Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 189 (2023)

Heft: 1-2

Artikel: Cyberwar im Ukraine-Krieg : eine Analyse

Autor: Ruef, Marc

DOI: https://doi.org/10.5169/seals-1046414

Cyberwar im Ukraine-Krieg – eine Analyse

Es gibt einige staatliche Akteure im Cyberraum, denen eine hohe Professionalität beigemessen wird. Dazu gehören Länder wie USA, China, Israel und eben auch Russland. Seit Jahren wird darüber diskutiert, ob und inwiefern virtuelle Aktivitäten den klassischen militärischen Konflikt ersetzen oder mindestens ergänzen kann. Eine klar abgrenzbare Analyse anhand eines konkreten Beispiels blieb bisher glücklicherweise aus – bis zum 24. Februar 2022. Nun zeigt sich, welche Rolle Cyber im Ukraine-Krieg spielt.

Marc Ruef

Ich leite eine Abteilung, die sich mitunter auf Analysen im Cyberraum spezialisiert hat. Dabei führen wir sogenannte Cyber Threat Intelligence (CTI) durch: Hierbei werden Aktivitäten und Akteure analysiert, um ihre Absichten und ihr Vorgehen ermitteln, voraussagen und dadurch antizipieren zu können.

Unser Ansatz ist weltweit einzigartig, analysieren wir nämlich breitflächig Aktivitäten einzelner Personen und Gruppierungen im Internet. Dazu gehören auch scheinbar unwichtige Dinge wie zum Beispiel die Beiträge in sozialen Medien oder der Austausch in Online-Foren. Das automatisierte Analysieren dieser Aktivitäten sowie das Attributisieren der Personen macht es möglich, ein konkretes Lagebild erstellen zu können. So wird es durchaus möglich, schon sehr früh sich abzeichnende strategische Entscheide als solche festzustellen.

Russland vor dem Einmarsch

Da Russland als einer der Hauptakteure im Cyberraum gilt, haben wir unsere Analysen mitunter auch auf diesen Kultur- und Sprachraum optimiert. Dies macht es uns möglich, entsprechende Kommunikationen sehr konsequent überwachen und Signale frühestmöglich erkennen zu können.

Dabei ist uns ab dem 7. Februar 2022 aufgefallen, dass die russischen Aktivitäten im Cyberraum konsequent zugenommen haben. Schwankungen dieser Art sind nicht untypisch. Sie sind oft auf banale Gründe wie Wochenenden, Feiertage oder Ferien zurückzuführen. Manchmal illustrieren sie aber auch einfach die natürliche Dynamik von Interessen, die zum Beispiel mit quartalsweisen Durchführungen von «Hacking-Kursen» an Universitäten zu tun haben. Ein Effekt, den wir immer wieder im asiatischen Raum (vor allem in Indien und China) beobachten können.

Der sich abzeichnende Ausschlag von Russland war aber tatsächlich ungewöhnlich. Innert drei Tagen war ein Anstieg von 52.9 Prozent der offensiven Merkmale zu verzeichnen und er erreichte seinen Höhepunkt am 10. Februar.

Dann begann ein gemeinsames militärisches Manöver mit Belarus im Grenzgebiet zur Ukraine. Und die Cyberaktivitäten sind wiederum zurückgegangen. Bis zum 17. Februar nahmen sie dann wieder zu, um bei der ersten Eskalation wieder zu schwinden. Auch vor dem Einmarsch am 24. Februar konnten erhöhte Aktivitäten im Cyberraum festgestellt werden, die dann wieder abnehmen sollten.

Dieser Effekt ist immer wieder zu beobachten: Es finden nachrichtendienstliche Vorbereitungen statt, die ein erhöhtes Mass an Aktivitäten im Cyberraum zur Folge haben. Doch mit der Transition der Auseinandersetzung in den physischen Raum nahmen die virtuellen Zugriffe wieder ab. Ergo: Eine Zunahme der virtuellen Aktivitäten kündigt stets eine neue physische Handlung an.

Cyber mit niedriger Priorität

Damit sollte bewiesen sein, dass in der russischen Kriegsführung der Cyberraum nur eine untergeordnete Rolle spielt. Eine klassische Kriegsführung, bei der die Cyberaktivitäten stiefmütterlich behandelt werden sollten, sind zu beobachten. Böse Zungen könnten behaupten, dass also auch auf dieser Ebene archaische Paradigmen dominieren.

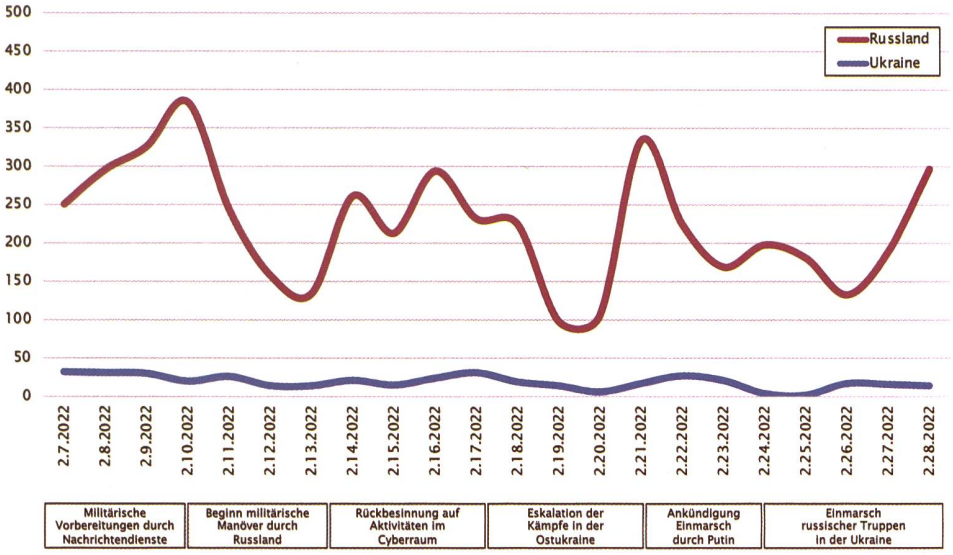
Dies erstaunt, entspricht es doch so gar nicht dem gehobenen Stand, der eigentlich Russland beigemessen wird. Nun stellt sich die Frage, ob Russland eines Cyberkriegs nicht fähig oder nicht willens ist. Um diese Frage zu beantworten, müssen wir die Eigenarten der Struktur Russlands betrachten.

In vielen Ländern kann konsequent zwischen staatlichen Akteuren mit politischen Interessen und Cyberkriminellen mit wirtschaftlichen Absichten unterschieden werden. Doch in einigen Staaten, besonders solche mit einem eher hohen Mass an Kriminalität in gehobenen Kreisen, lässt sich eine Vermengung dieser Interessen beobachten. Dazu gehört ebenfalls Russland, das im Korruptionsindex 2021 den 136. Platz belegt hat.

Russland war seit den 1990er-Jahren bekannt für einige sehr begabte Malware-Entwickler. Es war also absehbar, dass dort das Thema Ransomware ebenfalls eine wichtige Rolle einnehmen würde. Ransomware ist in erster Linie Cyberkriminellen zuzuschreiben, die mit verschlüsselten Daten von ihren Opfern Geld erpressen wollen. In Osteuropa gibt es also definitiv Leute, die das Wissen und die kriminelle Energie haben, erfolgreiche Angriffe im Cyberraum auf professionellem Niveau durchzuführen.

Dass diese konsequent in militärische Prozesse eingebunden sind, ist zu bezweifeln. Es wird sicher eine überproportional grosse Schnittmenge geben. Diese konnte sich aber im Konflikt in der Ukraine bisher nicht nachhaltig bemerkbar machen. Der politische und militärische Apparat in Russland hat es entweder versäumt, diese Kräfte für sich zu gewinnen oder er wollte sie nicht im Rahmen der militärischen Offensive heranziehen.

Diese Worte sind also in erster Linie als Kritik an der russischen Führung anzusehen, die das Potenzial ihrer Landsleute nicht rechtzeitig einbinden konnte. Dies mag in einem Konflikt mit der Ukraine nicht von besonderer Wichtigkeit gewesen



◀ **Quantitative Übersicht der Aktivitäten auf russischer und ukrainischer Seite vor und zu Beginn der physischen Kampfhandlungen.**
Grafik: Marc Ruef

sein. Russland müsste aber bei Auseinandersetzungen mit grösseren Gegnern sämtliche Möglichkeiten in Betracht ziehen, um bestehen zu können.

Absichten russischer Aktivitäten

Im Rahmen der Sprachanalyse geht es unter anderem darum zu erkennen, welche Themen durch die Akteure erforscht und attackiert werden. Der Austausch wird also in Bezug auf Hersteller, Produkte, Technologien und Schwachstellen untersucht. Spricht ein Akteur, dem ein hohes Wissen bezüglich Windows beigemessen wird, über spezielle Netzwerkzugriffe, ist dies ein Indiz, dass entsprechende Forschung oder Angriffe in diesem Bereich absehbar sind.

Der Fokus offensiver Aktivitäten aus Russland im Jahr 2021 war vielseitig. Einerseits hat man sich für Schwachstellen in Windows-Systemen interessiert. Dies ist zwar auch für Cyberkriminelle, wie zum Beispiel Ransomware-Gangs, von Interesse. Betriebssysteme sind aber auch stets eine typische Diskussion, die in nachrichtendienstlichen Kreisen ihre Berechtigung hat. Dies ist auf die enorme Angriffsfläche und die verheerende Durchschlagskraft erfolgreicher Attacken zurückzuführen.

Klar ist aber auch zu erkennen, dass gewisse webbasierte Ziele absehbar waren. Angriffe auf Webserver (Apache) und Webapplikationen (Content Management Systeme wie October CMS oder WordPress) waren populär.
Dies hat sich geändert, wenn man den Zeitraum zu Beginn von 2022 vor dem Einmarsch analysiert. Angriffe auf Windows- und Linux-Systeme wurden plötzlich bedeutend wichtiger, haben Content-Management-Systeme fast nahezu aus der Topliste verbannt. Dies deutet darauf hin, dass sich der Fokus naturbedingt verschoben hat, dass statistisch klassische Geschäftsmodelle von Cyberkriminellen mit finanziellen Zielen den unmittelbar gewachsenen politischen Bedürfnissen gewichen sind.

Ukraine im Vergleich

Betrachtet man nun die Aktivitäten der Ukraine im Cyberraum, dann fällt als Erstes auf, dass diese in Bezug auf ihren Umfang in keiner Weise mit denen von Russland vergleichbar sind. Sie machen in ihrem Umfang nur etwa 8.3 Prozent der russischen Aktivitäten aus.

Aber, und das zeigt sich ganz deutlich, sie sind sehr konsequent und stabil. Dies bedeutet, dass die Ukraine dem Cyberraum eine gewisse Wichtigkeit beimessen, die durch den Konflikt nicht nachhaltig beeinträchtigt wurde. Dies korreliert mit der Beobachtung des Verhaltens der ukrainischen Führung in Bezug auf die wirtschaftliche Ausrichtung vor und dem medialen Umgang während des Krieges.

Diskutiert man den Fokus offensiver Aktivitäten der Ukraine, dann wird klar, dass die Beherrschung des Narrativs im Internet eine hohe Priorität geniesst. Denn viele ihrer offensiven Tätigkeiten zielen auf Webdienste ab. Diese anzugreifen, um die Kommunikation des Gegners zu stören, diesen medial zu entblössen oder eigene Propaganda zu etablieren, ist ein erklärtes Ziel.

Hierbei ist es jedoch schwierig zu unterscheiden, ob diese Aktivitäten von der ukrainischen Regierung initiiert und durchgeführt werden oder ob es sich um den virtuellen Partisanenkampf einiger Idealisten handelt.

Zukünftige Entwicklungen

Dass sich die strategische Ausrichtung der russischen Kampfhandlungen im Cyberraum verändern wird, ist unwahrscheinlich. Zu starr scheinen die archaischen Strukturen zu sein, um die neuen Möglichkeiten zeitnah und flexibel adaptieren zu können. Vor allem in der Hektik des offenen Konflikts wird der Fokus anderswo liegen und keine Möglichkeiten bestehen, sich doch noch auf das Thema Cyber zu besinnen.

Im Gegensatz dazu wird die Ukraine ihren Kurs beibehalten. Die Beherrschung des Narrativs, gerade in den sozialen Medien, bleibt von zentraler Wichtigkeit. Dass damit gewisse offensive Tätigkeiten einhergehen, um russische Elemente zu stören, bleibt unverändert.

Auch wenn zu einem gewissen Grad die Priorität von Cyber bei Kriegshandlungen widerlegt ist, darf der hier geschilderte Sachverhalt nicht als Exempel verstanden werden. Die russische Doktrin scheint im Cyberbereich hoffnungslos veraltet zu sein. Die negativen Auswirkungen in der Ukraine bleiben vielleicht überschaubar. Langfristig zementiert es aber nur die Schwäche eines starren Gefüges, das im Begriff ist, von der Zukunft überrollt zu werden. Unter Putin wird sich das sicher nicht mehr ändern. Da braucht es eine neue Generation in der Führung, die sich nicht mehr nur im Kalten Krieg verankert sieht. ■

Marc Ruef
Head of Research scip AG
8048 Zürich