Über Bedrohung durch Cyberangriffe

Früher gab es auf dieser Site öfters zur Weltpolitik auch die Darstellungen der russischen Seite, das wurde schon länger vernachlässigt, heute darum wieder einmal so ein Text:

Scott Ritter schrieb am 21. Juni 2021 auf RT darüber:

Bedrohung durch Cyberangriffe ist real und könnte in Atomschlag enden

Die NATO hat deutlich gemacht, dass eine hinreichend schwere Cyberattacke wie ein konventioneller Angriff behandelt werden kann. Als solcher könne eine Reaktion ausgelöst werde – theoretisch auch einen Atomschlag. Ein Abkommen zur Cybersicherheit erscheint unerlässlich.

In einer aktuellen Erklärung hat NATO-Generalsekretär Jens Stoltenberg deutlich gemacht, dass Cyberangriffe, ob nun tatsächliche oder behauptete, zu einem nuklearen Konflikt führen könnten, der selbst die schlimmste Cyberattacke im Vergleich dazu verblassen lässt. Während eines Besuches in Washington sagte Stoltenberg, die NATO habe beschlossen, dass Cyberangriffe Artikel 5 der NATO Charta den Bündnisfall auslösen können. Es spiele keine Rolle, ob es sich bei einem Angriff um einen kinetischen oder einen digitalen handelt. Man werde als Verbündete bewerten, ob diese Messlatte erreicht sei und sende damit auch eine Botschaft, dass die NATO Cyber-Verbündete sind. Stoltenberg hatte bereits im August 2019 einen Artikel verfasst, in dem er erklärte, dass die NATO mit der "Anpassung an diese neue Realität“ (d. h. Cyberangriffe) den Grundsatz der Verteidigungsklausel in der NATO-Charta erweitert hat. In ihr ist festgehalten, dass ein Angriff gegen einen Verbündeten als Angriff gegen alle behandelt wird. Stoltenberg schrieb: ***"Wir haben den Cyberspace als einen Bereich erkannt, in dem die NATO genauso effektiv operieren und sich verteidigen wird, wie in der Luft, zu Lande und auf See."*** Abgesehen von der Problematik dieser Aussage unternahmen Stoltenberg und die NATO damit Schritte, durch die in Zukunft Cyberangriffe mit einer bewaffneten Aggression gleichgesetzt werden können.

"NATO hat Cyberraum zum Militärbereich erklärt, nicht wir" – Putin fordert Kooperation im Cyberspace

Diese gefährliche Eskalation kann nicht einfach beiseitegeschoben und als Hysterie abgetan werden. Im Februar 2018 veröffentlichte die Trump-Regierung ein Dokument zu ihrer Haltung in der strategischen Auslegung nuklearer Bewaffnung, das den Einsatz von Nuklearwaffen als Vergeltung auf verheerende, nicht nukleare Angriffe auf die amerikanische Infrastruktur erlaubt. Das schließt auch eine lähmende Cyberattacke ein, in der Art, wie sie von den Vereinigten Staaten selbst gegen Russland und andere Staaten, wie etwa dem Iran, vorgesehen wäre.

Es ist eine Tatsache, dass amerikanische Cyberwaffen nachweislich für den Einsatz gegen US-Ziele umfunktioniert werden können. So ist es denkbar, dass die USA mit ihren eigenen, in den USA hergestellten Cyberwaffen attackiert werden könnten und dass dieser Angriff Anlass für eine nukleare Reaktion sein könnte.

Nie zuvor gab es einen größeren Bedarf oder eine größere Dringlichkeit als jetzt für einen Vertrag über Cybersicherheit oder ein Abkommen darüber zwischen den USA und Russland. Das Weiße Haus sagte, Präsident Biden plane bei seinem Treffen mit Präsident Putin angebliche russische Cyberaktivitäten anzusprechen. Washington beschuldigt russische Hacker, die Täter einer jüngsten Flut von Angriffen mit Erpressungstrojanern zu schützen, sie entweder direkt angestiftet oder es versäumt zu haben, gegen diese kriminellen Gruppen vorzugehen.

Von Präsident Putin wird erwartet, dass er seinerseits auf jede Diskussion über Cyberangriffe mit einer eigenen Beschwerdeliste reagiert. Er solle einen Lösungsvorschlag machen in Form eines vier Punkte umfassenden "Programmes praktischer Maßnahmen zur Wiederbelebung unserer Beziehungen im Bereich der Sicherheit bei der Nutzung von Informations- und Kommunikationstechnologien", den Putin im vergangenen September erstmals zur Sprache brachte.

Russland drängt seit über einem Jahrzehnt auf einen Cyber-Vertrag, nach dem Vorbild der Chemical Weapons Convention (Chemiewaffenkonvention, CWC). In einer Rede aus dem Jahr 2009 legte Wladislaw Scherstjuk, stellvertretender Sekretär des russischen Sicherheitsrates, die grundlegenden Bedingungen Russlands für einen solchen Vertrag dar. Sie beinhalten nämlich das Verbot für jedes Land, heimlich bösartige Codes oder Schaltkreise in die gegnerische Infrastruktur einzubetten, die während eines Konfliktes aus der Ferne aktiviert werden können.

London: Moskau und Peking nutzen Cyber-Fähigkeiten zum Sabotieren, der Westen jedoch für "das Gute"

Russlands Sorgen waren alles andere als theoretisch. Geheime Dokumente, vom Whistleblower Edward Snowden veröffentlicht, zeigen, dass die für offensive Cyberoperationen zuständige Abteilung der National Security Agency (NSA) ab Juni 2010 damit begann, kommerzielle Lieferungen von Netzwerkgeräten (Server, Router usw.), die in die ganze Welt exportiert werden, an geheime Orte umzuleiten. Dort wurden Abhörmodule direkt in die elektronischen Geräte installiert.

Auf in den Dokumenten enthaltenen Fotos sieht man NSA-Mitarbeiter neben einem geöffneten Versandkarton, die bei einem Cisco-Router Abhörmodule installieren. Cisco war zu dieser Zeit ein bedeutender Anbieter von Hightech-Internettechnologie und bot russischen Kunden, darunter angeblich dem FSB und dem Verteidigungsministerium, hoch entwickelte Internet-Komponenten an, ähnlich jenen, die von der NSA modifiziert wurden.

Die Aktivitäten der NSA scheinen Teil eines umfassenden offensiven Cyberprogrammes zu sein, das unter Präsident Obama eingeleitet wurde. Es zielt auf zwei Arten auf Russland ab: Erstens, indem man Operationen durchführt, die keinen erheblichen Schaden anrichten. Sie sollen aber entdeckt werden, um damit ein Signal über die potenzielle Reichweite der Fähigkeiten der USA im Cyberspace zu senden.

Die zweite Herangehensweise ist ehrgeiziger und beinhaltet den Einsatz von "Implantaten", die in den Snowden-Dokumenten erwähnt werden. Sie dringen in kritische russische Netzwerke ein, um "Schmerzen und Unbehagen" zu verursachen, wenn man diese lahmgelegt. Diese Implantate sind so konzipiert, dass sie als Reaktion auf jede russische Cyber-Aggression aus der Ferne ausgelöst werden können.

"Inside Job": Russische IT-Expertin Kaspersky vermutet CIA hinter Hackerangriff auf US-Pipeline

Es versteht sich von selbst, dass sich die USA dem Vorschlag Russlands für einen Cyber-Vertrag im Stil des CWC widersetzen. Wenn er nach den von Russland vorgeschlagenen Richtlinien umgesetzt wird, würden die USA ihre gesamte Strategie im Bereich der Cybersicherheit untergraben. Denn diese beruht fest auf dem Grundsatz, dass die beste Verteidigung ein guter Angriff ist. Kurz gesagt, wenn offensive Cyberoperationen völkerrechtlich verboten werden, würden sich in den USA plötzlich ganze Organisationen und Zehntausende Cyberspione und -krieger arbeitslos wiederfinden.

Aus diesem Grund ist die Position der USA in Bezug auf internationale Zusammenarbeit, die Angelegenheit als Sache der Strafverfolgungsbehörden zu behandeln. Dabei befürwortet das US-Außenministerium die Konvention des Europarates über Computerkriminalität von 2004 als Vorbild, die von 22 Nationen, darunter den USA, unterzeichnet wurde – aber nicht von Russland.

Russische Einwände basierten auf Vorstellungen von Souveränität. Das betraf insbesondere, dass die Konvention Strafverfolgungsbehörden anderer Länder erlaubt, mutmaßliche cyberkriminelle Aktivitäten mit Ursprung in Russland zu untersuchen, ohne zuvor die russischen Behörden zu informieren.

Aber der wahre Grund könnte so praktisch sein wie die Zurückhaltung der USA in Bezug auf einen Cyber-Vertrag im CWC-Stil. Der Beitritt zu der Konvention könnte Russland verpflichten, mit externen Behörden gegen kriminelle Cyber-Aktivitäten mit Ursprung in Russland vorzugehen. Russland würde die Arbeit privater Organisationen und Hackergruppen behindern, die angeblich ihre geopolitischen Rivalen von seinem Territorium aus angreifen – egal ob in direkter Verbindung mit dem Staat oder nicht.

Wenn die beiden Präsidenten in Genf zusammenkommen, kann man nur erwarten, dass Putin in Sachen Cybersicherheit so viel rausholen kann wie möglich. Hoffentlich werden die beiden Staatsführer in der Lage sein, der Versuchung zu widerstehen, Bidens theatralischen "Putin ist ein Killer"-Moment zu wiederholen und erkennen, dass die Bedrohung durch Cyberangriffe real und gegenseitig ist. Wenn sie nicht behoben wird, kann sie zu Instabilität führen, die schnell zu viel verheerenderen Dingen führen könnte als ein bloßer Cyberangriff.

RT DE bemüht sich um ein breites Meinungsspektrum. Gastbeiträge und Meinungsartikel müssen nicht die Sichtweise der Redaktion widerspiegeln. Übersetzt aus dem Englischen. Scott Ritter ist ein ehemaliger Geheimdienstoffizier im US Marine Corps und Autor von "SCORPION KING: America's Suicidal Embrace of Nuclear Weapons from FDR to Trump". Er diente in der Sowjetunion als Inspektor bei der Umsetzung des INF-Vertrags, im Stab von General Schwarzkopf während des Golfkriegs und von 1991–1998 als UN-Waffeninspektor.
