Christian Colen/Flickr

Deutschland bereitet sich auf den Krieg der Zukunft vor

Berlin hat eine neue Teilstreitkraft geschaffen, um die Führung im Hightech-Hybridkrieg zu übernehmen.

- Josue Michels
- 09.06.2017

Hunderttausende von Zielen überall auf der Welt wurden im Mai mit gefährlichen Waffen angegriffen. Diese Waffen waren weder kinetisch, noch biologisch, chemisch oder nuklear – sie waren elektronischer Natur. Die Angriffsziele waren Computer in 150 Ländern, darunter schätzungsweise 70.000 Geräte des staatlichen Gesundheitsdienstes Großbritanniens wie zum Beispiel Computer, Scanner und Speichergeräte. Der Angriff traf auch FedEx, die Deutsche Bahn, Telefónica, Taiwan Power Co., Investmentfirmen, Versicherungen und zahlreiche andere Firmen, Organisationen und Personen.

Die Waffen waren verschiedene Varianten eines Cyberangriffs, der WannaCry genannt wird. Die Schadprogramme greifen auf Computerdateien zu, verschlüsselt sie und benutzt sie für Erpressungen, bei denen 300 bis 600 $ pro Computer verlangt werden, um die Dateien in ihren unverschlüsselten Zustand zurückzuversetzen. Europol sprach von einem beispiellosen Angriff.

WannaCry erinnert uns daran, dass die Welt in ein neues Zeitalter eingetreten ist, das es früher nur in Science-Fiction-Filmen gab. Aber jetzt gibt es den Cyberkrieg nicht nur in Fantasiefilmen, sondern auch in der realen Welt und er bedroht ganze Nationen. Ein neues Wettrüsten hat begonnen; nicht mit Kriegsschiffen, Flugzeugen, Panzern oder sogar Atomwaffen, sondern mit Cyberwaffen.

Und Deutschland hat sich im großen Stil an die Spitze dieses Wettrüstens gesetzt.

Am 1. April startete das deutsche Militär sein größtes Unternehmen, um Cyber-Bedrohungen zu bekämpfen und richtete eine sechste Teilstreitkraft ein: Das Kommando Cyber- und Informationsraum (KdoCIR). Das Kommando wird auf dem gleichen Niveau wie die Armee, die Luftwaffe und die Marine operieren.

Die Verteidigungsministerin Ursula von der Leyen ernannte Generalleutnant Ludwig Leinhos zum ersten deutschen Cybergeneral. Leinhos wird nächstens der Chef einer Gruppe von 13.500 Computerspezialisten sein, von denen viele bereits an verschiedenen Standorten bei der Bundeswehr angestellt sind. Das ist eine enorme Streitmacht. Das damit beschäftigte Personal ist annähernd so zahlreich wie das der deutschen Marine.

Deutschland braucht so eine riesige Cybermilitäreinheit und bildet sie nicht nur zur Verteidigung gegen Angriffe wie WannaCry aus, sondern auch, um seine eigenen Cyberangriffe zu starten.

‚Mehr als nur ein Meilenstein'

Der 5. April war der erste Arbeitstag für das neue Team und ein großer Tag in der deutschen Militärgeschichte. Frau von der Leyen sagte, es „ist für die Bundeswehr mehr als ein Meilenstein. Damit stellen wir uns international im Spitzenfeld auf", sagte sie.

Die Wochenzeitung der deutschen Streitkräfte *Bundeswehr Aktuell,* rühmte das neue Kommando im April und meinte, „die Bundeswehr nimmt … in der NATO eine Vorreiterrolle ein."

Deutschlands Verteidigungsministerium sagt, dass die Cybersicherheit entscheidend ist. Es schätzt, dass bis zu 80 Prozent

der wichtigen neuen Entwicklungen für das Militär zum Cyberbereich gehören und dass die meisten Konflikte heutzutage – teilweise oder ganz – im Cyberraum ausgefochten werden.

Nur in den ersten neun Wochen dieses Jahres richteten sich 284.000 Angriffe gegen Bundeswehrcomputer.

Deutschland wird auch ein Cyberforschungszentrum an der Universität der Bundeswehr in München einrichten. Diese Cyber-Innovationsschmiede hat zum Ziel, die Ressourcen der Bundeswehr mit dem Einfallsreichtum des Privatsektors – der Startup-Unternehmer – zu kombinieren. 2016 nahm die Bundeswehr 60 Prozent mehr Computerexperten unter Vertrag als 2015, was größtenteils auf erfolgreiche Werbekampagnen und großzügige Bezahlung zurückzuführen ist. Wenn sich dieser Trend fortsetzt, werden die Schwierigkeiten, qualifiziertes Personal für die Bundeswehr zu bekommen, der Vergangenheit angehören.

Die beste Verteidigung ist ein guter Angriff

Wie bei jeder anderen Art von Kriegsführung ist Angriff die beste Verteidigung. Die einzige Möglichkeit, der Bedrohung eines Cyberangriffs zu entgehen, ist, die Quelle des Angriffs zu eliminieren.

„Wenn die Netze der Bundeswehr angegriffen werden, dann dürfen wir uns auch wehren“, sagte Frau von der Leyen bei der Einweihung der neuen Einrichtung. „Sobald ein Angriff die Funktions- und Einsatzfähigkeit der Streitkräfte gefährdet, dürfen wir uns auch offensiv verteidigen.“

Die Staatssekretärin im Bundesministerium für Verteidigung Katrin Suder sagte, ein Teil der Aufgaben des Cyber-und Informationsraumkommandos beim Auslandseinsatz bestünde in der Überwachung, Störung und Isolierung der Kommunikationen des Gegners.

Das neue Team wird die technologischen Mittel und die Ausbildung haben, offensive Maßnahmen zu ergreifen, aber die gesetzlichen Grundlagen müssen noch geklärt werden. In einem Interview mit der *Welt* veröffentlicht am 16. April sagte Frau von der Leyen, dass es der Bundeswehr nach dem Grundgesetz nur gestattet sei, zurückzuschlagen, wenn die Streitkräfte selbst angegriffen würden. Sie sagte, dasselbe gelte auch für den Cyberspace. Aber die Situation ist eine andere, wenn der deutsche Staat angegriffen wird. Wenn zum Beispiel der Bundestag angegriffen wird, dann will Frau von der Leyen, dass die Streitkräfte in der Lage sind zurückzuschlagen. Da die Abwehr von Cyberattacken erst lange Zeit nach der Formulierung des Grundgesetzes entwickelt wurde, werden deutsche Gerichte erst einmal klären müssen, inwieweit das Team seine Offensivkapazitäten einsetzen darf.

Eine Ära nach der Abschreckung

Ohne Rücksicht auf die Rechtmäßigkeit baut Deutschland seine Kapazitäten für Cyberattacken in einer Ära aus, in der wir gerade erst beginnen, die potentielle Macht solcher Angriffe zu verstehen. Führende Politiker vergleichen die potentielle Macht der Cyberwaffen mit der von Atomwaffen. Schon 2013 nannte US-Senator John Kerry die neuen Cybertechnologien „vergleichbar mit Atomwaffen des einundzwanzigsten Jahrhunderts“.

Ein Land braucht die Atomwaffen seines Gegners nicht mehr zu fürchten, wenn es in der Lage ist, mit Cyberkriegsführung die Fähigkeit des Gegners auszuschalten, diese Waffen abzufeuern. Das Land mit einer überlegenen Cybertechnologie könnte die Infrastruktur seines Gegners erstarren lassen und ihn so daran hindern, überhaupt in den Krieg zu ziehen.

Es ist nur wenige Jahrzehnte her, da war Deutschland noch die größte Bedrohung des Weltfriedens. Heute ist es dabei, eine mächtige Technologie zu entwickeln, die eine noch größere Bedrohung darstellen könnte, aber die Welt macht sich deshalb keine Sorgen.

Die amerikanische Wirtschaft und das Militär hängen stark von genau der Art von Informationssystemen ab, die auch für Cyberattacken eingesetzt werden kann. Man könnte denken, die Vereinigten Staaten müssten doch ihr Bestes tun, bei diesem Rennen den anderen immer eine Nasenlänge voraus zu sein, damit niemand die Schwächen der USA auf diesem Gebiet ausnutzen kann. Aber in Wirklichkeit drängen die Vereinigten Staaten das deutsche Militär tatsächlich dazu, aufzuholen. Washington hat Deutschland sogar ermutigt, seinen Militärhaushalt zu verdoppeln und es hat seine in Deutschland stationierten Atomwaffen modernisiert.

Die Welt wäre erschüttert, wenn sie erleben würde, dass Deutschland plötzlich auch am nuklearen Wettrüsten teilnimmt, doch es hat gerade bei einem anderen drohenden Wettrüsten dramatische Fortschritte gemacht. Der Gewinner dieses Rennens wird die Oberhand über seinen Gegner erlangen, ohne eine einzige Rakete abzuschießen oder auch nur eine einzige Bombe abzuwerfen.

Niemand zieht in den Krieg

Wie würde ein Krieg aussehen, wenn ein Land wie die USA angegriffen würde und seine Streitkräfte in den Krieg schicken wollte, aber seine Schiffe, Flugzeuge oder Panzer sich plötzlich nicht mehr bewegen könnten?

Die Bibel beschreibt genau dieses Szenario. Der Chefredakteur der Posaune, Gerald Flurry wies 2005 auf diese Beschreibung hin: „Ich glaube, dass eine wichtige *Endzeitprophezeiung in der Bibel* sich durch … den Cyberterrorismus …

erfüllen könnte: ‚Lasst sie die Posaune nur blasen und alles zurüsten; es wird doch niemand in den Krieg ziehen, denn mein Zorn ist entbrannt über all ihren Reichtum‘“ (Hesekiel 7, 14). Die Posaune, die zum Krieg aufruft, wird in Israel geblasen – im Wesentlichen in Amerika und Großbritannien. … Scheinbar erwartet jeder, dass unsere Leute in den Kampf ziehen, aber die größte Katastrophe, die man sich vorstellen kann, passiert! Niemand zieht in den Kampf – obwohl die Posaune zum Krieg aufruft! Könnte der Grund dafür vielleicht der Computer-Terrorismus sein?“ (*Trumpet,* Mai 2005).

Die Technologie hat endlich eine Prophezeiung erreicht, die vor mehr als 2000 Jahren niedergeschrieben wurde.

Die Gefahr ist real und jeder kann sie erkennen. Aber offenbar hat man schon längst vergessen, was in den zwei Weltkriegen passierte und die Welt scheint sich wegen Deutschlands Fortschritten beim Cyberkrieg keine Sorgen zu machen. Das wird sich als problematische Fehleinschätzung erweisen. Durch die Technologie kommt eine ungewisse Zukunft einer neuen Dimension der Kriegführung auf uns zu und Deutschland ist dabei, sich an vorderster Front zu positionieren. ▪