



Mittwoch, 14. Oktober 2026, 17:00 Uhr
~13 Minuten Lesezeit

Kriegsrelevante Internetdienstleister

Sowohl im Nahen Osten als auch in der Ukraine werden Rechenzentren systematisch unter Beschuss genommen.

von Peter Frey
Bild: Collage mit Fotos von Shutterstock.com (DC Studio, isoprotonic)

*So erstaunlich leistungsfähig das, was wir unter
Internet verstehen, auch ist, so komplex und*

angreifbar ist es. Erst recht dann, wenn dieses ganze Ökosystem eine so gewichtige Rolle wie zum Beispiel im Ukrainekrieg einnimmt. Dieses Ökosystem ist auch essenziell für die Kriegsführung auf Basis der sogenannten künstlichen Intelligenz (KI) und stellt den Unterbau von quasi mit Echtzeitdaten gesteuerten und ausgewerteten, komplexen Operationen auf dem Schlachtfeld (<https://peds-ansichten.de/2026/09/starlink-rassvet-volna-kupol-garant-krieg-weltraum-all/>). Da kann es kaum verwundern, wenn es selbst zum Angriffsziel wird.

Seit September haben Raketen und Drohnen der russischen Streitkräfte verstärkt und systematisch Einrichtungen der ukrainischen Kommunikationsinfrastruktur außer Betrieb genommen. Das hatte es in diesem Umfang zuvor nicht gegeben – und die Blaupause dafür wurde nur Monate zuvor im Nahen und Mittleren Osten erstellt.

Der Cloud-Anbieter Amazon Web Services (AWS) hat am 15. September 2026 eingeräumt, dass wiederholte, seit März des Jahres andauernde iranische Drohnenangriffe einige seiner Rechenzentren inzwischen schwer beschädigt haben. Die Schäden sind teilweise so groß, dass es AWS in lokalen Rechenzentren nicht mehr gelang, Ressourcen und Daten wiederherzustellen. Dies auch deshalb, weil der Iran gleichzeitig mehrere Rechenzentren einer Zone erfolgreich attackierte und so die physische Redundanz für Systeme und Daten (Ausfallsicherheit) nicht mehr gegeben war (1).

„Amazon muss Segel streichen. Laut Firmenangaben stellt der Datenkonzern seine Bemühungen ein, Daten wiederherzustellen, die

ausschließlich in einem betroffenen Rechenzentrum gespeichert waren. Die jeweiligen Kunden werden auf ihre eigenen Backups verwiesen. Dies betrifft alle drei AWS-Rechenzentren in Bahrain sowie eines von drei in den Vereinigten Arabischen Emiraten. Bei den beiden anderen hat AWS die Hoffnung noch nicht aufgegeben: Alle AWS-Daten in Bahrain sind im Irankrieg zerstört“ (2).

Was in Meldungen wie dieser nicht zum Ausdruck kam, besteht in der Tatsache, dass Amazon ein aktiver „Mitspieler“ im Krieg gegen den Iran ist – und nicht nur in diesem.

Als Ende Februar Israel und die USA ein weiteres Mal den Iran angegriffen hatten, versicherte ihnen der Iran eine asymmetrische Antwort, die nicht lange auf sich warten ließ. Eine Reihe von US-Konzernen mit Unternehmungen auf der arabischen Halbinsel wurden zu legitimen Angriffszielen erklärt.

Die Liste enthielt neben den Rüstungs- und Technologiekonzernen Boeing und General Electric eine Reihe von Konzernen mit Schwerpunkt Informationstechnik. So Intel, HP, IBM, Dell, Cisco und Nvidia, welche die physische Infrastruktur bereitstellen. Schließlich wurden auch Microsoft, Google, Meta, Oracle und Palantir genannt – weltweit führende Cloud-Anbieter, Software-Konzerne und dabei stark involviert in Bereichen der künstlichen Intelligenz (KI). Dazu kommt interessanterweise noch der Finanzkonzern JP Morgan (3).

Weniger bekannt ist das ebenfalls ins iranische Visier geratene KI-Unternehmen G42 aus den Vereinigten Arabischen Emiraten (VAE) – auch ein Investitionsobjekt US-amerikanischer Konzerne wie Microsoft und SilverLake. G42 wiederum hat die Technologie-Investmentfirma MGX mitbegründet, die ihrerseits Beteiligungen an und Partnerschaften mit KI-Unternehmen wie OpenAI und Anthropic unterhält (3i).

„Insbesondere das US-Militär hat KI-Systeme in großem Umfang zur Entscheidungsunterstützung bei seinen Angriffen auf den Iran und Venezuela eingesetzt. Angesichts der Bedeutung von Rechenzentren könnten iranische Streitkräfte gezielt die Infrastruktur angreifen, von der die iranische Führung glaubt, dass sie Angriffe auf den Iran unterstützt“ (a1, 4).

Der Iran setzte seine Angriffe auf die Internet-Dienstleister, gerade auch AWS (Amazon), immer dann fort, wenn die USA den Krieg wieder eskalierten. Die Wirkung ist kaum zu überschätzen. Kaum zu überschätzen in einer Zeit, in der Gewinnung, Auswertung und Kommunikation von Daten, Programmlogik und pure Rechenleistung Einfluss auf das Kriegsgeschehen haben. Schwenken wir von der arabischen Halbinsel nach Europa, in die Ukraine. Ist Amazon möglicherweise auch in der Ukraine Kriegsteilnehmer?

„Die Angriffe vom 23. und 24. September beschädigten mehrere Einrichtungen im Telekom- und Hosting-Sektor. UTELS meldete Schäden an einem Rechenzentrum, in dem sich die zentrale Netzausrüstung befand. Aufgrund von Stromausfällen kam es zu Unterbrechungen beim Internetzugang. Auch das Unternehmen ‚Pavutyna‘ berichtete über Schäden an einem Rechenzentrum und Störungen im Netzwerk. Etherlink teilte am 24. September mit, dass sein zentraler Netzwerkknoten beschädigt worden sei, und entschied sich, ihn an einen anderen Standort zu verlegen“ (5).

Crazy Network, das nicht nur in Kiew aktiv ist, bekam nach der Beschädigung eines Internetknotens große Probleme bei der Bereitstellung der Internetzugänge für seine Kunden. Es waren neben den Kunden in der Hauptstadt weitere in den Regionen Winniza und Chmelnizki von Ausfällen betroffen. Auch die Hosting-Infrastruktur erlitt erhebliche Beschädigungen. MiroHost, einer der größten ukrainischen Anbieter, informierte, dass das Rechenzentrum, in dem seine Infrastruktur untergebracht war, vollständig zerstört worden sei. Ein Zeitpunkt für die

Wiederinbetriebnahme läge in weiter Ferne. Bei Cityhost wurde ein Teil der Hosting-Infrastruktur zerstört, die Sicherungen mussten auf ausländischen Servern in Betrieb genommen werden.

Laut Schätzungen des Ministeriums für Digitale Transformation der Ukraine waren allein nach dem Angriff vom 23. September 100.000 Haushalte in Kiew ohne oder mit gestörtem Internetzugang (5i, 6, 7).

Wenn man davon spricht, dass die angegriffenen Objekte zivile Infrastruktur darstellen, ist das allerdings nur die halbe Wahrheit:

„Bei Angriffen auf Rechenzentren geht es nicht nur um die Zerstörung von Hardware. Da die Ukraine einen erheblichen Teil ihrer staatlichen Dienstleistungen, des Bankwesens, der Logistik und der militärischen Führung längst digitalisiert hat, führt der Verlust von Serverkapazitäten zur Lähmung ganzer Sektoren. In diesem Sinne ist ein Rechenzentrum ein ebenso legitimes militärisches Ziel wie ein Kommandoposten oder eine Kommunikationszentrale – nur dass es über ein Gebiet verteilt und als zivile Einrichtung getarnt ist“ (8).

Die Schwächung der informellen Logistik des Kriegsgegners in dessen Hinterland hat mittelbar schwerwiegende Konsequenzen für das Geschehen an den Fronten. Netzwerkinfrastrukturen und deren Komponenten sind mehrfach abgesichert. Deren Außerbetriebsetzung bedarf eines systemischen und zeitlichen Aufwands, und den betreibt Russlands Militär:

„In der Nacht vom 23. September beschädigten russische Angriffe auf die Telekommunikationsinfrastruktur der ukrainischen Hauptstadt gleich drei Rechenzentren, in denen die Ausrüstung lokaler Internet-Dienstleister untergebracht war. Dies erklärte Alexander Polujow, Inhaber des Unternehmens Utels, und präzisierte, dass die Namen der betroffenen Objekte aus Sicherheitsgründen nicht veröffentlicht werden. Seinen Worten zufolge war der Angriff einer der

umfangreichsten für die Telekommunikationsinfrastruktur seit Juli dieses Jahres“ (9).

Die ukrainischen Behörden sind sich inzwischen auch darüber im Klaren, dass das Ganze nicht so schnell aufhören wird:

„Laut einem der für die Internetknoten Verantwortlichen plant die russische Seite neue Angriffe auf Rechenzentren und Standorte der Internetverbindung. Bestätigungen dieser Informationen aus offiziellen Quellen lagen zum Zeitpunkt der Veröffentlichung des Artikels nicht vor“ (9i).

In öffentlich-rechtlichen Medien hierzulande wurde über diese Vorfälle im Rahmen der Berichterstattung zu russischen Angriffen auf Kiew kaum etwas berichtet (10). Am 28. September fand sich allerdings ein versteckter Hinweis in einem Bericht der ARD-Tagesschau (zu UkrTelecom erfährt der Leser weiter unten noch mehr):

„Auch eine Klinik ist bei den Angriffen getroffen worden. (...) Zu möglichen Opfern dieses Angriffs wurden keine Angaben gemacht. Die private Klinikette Dobrobut bestätigte der Nachrichtenagentur Interfax-Ukraine zunächst einen Einschlag in einer Einrichtung. Später konkretisierte das Unternehmen die Niederlassung. Vor dem Einzug der Klinik beherbergte das Gebäude eine Filiale des Telekommunikationsunternehmens UkrTelecom“ (11).

Zuvor hatte sich die ARD in ihrer Hauptbotschaft zum wiederholten Male als offizielle Verlautbarungsstelle des ukrainischen Präsidenten Selenskyj geriert („Historische Akademie in Flammen“). Im letzten Teil des Berichts, dort, wo viele Leser gar nicht mehr lesen, wurde der Sender schließlich doch noch konkreter:

„Ziel der Angriffe sind inzwischen vor allem Tankstellen, Lagerhallen von Supermärkten und Rechenzentren. Mobilfunkanbieter hatten

zuletzt vermehrt Ausfälle des Internets gemeldet. Das Verteidigungsministerium in Moskau bestätigte auch bei der jüngsten Angriffswelle den Beschuss von Datenzentren in Kiew. Sie hätten die ukrainischen Streitkräfte mit Mobilfunk und Internet versorgt, hieß es zur Begründung“ (11i).

Inzwischen ist man auch in der hiesigen Öffentlichkeit über die militärische Relevanz der Starlink-Satelliten und der an sie gebundenen Netzwerke, gerade für den NATO-Krieg in der Ukraine und Russland, wohlinformiert. Da kann es nicht überraschen, wenn russische Raketen und Drohnen neuralgische Punkte dieser Netzwerke anvisieren:

„Nach Angaben des russischen Verteidigungsministeriums wurde ein Rechenzentrum von Cosmonova getroffen, das den mobilen Internetbetrieb sowie die von den ukrainischen Streitkräften genutzten Starlink-Satellitenkommunikationssysteme unterstützte. Der Internetanbieter Kolo.TV teilte mit, dass seine Anlagen in Kiew bereits zum dritten Mal getroffen worden seien“ (12).

Die russischen Streitkräfte greifen Rechenzentren in Kiew an, welche die ukrainischen Streitkräfte mit Internetzugang und weiteren Kommunikationskanälen sowie mit Aufklärungsdaten versorgen. Dazu gehören Rechenzentren von UkrTelecom, DreamLine, Omega Telecom, Kyivstar, Vodafone und Datagroup. Inzwischen sind zusätzlich die Programme mehrerer TV-Anbieter in der Ukraine gestört (13).

Die strategische Vorgehensweise Russlands ist begründet, wohldurchdacht und erfolgt zeitlich abgestimmt. Zunächst erfolgten Angriffe auf militärische Produktionsstätten und Logistiklager. Dann verlagerte man den Schwerpunkt auf die Isolierung des Hafens von Odessa und die Zerschlagung der Schwerindustrie. Nunmehr sind Rechenzentren und die Telekommunikationsinfrastruktur die Hauptziele. Zwischen dem 20. und 28. September führten russische

Streitkräfte eine Reihe von Angriffen auf Kiews Einrichtungen zur Datenspeicherung, -verarbeitung und -übertragung durch.

Rechenzentren sind absolute Hochwertziele. Ein einziges großes Rechenzentrum beherbergt gleichzeitig Telekommunikationsausrüstung für mehrere Internetdienstleister, Cloud-Computing-Infrastruktur, Unternehmensinformationssysteme, Datenbanken staatlicher/militärischer Dienste und Netzwerkknoten, über die erheblicher Internetverkehr läuft.

Die Beschädigung einer einzigen Anlage kann eine Kettenreaktion bei mehreren unabhängigen Betreibern auslösen und so gleichzeitig den Internetzugang, Unternehmensnetzwerke, Cloud-Anwendungen und Mediendienste stören.

Die jüngsten Angriffe fanden in der Nacht zum 28. September statt. UkrTelecom – das ist einer der größten ukrainischen Anbieter von Festnetz-, Mobilfunk- und Hochgeschwindigkeits-Internetdiensten, der die Streitkräfte mit Internetverbindungen versorgt – wurde getroffen. Auch Dreamline, ein weiterer großer Anbieter, der ebenfalls Daten für militärische Dienste vorhält, verzeichnete Angriffe.

Was die Angriffe auf Kiew zusätzlich bemerkenswert machte, war die verwendete Technologie. Ein Technologieberater des ukrainischen Präsidenten, bekannt unter dem Rufzeichen „Flash“, beschrieb das im Internet veröffentlichte Filmmaterial wie folgt:

„Die Russen filmten den Angriff auf das Inkom-Geschäftszentrum mit einer jetgetriebenen Geran-Drohne, die gleichzeitig als MESH-Relais (a2) für eine Geran-5-Drohne diente und Live-Videomaterial des Angriffs übertrug. Danach flog die Drohne aus Kiew heraus und griff ein McDonald's-Lager an“ (14).

Hier wird erahnbar, wie weit inzwischen die Entwicklung der russischen Drohnenkriegsführung fortgeschritten ist. Eine einzige Drohne – in der Lage, hoch, lange und schnell zu fliegen – vereint Echtzeitaufklärung und Angriffsfähigkeit in einer einzigen Mission. Die Auswirkungen von Angriffen auf die Internetinfrastruktur gehen über die akute Störung der Verfügbarkeit hinaus. Der ukrainische Ministerpräsident Serhij Koryntskyj: „Es besteht die Gefahr, das Internet zu verlieren, daher bereitet sich der Staat auf das schwierigste Szenario vor.“ In der heutigen Ukraine läuft die Kommunikation der Regierung mit der Bevölkerung auf allen Ebenen hauptsächlich über das Internet. Eine Störung dieses Kanals – alles vor dem Hintergrund von Kriegsmüdigkeit, anhaltenden Luftschuttsirenen, sinkendem Lebensstandard und Zwangsmobilisierung – birgt die Gefahr, den sozialen Zusammenhalt zu untergraben, der die Kriegsanstrengungen von innen heraus noch immer stützt (14i).

Der Iran hat statt oder neben Staaten Konzerne als Feinde des Landes, als aktiv Krieg führende Teilnehmer ausgemacht. Dazu gehören Amazon und Microsoft.

Konzerne, die nicht nur am Irankrieg verdienen, sondern auch am Ukrainekrieg. Solche Konzerne haben die Macht, Krieg zu gestalten, sogar mitzuentwickeln. Der Coronakrieg gegen die Bevölkerungen war auch ein Krieg der Konzerne. Das waren eben nicht nur Pharmakonzerne. Es waren auch und gerade Internet- und Technologiekonzerne.

Amazon und Microsoft waren PLandemie-Gewinner. Und wie ist es nun im Ukrainekrieg?

Was passiert da im Einzelnen, wie funktioniert das Ökosystem, das Russland versucht auszuschalten? Die Cloud-Infrastruktur der Ukraine wird, wie auf der arabischen Halbinsel (siehe ganz oben), von zwei westlichen Konzernen beherrscht: Amazon und Microsoft.

Seit 2022 betreibt die ukrainische Regierung ihre IT-Systeme verteilt, und dezentral werden auch die Daten abgespeichert, ein Teil davon in Cloud-Systemen in anderen Staaten der Europäischen Union. Ein Großteil der Daten, nicht nur der Regierung, wird durch Cloud Computing Services (CCS) von Amazon gehalten, genauer gesagt durch deren Amazon Web Services (AWS). Das ist nicht so offensichtlich, aber großzügig angebotene Schnittstellen für öffentliche Dienste in der Ukraine zur AWS-Infrastruktur weisen darauf hin (15). Russischen Quellen zufolge beherbergt AWS zum Beispiel mehr als 75 Petabyte Daten von Behörden und regierungsnahen Organisationen (16). Aber dort unter anderem stecken auch die Daten samt Programmen, die man für die Kriegsführung der neuesten Generation benötigt.

Der Grund, warum russisches Militär Rechenzentren in der Ukraine angreift, ist der gleiche, warum iranisches Militär Rechenzentren auf der Arabischen Halbinsel angreift. In beiden Fällen sind die Objekte solche mit doppeltem Verwendungszweck (Dual Use), werden also mit für die Kriegsführung genutzt. Und interessanterweise sind in beiden Regionen Amazon und Microsoft dominant. Deren wirtschaftliche Dominanz geht jedoch einher mit politischer Macht, die wiederum zur Durchsetzung der Eigeninteressen gebraucht wird. Ist das nicht aufschlussreich? Der Iran und Russland bekämpfen vorrangig vielleicht gar nicht Staaten, sondern Konzerne?

Wie schwerwiegend die Folgen der russischen Angriffe auf Rechenzentren in Kiew waren, bezeugt folgende Geschichte: Drei Tage nach diesen Angriffen wurde auf Veranlassung des CSO (Chief Security Officer) von AWS eine nicht näher bestimmte Zahl von sogenannten, jeweils 80 Terabyte großen Snowball-Laufwerken über Dublin und Krakau nach Polen gesendet. Das sind externe Datenspeicher, die speziell für die Aufnahme von in der Amazon-Cloud abgelegten Daten vorbereitet sind. Vor Ort wurden diese Speicher mit Daten gefüllt und wieder zurückgebracht. Im Ausland

wurden die Daten schließlich wieder in die AWS-Cloud hochgeladen und über die Netzwerkreplikation weltweit verfügbar gemacht (17). Ein Vorgang, der Tage benötigte und ganz erheblich Produktions- und Logistikprozesse beeinträchtigte – und darüber hinaus die Kriegsführung der neuesten Generation, die auf Echtzeitdaten und schnelle Verarbeitung angewiesen ist (16i).

„Zur Vertiefung ihrer Argumentation betonten Analysten, dass die Zuständigkeiten derzeit aufgeteilt sind. AWS ist das Zentrum des Systems. Ministerien und Energieunternehmen (Ukrenergo; Microsoft hatte bereits vor Beginn des CBO 16 der 17 Ministerien ausgegliedert) werden von Azure [der Microsoft-Cloud] verwaltet. Ukrainische Cloud-Anbieter wie GigaCloud unterhalten ihr eigenes Backup in Polen, wohin 60 Prozent ihrer Kunden im Jahr 2022 umgezogen sind.“ (16ii)

Direkte Bestätigungen für die aus den russischen Quellen extrahierten, obigen Informationen waren schwer und nur teilweise auffindbar (18). Dafür, dass westliche Konzerne bereits seit Jahren kritische Infrastruktur im Bereich Internet-Dienstleistungen (nicht nur) in der Ukraine übernommen haben, gibt es Ehrungen:

„Die ukrainische Regierung hat Microsoft Azure und Amazon Web Services (AWS) Friedenspreise für die Bereitstellung wichtiger Cloud- und digitaler Dienste während der unprovokierten Invasion Russlands verliehen. Im Mai [2022] hatte die Ukraine Google denselben Preis verliehen, ohne jedoch die Gründe dafür zu nennen. »Die großen Tech-Unternehmen unterstützen die Ukraine«, sagte Mykhailo Fedorov, [damaliger] stellvertretender Ministerpräsident und Minister für digitale Transformation der Ukraine. »Eine Delegation von Microsoft wurde heute vom ukrainischen Präsidenten Selenskyj mit dem ‚Friedenspreis‘ ausgezeichnet. Wir sind dankbar, dass ihr auf der hellen Seite der Digitalisierung steht. Microsoft steht für Wahrheit und Frieden.«“ (18i)

Der Autor sprach davon, dass Tech-Giganten wie Amazon und

Microsoft aktiv in Kriege dieser Welt involviert sind.
Kriegsteilnehmer verraten sich durch ihr ausgeprägtes Feindbild.
Ein Feindbild, was die Kriegsführung nicht nur gegenüber dem
äußeren, sondern eben auch dem inneren Feind – das sind wir, Sie
und ich – zum Ausdruck bringt:

„Außerdem hat es [Microsoft] ein System auf Basis künstlicher
Intelligenz entwickelt, das Uhrzeit und Datum russischer
Bombenangriffe protokolliert, um diese Daten bei künftigen
Ermittlungen wegen Kriegsverbrechen nutzen zu können. Es ist
wichtig, dass wir die Grundlage dafür schaffen, das zu tun, was nach
dem Zweiten Weltkrieg an einem Ort wie Nürnberg getan wurde“,
sagte Microsoft-Präsident Brad Smith im Mai.“ (18ii)

Im Zitat oben verraten die Microsoft-„Götter“ jedoch nicht nur ihr
Feindbild. Sie verraten auch, was sie wirklich tun. Wer glaubt
ernsthaft, dass es für die „Protokollierung von Uhrzeit und Datum
russischer Bombenangriffe als Grundlage für ein Nürnberg 2.0“
eines KI-Systems bedarf? Das ist Nonsense. Das KI-System gibt es
allerdings sehr wohl. Doch ist der Zweck ein anderer. Microsoft
befindet sich gleich Amazon permanent im Krieg, richtiger in
Kriegen. Aus dem Corona-Krieg gingen sie ohne Zweifel als Sieger
hervor, doch muss das in späteren Kriegen nicht so bleiben.
Bitte bleiben Sie schön aufmerksam, liebe Leser.

Dieser Artikel erschien zuerst unter dem Titel „**Kriegsrelevant:**
Internet-Dienstleister (<https://peds-ansichten.de/2026/10/ukraine-iran-krieg-cloud-ki-rechenzentren-amazon-microsoft/>)“ auf **Peds Ansichten**
(<https://peds-ansichten.de/>). Er ist unter einer Creative
Commons-Lizenz (**Namensnennung – Nicht kommerziell – Keine**
Bearbeitungen 4.0 International
(<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>))

lizenziert. Unter Einhaltung der Lizenzbedingungen kann er – einschließlich der prominenten Angabe der Primärquelle – gern weiterverbreitet und vervielfältigt werden. Bei Verlinkungen auf weitere Artikel von Peds Ansichten finden Sie dort auch die externen Quellen, mit denen die Aussagen im aktuellen Text belegt werden.



Peter Frey, Jahrgang 1960, ist seit 1965 Dresdner, gelernter Autoschlosser, war LKW-Fahrer, Taxifahrer, selbständig in der IT-Beratung. Nach der Insolvenz war er Sozialhilfeempfänger, Hartz-IV-Empfänger, und studierte schließlich ab 2004 Informationstechnik und ist seit Jahren in Dresden in der Friedensbewegung aktiv. Er will Menschen aufwecken und so zu aktivem, selbst bestimmten, dem kleinen wie dem großen Frieden gewidmeten Handeln bewegen. Seit einigen Jahren ist er hauptberuflich als Administrator tätig und betreibt nebenher den Blog **Peds Ansichten** (<http://peds-ansichten.de>).