Cyberwar 2.0

Sergei Boeke

Oktober was cyber security-maand. Of scherper geformuleerd: *cyber security awareness month*, met conferenties en andere activiteiten om de bewustwording te vergroten. Vorige maand werd dit ondersteund door bijzonder veel praktijkvoorbeelden. Deze betroffen onder meer de Binance hack van 6,4 miljard dollar, kritieke kwetsbaarheden in de PHP2Shell, de LiteLLM-aanval op de software-keten, en supermarkten met ontdooide diep-vriesvoorraden. Cyberprofessionals spraken van 'Black October' en hadden niet eerder zoveel ernstige incidenten in een maand gezien.
Het identificeren van de hackers was, zoals gewoonlijk in de cyber securitywereld, geen uitgemaakte zaak. Er zijn over het algemeen vier categorieën daders. De figuurlijke vijftienjarige die nog thuis woont (motief hack: omdat het kan); de hacktivisten (gedreven door ideologie of onrecht), cybercrime-groepen (jagen het grote geld na) en tot slot, statelijke actoren – die handelen voor de nationale veiligheid.
De laatste groep heeft in de regel de meeste middelen beschikbaar om zowel de hack te zetten als onherleidbaar te blijven. Bovendien kunnen zij zich ook nog voordoen als een van de drie andere categorieën, en hier zijn legio voorbeelden van. Attributie – het identificeren van de dader – is dus een uitdaging.

Sinds de jaren negentig is gewaarschuwd voor cyberoorlog: een 'Cybergeddon' of een 'digital Pearl Harbor' zou de maat-schappij lam leggen. Ook in aanloop naar de Russische invasie van Oekraïne in 2022 vreesde men een grootscheepse cyberaanval die de kritieke infrastructuur zou uitschakelen. Maar eigenlijk wordt deze zogeheten cyberoorlog al in vredestijd uitgevoerd, zoals Huib Modderkolk in zijn boek betoogt.[1] Verschillende hacks op overheidsinstellingen, energiecentrales en andere doelwitten verstoren dienstverlening en veroorzaken schade. Vaak duurt het lang om de aanvallers op te sporen, en hun publieke attributie kan een ingewikkeld politiek besluit zijn. Zo behouden daders vaak *plausible deniability*. Rusland, China, Iran, Noord Korea: ze zijn allemaal zeer actief in cyberspace, als onderdeel van hun hybride operaties. Maar een van de meest toonaangevende voorbeelden, vaak aangehaald in het debat over cyberoorlog, betreft het Stuxnet-virus (Operation Olympic Games). In 2006 hadden de Amerikaanse National Security Agency (NSA) en de Israëlische cyber/sigint eenheid 8200 een complex virus ontwikkeld dat op zeer vernuftige wijze het Iraanse nucleaire verrijkingsprogramma saboteerde.[2] Tot 2024-2025 waren er weinig – wellicht geen – andere diensten die zo'n geavanceerde cyberaanval konden ontwikkelen en uitvoeren. Toen kwam Artificial Intelligence (AI) beschikbaar. Wat eerder voorbehouden was aan eliteteams van hackers kan AI nu veel beter en sneller doen.

Cyber en AI zijn beide 'hot' en genieten veel politieke en wetenschappelijke aandacht. Toch worden (internationale) discussies vaak gevoerd zonder enig begrip van de fundamenten van het veld, en worden mooie termen gebruikt die iedereen ongemerkt anders definieert. Bij Defensie is dit niet anders. De zogeheten cyberhygiëne van medewerkers is de laatste tijd beter, maar begrip over hoe cyber militaire operaties kan



1 Huib Modderkolk, *Het is oorlog, maar niemand die het ziet* (Amsterdam, Podium, 2020).
2 Verplichte leeskost voor degene met interesse in cyber security: Kim Zetter, *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon* (New York, Crown, 2014).

ondersteunen blijft oppervlakkig. Cyber is ook een van de onderwerpen waar NAVO-commandanten, op zowel het tactische, operationele als strategische niveau, niet sterk zijn (de andere zijn targeting procedures, enablement en space). Men blijft vooral steken op bijvoorbeeld simpele shapingsoperaties in social media. Dit is ergens ook logisch, want het echte strategische werk – bijvoorbeeld het hacken van de vijandelijke luchtverdediging of C2 – blijft voorbehouden aan de inlichtingendiensten. En die opereren niet alleen in het geheim, maar hebben ook de neiging om alles te overclassificeren en geheim te houden. In 2022 schreven twee analisten van de MIVD (anoniem) een goed stuk over de uitgangspunten van het militair optreden in cyberspace. Het was 'All about access': ongemerkt toegang verkrijgen in een netwerk door unieke kwetsbaarheden te gebruiken, vaak meerdere per operatie, en dit kostte veel tijd. Eenmaal in het netwerk is spionage wellicht het doel, maar de optie tot sabotage krijgt men gratis mee.[3] Dus om een geslaagde cyberaanval te kunnen uitvoeren moeten in principe eerst alle stappen van een cyberspionage-operatie worden doorlopen.

Voordat AI zijn intrede deed hadden aanvallers in cyberspace al een voorsprong op verdedigers. Verdedigers waren verantwoordelijk voor een groot oppervlak (*attack surface*), terwijl aanvallers maar één keer succesvol hoefden in te breken, en dat via tussenschakels of platforms konden doen. AI biedt nu een krachtige *force multiplier* voor aanvallers. Het is veel sneller, geautomatiseerd (dus 24/7), effectiever en alles is schaalbaar. De tijd tussen het ontdekken van een kwetsbaarheid (bijvoorbeeld een *zero day*) en het uitbuiten is ingekort van maanden naar uren of minuten. Voor een verdediger is de tijd tussen indringen en exploitatie zo snel dat oude *incident response*-procedures, geleid door mensen, niet meer werken. Hiernaast kan AI *phishing* effectief afstemmen op het doelwit, waarbij bijvoorbeeld met *deep fake*-videos bijna alle targets verleid worden om een link te openen of een andere handeling te verrichten (de 'CEO' komt met een spoedverzoek om geld over te maken…). In andere woorden: door AI is de balans nog verder verschoven in het voordeel van de aanvaller.

Sommige analisten stellen dat AI op termijn ook verdedigers kan helpen; anderen vrezen dat een *defense collapse threshold* nadert waarbij de verdediging geen enkele kans meer heeft.[4] Het staat in ieder geval vast dat AI het veld van cyber security net zoveel heeft getransformeerd als drones de fysieke domeinen van land, zee en lucht.

De zogeheten democratisering van het geavanceerd hacken heeft grote gevolgen voor de nationale veiligheid. De vitale sector met zijn kritieke infrastructuur, van energievoorziening tot het internet, is nu extra kwetsbaar. Als deze netwerken gecompromitteerd worden door vijandelijke actoren – zowel in vredestijd als in conflict – dan worden militaire capaciteiten snel irrelevant. Nationale veiligheid is daarom net zo gebaat bij een *cyber secure* vitale sector als een sterke krijgsmacht. Dit is nog niet doorgedrongen in bewustzijn, budgetten en bestuursmodellen, en het coördineren van het versplinterde cyber security-landschap blijft een uitdaging. Nederland heeft op cyber een unieke kennispositie, en als het om hacken gaat behoort de Joint Cyber Sigint Unit van de AIVD en MIVD tot de wereldtop. Maar terwijl kleine niches druk zijn om Cyberwar 2.0 te mitigeren, blijven grote delen van de vitale sector en Defensie nog steken bij een incompleet begrip van cyber security 1.0, laat staan de AI-transformatie. Een beter bewustzijn, minder geheimhouding, meer integratie van cyber security in reguliere processen zijn allemaal noodzakelijk – en wellicht een update van het 'All about access'-artikel. Er zijn nu zoveel incidenten dat meer inzetten op cyber security vanzelfsprekend zou moeten zijn. Oktober was weliswaar cyber security-maand, maar november, december en januari zouden dit ook zo maar kunnen worden. ■

3 Anoniem, 'All about access', *Militaire Spectator* 191 (2022) (9) 464-475. Zie: https://militairespectator.nl/artikelen/all-about-access.

4 Tim Green, 'The Collapse Equation. When AI Tips the Cybersecurity Balance Beyond Recovery', *SmarterArticles*, 4 maart 2026. Zie: https://smarterarticles.co.uk/the-collapse-equation-when-ai-tips-the-cybersecurity-balance-beyond-recovery.