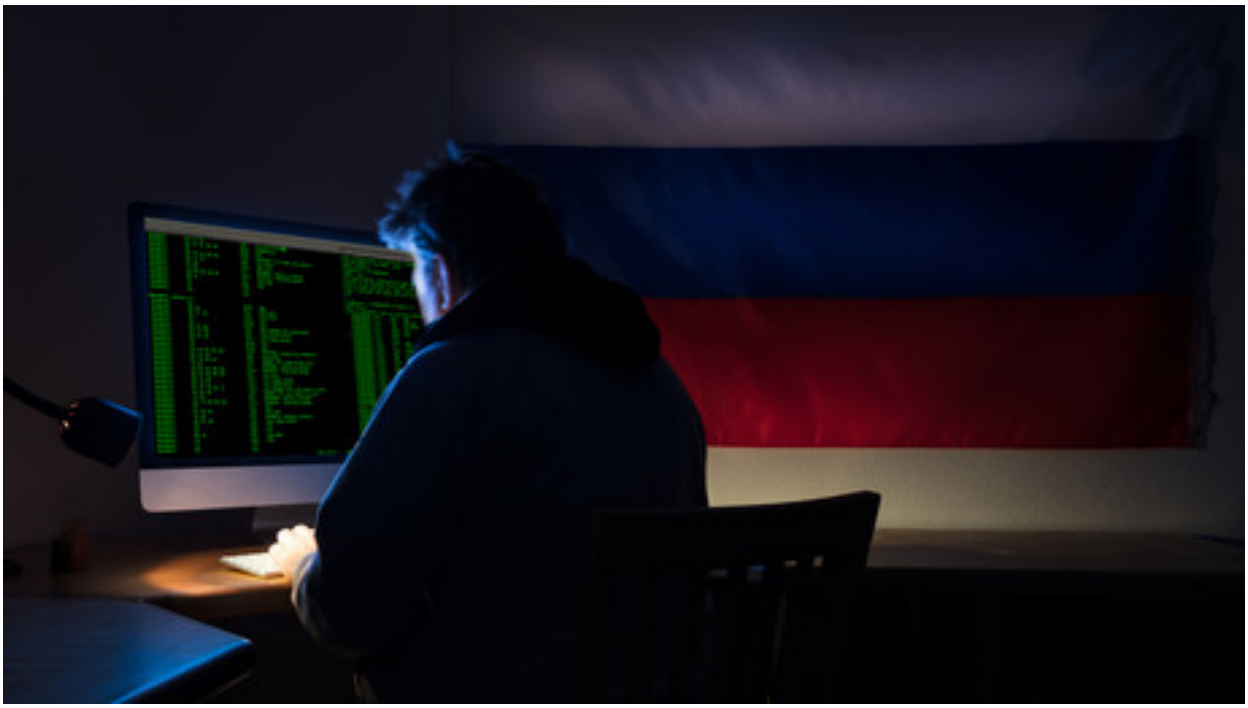
Kampf im digitalen Nebel: Russische Hacker gegen den Westen

2 Juli 2022 12:12 Uhr

In den westlichen Massenmedien wird oft von russischen "Bot-Fabriken" gesprochen, die vermeintlich im direkten Dienst des Kremls agieren und westlichen Institutionen "grundlos" das Leben schwer machen. Hinter diesen Falschdarstellungen versteckt sich jedoch ein wahrer Kern.



Quelle: Gettyimages.ru © Bill Oxford
Symbolbild: Russischer Hacker

Eine Analyse von Elem Raznochintsky

Das russische Hacker-Kollektiv "Killnet" hat im Mai gemeldet, es habe zehn russophoben Staaten den Cyberkrieg erklärt. Hintergrund sind die Entwicklungen, die auf den Beginn der militärischen Spezialoperation Russlands in der Ukraine folgten. Unter den von "Killnet" genannten Staaten befindet sich die Ukraine selbst, aber auch Polen, Großbritannien und, natürlich, die USA.

Jüngstes Fallbeispiel dieser Ankündigung ist der Montagsangriff auf über eintausend litauische Webseiten. Dieser erste Vergeltungsschlag für die litauische "Kaliningrader Blockade" betrifft höchste Verwaltungs- und Regierungsdomänen Litauens. Das Video dazu wurde noch am vorigen Freitag veröffentlicht und beinhaltete die 48-stündige Bedenkzeit, die von der litauischen Führung bislang nicht in Anspruch genommen wurde. Laut dem russischen Hacker-Kollektiv wird die Aktion erst dann eingestellt werden, wenn der Forderung stattgegeben wird.

Außerdem sei die bisherige Strategie der litauischen Medien, diesen Angriff und die damit verbundenen Unannehmlichkeiten an die kleinstmögliche Glocke zu hängen.

Eine "bedauerliche" Geschichte von Exzellenz

Wer sind also diese ominösen, politisch hochmotivierten Hacker aus Russland? Ihre Geschichte geht weiter zurück, als man zuerst denken würde.

Viel Stichfestes ist über diese weitestgehend anonymen Persönlichkeiten nicht bekannt, was auch mit der Natur der ganzen Sache korrespondiert.

Sicher soll wohl aber sein, dass die avancierten Fähigkeiten – die mathematische Disziplin, alte Probleme zu lösen und neue, bahnbrechende Probleme zu erschaffen – noch im naturwissenschaftlichen Akademiesektor der ehemaligen Sowjetunion vermittelt und akquiriert wurden.

Eine These, die mit der Zeit an Plausibilität gewonnen hat, ist, dass die Ursprünge all dessen auf die Stalin-Ära und ihre damals gegründeten mathematischen Fakultäten zurückzuführen sind. Dies war der fruchtbare Boden, den die klassische höhere Mathematik in der Sowjetunion, der späteren Informatik und ihren Zweigen, darbot.

Alle Programmiersprachen, aber auch Protokolle für damalige Internet-Infrastruktur, wurden von diesen sowjetischen, post-sowjetischen und später russischen Studenten internalisiert durch klassisches Auswendiglernen der Sprachen und Systeme. In den meisten Fällen war der damals gängige Luxus im Westen, dieses Wissen und Handwerk an einem Computer im eigenen Wohnzimmer sofort zu erproben, in der Sowjetunion noch verwehrt oder zumindest extrem eingeschränkt. Hatte ein naturwissenschaftliches Institut oder eine Uni einen funktionierenden Computer, so gab es dort sporadische Möglichkeiten, die eigenen Fähigkeiten in die Tat umzusetzen.

Das gesellschaftliche Konzept eines "persönlichen Computers" in einem durchschnittlichen Haushalt kam in Russland mit einer zivilisatorischen Verspätung. So folgte ein "Glück im Unglück", da spartanische Umstände dann zu Spartanern in der Hacker-Sphäre führten. Tugenden wie Disziplin, bedachter Trotz, kluger Widerstand, kämpferische Belastbarkeit und ein in der Not geborener Erfindungsreichtum waren und sind die Folge.

Zwar kein Hacker, aber ein sinnbildlich reiches Beispiel für eben beschriebenes Niveau der mathematisch-naturwissenschaftlichen Ausbildung in der Sowjetunion und Russland ist Grigori Perelman: Ein Petersburger Mathematiker, der das lange Zeit unbewiesene mathematische Problem namens "Poincaré-Vermutung" im Jahr 2006 belegt hatte.

Wenn man einer kürzlich erschienenen Mini-Doku auf dem chinesischen YouTube-Kanal *i-Life小品生活* Glauben schenkt, so gab es noch vor der militärischen Sonderoperation Russlands in der Ukraine mindestens eine Art US-gesponserten, internationalen Hochleistungswettbewerb unter Hackern. Die drei dominantesten Ländervertretungen waren die Vereinigten Staaten von Amerika, die Volksrepublik China und die Russische Föderation. Die chinesischen Hacker mussten vier Stunden investieren, bevor sie das vorgegebene System knacken konnten. Die US-Hacker haben beim selben avancierten Systemeinbruch geschlagene 2 Stunden und 20 Minuten in Anspruch nehmen müssen. Der mit weitem Abstand erste Platz – mit 18 Minuten und 40 Sekunden – ging an die Hacker aus Russland.

Das Resultat solcher Wettbewerbe ist einer der eindringlichen Gründe, weshalb in den relevanten Tech-Communitys eigentlich nur zwei Arten von Hackern auf der Welt existieren: russische und all die anderen.

"Ihr könnt nicht zugleich dem Vaterland und dem Mammon dienen"

Bei genauerer Betrachtung scheinen russische Hacker eine sehr tief empfundene und komplexe politische Weltanschauung herausgearbeitet zu haben. Nämlich hin zu einem post-sowjetischen, russischen Patriotismus, der den westlichen Axiomen dort empfundener und propagierter Außergewöhnlichkeit mit aller Kraft trotzt. Es gibt Indizien, dass dieser Trend sich sogar in der Jelzin-Ära bereits zu formen begann: in einer Zeit, als russischer Patriotismus und ein Trachten nach erneuter Souveränität auf seinem absoluten historischen Tiefpunkt lagen. Eine Periode, die begleitet war von einer präzedenzlosen Unterwanderung der meisten russischen Institutionen mit liberalem, pro-westlichem Gedankengut, das zumindest erfolgreich genug war, um die 1990er Jahre als geopolitischen Sieg Washingtons zu verbuchen. Sich in diesem Klima, ohne eine konstruktive zentrale Anweisung, seines historischen Vermächtnisses sowie der technologischen Verantwortung bewusst zu werden und sich notgedrungen interdisziplinär – besonders politologisch – weiterzuentwickeln, grenzt an ein soziologisches Wunder.

Gab es russische Hacker, die sich hingegen von solch noblen Motiven nicht treiben ließen und in allererster Linie nach finanzieller Selbstbereicherung sehnten? Selbstverständlich. Genau von diesen Fällen, deren Verhaftungen, Fehlern, aber auch gelungener Flucht kann man bis heute lesen.

"Bots" und Hacker

Allein die Bezeichnung "russische Bots" hat semantisch bereits einen suggestiven Effekt: Er impliziert Automatismus, Unterwerfung, Entmenschlichung, Schwarm-Charakter, bedingungslose Aggressivität und Amoralität, die laut westlicher Propaganda vermeintlich gleichbedeutend mit dem russischen Staat sein sollen. Tatsache ist, dass DDoS-Attacken, die meist zur Lahmlegung von Internetseiten und deren Angebot dienen, durch sogenannte "Bot-Netze" erzielt werden. Bei diesen "Bot-Netzen" handelt es sich um Geräte, die mit dem Internet verbunden sind und gebündelt Schadprogramme auf konkrete Serverstrukturen jagen. Gesteuert werden diese "Bot-Netze" natürlich von Hackern. "Killnet" hat sein ganz eigenes "Bot-Netz" entwickelt.

Schubladen zum besseren Verständnis

Im Westen wird unter Hackern oft unterschieden zwischen den sogenannten "black hats", "white hats" und "gray hats". Diese ethischen Bildkategorien sind dem Kinogenre des Western entliehen worden. Demnach sind die "schwarzen Hüte" die anarchistischen Staatsfeinde, die sich unabhängig, oft gegen den Staat und somit jenseits des Gesetzes engagieren. Dies bedeutet aber nicht zwangsläufig, dass die Abwesenheit eines moralischen Codes vorliegt – lediglich fehlende Unterwerfung dem Staat gegenüber. Wie aber mittlerweile bekannt, hat der Staat oft die Tendenz, etwas bereits als feindlich einzustufen, wenn die Person oder das Kollektiv allein schon der bloßen Staatskontrolle entweicht.

Im Gegensatz dazu arbeiten die "weißen Hüte" als Staatsdiener und gehorchen dem Gesetz. Die "grauen Hüte" sind die moralisch stetig ambivalenten Agenten, die je nach Problematik und Herausforderung,

also dem jeweiligen Kontext entsprechend, die Seite des Staates beziehen können, in der nächsten Situation aber schon imstande sind, wieder das rechtliche Vakuum von außerhalb zu betreten.

Diese Kategorien sind auf die russischen Hacker von "Killnet" und ihre Kollegen schwer anzuwenden. Zum einen sind sie durchaus "black hats", da sie nun einmal vollkommen unabhängig vom russischen Staat agieren. Gleichzeitig ist ihr Aktivismus und unter Umständen "digitaler Terrorismus" gegen Länder, die Russland angreifen, im Einklang mit der Staatsräson Moskaus, was sie de facto zu "white hats" machen könnte, oder zumindest zu "grey hats".

Während der Kreml die Aktivitäten dieser Hacker nicht offiziell gutheißt, Neutralität und fehlende Anteilnahme bekundet, ist die Tatsache, dass diese aufmüpfigen Fachleute in Russland nicht geahndet werden, aussagekräftig genug, um dies zumindest als willentliche Duldung zu interpretieren. Dazu gehören auch Hacker-Persönlichkeiten wie Maksim Jakubez oder Jewgeni Bogatschow, die beide unabhängig voneinander den USA großen finanziellen Schaden bereitet haben sollen.

Mehr noch: Hackergruppen wie "Killnet" sind dem russischen Staat sogar oftmals behilflich gewesen bei der Verfolgung und digitalen Ahndung pro-westlicher Hacktivisten, die im Inneren Russlands versuchten, Schaden anzurichten.

Im Westen hat sich die weltweit weitaus bekanntere Hacker-Organisation "Anonymous" zur Feindschaft gegenüber "Killnet" bekannt und die Position der NATO und des jetzigen Kiewer Regimes bezogen.

Motive kristallisieren sich schnell heraus

Fortgeschrittene Hacker, die politisch motiviert sind, gleichen in ihrer Unantastbarkeit Geistern. Wenn man einem Hacker, der von Gier und Ego getrieben wird, früher oder später das Handwerk legen kann, so ist ein idealistisch getriebener Hacker viel vorsichtiger und bedachter in seiner digitalen Fortbewegung. Sein Ziel stellt sich auch als langfristiger dar.

Das geht ebenfalls aus dem Gespräch hervor, das *Lenta.ru* mit dem Anführer von "Killnet" im April führte. Dieser erklärte zudem, dass die aktive initiierte Digital-Gemeinde der Truppe bis zu 4.500 Personen umfasse.

Der weitverbreitete moralische Kodex unter russischen Hackern lautet: "Nicht in Russland arbeiten". Damit ist gemeint, dass man keine russischen Systeme, keine russische Infrastruktur ausschlachten oder angreifen solle. "Arbeite zum Wohle deines Landes" lautet eher die Devise. Patriotisch geeicht besagt diese, dass, selbst wenn es Projekte gibt, in denen Bereicherung an einer der ersten Stellen steht, diese in "unfreundlichen" Staaten durchgeführt werden sollen.

Dass es sich im Falle von "Killnets" Videomanifest aus dem Monat Mai um eine ernstzunehmende Kampfansage handelt, zeigt deren bisherige Kontoführung, die bereits viele Angriffe auf westliche Ziele bescheinigt. Da wären die Angriffe aufs tschechische Fernsehen sowie auf rumänische und moldawische Regierungswebseiten.

Das Kollektiv präsentiert auch einen Hang zu symbolträchtiger Theatralik: Das Lied, das im Hintergrund des Videos läuft, ist das mit Abstand bekannteste sowjetische Kriegslied des Großen Vaterländischen Krieges: "Священная война" (zu Deutsch: "Heiliger Krieg").

Jedem sei der Inhalt dieses Liedes empfohlen. Denn dort wird in vollkommen unmissverständlichen Tönen erklärt, womit es der faschistische Feind zu tun bekommt, sollte er es wagen, mit der Sowjetunion oder ihrem historischen Nachfolger – dem heutigen Russland – jemals Krieg zu führen.

Da nun aber im Westen die Säbel tatsächlich immer stärker herumfuchteln, während die Chance, sich seriöse Fehler gegenüber Moskau einzugestehen, rasant schwindet, sind die russischen Hacker-Kollektive bereits mit ausgegrabenem digitalem Kriegsbeil unterwegs.

RT DE bemüht sich um ein breites Meinungsspektrum. Gastbeiträge und Meinungsartikel müssen nicht die Sichtweise der Redaktion widerspiegeln.