Michael Ahlmann, Sylvia Johnigk, Hans-Jörg Kreowski und Kai Nothdurft

Cyberpeace und IT-Sicherheit

Editorial zum Schwerpunkt

Seit dem offiziellen Start unserer Cyberpeace-Kampagne sind inzwischen fast fünf Jahre vergangen. Motiviert durch die zunehmenden Gefahren, die sich aus der Nutzung von Computern als D-Waffen in einer zunehmend digitalisierten und vernetzten Welt ergeben, hat das FIfF besorgniserregende Entwicklungen vorausgesehen und aufklärend vor den Risiken eines Cyberkriegs gewarnt. Die Kampagne hatte und hat den ambitionierten Anspruch, diese Entwicklung einzudämmen und aufzuhalten. Auch sollten alternative Nutzungsszenarien insbesondere des Internets vorangetrieben werden. Diese mittelfristigen Ziele konnten nur sehr eingeschränkt verwirklicht werden, wie aktuelle Entwicklungen zeigen. Dss ist jedoch kein Grund zu verzagen oder gar aufzugeben, sondern sollte uns vielmehr als Ansporn dienen, unsere Bemühungen zu verstärken.

D-Waffen werden bereits unter Missachtung des Völkerrechts auch gegen zivile Infrastrukturen eingesetzt. So tauchte im Dezember 2017 mit *Triton* eine Malware auf, die nicht nur das Steuerungssystem von Industrieanlagen sabotiert, wie es bereits seit 2010 mit dem *Stuxnet*-Wurm geschieht, sondern die sogar gezielt deren Safety-Funktion zu sabotieren versuchte.[1] Die Safety-Funktion ist eine Notabschaltung, die bei einer Disfunktion ein geordnetes Herunterfahren der betroffenen Anlage gewährleisten soll. Durch einen Programmierfehler arbeitete die Schadsoftware nicht wie vom Angreifer gewünscht. Stattdessen löste sie genau diesen Shutdown aus. IT-Sicherheitsexperten, die die Malware analysierten, vermuten, dass eigentlich die Deaktivierung dieser Safety-Funktion intendiert war, da diese Funktion gezielt angegriffen wurde.[2] Damit wurde das erste Mal nachweislich eine Malware eingesetzt, die das explizite Ziel hatte, lebensbedrohende Manipulationen in Steuerungsanlagen herbeizuführen. Die Schadfunktion der Malware besitzt dieses Potenzial leider auch weiterhin, denn von dem Schadprogramm geht immer noch Gefahr aus. Gefunden wurde Triton erstmals in der Steuerungsanlage einer Gasraffinerie, wo Triton eine Explosion hätte auslösen können, wenn es wie vorgesehen funktioniert hätte. Die Malware-Funktionen wurden auch noch bei weiteren Angriffen nachgewiesen, und die angegriffene Safety-Funktion kommt noch in vielen anderen Anlagen zum Einsatz. Auch werden Steuerungssysteme, wenn überhaupt, wesentlich seltener und später gepatcht als etwa gängige Server-Betriebssysteme. Daher muss davon ausgegangen werden, dass weiterhin viele Steuerungsanlagen anfällig für Triton-basierte Angriffe sind.

Gerade die von uns durchgeführten Analysen der zu erwartenden Bedrohungen durch Cyberkrieg haben sich leider erneut als realistisch und keineswegs als Schwarzmalerei erwiesen. Umso mehr muss es auch in den nächsten Jahren eine Kernaufgabe des FIfF bleiben, Transparenz zu schaffen. Ebenso wichtig ist es, wahlentscheidend große Personengruppen zu diesem Thema aufzuklären und sich nicht auf die kritische Analyse im akademisch/fachlichen Diskurs zu beschränken. Das Internet gibt uns dazu die Werkzeuge an die Hand. Wer, wenn nicht wir, kann und sollte diese auch nutzen? Das im Rahmen der Kampagne entstandene Video *Cyberpeace statt Cyberwar* mit inzwischen über 14.900 Aufrufen auf YouTube und über 1.100 auf Vimeo war ein wichtiger Schritt in diese Richtung und darf nicht der letzte bleiben.

Unser aktueller Schwerpunkt umfasst verschiedene Themen aus dem Bereich *Informatik und Rüstung*, die vom Drohnenkrieg über autonome Waffen und Rüstungskontrollfragen bis zum Widerspruch zwischen dem IT-Sicherheitsgesetz und der Entwicklung offensiver Cyberwaffen reichen:

- *Ralf Cüppers*, *Siglinde Cüppers* und *Stephan Schlereth* erläutern zunächst die militärisch-strategische Geschichte und Funktion des Drohnen- und Tornado-Luftwaffenstandorts *Jagel* in Schleswig-Holstein und beschreiben anschließend den friedenspolitischen Widerstand dagegen.

- *Henning Lübbecke* stellt die Frage, ob autonome Kampfroboter einen „Silberstreif am Horizont" für kriegsführende Demokratien bedeuten können, da sie die Chance zu bieten scheinen, eigene Verluste zu begrenzen und ethische Regeln zu befolgen. Er zieht für seine Bewertung mehrere aktuelle Abhandlungen zu autonomen Systemen und Roboterethik heran.

Die weiteren Artikel behandeln Cyberpeace-Themen im engeren Sinne:

- *Thomas Reinhold* führt zunächst kurz ein in verschiedene Ansätze von Rüstungskontrolle im allgemeinen in seinem

Beitrag *Rüstungskontrolle für den Cyberspace – Herausforderungen und erste Ansätze. Dann widmet er sich* den spezifischen Anforderungen, vor denen die Rüstungskontrolle bei digitalen Waffen steht. Diese reichen von Kontroversen bei Definitionen, was Gegenstand und Umfang der Kontrolle sein soll, bis zu der Frage, welche Institution für die Kontrollaufgabe legitimiert sei. Er gibt eine Übersicht über verschiedene Ansätze von internationalen Institutionen und nationalen Initiativen und bewertet diese.

- *Ingo Ruhmann* und *Ute Bernhardt* untersuchen in ihrem Beitrag zum IT-Sicherheitsgesetz, inwieweit sich staatliche Institutionen strafbar machen, wenn sie offensiv „Cyber"-Angriffe durchführen und in Konflikt mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität Informationstechnischer Systemen geraten.

Anmerkungen

1 *https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/*

2 *https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html*

Ralf Cüppers, Siglinde Cüppers, Stephan Schlereth

Jagels Beitrag zur vernetzten Operationsführung von Bundeswehr und NATO und unser friedenspolitischer Widerstand

In Jagel befindet sich der größte Militärflughafen der NATO in Europa. Unser Artikel beleuchtet den Drohnen- und Tornadostandort der Luftwaffe bei Schleswig und seine militärisch-technische Ausrüstung, die vernetzte Operationsführung von Bundeswehr und NATO und den Anteil Jagels dran. Wir beschreiben die seit Juni 2015 in Jagel monatlich stattfindenden Mahnwachen und weiteren Aktionen, die von der Deutschen Friedensgesellschaft – Vereinigte KriegsdienstgegnerInnen (DFG-VK) – organisiert und mit verschiedenen Organisationen gegen diesen Standort gestaltet werden. Weitere Informationen liefert die Website www.bundeswehrabschaffen.de*, auf der auch weitere Aktionen zu diesem Thema angekündigt werden und dokumentiert sind.*

NATO und Bundeswehr in Jagel

Schon in den Kriegen während des Zerfalls von Jugoslawien von 1991 bis 2001 waren verschiedene Tornado-Varianten – Mehrzweckkampfflugzeuge, die jetzt [illegible] elektronischen Kampfführung u[illegible] sind darauf spezialisiert, gegner[illegible] orten und mit Raketen „auszusch[illegible] bat Reconnaissance). Tornados [illegible] (Recce = Kurzform von Reconnaissance) aus Jagel flogen hinterher und scannten das Land ein – Brücken, Transformatorstationen oder auch die chinesische Botschaft. HARM-Raketen (Homing Anti Radiation Missile), die von den Tornados transportiert werden, verfügen über eine Fähigkeit, die „fire and forget" genannt wird. Sie suchen selbständig ihr Ziel und zerstören es.

Die Heron-1-Drohnen, die Piloten aus Jagel in Masar-e Sharif in Afghanistan steuern, sind dort seit 2010 im Spionageeinsatz – die gesammelten Daten tragen zum Lagebild der NATO bei. Das Töten übernehmen NATO-Bomber – mal Militärstellungen der Aufständischen, mal Hochzeitsgesellschaften. Aufklärung ist auch hier Beihilfe zum Mord. Krieg beginnt also in Schleswig-Holstein.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Jagels militärische Aufträge

- Erhalt der militärischen Einsatzbereitschaft mit bemannten und unbemannten Flugobjekten (Tornados und Drohnen),
- Durchführung von Aufklärungsaufträgen,
- Beteiligung an militärischen Einsätzen zur Landes- und Bündnisverteidigung, der NATO, und unter dem Mandat der Vereinten Nationen,
- [illegible] der weiträumigen Signal- und [illegible] SIGINT),
- [illegible] sserzielen mit *Fire and Forget*- [illegible] und IRIS T (seit 2009),
- Unterstützung der Elektronischen Kampfführung (EloKa) aus der Luft durch signalerfassende Aufklärung feindlicher Radarstationen und Funkstationen, Ortung und Zerstörung feindlicher Radaranlagen und Funkstationen mit HARM (seit 2013); damit wurde der militärische Auftrag des aufgelösten Jagdbombergeschwaders 32 Lechfeld vom Jagdbombergeschwader 51 Jagel vollständig übernommen,
- Übernahme des Ausbildungszentrums für die abbildende und signalerfassende Aufklärung der Luftwaffe (seit 2016); damit wurde auch dieser militärische Auftrag vom Jagdbombergeschwader 51 Jagel vollständig übernommen; seitdem werden alle Soldaten aller Teilstreitkräfte der Bundeswehr, die mit abbildender oder Signalaufklärung befasst sind, in Jagel ausgebildet,
- Auswertung der Einsatzbilder aus den Aufklärungsflügen direkt am Standort Jagel (seit 2016),
- Ausbildungs- und Übungsflüge aller Drohnenpiloten der Heron I, vor allem am Flugsimulator (seit April 2017),