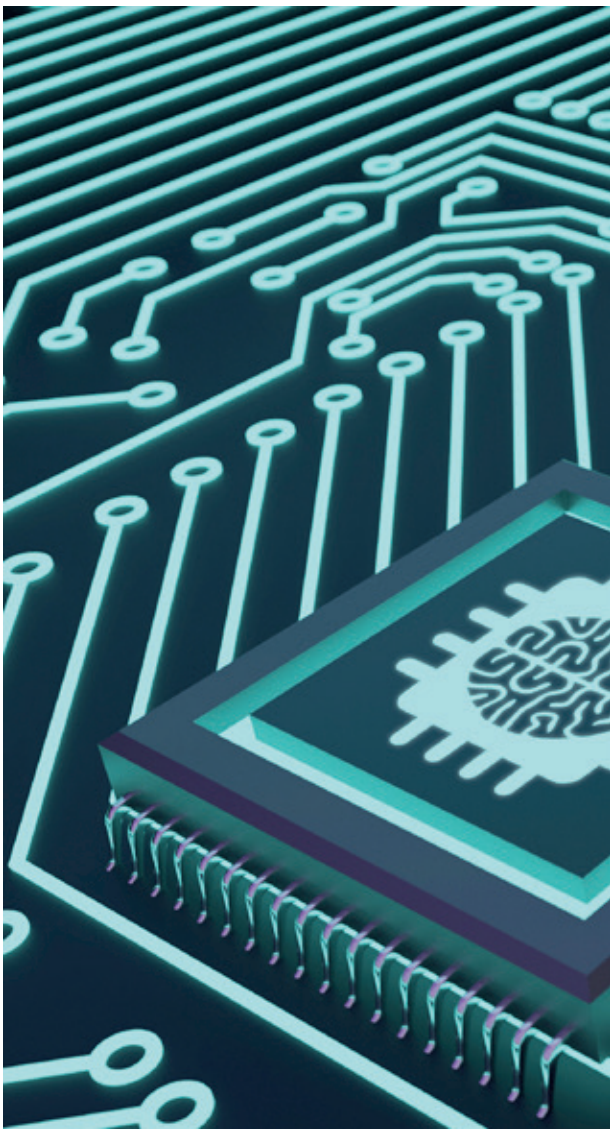
Wiperware: een nieuw cyberwapen voor de militaire toolbox?

Luitenant-kolonel K.L. Arnold ESMD MSc en drs. S. van Dorst*

In het huidige Russisch-Oekraïense conflict vinden dagelijks cyberaanvallen plaats; niet alleen gericht tegen Rusland en Oekraïne, maar ook tegen derde landen. Het overgrote deel van die cyberaanvallen betreft relatief onschuldige *denial-of-service*-aanvallen, *defacements* of *hack-and-leak*-operaties met bescheiden militaire impact. Slechts een enkele cyberaanval staat uitgebreid in de belangstelling en heeft meer (militaire) betekenis. Daartussen bevindt zich een categorie cyberaanvallen met een destructief karakter; klein in aantal, maar met potentie om via digitale oorlogvoering daadwerkelijk tastbare schade aan te richten: zogeheten 'wiperware'. Maar wat is wiperware? Wat doet het en hoe werkt het? Wat is de militaire meerwaarde ervan? Past het in de gereedschapskist van onze eigen krijgsmacht? Dit artikel gaat in op de mogelijkheden van wiperware voor militaire doeleinden.

Wat is wiperware, en heeft het militaire toepassingen?
FOTO DARPA



Cyberaanvallen vinden tegenwoordig dagelijks plaats, maar alleen de meest opvallende worden geregistreerd en geanalyseerd en komen in het nieuws. Dit geldt ook voor de Russisch-Oekraïense cyberoorlogvoering. Er lijkt weinig te gebeuren in cyberspace, maar niets is minder waar. Sinds de invasie op 24 februari 2022 zijn 2.776 aan deze oorlog gerelateerde cyberaanvallen geregistreerd.[1]

Grofweg kun je cyberaanvallen indelen in drie categorieën.[2] Allereerst zijn er cyberaanvallen met een strategische impact. In de Russisch-Oekraïense oorlog is vooralsnog één cyberaanval

aan te wijzen die een dergelijke strategische impact had; of had kunnen hebben. Op de vooravond van de invasie vielen hackers modems aan van het Viasat satelliet-internet-communicatiesysteem. Met elektronische oorlogvoering (EOV) verminderden de Russen reeds de effectiviteit van drie van de vier hoofdvormen van draadloze communicatie[3] van de Oekraïense strijdkrachten. De uitschakeling van Viasat completeerde het verlies van militaire communicatie, met name in de regio van het destijds zwaar bedreigde Kyiv.[4] De Viasat-cyber-aanval maakte de Oekraïense troepen vrijwel blind voor de Russische troepen en hun bewegingen.[5] Met steun van Elon Musks Starlink satellietontvangers[6] en tienduizenden nieuwe Viasat-modems[7] kon de Oekraïense internet-communicatie echter snel worden hersteld,

* Kraesten Arnold is cyberonderzoeker en -docent aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie in Breda; Sander van Dorst is als medewerker verbonden aan het team Concepten & Doctrine van het Cyber Warfare & Training Centre.

1 CyberPeaceInstitute, status per 30 september 2023. Zie: https://cyberconflicts.cyberpeaceinstitute.org/impact.

2 Jon Lindsay en Erik Gartzke, 'Coercion through Cyberspace: The Stability-Instability Paradox Revisited', in: K.M. Greenhill en P.J.P. Krause (red.), *The Power to Hurt: Coercion in Theory and in Practice* (Oxford, Oxford University Press, 2016) 179–203; B.M.J. Pijpers en Kraesten L. Arnold, 'Arms Control in Cyberspace?', *Altantisch Perspectief* 47 (2023) (2) 35–40.

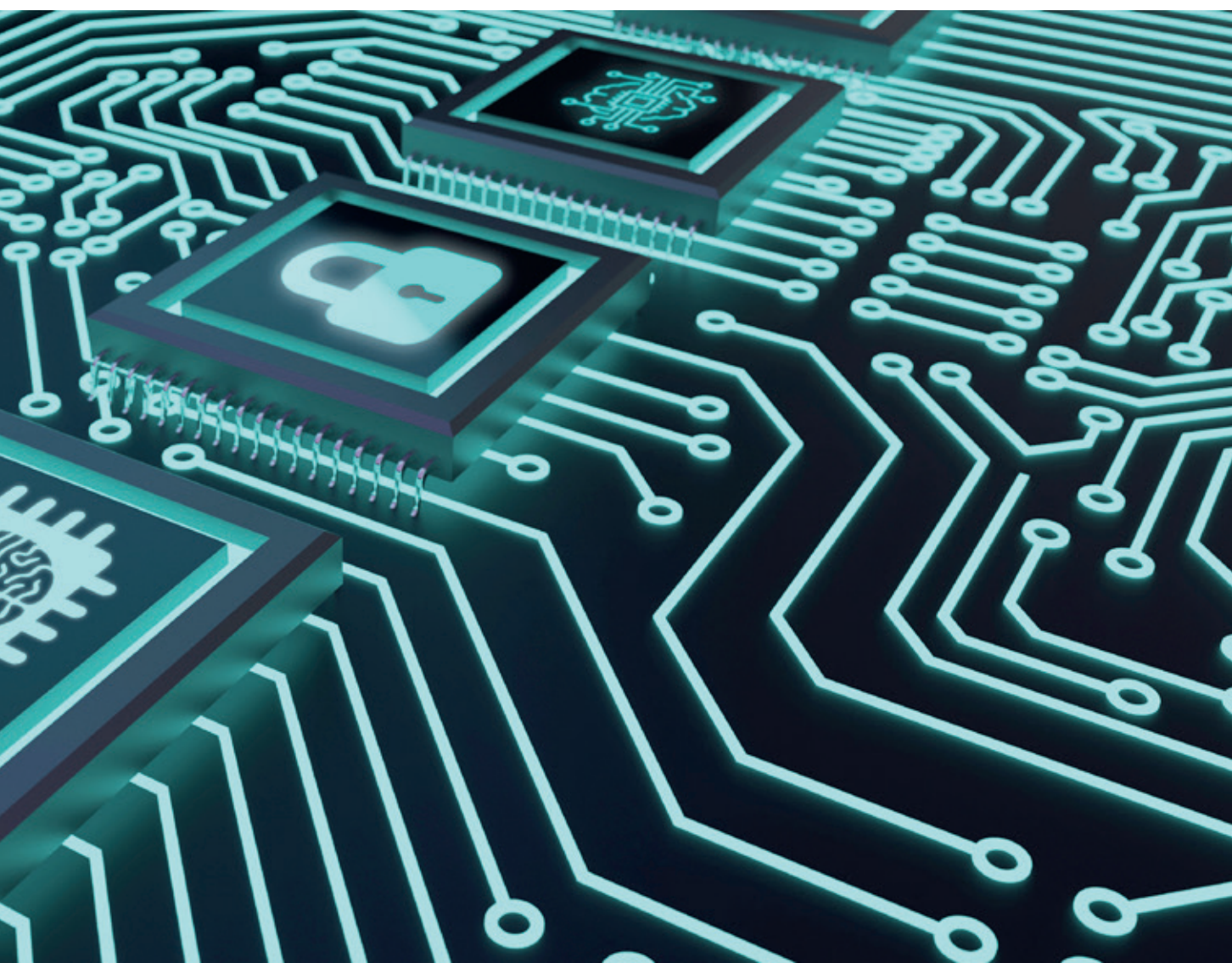
3 *Legacy* analoge radiosystemen; nieuwe, beveiligde digitale radiosystemen; LTE mobiele telefonie; satellietcommunicatie (SATCOM).

4 Dan Rice, 'The Untold Story of the Battle for Kyiv', *Small Wars Journal*, 31 mei 2022. Zie: https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv.

5 Jason Blessing, 'Revisiting the Russian Viasat Hack: Four Lessons About Cyber on the Battlefield', *American Enterprise Institute*, 2 september 2022.

6 Hyunjoo Jin, 'Musk Says Starlink Active in Ukraine as Russian Invasion Disrupts Internet', *Reuters*, 2022.

7 Viasat Corporate News, 'KA-SAT Network cyber attack overview', 30 maart 2022. Zie: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.



Het gebruik van wiperware als cyberwapen is vermoedelijk te herleiden naar de VS FOTO DARPA

waardoor de negatieve gevolgen voor Oekraïne beperkt bleven.

Van een geheel andere orde zijn cyberaanvallen die weliswaar veelvuldig voorkomen, maar eerder vervelend dan schadelijk zijn. Die aanvallen veroorzaken geen dood en verderf, en dienen ogenschijnlijk geen militair doel, maar zijn desondanks wel hinderlijk. Het merendeel van de waargenomen en geregistreerde cyberaanvallen die zijn te relateren aan de Russisch-Oekraïense oorlog bestaat uit dat soort hinderlijke denial-of-service aanvallen,[8] website defacements,[9] phishing[10] en hack-and-leaks.[11]

De derde categorie betreft cyberaanvallen die op een operationeel niveau (in)direct militaire of diplomatieke campagnes ondersteunen. Rusland en Oekraïne verzamelen beide digitaal inlichtingen en beide landen voeren digitale verkenningsoperaties uit ter ondersteuning van hun militaire operaties. Maar er is nog een type cyberaanvallen dat in deze oorlog door pro-Russische actoren is ingezet tegen een scala aan Oekraïense entiteiten: aanvallen met ransomware en wiperware, ofwel kwaadaardige software bedoeld om respectievelijk data te versleutelen, of data én computers onherstelbaar te beschadigen.

Met dit artikel willen we inzicht verschaffen in de mogelijkheid wiperware in te zetten als operationeel cyberwapen ter ondersteuning van militaire operaties. We starten met een uitleg wat wiperware omvat: wat het is, wat het doet en

8 Bij een denial-of-service (DOS)-aanval wordt een computer of netwerk bestookt met dusdanig veel opdrachten of verzoeken dat de werking van die computer of dat netwerk ernstig wordt beperkt of zelfs onmogelijk gemaakt. Een distributed denial-of-service (DDoS) aanval gebruikt meerdere computers voor de cyberaanval.

9 Bij een website defacement verandert de aanvaller het 'uiterlijk' van een website door die te vullen met andere inhoud (tekstueel en visueel), zoals politieke, sociale of religieuze boodschappen.

10 Phishing is het 'hengelen' naar vertrouwelijke informatie zoals gebruikersnamen, wachtwoorden en creditcardgegevens.

11 Onder hack-and-leak wordt verstaan het inbreken in een computer, om vervolgens gevoelige informatie te stelen en naar buiten te brengen.

welke effecten je ermee kunt creëren. Dan kijken we naar de ontstaansgeschiedenis van deze vorm van malware, waarbij enkele roemruchte cyberaanvallen aan de orde komen. Vervolgens gaan we in op het specifieke gebruik van dit soort cyberwapens in het Russisch-Oekraïense conflict; welke doelwitten zijn bestookt; door welke actoren; in hoeverre diende dit een militair doel en; was het effectief? Hieruit volgt een analyse waarna we aangeven in hoeverre wiperware een praktisch bruikbaar cyberwapen kan zijn voor onze eigen krijgsmacht.

Wat is wiperware?

Als je in een gangbaar computer besturingssysteem[12] (*Operating System*, OS) een bestand verwijdert, dan gebruik je bijvoorbeeld *delete* (bij een Microsoft Windows OS) of *remove* (bij een Linux OS).[13] Met dat commando verwijder je evenwel alleen de verwijzing naar dat bestand zodat het besturingssysteem dat bestand niet meer 'ziet'. De inhoud van het bestand zelf wordt echter niet gewijzigd. Een bestand dat op die manier is 'verwijderd', kun je dan ook relatief eenvoudig weer terughalen.[14] Als je de inhoud van een bestand permanent wil verwijderen of onleesbaar maken, dan moet je die inhoud geheel of gedeeltelijk vervangen door andere, bijvoorbeeld willekeurig gegenereerde gegevens. Hoe vaker je dat proces herhaalt, des te lastiger het is om de originele informatie nog terug te halen. Op een bepaald moment is dat niet meer mogelijk.

De term 'wiper' in wiperware slaat op de primaire functie van dergelijke software, die is bedoeld om data definitief te wissen van het permanente computergeheugen.[15] In werkelijkheid worden specifieke computerbestanden,[16] of bepaalde gedeeltes van een harde schijf,[17] meerdere keren overschreven met andere data, maar soms ook met (politieke) boodschappen of foto's.[18] De originele informatie is dan onherstelbaar beschadigd ('gewist').

Behalve gegevensbestanden (*files*) permanent wissen, kan wiperware ook andere software beschadigen, zoals het programma dat nodig is om de computer op te starten (*bootloader*);[19] de software die zorgt voor de virtuele indeling ('partities') van het computergeheugen,[20] of andere *firmware*.[21] Een geheel andere methode is het onomkeerbaar cryptografisch versleutelen van specifieke databestanden, gedeeltes van de harde schijf, of essentiële systeembestanden die nodig zijn om een computersysteem op te starten. De gedachte erachter is hierbij hetzelfde. De computer, of het apparaat waar die computer in zit, werkt niet meer naar behoren of kan zelfs helemaal niet meer opstarten. De computer is dan niet meer te gebruiken.

Omdat voornoemde wipe-methodes elk hun specifieke voor- en nadelen hebben, bestaat wiperware vaak uit een combinatie van die methodes om een zo groot mogelijk destructief effect te creëren. De reden voor een wiper-aanval kan variëren, maar in tegenstelling tot ransomware ligt bij wiperware een financiële drijfveer

12 Een besturingssysteem zorgt ervoor dat, na het opstarten van de computer, de hardwarecomponenten met de verschillende softwareprogramma's kunnen communiceren.
13 Andere gangbare besturingssystemen zijn macOS, Unix, Android, BSD, VMkernel, IOS, Solaris.
14 Het verwijderen van een computerbestand en vervolgens de prullenbak legen is niet voldoende om gegevens op een computer of gegevensdrager (harde schijf, SDD USB, CD-rom, flash-geheugen) permanent te wissen. Zelfs het (eenmalig) formatteren van dat geheugen is daartoe niet afdoende. Met *data recovery software* zijn die gegevens namelijk weer te achterhalen.
15 Dit betreft zowel vast als verwisselbaar geheugen, zoals een hard disk, solid state drive of USB-stick.
16 *Data destruction*, zie: https://attack.mitre.org/techniques/T1485/.
17 *Disk content wipe*, zie: https://attack.mitre.org/techniques/T1561/001/.
18 De aanval met Shamoon wiperware in 2012 toonde een brandende Amerikaanse vlag. De Shamoon wiperware van 2016 toonde de foto van een gevlucht Syrisch kind; verdronken en aangespoeld op het strand. Sean Gallagher, 'Shamoon wiper malware returns with a vengeance', *Ars Technica*, 12 januari 2016. Zie: https://arstechnica.com/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/.
19 Een bootloader betreft software die na het opstarten van een computer bekijkt welke hardware aanwezig is en welke stuurprogramma's voor die hardware moeten worden geladen. Deze opstartsoftware is ook nodig om het besturingssysteem op te starten. Voorbeelden van opstartsoftware zijn de Unified Extensible Firmware Interface (UEFI) en het wat oudere Basic Input / Output System (BIOS).
20 Bij het partitioneren van het computergeheugen deel je de fysieke opslagruimte op de harde schijf op in gedeeltes. Zo kun je bijvoorbeeld één opstartbare partitie gebruiken voor het besturingssysteem, één partitie voor programma-toepassingen en één partitie om gegevens op te slaan. Een dergelijke indeling wordt gemaakt door de (oudere) Master Boot Record (MBR) of (nieuwere) GUID Partition Table (GPT).
21 Firmware is software die is ingebed in de hardware van een computer. Firmware zorgt ervoor dat een computer of computeronderdelen, of het apparaat waar die computer in zit, kunnen opstarten en vervolgens goed kunnen functioneren.

niet voor de hand.[22] Logischer is dat een aanvaller een wiper bijvoorbeeld gebruikt om sporen van andere activiteiten, zoals spionage, te wissen. Het kan uiteraard ook gewoon de bedoeling zijn om permanente schade aan te richten.

Ontstaansgeschiedenis

In 2012 vielen onbekende hackers Saudi Aramco aan; een Saoedisch staatsoliebedrijf en een van de grootste oliebedrijven ter wereld. De schade was ongekend. Van meer dan 35.000 Windows-computers werden alle gegevens gewist en de computers zelf werden vervolgens onherstelbaar beschadigd. Hoewel de olie*productie* onverminderd doorliep, was het *handelen* erin nagenoeg onmogelijk geworden.[23] Een groep die zichzelf Cutting Sword of Justice noemde, claimde de verantwoordelijkheid. De malware kreeg de naam 'Shamoon'. Het vermoeden bestond dat de cyberaanval het werk was van Iraanse statelijke actoren.[24] Het land reageerde met deze aanval waarschijnlijk op een soortgelijke aanval eerder dat jaar gericht tegen het Iraanse ministerie van olie en de nationale Iraanse Oliemaatschappij. In 2016,[25] 2017,[26] en 2018[27] keerde Shamoon nagenoeg ongewijzigd terug op het toneel en wederom waren computers van de oliesector in Saoedi-Arabië het doelwit.

Het Russische cybersecuritybedrijf Kaspersky onthulde in 2012 dat Shamoon gelijkenissen vertoonde met malware die eerder juist tegen Iran was gebruikt. Kaspersky's onderzoek leidde destijds tot de ontdekking van de zogeheten *Flame*-malware.[28] Op zich lijkt dat niet zo relevant, ware het niet dat die Flame-malware[29] op zijn beurt weer gelijkenissen vertoonde met het *Stuxnet*-virus,[30] de (vermeend) Amerikaans-Israëlische malware die schade aanrichtte bij de Iraanse uraniumverrijkingsinstallatie in Natanz.[31] Kaspersky vond aanwijzingen dat de makers van Stuxnet dezelfde waren als de zogeheten Equation Group en daarmee de Amerikaanse National Security Agency (NSA); of daarmee op zijn minst nauwe banden hadden.[32] Het initiële gebruik van wiperware als cyberwapen is daarmee vermoedelijk te herleiden naar de Verenigde Staten.

In 2013 maakte de, aan de Noord-Koreaanse staat gelieerde, hackergroep Dark Seoul gebruik van wiperware (*Trojan.Jokra*) tegen Zuid-Koreaanse doelwitten in de financiële en mediasector. Hoewel de malware 32.000 computers beschadigde van zes financiële en mediabedrijven,[33] bleek de gebruikte techniek vrij eenvoudig.[34] Enkele doorgaans door *Advanced Persistent Threats* (APT)[35] gebruikte technieken waren bijvoorbeeld niet benut. Deze wetenschap

22 Bij ransomware verstrekken hackers doorgaans tegen betaling de cryptografische sleutel waarmee het slachtoffer de versleutelde data zou kunnen terughalen. Bij wiperware is het doel data of computers vernietigen, niet om die data of computers na betaling weer te herstellen.

23 Jose Pagliery, 'The inside story of the biggest hack in history', *CNN Business*, 5 augustus 2015. Zie: https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

24 Council on Foreign Relations, Cyber Operations tracker, 'Compromise of Saudi Aramco and RasGas', 2012. Zie: https://www.cfr.org/cyber-operations/#Timeline.

25 Symantec Threat Hunter Team, 'Shamoon: Back from the dead and destructive as ever', 30 november 2016. Zie: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shamoon-back-destructive.

26 'Saudi Arabia warns on cyber defense as Shamoon resurfaces', *Reuters*, 23 januari 2017. Zie: https://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR.

27 In 2018 was weliswaar een Italiaans bedrijf in de oliesector het doelwit, maar grootste klant van dat bedrijf was Saudi Aramco. Zie 'Saipem says Shamoon variant crippled hundreds of computers', *Reuters,* 12 december 2018, https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA.

28 Kaspersky Lab Expert, 'Shamoon the Wiper – Copycats at Work, 16 augustus 2012. Zie: https://web.archive.org/web/20120820041239/http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work.

29 Flame had overigens de mogelijkheid om alle sporen van de eigen aanwezigheid te wissen na ontvangst van een *kill*-commando. Dergelijke ingebouwde zelfdestructie (*self-kill logic inside*) heeft overeenkomsten met de technieken die zijn benodigd voor destructie van data of andere computerbestanden.

30 Boldizsár Bencsáth et al, 'The Cousins of Stuxnet: Duqu, Flame, and Gauss', *Future Internet* 4 (2012) (4) 971-1003. Zie: https://doi.org/10.3390/fi4040971.

31 Kim Zetter, *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon* (Crown, 2015); James Long, 'Stuxnet : A Digital Staff Ride', Modern War Institute, 2019.

32 Kaspersky Lab, 'Equation Group Questions and Answers', februari 2015. Zie: https://web.archive.org/web/20150217023145/https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf.

33 Michael Pearson, K.J. Kwon, en Jethro Mullen, 'Hacking attack on South Korea traced to China, officials say', *CNN*, 20 maart 2013. Zie: https://edition.cnn.com/2013/03/20/world/asia/south-korea-computer-outage/index.html.

34 Jonathan A.P. Marpaung en HoonJae Lee, 'Cyber Attack: Could it be worse?', *CISAK 2012 – C1/O/8*. Zie: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/Dark_Seoul_Cyberattack.pdf.

35 Een *Advanced Persistent Threat* (APT) betreft een veelal statelijke tegenstander die beschikt over technologisch hoogwaardige kennis en voldoende middelen om langdurig en via meerdere aanvalspaden zijn doelen te bereiken.

duidt op het gevaar dat ook hackers met minder geavanceerde kennis en kunde dit soort destructieve malware kunnen ontwikkelen en inzetten.

Op 27 juni 2017, de avond voorafgaand aan de dag waarop in Oekraïne de onafhankelijkheid van de Sovjetunie wordt gevierd, voerden Russische hackers cyberaanvallen uit op Oekraïne, waarbij onder meer de financiële, media- en energiesector werden getroffen.[36] Kort daarop verspreidde deze malware zich over andere delen van de wereld, waaronder de VS, Europa en Rusland. De malware werd berucht onder de naam *NotPetya*.[37] Het kreeg deze benaming omdat de gebruikte code grotendeels leek op de in 2016 opgedoken *Petya*-gijzelsoftware (ransomware), maar deels ook niet. Waar de Petya-malware echter een crimineel doel nastreefde (bestanden versleutelen en deze na betaling van losgeld vrijgeven), leek de NotPetya-malware zuiver bedoeld om zowel data als computers onherstelbaar te beschadigen.[38] Het vernuftige aan deze aanval was vooral de wijze waarop de malware bij de slachtoffers werd binnengeloodst. De aanval vond plaats via een *supply-chain attack*. De aanvallers hackten een Oekraïense leverancier van populaire boekhoudsoftware en besmetten vervolgens hun legitieme software met malware. De slachtoffers haalden vervolgens met een reguliere software-update automatisch de malware binnen. De schade die NotPetya wereldwijd aanrichtte, werd geschat op een miljard dollar.[39]

In 2018 verstoorden hackers de openingsceremonie van de Olympische Winterspelen in het Zuid-Koreaanse Pyeongchang. De technologisch geavanceerde wiperware *Olympic Destroyer* vernietigde een beperkte hoeveelheid databestanden en enkele computers, alle direct gerelateerd aan de Winterspelen. De malware dupliceerde en verspreidde zichzelf, waardoor wordt aangenomen dat het daadwerkelijke doelwit zich dieper in het netwerk bevond.[40] Opvallend aan deze aanval was dat de malware zodanig was geprogrammeerd, dat die niet zijn eigen sporen wiste. Het leek erop dat de aanvaller juist wilde dat de malware werd ontdekt. De forensische sporen in de malware duidden op meerdere mogelijke daders, waaronder Noord-Korea, Rusland en China. In een diepgaand onderzoek stuitten onderzoekers op meerdere *false flags*,[41] waaronder bewust aangebrachte 'digitale vingerafdrukken', waarschijnlijk bedoeld om daarmee de attributie van deze cyberaanval te bemoeilijken. Achter deze cyberaanval bleken uiteindelijk hackers van de Russische militaire inlichtingendienst (GRU) schuil te gaan.[42]

Naast voornoemde cyberaanvallen die internationaal de aandacht trokken, vonden in 2017 en 2019 aanvallen plaats met twee nagenoeg identieke wipers vermomd als ransomware, respectievelijk *Ordinypt*[43] en *GermanWiper*,[44] die hun pijlen alleen richtten op Duitstalige doelwitten. En in 2019 en 2020 was het Midden-Oosten wederom het toneel van wiperware-aanvallen. De *Dustman* en *ZeroCleare* malware vertoonden gelijkenissen met het eerder gebruikte Shamoon. De doelwitten bevonden zich wederom in de energiesector, met name de olie- en gasindustrie. Onderzoekers van IBM

36 U.S. Department of Justice, United States District Court Western District of Pennsylvania, Indictment No. 20-316, 15 oktober 020, 16. Zie: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiZkob246DvAhUM1hoKHX4WDJAQFjABegQIARAD&url=https%3A%2F%2Fwww.justice.gov%2Fopa%2Fpress-release%2Ffile%2F1328521%2Fdownload&usg=AOvVaw0vAt3KDfKocmOCkUj0gujJ.

37 Andere benamingen zijn: Nyetya, ExPetr, PetrWrap, Win32/Diskcoder.C.

38 Anton Cherepanov, 'TeleBots are back: Supply-chain attacks against Ukraine', ESET, 30 juni 2017. Zie: https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/.

39 U.S. Department of Justice, 'Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace', 19 oktober 2020. Zie: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

40 Andy Greenberg, '"Olympic Destroyer" Malware Hit Pyeongchang Ahead of Opening Ceremony', *Wired*, 12 februari 2018. Zie: https://www.wired.com/story/olympic-destroyer-malware-pyeongchang-opening-ceremony/.

41 *False flags* zijn bewust aangebrachte of gefalsificeerde 'bewijzen' die zijn bedoeld om het onderzoek naar de identiteit van een daadwerkelijke dader van een activiteit te bemoeilijken.

42 De GRU staat voor *Glavnoye Razvedyvatelnoye Upravlenie* (Hoofdbureau voor Inlichtingen), zie ook: U.S. Department of Justice, 'Six Russian GRU Officers Charged'.

43 Catalin Cimpanu, 'Ordinypt Ransomware Intentionally Destroys Files, Currently Targeting Germany', *BleepingComputer*, 9 november 2017. Zie: https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/.

44 Catalin Cimpanu, 'GermanWiper ransomware hits Germany hard, destroys files, asks for ransom', *ZDnet*, 2 augustus 2 2019. Zie: https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/.

wezen Iraanse statelijke actoren aan als vermoedelijke daders.[45]

Explosie aan wipers in Oekraïne

De huidige Russisch-Oekraïense oorlog is vooral een kinetisch gevecht waarbij de fysieke verwoesting alle andere activiteiten overschaduwt. Daardoor lijkt cyberoorlogvoering in dit conflict geen rol van betekenis te spelen. Desondanks woedt er wel degelijk ook een gevecht in cyberspace. In de aanloop naar de invasie op 24 februari 2022, en in de weken direct daarna, voerden pro-Russische hackers cyberaanvallen uit ter ondersteuning van, en afgestemd op, Russische kinetische militaire operaties.[46] Vooral het gebruik van wiperware als cyberwapen viel daarbij op. Uit de hierboven beschreven ontstaansgeschiedenis blijkt dat het afgelopen decennium slechts een bescheiden aantal wipers is ingezet om verscheidene redenen en tegen uiteenlopende doelwitten. Sinds de Russische invasie is het gebruik van wiperware voor militaire doeleinden significant gestegen. Mandiant telde in de eerste maanden van 2022 meer destructieve malware dan de afgelopen acht jaar.[47] En waar eerst voornamelijk de kantoorautomatisering of informatietechnologie (IT) het doelwit was, worden de pijlen inmiddels ook gericht op (de computers van) de operationele technologie (OT); ofwel de industriële controlesystemen (ICS) die zorgen voor het monitoren en aansturen van industriële processen en systemen van bijvoorbeeld kritieke infrastructuur, zoals de olie en gasindustrie, watervoorziening, telecommunicatie of energiecentrales.

Halverwege januari 2022 (dus nog voor de invasie) maakte Microsoft bekend dat het een malware-aanval had ontdekt die was gericht tegen meerdere instanties in Oekraïne.[48] Deze wiperware (*Whispergate*) leek weliswaar op gijzelsoftware,[49] maar was dat klaarblijkelijk niet. De malware wiste de data op de aangevallen Windowscomputers en vernietigde vervolgens het opstartmechanisme van die aangevallen computers waardoor ze niet meer te gebruiken waren.

Op de dag voorafgaand aan de invasie vielen pro-Russische hackers het Viasat satelliet-internetcommunicatiesysteem aan. Dat het communicatiesysteem was gehackt, bleek overigens pas nadat de bewakings- en regelapparatuur van zo'n 5.800 windturbines in Duitsland(!) op onverklaarbare wijze was weggevallen.[50] De wiperware (*AcidRain*) bleek ontwikkeld om gegevens van modems en routers te wissen, waardoor die onbruikbaar werden. Als gevolg van die cyberaanval hadden grote delen van Oekraïne geen toegang meer tot internetcommunicatie. Het verlies aan *battlefield communications* in de regio van het destijds zwaar bedreigde Kyiv maakte de Oekraïense troepen aldaar nagenoeg blind voor Russische troepen en hun bewegingen.[51] De aanval op Viasat laat zien dat – mits gecoördineerd en afgestemd in tijd – cyberaanvallen operationele steun kunnen bieden aan andere militaire operaties door technologie van de tegenstander te ontregelen of te vernietigen.[52]

Op diezelfde dag voorafgaand aan de invasie maakten meerdere cybersecuritybedrijven melding van nieuw ontdekte *disk-wiping* mal-

45 IBM Security Intelligence, 'Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East', *IBM X-Force*, december 2019. Zie: https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/.

46 Paul A.L. Ducheine, B.M.J. Pijpers, en Kraesten L. Arnold, 'The "Next" War Should Have Been Fought in Cyberspace, Right?', in: Jeff Michaels en Tim Sweijs (red.), *Debating the Future of War (after the Invasion of Ukraine)* (Hurst Publishers, nog te verschijnen 2023); Jon Bateman, 'Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications', *Carnegie Endowment for International Peace*, december 2022.

47 Mandiant, M-Trends 2023, Mandiant Special Report, *Initial Destructive Cyber Operations and Military Invasion (February 2022–April 2022)* 57. Zie: https://mandiant.widen.net/s/dlzgn6w26n/m-trends-2023.

48 Microsoft Threat Intelligence Centre (MSTIC), 'Destructive malware targeting Ukrainian organizations', 15 januari 2022.

49 De malware toonde een bericht waarin om losgeld werd gevraagd, waardoor de aanval leek op een ransomware aanval van criminelen.

50 Juan Andrés Guerrero-Saade, 'AcidRain | A Modem Wiper Rains Down on Europe', *Sentinel Labs*, 31 maart 2022. Zie: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

51 Blessing, 'Revisiting the Russian Viasat Hack'.

52 Patrick Howell O'Neill, 'Russia hacked an American satellite company one hour before the Ukraine invasion', *MIT Technology Review*, 10 mei 2022. Zie: https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

ware. *HermeticWiper*[53] was gericht tegen honderden computersystemen in Oekraïne; voornamelijk in de financiële sector, de krijgsmacht, de luchtvaart en de IT-sector.[54] De wiper-aanval volgde op een wekenlange reeks DDoS-aanvallen op Oekraïense overheidswebsites.[55] De makers gebruikten voor hun cyberaanval eenvoudige, legitieme software om gegevens te wissen.[56]

Op 24 februari 2022, de dag van de invasie, ontdekte cybersecuritybedrijf ESET wederom nieuwe wiperware (*IsaacWiper)*.[57] Ditmaal waren vooral netwerken van de Oekraïense overheid het doelwit. Uit forensisch bewijs blijkt dat de aanval enige maanden tevoren was voorbereid en wellicht zelfs eerder was ingezet tegen andere doelwitten. De malware werkte schijnbaar niet geheel naar wens, want een dag na de initiële inzet lanceerden de aanvallers een nieuwe versie met daarin de mogelijkheid om fouten te kunnen opsporen.

In de eerste week na de invasie trachtten Russische troepen en pro-Russische hackers hun grip op de informatieomgeving in Oekraïne te

53 De malware misbruikte een 'digitaal echtheidscertificaat' van het Cypriotische bedrijf 'Hermetica Digital Ltd', vandaar dat de ontdekkers de malware deze naam gaven. Het bedrijf 'Hermetica' zelf zat niet achter die aanval.

54 Symantec Threat Hunter Team, 'Ukraine: Disk-wiping Attacks precede Russian Invasion', 24 februari 2022.

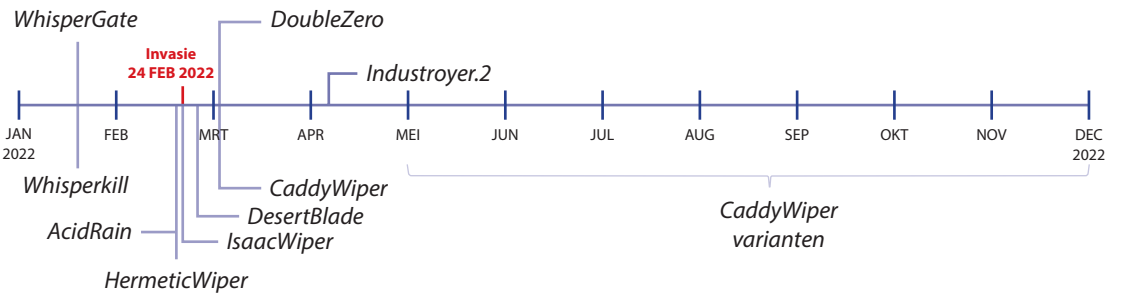
55 ESET, 'HermeticWiper: New data-wiping malware hits Ukraine', 24 februari 2022. Zie: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/.

56 Juan Andrés Guerrero-Saade, 'HermeticWiper / New destructive malware used in Cyber Attacks on Ukraine', *Sentinel Labs*, 23 februari. Zie: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/.

57 ESET Research, 'IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine', 1 maart 2022. Zie: https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.

USAID-bestuurder Samantha Power (rechts) en de Amerikaanse ambassadeur in Oekraïne Bridget Brink bezoeken een door Russische aanvallen beschadigde energiecentrale in Kyiv. Russische cyberaanvallen met wiperware ondersteunen kinetische militaire campagnes en richten zich ook op kritieke infrastructuur zoals energiecentrales

FOTO U.S. EMBASSY KYIV



Figuur 1 (Ontdekking van) negen soorten wiperware rondom de grootschalige Russische invasie van Oekraïne in 2022

verstevigen. Op 1 maart kondigde Rusland aan doelen uit te schakelen die 'desinformatie' zouden verspreiden.[58] Zijn krijgsmacht voerde vervolgens raketaanvallen uit op onder meer een televisietoren in Kyiv. Diezelfde dag vielen hackers een grote omroepmaatschappij aan met wiperware (*DesertBlade*). De aanvallen suggereerden een gesynchroniseerde actie, erop gericht om zowel kinetische als cybereffecten te creëren tegen de belangrijkste informatiebronnen van de Oekraïense bevolking. Pogingen om mediabedrijven van een afstand uit te schakelen met malware is een trend die in dit conflict voortdurend wordt waargenomen.[59]

In de derde week na de invasie trof cybersecuritybedrijf ESET een nieuwe wiperware aan in de computers en netwerken van Oekraïense organisaties.[60] Deze malware (*CaddyWiper*) blijkt technologisch relatief eenvoudig en vertoont geen overeenkomsten met eerder ontdekte wipers. Dit suggereert dat de malware is ontwikkeld door andere hackers. Rond diezelfde periode dook ook *DoubleZero* op. Deze wiperware hanteerde twee verschillende technieken om gegevens te wissen en was gericht tegen bedrijven in de communicatie- en mediasector.[61]

In april voerden hackers een cyberaanval uit op het Oekraïense elektriciteitsnetwerk. De zogeheten *Industroyer2*-malware was speciaal ontwikkeld tegen ICS en gebaseerd op eerder gebruikte malware die in 2016 (eveneens in Oekraïne) stroomuitval veroorzaakte. Ditmaal was de ICS-malware aangevuld met maar liefst vier verschillende destructieve wiperwarefamilies, gericht tegen verschillende computersystemen en netwerken.[62] Industroyer2 sloot de eerste golf aanvallen met destructieve wipers af.

In de zomermaanden van 2022 bestookten pro-Russische hackers voornamelijk de Oekraïense logistieke en transportsector.[63] Het was de tijd dat wapens en voorraden vanuit het westen werden aangevoerd naar het oostfront, terwijl vluchtelingen via diezelfde routes, maar in tegengestelde richting, een veilig heenkomen zochten. Rusland bestookte de Oekraïense transport-infrastructuur met zowel raketten als wiperware en ransomware. Tegelijkertijd werd de transportsector van NAVO-lid Polen (en knooppunt in de logistieke keten naar en vanuit Oekraïne) bestookt met *Prestige*-ransomware.

Ook in de maanden na de initiële reeks destructieve cyberaanvallen zijn wipers ingezet,

58 TASS Russian News Agency, 'Russian Defense Ministry warns about strikes being prepared on military sites in Kiev'. Zie: https://web.archive.org/web/20220301133913/https://tass.com/defense/1414199.

59 Microsoft Digital Security Unit, *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*, 12.

60 ESET, 'CaddyWiper: New wiper malware discovered in Ukraine', 15 maart 2022. Zie: https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/.

61 Andrii Bezverkhyi, 'DoubleZero Destructive Malware Used in Cyber-Attacks at Ukrainian Companies: CERT-UA Alert', 22 maart 2022. Zie: https://socprime.com/blog/doublezero-destructive-malware-used-in-cyber-attacks-at-ukrainian-companies-cert-ua-alert/.

62 Naast CaddyWiper (tegen ICS-netwerk) gebruikten de aanvallers ook de wipers *OrcShred, SoloShred* en *AwfulShred* (alle gericht tegen Linux en Solaris netwerken). Zie: ESET Research, 'Industroyer2: Industroyer reloaded', 12 april 2022.

63 Microsoft Threat Intelligence, 'A year of Russian hybrid warfare in Ukraine, What we have learned about nation state tactics so far and what may be on the horizon', 15 maart 2023, 8.

maar de aanvallen leken steeds meer gehaast, en minder gecoördineerd uitgevoerd. Bovendien leken spionageactiviteiten en destructieve aanvallen op dezelfde systemen elkaar te dwarsbomen. Verder kon de Oekraïense cyberverdediging die aanvallen veelal snel en effectief identificeren en mitigeren, nog voordat de cyberwapens hun schadelijk werk konden verrichten.

Analyse: strategische effecten?

In een jaar tijd zijn varianten van negen 'wiperware-families'[64] ingezet tegen vooral civiele objecten van de Oekraïense overheid, kritieke infrastructuur (informatietechnologie, communicatie, energie, transport, gezondheidszorg), het bedrijfsleven en de media. Een klein percentage was rechtstreeks gericht tegen de strijdkrachten.[65] Het is opvallend dat de inzet van deze wipers vooral samenviel met de aanloop naar de invasie en de paar weken daarna. Het is goed mogelijk dat de cyberoperaties bewust waren afgestemd op de geplande kinetische operaties.[66] Deze aanpak zou dan volledig in lijn zijn met het belang dat Rusland hecht aan een beslissende aanval (*decisive impact*) in de eerste weken van een oorlog.[67]

Na de eerste golf cyberaanvallen leken de aanvallers bestaande technieken te standaardiseren en te vereenvoudigen. De malware was bovendien minder gelaagd. De aanvallers verrichtten minder inspanning om hun kwaadaardige computercode te verhullen en namen ook niet meer de moeite om te suggereren dat er sprake was van criminele ransomware.

De aanvallers stapten ook af van de verschillende wipers en concentreerden zich vooral op de doorontwikkeling van de snel aanpasbare en multi-inzetbare CaddyWiper. Door de code van de malware steeds licht te wijzigen, was deze door cybersecurity-systemen moeilijker te detecteren. De aanvallen concentreerden zich in de loop van het conflict weliswaar op de Oekraïense overheid, maar leken desondanks niet echt doelgericht. Het hoge operationele tempo waarin de aanvallers nieuwe malware loslieten op hun slachtoffers, wellicht in een poging om het kinetische gevecht te kunnen ondersteunen, leidde tot fouten en daarmee verminderde effectiviteit van die malware.[68] De eenvoudige CaddyWiper was dan weliswaar minder geavanceerd dan de eerder gebruikte technologisch hoogwaardige NotPetya, maar ook met deze *quick-and-dirty*-wipers bleek Rusland nog steeds in staat digitale chaos te creëren.[69]

In de laatste maanden van 2022 veranderde het aanvalspatroon. De cyberaanvallen leken op de eerder uitgevoerde, gehaaste aanvallen, maar werden wel uitgevoerd tegen geselecteerde targets. In lijn met de kinetische aanvallen was de energiesector daarbij het uitgesproken doelwit. Naast meer selectieve aanvallen bleken de aanvallers ook te kiezen voor variatie in de aanvalswapens; naast wiperware ook ransomware. Rusland zette deze vorm van malware in, al dan niet via (pseudo-)hacktivisten om de inzet van deze eveneens schadelijke malware te kunnen ontkennen.[70]

Van de negen wiper-families waren er zes gericht op het vernietigen van (data op) computers met een Windows-besturingssysteem. Twee wipers zijn ingezet tegen Linux-computers en één tegen een computer met een Solaris-besturingssysteem. Onderzoekers die de malware ontleedden, ontdekten nauwelijks tot geen overeenkomsten in de gebruikte computercode.[71] De enige analogie tussen de wipers was hun destructieve intentie. Dat zou erop kunnen wijzen dat de aanvallen het werk waren van verschillende hackergroepen.

64 Een malware-familie bestaat uit verschillende softwareprogramma's die onderling veel gelijkenissen vertonen in hun computercode.
65 Microsoft Threat Intelligence Centre, 'A year of Russian hybrid Warfare in Ukraine', 5.
66 Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War', *Microsoft*, 2022, 3.
67 Michael Kofman et al, *Russian Military Strategy: Core Tenets and Operational Concepts*, CNA Research Memorandum, 19 oktober 2021, 3. Zie: https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts.
68 Mandiant, 'M-Trends 2023', 60.
69 Andy Greenberg, 'Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless', *Wired*, 18 november 2022. Zie: https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.
70 Microsoft Threat Intelligence Centre, 'A year of Russian hybrid Warfare in Ukraine', 12.

Opvallend is dat van alle gebruikte wipers er slechts één (HermeticWiper) werd ingezet in combinatie met een 'worm'-component.[72] Door die worm-functie kon deze malware zichzelf reproduceren en verspreiden over het aangevallen netwerk en dus zonder verdere (menselijke) aansturing zijn vernietigende werk doen. Wel was HermeticWiper zo geprogrammeerd dat de 'gewenste' schade bewust beperkt bleef tot lokale IP-adressen binnen het specifiek aangevallen netwerk. De overige wipers hadden alle geen worm-component en konden zich daardoor sowieso niet ongecontroleerd verspreiden. Een onvoorziene uitbraak, en daarmee onvoorziene schade buiten het bewust aangevallen netwerk, zoals eerder wel het geval was met de NotPetya-cyberaanval, is hierdoor niet mogelijk. Dit kan erop duiden dat de aanvallers niet het risico wilden lopen om abusievelijk andere landen (waaronder NAVO-lidstaten) te treffen.

Eveneens opmerkelijk zijn het gewijzigde aanvalspad en aanvalstechnieken van APT28.[73] Deze Russische statelijke actor richtte zijn aanvallen niet langer direct op de computers van zijn slachtoffers, maar op de infrastructuur aan de randen van een netwerk. In plaats van te phishen naar authentieke inloggegevens van gebruikers, exploiteerde de groep voornamelijk kwetsbaarheden in bijvoorbeeld firewalls, routers en email-servers. Zo kreeg de groep indirect toegang tot de gewenste computersystemen, om vervolgens alsnog de gegevens daarvan te wissen en de computers zelf te beschadigen. De rand-netwerkinfrastructuur zelf lieten de aanvallers onaangetast. Hierdoor creëerden zij een permanente aanwezigheid in de netwerken van hun slachtoffers. Deze indirecte manier van aanvallen stelde de hackers in staat om dezelfde computernetwerken snel en meermaals achter elkaar aan te vallen; of na een wiperware-aanval toegang tot dat netwerk te behouden voor bijvoorbeeld spionagedoeleinden zodra het aangevallen netwerk was hersteld.[74] De Russische militaire inlichtingendienst hoeft daardoor niet langer te kiezen tussen bespioneren of vernietigen van een systeem; op deze wijze zijn beide mogelijk.

In de oorlog in Oekraïne is wiperware vooral ingezet vlak voor de Russische invasie en de eerste fase van de oorlog. De wipers brachten schade toe aan Oekraïense computersystemen en -netwerken, maar leken vooral bedoeld om de militair-operationele campagnes te ondersteunen. Mits goed gepland, zorgvuldig in tijd gesynchroniseerd, en gecoördineerd met andere militaire machtsmiddelen, kan een wiper-aanval zelfs strategische effecten teweegbrengen. De aanval op het Viasat satelliet-internetcommunicatiesysteem kwam hiervoor in aanmerking, als deze succesvol was geweest en de effecten niet tijdig door de inzet van Starlink waren geneutraliseerd.

Lessons to learn voor de Nederlandse krijgsmacht

De vraag is nu of uit het gebruik van wipers in het recente Russisch-Oekraïense conflict conclusies zijn te trekken voor de ontwikkeling van dergelijke cyberwapens voor de Nederlandse krijgsmacht. Daarbij merken we allereerst op dat het heimelijke karakter van cyberoperaties de afhankelijkheid van informatie uit open bronnen buitengewoon groot maakt. Deze afhankelijkheid begrenst niet alleen de volledigheid van bronnenmateriaal, maar kan ook de juistheid van een analyse ondergraven. Daar komt bij dat analyses van een lopend conflict ernstig worden bemoeilijkt door de inherente misleiding waarmee oorlogvoering nu eenmaal gepaard gaat. Ondanks de ongetwijfeld bewuste manipulatie van de beschikbare informatie van zowel Russische als Oekraïense zijde, is het toch mogelijk om bepaalde lessen – positieve en negatieve – te trekken uit de Russische inzet van destructieve softwareprogramma's.

71 Recorded Future, 'Overview of the 9 Distinct Data Wipers Used in the Ukraine War', Insikt Group, 12 mei 2022.

72 Een computerworm is een schadelijk softwareprogramma dat zich zelfstandig, dus zonder enige menselijke interactie, kan vermenigvuldigen en snel en ongecontroleerd verder kan verspreiden in een computernetwerk.

73 APT28 is een beruchte, aan de Russische militaire inlichtingendienst GRU gerelateerde statelijke actor/hackergroep.

74 Mandiant, M-Trends 2023, 57.

Past wiperware in de gereedschapskist van de Nederlandse krijgsmacht? FOTO MCD, ZADRACH SALAMPESSY

Het eerste en belangrijkste verschil tussen de ingezette Russische destructieve programmatuur en een eventuele toepassing van dergelijke cybermiddelen door de Nederlandse krijgsmacht in tijd van een gewapend conflict betreft *targeting*. Waar Rusland de wipers inzette tegen een schijnbaar willekeurige mix van militaire doelwitten, civiele objecten en *dual use*-systemen, is de eigen krijgsmacht uiteraard gebonden aan een verantwoord gebruik van dergelijke middelen. Zonder mogelijkheid om toegebrachte schade te kunnen terugdraaien, zouden wipers die onherstelbare schade aanrichten enkel kunnen worden ingezet tegen militaire doelwitten, zoals wapen-, radar- en (personele en materiële) logistieke systemen of *command and control*-systemen. Deze militaire systemen werken doorgaans met andere (soms *custom made*) besturingssystemen dan commerciële computers, wat de kans op onbedoelde nevenschade aanzienlijk verkleint. Desondanks zijn aanvullende maatregelen noodzakelijk om te garanderen dat de destructieve uitwerking beperkt blijft tot de specifiek aangevallen middelen en dat de middelen geen onbedoelde en ongewenste schade aanrichten in andere omgevingen.

Voor andere doelwitten kan een variant van ransomware in aanmerking komen; zonder de gebruikelijke afpersingsfunctionaliteit, maar met behoud van de mogelijkheid om schade ongedaan te maken. Door computerbestanden van het doelwit cryptografisch te versleutelen, kan worden voldaan aan de eisen van subsidiariteit en proportionaliteit van optreden. Ongewenst of onvoorzien aangerichte schade kan dan, met een cryptografische sleutel,[75] ongedaan worden gemaakt. De mogelijkheid om die 'sleutel' te verschaffen aan getroffen partijen kan zowel nevenschade inperken, als in voorkomend geval na afloop van een conflict een tegenstander in staat stellen schade te herstellen.

75 Een cryptografische sleutel is een speciale set gegevens die onder meer wordt gebruikt voor het coderen en decoderen van computerbestanden of berichten. Is de cryptografische sleutel niet (meer) beschikbaar, dan is het in beginsel onmogelijk om de versleutelde (onleesbare) gegevens weer te ontcijferen.

Een volgende les betreft dan ook de beperkte duur van een eventueel ontzeggingseffect van destructieve programmatuur. Als databestanden zijn gewist, dan is dat vervelend, maar wel relatief makkelijk te herstellen. Als een aangevallen partij over goede back-ups beschikt (niet op hetzelfde computersysteem, maar bijvoorbeeld offline, of in de cloud), dan kan die de schade relatief snel herstellen. Bij eerder militair cyberoptreden van het U.S. Cyber Command tegen ISIS was al gebleken dat zelfs een tegenstander met beperkte technische mogelijkheden relatief snel infrastructuur kon herstellen.[76] Het kennelijke verloop van de wiperinzet door Rusland in Oekraïne lijkt deze eerdere les te bevestigen. Hierbij moet wel worden opgemerkt dat Oekraïne daarbij wordt ondersteund door een breed scala aan westerse overheden (VS, VK, EU) en commerciële IT- en cybersecuritybedrijven (waaronder Microsoft, ESET, Google en Mandiant).[77]

Het herstellen van vernietigde besturingssystemen is weliswaar ook mogelijk,[78] maar vergt een grotere inspanning dan het eenvoudig terugzetten van gewiste databestanden. Vanwege die herstelmogelijkheid is in doctrinaire termen het effect van destructieve programmatuur in beide gevallen eerder te bestempelen als verstoring (*disruption*) dan als vernietiging (*destruction*). Voor langdurig ontzeggen van systemen vallen de Russen dan ook terug op kinetische middelen. Het herstel van kinetisch aangerichte fysieke schade aan digitale infrastructuur en overige middelen vergt een grotere inspanning of duur dan herstel van beschadigde virtuele objecten.

De beperkingen aan de duur van ontzegging van middelen hebben een direct verband met de derde les: de noodzaak om een cyberoperatie af te stemmen op andere vormen van militaire inzet, zodat de effecten van beide soorten operaties elkaar kunnen versterken. In het conflict in Oekraïne lijkt een dergelijke afstemming in veel gevallen gebrekkig, al zijn daar wel degelijk uitzonderingen op. Ten dele ligt dat aan de verschillen in de planningscyclus. In tegenstelling tot kinetische wapens worden cyberwapens niet geproduceerd in een fabriek volgens standaardspecificaties met een standaardeffect; noch liggen die cyberwapens ruim van tevoren klaar voor gebruik. Het ontwerpen, ontwikkelen, maken en inzetten van cyberwapens is een proces dat vaak een aanzienlijke voorbereidingstijd nodig heeft. De planning van een cyberoperatie vraagt dan ook meer tijd dan de dagen of uren van de planning van andere vormen van militair optreden. Toch lijkt het erop dat de Russen hiermee in hun voorbereiding op de invasie wel degelijk rekening hebben gehouden. De (wiper)effectoperaties zijn uitgevoerd op systemen waarop de aanvallers in een eerder stadium al toegang en volledige controle hadden verworven. Een effectoperatie is op die manier sneller uit te voeren dan wanneer de hackers de gehele aanvalsketen (*cyber kill chain*) hadden moeten doorlopen vanaf het moment van de invasie.

In een eerder stadium toegang verkrijgen tot een computer of netwerk en pas nadien (op het gewenste moment) effectbrengers inzetten,[79] stelt de aanvallers in staat om de middelen voor een destructief effect eenvoudig te houden; de cyberwapens hoeven slechts in één enkele functionaliteit te voorzien: destructie. Hebben de aanvallers eenmaal toegang tot een systeem, dan kunnen zij ook gebruik maken van 'living off the land'-technieken; ofwel gebruik (misbruik) maken van organieke, legitieme functionaliteiten van het aangevallen doelwitsysteem. Gebruik van organieke en legitieme functionaliteiten vermindert niet alleen het risico op vroegtijdige ontdekking van de cyberaanval door het doelwit, maar voorkomt ook eventuele ontwerp- of programmeerfouten bij het ontwikkelen van *tailormade* malware. Dezelfde technieken kunnen bovendien herhaald worden ingezet zonder aanpassing of desgewenst met minimale wijzigingen.

76 David E. Sanger en Eric Schmitt, 'U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS', *The New York Times*, 12 juni 2017.

77 Bateman, 'Russia's Wartime Cyber Operations in Ukraine', 14.

78 Bijvoorbeeld door een gewiste ingebouwde harde schijf (met ingebouwd besturingssysteem) compleet te vervangen door een nieuwe, of door een nieuwe externe harde schijf op het systeem aan te sluiten.

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

Omdat een hacker van tevoren nooit zekerheid heeft over het aan te vallen doelwit,[80] zijn vooraf gecreëerde halffabricaten doorgaans niet praktisch bruikbaar om ongeautoriseerd toegang te verkrijgen tot een computer of netwerk (*access operations*). Voor destructieve programmatuur die wordt gebruikt nadat de noodzakelijke toegang is verkregen, kunnen deze voorbereide producten wel degelijk nuttig zijn. Deze opzet is dan ook als een navolgenswaardige *best practice* over te nemen voor het Nederlandse optreden.

De volgende les gaat over de ontwikkeling van destructieve programmatuur. Zoals hierboven genoemd, is het aanmaken van halffabricaten nuttig. De ontwikkeling daarvan vindt bij voorkeur modulair plaats en in gescheiden ontwikkelstraten;[81] dit ondervangt een eventueel *single point of failure*. De naleving van (software)ontwikkelstandaarden borgt de kwaliteit van de op te leveren producten. Het inzetten van ondoordachte of gebrekkig ontwikkelde code kan leiden tot onvoorziene en wellicht zelfs ongewenste uitkomsten. Omdat een slachtoffer het gebruik van destructieve malware waarschijnlijk snel onderkent, is het raadzaam dergelijke middelen bij voorkeur niet als multifunctioneel 'Zwitsers zakmes' te ontwikkelen, maar als specifiek toegespitste code ten behoeve van slechts één enkele functionaliteit. Dat voorkomt dat overige functionaliteiten onnodig vroegtijdig worden onderkend door eventuele opponenten.

Conclusie

In het huidige Russisch-Oekraïens conflict is het gebruik van (destructieve) wiperware om data en computers te vernietigen significant: in de eerste maanden van 2022 is meer wiperware ingezet tegen Oekraïne, dan tegen landen wereldwijd in de afgelopen acht jaar. De inzet van deze wipers viel samen met de aanloop naar de invasie en de paar weken daarna. Het is goed mogelijk dat de cyberoperaties bewust waren afgestemd op de geplande kinetische operaties.

In een gewapend conflict kunnen wipers (ondersteunend) worden ingezet tegen militaire doelwitten, zoals wapen-, radar- en (personele en materiële) logistieke systemen of command and control-systemen. Deze systemen werken doorgaans met andere besturingssystemen dan commerciële computers, wat de kans op nevenschade verkleint. Aanvullende maatregelen voorkomen onbedoelde en ongewenste schade in andere omgevingen.

De inzet van destructieve programmatuur heeft een beperkt ontzeggingseffect in tijdsduur; de schade is relatief snel te herstellen. Doctrinair gezien is er daarom eerder sprake van verstoring (disruption) dan van vernietiging (destruction). De gelimiteerde tijdspanne waarin het effect wordt gecreëerd, noopt tot afstemming van dit soort cyberoperaties op andere vormen van militaire inzet, zodat de effecten van de operaties elkaar optimaal kunnen versterken.

De inzet van cybermiddelen kent een significant langere planningscyclus dan de planning van andere militaire middelen. Vroegtijdige toegang tot een computer of netwerk stelt de aanvaller in staat de middelen voor een destructief effect eenvoudig te houden; de malware hoeft slechts één functionaliteit te bezitten (wipen) en kan van tevoren worden ontwikkeld als halffabricaat.

Vanwege de benodigde planningscyclus en door de herstelmogelijkheid van schade zou de Nederlandse krijgsmacht wiperware bij uitstek strategisch kunnen inzetten, vooral bij een initiële (verrassings)aanval in combinatie met andere militaire middelen. Voor operationeel of zelfs tactisch gebruik in een dynamisch gevecht zijn deze middelen minder of in het geheel niet geschikt. ■

80 Onder meer besturingssystemen, netwerkconfiguratie, hardware, software, firmware, firewalls, indringer preventie en -detectiesystemen, plus alle versies, updates en patches, verschillen doorgaans per doelwit.

81 Kleine teams van ontwikkelaars en programmeurs werken daarbij in verschillende fasen (ontwikkelen, testen, acceptatie, productie) gecompartimenteerd aan bepaalde functionaliteit van de malware.