées. Au premier abord, on pourrait soutenir la thèse que le recours à des moyens non militaires n'est pas neuf en soi : Sun Tzu¹, au V^e siècle avant notre ère, privilégiait déjà l'attaque de l'adversaire dans les domaines où il est le plus vulnérable.

La guerre de nouvelle génération, telle que la pratique la Russie, constitue néanmoins un véritable changement de paradigme. Elle se distingue par les vecteurs qu'elle emploie, qui visent ou instrumentalisent des secteurs issus eux-mêmes de l'innovation technologique et qui ne sont pas encore tous structurellement intégrés dans nos plans de défense. Les sabotages d'infrastructures critiques sous-marines, les cyberattaques par déni de service qui frappent nos services publics mais aussi nos aéroports et nos hôpitaux, le recrutement de sous-traitants criminels via le *darknet*² ou encore l'utilisation coordonnée de moyens informationnels et numériques pour déstabiliser nos démocraties et altérer les perceptions et les émotions de certains groupes-cibles.

Face à ce changement de paradigme, il est indispensable et urgent de repenser le concept de défense lui-même et de l'étendre à des domaines d'activité où les forces armées ne sont pas nécessairement le premier répondant. Et comme la « défense » ne relève plus uniquement de la « Défense », il faut étendre le concept à la résilience, entendue comme une responsabilité partagée entre l'État, le monde économique et la société au sens large. Selon une définition largement partagée et reprise par l'OTAN et l'Union européenne, la résilience désigne la capacité de prévenir les attaques, d'en absorber le choc, de contenir l'atteinte aux fonctions vitales et de rétablir rapidement un fonctionnement acceptable de la vie publique et des infrastructures qui la soutiennent^{3,4}.

¹ Sun Tzu, *L'Art de la guerre*, traduit du chinois par Jean Lévi (Paris : Flammarion, 2008), 15.

² Le *darknet* désigne des réseaux et des services accessibles uniquement via des logiciels ou des configurations spécifiques, offrant un anonymat relatif, utilisé pour héberger des contenus illicites.

³ OTAN, Comité pour la résilience, préparation du secteur civil et article 3, https://www.nato.int/cps/fr/natohq/topics_132722.htm.

⁴ Directive (UE) 2022/2557 du Parlement et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2557>.

Dans cette logique de défense étendue à la résilience, l'action coordonnée de tous les acteurs doit être planifiée et connue de la population. Elle doit impérativement faire l'objet d'exercices afin de s'assurer du bon fonctionnement des mesures de prévention, d'action et de récupération lorsqu'une attaque se produit. Les pays nordiques comme la Finlande et la Suède offrent, à cet égard, des exemples concrets de complémentarité entre la défense militaire et la défense civile. En Suède, le *Totalförsvaret* – ou « défense totale » – définit et attribue des tâches spécifiques aux autorités publiques, aux entreprises, aux collectivités et à chaque citoyen âgé de 16 à 70 ans pour assurer la continuité des fonctions vitales du pays. La mise en œuvre des plans de résilience est confiée à l'Agence de défense civile, qui coordonne aussi les exercices de gestion de crise en collaboration avec les forces armées. En Belgique, la Stratégie de sécurité nationale, publiée en décembre 2021 et actuellement en cours de révision, doit articuler la collaboration entre les différents niveaux de pouvoir, ainsi qu'entre la Défense et les autres services chargés de la sécurité.

Dans certains domaines, cette nécessité d'intégration des moyens civils et militaires est évidente. Les capacités médico-hospitalières doivent être réévaluées pour pouvoir répondre à des scénarios de conflit de haute intensité. Pendant la guerre froide, nos armées disposaient d'infrastructures de soins dimensionnées pour absorber des afflux massifs de blessés. À l'instar des autres composantes des forces armées, ces capacités ont été progressivement réduites au profit d'une prise en charge plus importante par le secteur civil. Or, dans un contexte de réarmement et de vulnérabilité accrue des populations européennes, la résilience passe aussi par la garantie que les systèmes de santé puissent fonctionner de manière intégrée en cas de crise majeure, qu'elle touche des militaires, des civils ou les deux simultanément. Outre les aspects logistiques pour l'accueil de blessés, il faut aussi partager les connaissances et le savoir-faire spécifiques liés à la traumatologie de combat, à la médecine de catastrophe et à la gestion simultanée de nombreux blessés. Une telle approche, qui relève pleinement de la défense au sens le plus large, suppose des protocoles communs, des exercices conjoints et un cadre de gouvernance clair entre autorités militaires, santé publique et hôpitaux.

Si les soins de santé font clairement partie de la première ligne des besoins en matière de résilience, d'autres secteurs comme la sécurité énergétique, la sécurité des moyens de communication, l'approvisionnement en denrées alimentaires et en eau potable sont tout aussi importants et supposent un partage d'informations et de connaissances entre militaires et civils.

Cette collaboration ne doit et ne peut toutefois pas se limiter à la seule gestion de crises. À une époque où l'accès à de nouveaux outils technologiques accélère de manière exponentielle l'accroissement des connaissances, il est impératif d'établir des interfaces professionnelles et techniques entre métiers militaires et civils. Au-delà de simples mécanismes de collaboration, il faut favoriser une véritable osmose entre les connaissances des mondes civil et militaire. Si l'innovation procédait autrefois souvent d'un besoin militaire avant d'être déclinée en applications civiles, en revanche, ces dernières années, les nouvelles technologies proviennent massivement du secteur commercial civil : capteurs, intelligence artificielle, robotique, communications, imagerie, biotechnologies. La sauvegarde d'une supériorité opérationnelle militaire supposera donc une bonne compréhension de ces nouveaux domaines afin de pouvoir intégrer rapidement, dans les systèmes d'armement, des composants civils adaptés aux besoins et aux conditions des militaires.

Enfin, il y a des domaines qui résultent d'innovations de rupture et où les responsabilités respectives et les modèles de collaboration restent largement à définir. La guerre de nouvelle génération s'est invitée dans la sphère cognitive, qui échappe encore souvent aux cadres d'analyse traditionnels lorsqu'on cherche à comprendre les mécanismes par lesquels nos adversaires manipulent la pensée de nos propres sociétés. Parce qu'elles se fondent et se confondent souvent avec notre propre débat démocratique, ces attaques sont difficiles à identifier. Elles mobilisent à la fois la psychologie sociale et des technologies telles que l'intelligence artificielle ou le microciblage. Leur objectif est, sur le long terme, de miner la confiance de certains groupes de citoyens dans leurs institutions ou d'influencer le débat médiatique sur des sujets sensibles. Les retours d'expérience de pays qui sont aux premières loges et donc les premières cibles de ces actions de guerre cognitive appellent à développer une hygiène informationnelle agile et crédible qui puisse

prémunir la société contre ces attaques insidieuses. Les dispositifs européens de lutte contre la désinformation et le travail des centres d'excellence alliés fournissent des cadres utiles pour le partage des bonnes pratiques, mais le travail de terrain ne peut être réalisé qu'au niveau des structures de l'État.

Ces quelques exemples démontrent à quel point la terminologie de « défense totale » qu'a choisie la Suède pour décrire son plan de résilience est pertinente. Lorsqu'il s'agit de planifier des opérations, de déployer des forces pour faire face à une situation de crise ou de conduire des exercices pour s'y préparer, les militaires se trouvent dans leur zone de confort ; la préparation et la capacité de s'adapter à des circonstances extraordinaires sont inscrites dans leur ADN. En revanche, la réflexion sur la résilience nationale implique de plus en plus de domaines où les militaires sont tributaires des connaissances et de l'expertise de leurs collègues civils. La symbiose entre les divers domaines ne pourra pas se réaliser par la seule somme horizontale des expertises et compétences. Entre collaboration, intégration ou fusion, le point commun est le partage des connaissances et de l'information. Même dans les aspects tels que la guerre cognitive, militaires et civils doivent construire ensemble les lignes de défense narratives et les stratégies de communication pour se prémunir et contrer les attaques insidieuses et subversives de nos adversaires.

« Défense totale » sont donc les deux mots par excellence à retenir quand nous pensons à notre sécurité de demain.

Capitaine de vaisseau Kurt Engelen