Strategische Analyse: China’s Cybermilitie en de Doctrine van 'Onbeperkte Oorlogsvoering'

1. Inleiding: De Dubbele Aard van China's Cyberoorlogsvoering

De groeiende cybermacht van de Volksrepubliek China wordt gedragen door een strategische aanpak met een dubbele aard. Enerzijds is er de zichtbare modernisering van de formele militaire cyberstrijdkrachten, zoals de People's Liberation Army Cyberspace Force (PLACSF). Anderzijds, en vaak minder belicht, is er de ontwikkeling van een asymmetrische capaciteit via de systematische integratie van civiele milities. Deze strategie is diep geworteld in de doctrine van 'Onbeperkte Oorlogsvoering' en maakt gebruik van de expertise en middelen van de private sector om de militaire slagkracht te vergroten. Het is juist dit tweede, minder zichtbare aspect—de mobilisatie van civiele cyberkrachten—dat cruciaal is voor een correcte inschatting van de dreiging die van Beijing uitgaat.
Recente analyses van China's cybermilitiesysteem tonen een significante transformatie van een perifeer instrument naar een strategisch relevant onderdeel van de PLA's cyberoorlogsvoeringsarchitectuur. De kernbevindingen van deze ontwikkeling laten zich als volgt samenvatten:

- **Verhoogde Veerkracht en Surge-capaciteit:** Het militiesysteem biedt het Volksbevrijdingsleger (PLA) een schaalbare reservemacht die de operationele capaciteit in het netwerkdomein met minimale voorbereidingstijd kan uitbreiden. In tegenstelling tot conventionele reserves, maken cybermilities gebruik van burgers die reeds beschikken over waardevolle technische expertise. Hierdoor is de functionele kloof tussen actieve en reserve-eenheden aanzienlijk kleiner dan in traditionele militaire domeinen.
- **Essentiële Rol in Hoog-risico Scenario's:** Militaire planners van de PLA hebben de cybermilities geïdentificeerd als een vitale ondersteunende kracht in specifieke scenario's, zoals een toekomstige invasie van Taiwan of een crisis in de Zuid-Chinese Zee. Deze eenheden worden niet alleen ingezet voor ondersteunende taken, maar ook om offensieve cybermissies aan te vullen, zoals misleidingsoperaties en de beïnvloeding van de publieke opinie.
- **Professionalisering en Diversificatie:** Onder leiding van Xi Jinping heeft de Partij-staat hervormingen doorgevoerd die de professionaliteit van de milities vergroten. De rekrutering, die traditioneel gericht was op universiteiten en staatsbedrijven, is uitgebreid naar commerciële cyberbeveiligingsbedrijven van wereldklasse. Door middel van een combinatie van dwingende beleidsmaatregelen en financiële prikkels wordt de private sector steeds dieper geïntegreerd in de nationale defensiestructuur.

Deze georganiseerde fusie van civiele en militaire cybercapaciteiten is geen toevallige ontwikkeling, maar de logische uitkomst van een decennialang gerijpte militaire doctrine.

2. De Doctrinaire Basis: 'Onbeperkte Oorlogsvoering'

De intellectuele pijler onder China's asymmetrische cyberstrategie is het concept van 'Onbeperkte Oorlogsvoering' (Unrestricted Warfare), geformuleerd in 1999 door twee PLA-kolonels, Qiao Liang en Wang Xiangsui. De strategische essentie van deze doctrine is het neutraliseren van een technologisch superieure tegenstander, zoals de Verenigde Staten en de NAVO, door conventionele militaire confrontatie te vermijden en in te zetten op de kwetsbaarheden van de tegenstander buiten het traditionele slagveld.

De kernprincipes van de doctrine zijn diep beïnvloed door de eeuwenoude leringen van de Chinese strateeg Sun Tzu, die pleitte voor het aanvallen van de zwakke punten van de vijand en het vermijden van diens sterke punten. Qiao en Wang concludeerden dat de grootste kwetsbaarheid van het Westen de diepe afhankelijkheid van technologie is, zowel op militair als op civiel gebied. Command & control, navigatie, financiële transacties en kritieke infrastructuur zijn allemaal afhankelijk van satellietnetwerken en computersystemen. Het uitschakelen van deze "technologische kruk" zou niet alleen de militaire slagkracht van het Westen verlammen, maar kan ook leiden tot de ineenstorting van de samenleving. In plaats van "de strijd te voeren die bij de wapens past", zoals westerse mogendheden volgens hen doen, moet China "de wapens bouwen die bij de strijd passen". Concrete voorbeelden die zij noemen, zijn een door de mens veroorzaakte beurscrash of een computervirus, die beide als "new-concept weapons" worden beschouwd.

Dit leidt tot het concept van de **"Assassin's Mace"**: het strategische principe om een technologisch superieure tegenstander te neutraliseren door de inzet van specifieke, vaak goedkopere, 'game-changing' capaciteiten die de conventionele krachtsverhoudingen tenietdoen. Cyberaanvallen zijn een perfect voorbeeld van een dergelijk wapen. Ze zijn kostenefficiënt, moeilijk te attribueren en kunnen verwoestende schade toebrengen aan de economische en sociale stabiliteit van een tegenstander. In bredere zin kan het cybermilitiesysteem als geheel worden beschouwd als de belichaming van deze doctrine: een relatief goedkope, asymmetrische methode om een massale, schaalbare cybercapaciteit te genereren die een technologisch superieure maar numeriek beperkte tegenstander kan overweldigen.

De praktische toepassing van deze doctrine is zichtbaar in een reeks recente, grootschalige Chinese cyberoperaties:

- **Salt Typhoon:** Een operatie die de wereldwijde communicatie-infrastructuur die het internetverkeer draagt, heeft gecompromitteerd. De schaal van deze aanval was zo groot dat westerse inlichtingendiensten het een "nationale defensiecrisis" noemden.
- **Volt Typhoon:** Deze operatie richtte zich op kritieke infrastructuur in de Verenigde Staten, waaronder de energie-, water- en communicatiesector. Volgens de voormalige FBI-directeur Christopher Wray werden de systemen van 23 verschillende pijpleidingoperatoren gecompromitteerd, met als doel om *pre-positioned access* te verkrijgen voor toekomstige aanvallen.
- **APT31 en APT40:** Deze door de staat gesponsorde groeperingen hebben zich gericht op een breed scala aan doelwitten, waaronder politieke dissidenten, overheidsfunctionarissen, bedrijven en universiteiten in de VS en Europa, met als doel spionage en het verkrijgen van intellectueel eigendom.

Deze operaties illustreren een strategie die niet gericht is op een directe militaire confrontatie, maar op het systematisch ondermijnen van de technologische fundamenten van de tegenstander. Om deze doctrine effectief uit te voeren, heeft China een specifieke organisatorische structuur ontwikkeld.

3. Operationalisering van de Doctrine: Het Cybermilitiesysteem

Het cybermilitiesysteem is het onvermijdelijke organisatorische antwoord op de strategische vragen die de doctrine van 'Onbeperkte Oorlogsvoering' oproept. Waar de doctrine pleit voor het uitbuiten van de maatschappelijke zwaktes van een tegenstander, biedt het militiesysteem het concrete mechanisme om de maatschappelijke elementen—in dit geval de technologische

experts en middelen van de civiele sector—te mobiliseren die nodig zijn om dit te bereiken. Dit systeem vertaalt de abstracte principes van 'Onbeperkte Oorlogsvoering' en Militair-Civiele Fusie (MCF) naar een concrete, inzetbare strijdmacht, waarmee de PLA zijn formele strijdkrachten kan ontlasten en tegelijkertijd een enorme reserve aan talent kan aanboren.

3.1 Evolutie onder Xi Jinping: De Professionaliseringsslag

Onder het leiderschap van Xi Jinping is de status van de cybermilities getransformeerd van een perifeer, losjes georganiseerd geheel naar een meer professionele en operationeel relevante reservemacht. Een artikel uit 2017 van An Weiping, destijds plaatsvervangend stafchef van het Northern Theater Command van de PLA, identificeerde vier centrale focusgebieden voor deze hervorming:

1. De coördinatie van militair-civiele fusieafdelingen op alle niveaus van overheid en leger.
2. De versterking van het juridische en regelgevende kader om de inzet van civiele cybercapaciteiten te standaardiseren.
3. Investeringen in infrastructuur voor duaal gebruik, zoals cyber-oefenterreinen en communicatienetwerken.
4. Een strakkere integratie tussen civiele en militaire actoren voor zowel training in vredestijd als inzet in oorlogstijd.

De *2018 National Conference on Cybersecurity and Informatization* was een cruciaal keerpunt. De beleidsaanpassing die hieruit voortkwam, was de erkenning dat de private sector onmisbaar is voor nationale cyberdefensie, maar dat de inzet hiervan uitsluitend mag plaatsvinden onder een strikt "gemilitariseerd, gesystematiseerd en systemisch" kader van toezicht door de Partij-staat. Dit moest voorkomen dat de staatscontrole over de nationale veiligheid zou eroderen. De hervormingen die sindsdien zijn doorgevoerd, kunnen in vier dimensies worden samengevat:

Hervormingsgebied	**Kerninitiatieven**
Juridisch & Regelgevend	Gebruik van permissieve wetgeving (zoals de Cybersecurity Law 2017) en interne Partij-kaders om lokale experimenten en de normalisering van civiele mobilisatie te legitimeren.
Organisatorisch	Ontwikkeling van "cyber defense talent databases", verbeterde data-uitwisseling met Theater Commando's, en de oprichting van een nieuw Joint Command Organization and Operation System.
Menselijk Kapitaal	Diversificatie van rekrutering (van studenten naar professionals), uitbreiding naar de private techsector, en versterking van technische training en politiek-ideologische educatie.
Materieel & Infrastructuur	Co-ontwikkeling van cyber training ranges in publiek-private partnerschappen en het verstrekken van moderne uitrusting (zoals commandovoertuigen en voor BeiDou-satellieten geschikte handheld terminals).

3.2 Huidige Structuur en Functie

Het genereren van troepen (*force generation*) voor de cybermilitie is een gelaagd proces. Provinciale en gemeentelijke comités coördineren de identificatie van middelen, terwijl de implementatie wordt overgelaten aan de People's Armed Forces Department (PAFD)-kantoren op districtsniveau. Deze kantoren werken samen met werk-eenheden (*danwei*), zoals universiteiten en bedrijven, om personeel toe te wijzen en de paraatheid te monitoren.

Traditioneel was de rekrutering gebaseerd op administratieve druk op staatsbedrijven en universiteiten. Steeds vaker worden echter op prikkels gebaseerde modellen toegepast om de private sector te betrekken, zoals belastingvoordelen, voorkeursbehandeling bij openbare aanbestedingen en toegang tot overheidsleningen.
De cybermilitie-eenheden zijn onderverdeeld in drie hoofdcategorieën:

- **Standaardeenheden (常备型):** Dit zijn permanente formaties die zijn ingebed in overheidsinstanties en grote staatsbedrijven in de telecomsector. Ze handhaven een constante operationele paraatheid.
- **Reserve-eenheden (储备型):** Dit is een talentenpool van technisch personeel afkomstig uit het MKB in de IT-sector en georganiseerde netwerken van cyber-enthousiastelingen. Zij bieden *surge*-capaciteit in tijden van crisis.
- **Experteenheden (专家型):** Deze eenheden bestaan uit elite-personeel van universiteiten, onderzoeksinstituten en R&D-bedrijven. Zij vervullen complexe, adviserende of missiekritieke rollen.

Lidmaatschap vereist een combinatie van "rood" (politieke betrouwbaarheid en loyaliteit aan de Partij) en "expert" (technische competentie). De selectie geeft prioriteit aan "high-tech talent, professionele vaardigheden en gedemobiliseerd militair personeel" om te verzekeren dat de eenheden zowel ideologisch zuiver als technisch capabel zijn.

3.3 Missiespectrum: Van Defensie tot Offensieve Ondersteuning

De cybermilities hebben een breed en divers missiespectrum dat vier primaire categorieën omvat:

1. **Beveiliging van Kritieke Netwerkinfrastructuur:** Milities worden beschouwd als de "hoofdmacht" (*main force*) in de verdediging van vitale infrastructuur, zoals telecomnetwerken, industriële controlesystemen en DNS-infrastructuur. Ze identificeren kwetsbaarheden en herstellen systemen na cyberaanvallen of fysieke verstoringen.
2. **Strategische Reserve voor de PLA:** De milities fungeren als een strategische reserve voor de PLA met capaciteiten die parallel lopen aan die van de formele cyberstrijdkrachten (PLACSF en PLAISF). In vredestijd nemen ze ondersteunende taken op zich, zoals firewall-onderhoud, waardoor elite-eenheden zich kunnen richten op offensieve missies. In een conflictsituatie kunnen ze echter ook worden ingezet voor offensieve operaties zoals jamming, netwerkinbraken en de inzet van kwaadaardige code, met specifieke training voor scenario's in de Zuid-Chinese Zee en rond Taiwan.
3. **Strategische Misleiding:** Een minder gedocumenteerde maar belangrijke functie is het optreden als "valse en vermomde doelen" om vijandelijke targeting te compliceren. Dit kan inhouden dat ze honeypots opzetten die gevoelige systemen imiteren of valse command-and-control-communicatie genereren om de aandacht van de tegenstander af te leiden.
4. **Beheer van de Publieke Opinie:** Milities spelen een cruciale rol in *public opinion guidance* (舆论引导). Hun taken omvatten het monitoren van online discussies, het analyseren van sentiment, het onderdrukken van "schadelijke geruchten" en het actief promoten van de staatsnarratieven. De inzet tijdens de COVID-19-pandemie was meer dan alleen een voorbeeld van deze missie; het diende als een grootschalige, reële

stresstest voor het hele systeem. Het bood de PLA de gelegenheid om "smart mobilization"-instrumenten te beproeven en tekortkomingen in de interinstitutionele samenwerking onder crisisomstandigheden te identificeren en aan te pakken.

Deze theoretische structuur en missies worden in de praktijk gebracht door een voorhoede van toonaangevende technologiebedrijven die de visie van de Partij-staat op militair-civiele fusie belichamen.

4. De Voorhoede in Actie: Casestudies van Militair-Civiele Fusie

De cybermilitie-eenheden van bedrijven als Qihoo 360 en Antiy Labs zijn niet representatief voor de *gemiddelde* militie-eenheid in China. Ze vormen echter de voorhoede en dienen als het model dat de Partij-staat voor ogen heeft voor de toekomst van het systeem: een diepe, naadloze integratie van de meest geavanceerde private cybercapaciteiten in de nationale defensiestructuur.

4.1 Casestudy: Qihoo 360

De cyberveiligheidsmilitie-eenheid van Qihoo 360, bekend als de *Jiuxianqiao Street* eenheid in Beijing, is een van de meest prominente voorbeelden van militair-civiele fusie.

- **Missie en relatie met de Partij-staat:** De missie van de eenheid is het ondersteunen van de PLA om te "zegevieren in toekomstige cyberoorlogsvoering". De voorzitter van 360 Enterprise Security Group, Qi Xiangdong, benadrukte deze ideologische afstemming door te stellen dat "cyberveiligheid verbonden is met nationale veiligheid, consolidatie van het regime, sociale stabiliteit en de uitkomst van oorlog". De militie functioneert als een formeel kanaal om netwerkverdediging en dreigingsinformatie aan de PLA te leveren.
- **Samenstelling en training:** De eenheid wordt geleid door actieve militaire kaders en rekruteert personeel uit de technische afdelingen van Qihoo, met een sterke voorkeur voor Partijleden. De training is tweeledig: een ingebedde Partij-afdeling zorgt voor politieke en ideologische indoctrinatie, terwijl technische vaardigheden worden aangescherpt via gastcolleges van experts van de Academy of Military Sciences (AMS) en de National Defense University (NDU).
- **Operationele capaciteiten:** De competenties van de militie omvatten:
- Het bouwen van defensieve systemen voor militaire internetdiensten.
- Samenwerking met het MKB op het gebied van R&D voor defensieve oplossingen.
- Analyse en monitoring van Advanced Persistent Threats (APT's).
- Netwerkmonitoring, cyberaanval en -verdediging, en beheer van de publieke opinie.

4.2 Casestudy: Antiy Labs

Antiy Labs, een ander toonaangevend cyberbeveiligingsbedrijf, onderhoudt de grootste bekende cybermilitie-eenheid in China, met meer dan 100 personeelsleden.

- **Unieke relatie met de Partij-staat:** De oprichter van Antiy, Xiao Xinguang, heeft een unieke positie als lid van de Chinese People's Political Consultative Conference (CPPCC), een hoog politiek adviesorgaan. Hij gebruikt deze positie om het nationale beleid te beïnvloeden en Antiy Labs te positioneren als een nationaal model voor militair-civiele integratie.
- **Missie en focus:** De missie van Antiy's militie is gericht op incidentrespons en de bescherming van kritieke informatie-infrastructuur. Gezien de locatie van het

hoofdkantoor in Harbin, is er een waarschijnlijke focus op het noordoostelijke theater, dat grenst aan Rusland en Noord-Korea.
- **Beleidsinvloed:** Xiao Xinguang heeft beleidsvoorstellen gedaan die de strategische visie van Antiy weerspiegelen. Hij pleit voor een geïntegreerd nationaal noodresponsraamwerk dat middelen van de overheid en private bedrijven samenvoegt onder de centrale aansturing van de PLA's cyberstrijdkrachten (voorheen PLASSF, de inmiddels gereorganiseerde overkoepelende strategische eenheid, nu PLACSF/PLAISF).

Deze casestudies illustreren de geavanceerde implementatie van Militair-Civiele Fusie, maar onthullen ook de diversiteit in aanpak. Waar Qihoo 360 een technologische reus is die via formele Partijstructuren wordt geïntegreerd voor een breed missiespectrum, vertegenwoordigt Antiy Labs een meer gespecialiseerd, door de oprichter gedreven model dat het beleid actief van binnenuit vormgeeft. Deze flexibiliteit toont de verfijning van de MCF-strategie, die verre van een eenvormige aanpak is en zich aanpast aan de unieke capaciteiten van verschillende private actoren.

5. Strategische Beoordeling: Capaciteiten, Uitdagingen en Toekomstperspectief

China's cybermilitiesysteem heeft onder Xi Jinping onmiskenbaar grote vooruitgang geboekt. Toch wordt de huidige staat gekenmerkt door een fundamentele spanning die voortvloeit uit zijn dubbele aard: de ambitie van gecentraliseerde militaire controle versus de realiteit van een gedecentraliseerde, civiele basis. Hoewel de professionalisering is toegenomen, blijven er significante structurele uitdagingen bestaan die de strategische effectiviteit van het systeem kunnen ondermijnen.

Structurele Uitdagingen en Kwetsbaarheden

- **Structurele Fragmentatie en Afhankelijkheid:** Het systeem is sterk afhankelijk van lokale infrastructuur en menselijk kapitaal. Dit leidt tot grote capaciteitsverschillen tussen economisch ontwikkelde kustprovincies en minder ontwikkelde, maar strategisch belangrijke, binnenlandse regio's zoals Tibet en Xinjiang. Deze fragmentatie belemmert de flexibele inzet van eenheden op nationaal niveau.
- **Uitdagingen in Rekrutering, Training en Behoud:** Veel private bedrijven, met name het MKB, zijn terughoudend om hun schaarse en hoogwaardige technische personeel vrij te maken voor miltietaken. Bovendien missen veel technisch bekwame rekruten de nodige "battlefield literacy"—militaire discipline en operationele veiligheidsprotocollen. Het gebrek aan geschikte trainingsinfrastructuur, zoals cyber-oefenterreinen, verergert dit probleem.
- **Tekortkomingen in het Mobilisatiesysteem:** Er ontbreekt nog steeds een nationaal, verenigd strategisch reservemechanisme. Veel lokale autoriteiten vertrouwen nog op papieren administratie of verouderde databases, wat een real-time inventarisatie van cybermiddelen en een snelle, gecoördineerde mobilisatie bemoeilijkt.

Implicaties voor Westerse Veiligheid

Ondanks deze beperkingen is het niet langer houdbaar om de Chinese cybermilities als een perifeer fenomeen te beschouwen. De implicaties voor de westerse veiligheid zijn aanzienlijk:

- De grens tussen actieve en reserve cyberstrijdkrachten vervaagt. Dit geeft China een schaalbare *surge*-capaciteit die in een conflictsituatie snel kan worden geactiveerd, waardoor de druk op de tegenstander kan worden opgevoerd en volgehouden.
- Westerse inlichtingendiensten en dreigingsanalisten moeten hun focus verbreden. Een exclusieve aandacht voor staatsgestuurde APT-groepen is onvoldoende. De analyse moet worden uitgebreid naar het bredere ecosysteem van in de private sector ingebedde milities.
- Het risico van onderschatting is groot. Als deze opkomende component van China's cybermacht wordt genegeerd in operationele planning en dreigingsanalyses, kan de schaal en veerkracht van de Chinese cybercapaciteit in een toekomstig conflict ernstig worden onderschat.

Hoewel het cybermilitiesysteem nog onvolkomen is, wijst de voortdurende investering en hervorming door de Partij-staat op de potentiële opkomst van een formidabel instrument. De kern van deze strategie is een strategische paradox: de grootste kracht van het systeem—het aanboren van de enorme, innovatieve civiele sector—is tegelijkertijd de bron van zijn grootste zwakte: het gebrek aan gecentraliseerde militaire discipline en uniform commando. Toch creëert deze fusie van civiele expertise en militaire ambitie een latente, maar krachtige reservemacht die de strategische balans in een toekomstig conflict aanzienlijk kan beïnvloeden. Het Westen kan het zich niet veroorloven deze ontwikkeling te negeren.