LÄNDER–ANALYSEN

Nr. 267 | 02.05.2022

Ukraine–Analysen

- **Cyber-Operationen**
- **Digitalisierung**

Deutsche Gesellschaft für Osteuropakunde | Deutsches Polen-Institut | Forschungsstelle Osteuropa an der Universität Bremen | Leibniz-Institut für Agrarentwicklung in Transformationsökonomien | Leibniz-Institut für Ost- und Südosteuropaforschung | Zentrum für Osteuropa- und internationale Studien (ZOiS) gGmbH

DGO Deutsche Gesellschaft für Osteuropakunde e.V. | Deutsches Polen-Institut | Forschungsstelle Osteuropa | iamo Leibniz-Institut für Agrarentwicklung in Transformationsökonomien | IOS | ZOiS Zentrum für Osteuropa- und internationale Studien Centre for East European and International Studies

ANALYSE

Cyber-Operationen im Kontext des Russland-Ukraine-Krieges 2022

Matthias Schulze (Stiftung Wissenschaft und Politik, Berlin)

DOI: 10.31205/UA.267.01

Zusammenfassung

Im Vorfeld des russischen Einmarsches in der Ukraine befürchteten Analyst:innen schwerwiegende Cyber-Angriffe etwa gegen kritische Infrastrukturen, die so Strom oder Kommunikationsnetze abschalten könnten. Größere destruktive Cyber-Vorfälle sind bisher im Kontext des Krieges nicht eingetreten. Das Cyber-Konfliktbild ist von gezielten Angriffen, Cyber-Spionage und den störenden Tätigkeiten von pro-russischen oder pro-ukrainischen Hacktivist:innen gekennzeichnet. Insgesamt haben diese Angriffe jedoch kaum Effekte im Krieg auf dem Boden und in der Luft. Es werden fünf Gründe für das Ausbleiben schwerwiegenderer Cyber-Angriffe genannt: erstens eine gute Defensive der Ukraine, zweitens eine unklare Datenlage, drittens überzogene Erwartungen an ein »Cyber-Pearl Harbor«-Szenario, viertens staatliche Zurückhaltung und fünftens die hohe wechselseitige Verwundbarkeit.

Lehren aus der Vergangenheit

Im Vorfeld der russischen Invasion in der Ukraine warnten zahlreiche IT-Sicherheitsexpert:innen und Behörden vor großen russischen Cyber-Angriffen auf kritische Infrastrukturen. Die US-amerikanische Cybersecurity and Infrastructure and Security Agency (CISA) forderte etwa am 16. Februar, also eine Woche vor Kriegsbeginn, mit markigen Worten US-amerikanische Unternehmen auf, die »Schilde hochzufahren«. IT-Sicherheitspersonal und Administrator:innen sollten besonders wachsam sein. Auch das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte seit Anfang des Jahres mehrfach vor russischen Cyber-Angriffen auf kritische Infrastrukturen in Deutschland.

Dafür gab es berechtigte Gründe. Russland hatte in der Vergangenheit eine ganze Bandbreite seiner offensiven Cyber-Fähigkeiten zur Schau gestellt: Dazu gehörten Cyber-Spionage wie etwa der Bundestagshack 2015 oder die weltweite Solar Winds-Kampagne 2020, sogenannte Hack & Leak-Operationen zur Beeinflussung der amerikanischen und französischen Präsidentschaftswahlen 2016 und 2017 oder die Störungen mit Milliardenschäden durch den Ransomware-Wurm Not-Petya im Jahr 2017. Als Königsdisziplin gelten dabei physische Effekte durch Cyber-Angriffe: Russische Angreifer:innen deaktivierten einmal im Jahr 2015 und einmal im Jahr 2016 mit der Crashoverride/Industroyer Schadsoftware für wenige Stunden den Strom in der ukrainischen Hauptstadt Kyjiw. Die Ukraine wird seit der Annexion der Krim 2014 auch als »Testgebiet für Cyber-Warfare« bezeichnet, da sie in den letzten Jahren immer wieder mit Ausfällen durch Cyber-Angriffe zu kämpfen hatte. Mit der Invasion der Ukraine gab es also Grund zur Annahme, dass Cyber-Operationen kriegsbegleitend oder gar als Vergeltung gegen westliche Sanktionen eingesetzt werden könnten. Seit 2018 warnen westliche Behörden wie zum Beispiel der deutsche Verfassungsschutz, dass russische Bedrohungsakteure es zunehmend auch auf westliche kritische Infrastrukturen wie Stromnetze abgesehen haben.

Dahinter steht die vorwiegend westlich geprägte Sorge vor einem großen strategischen Cyber-Krieg, bei dem digitalisierte Länder aus der Ferne heruntergefahren werden und durch Stromausfälle die Wirtschaft und die Zivilgesellschaft komplett zum Erliegen komme. Solch ein »Cyber-Pearl Harbor«-Bedrohungsszenario geistert seit den 1990er Jahren durch westliche sicherheitspolitische Diskurse. Allerdings hat es wenig mit der Realität zu tun.

Vorstellung und Wirklichkeit

Der barbarische Krieg in der Ukraine tobt nun schon über zwei Monate. Derzeit muss allerdings konstatiert werden, dass der große Cyber-Krieg (bisher) ausgeblieben ist. Zu beobachten war schon eine ganze Bandbreite verschiedenster Cyber-Operationen, doch diese haben eher eine geringe bis mittlere Intensität. Physische Schäden, länger anhaltende Ausfälle kritischer Infrastrukturen oder gar Stromausfälle hat es bisher kaum gegeben. Allerdings gab es durchaus Versuche, Substationen des Stromnetzes zu sabotieren, die aber nach öffentlich verfügbaren Informationen abgewehrt werden konnten. Der Chef des britischen Nachrichtendienstes GCHQ fasste in einer Rede die Cyber-Lage wie folgt zusammen: »Während einige Leute nach einem ›Cyber-Pearl Harbor‹ gesucht haben, war es nie unsere Auffassung, dass ein katastrophaler Cyber-Angriff ein zentraler Bestandteil der russischen Cyber-Offensive oder ihrer Militärdoktrin ist.« Stattdessen sehe man eine gezielte Kampagne russischer Cyber-Akteure, die ukrainische Regierungs- und Militärsysteme angreifen und stören.

Der Chef der amerikanischen National Security Agency (NSA) und der United States Cyber Com-

mand (USCYBERCOM) Paul M. Nakasone vertrat in einer Kongressanhörung im März eine ähnliche Position. Man habe bisher nur drei bis vier bemerkenswerte russische Cyber-Angriffe gesehen. Er bezog sich dabei auf eine Serie sogenannter Wiper-Attacken gegen ukrainische Behörden, die Daten exfiltriert und gelöscht hatten. Wiper-Schadsoftware löscht Daten auf Systemen und macht so einzelne Rechner bzw. ganze Netzwerke unbrauchbar. Damit wurde die Arbeit ukrainischer Behörden und somit die Reaktionsfähigkeit auf eine Invasion massiv gestört. Das genaue Ausmaß der gelöschten Daten und betroffenen Ministerien ist bisher unklar. Aber der Einsatz von fünf verschiedenen Wiper-Generationen spricht dafür, dass man hier auf größtmögliche Reichweite setzte. Wiper sind in Cyber-Konflikten eher selten. Normalerweise gibt es nur wenige Vorfälle pro Jahr, da diese Schadsoftwarevariante als sehr aggressiv gilt. Auch wenn genaue Analysen und Attribution zum Teil noch ausstehen, ist anzunehmen, dass diese Schadsoftware-Varianten verschiedenen russischen Bedrohungsakteuren zugeschrieben werden können.

Bemerkenswert ist zudem der Hack von KA-SAT Sattelitenmodems der amerikanischen Firma Viasat. Die Modems von Internet-of-Things-Geräten wie Windturbinen erhielten am 24. Februar, also am Tag der Invasion, manipulierte Steuerungsbefehle, was zum Abbruch der Sattelitenverbindung führte, wobei die Turbinen selbst noch funktionierten. Die Kompromittierung erfolgte laut Viasat über eine gekaperte VPN-Verbindung einer Bodenstation und durch einen Wiper (AcidRain), der die Modems löschte. Da der Ausfall insbesondere die Region in Südosteuropa betraf und auch das ukrainische Militär über KA-Sat kommuniziert, liegt ein Zusammenhang mit dem Krieg nahe. Tausende Windkraftanlagen in Europa waren das Kollateralopfer von diesem Cyber-Angriff, darunter auch Anlagen des deutschen Betreibers Enercon. Viasat hat über 27.000 Kunden weltweit, so dass die Dunkelziffer der Betroffenen sicher noch höher ist. Westliche Nachrichtendienste gehen mittlerweile davon aus, dass das Ziel dieser Cyber-Angriffe die Störung der militärischen Kommunikation (Command & Control) der Ukraine war, um einen russischen Einmarsch zu erleichtern. Einiges spricht dafür, dass dies zumindest in den Anfangstagen des Krieges bis zu einem gewissen Grad erfolgreich war.

Neben destruktiven Wiper Angriffen betreibt Russland auch vermehrt Cyber-Spionage. Am 7. März meldete Googles Threat Analysis Group, dass sie vermehrte Aktivität von Phishing und Spionagekampagnen von APT28 (Russland) und Ghostwriter/UNC1151 sehen (vermutlich Belarus). Advanced Persistent Threats (APT) beschreiben Angriffskampagnen, die sich über lange Zeit auf wenige Ziele konzentrieren, um dauerhaften Zugriff zu erhalten. Meist sind dies staatliche Cyber-Operationen mit dem Ziel der Spionage oder der Sabotage von Systemen. APT sind im Vorgehen komplexer und kompetenter als etwa Cyber-Kriminelle oder Hacktivist:innen und sind deswegen gefährlicher. Auch die russische IT-Sicherheitsfirma Kaspersky meldete am 10. März, dass man seit Anfang Februar eine erhöhte Aktivität von Command & Control (C2) Infrastruktur der APT Gamaredon sehe. Gamaredon (auch Primitive Bear genannt) wird dem russischen Geheimdienst FSB zugeschrieben. Cyber-Angreifer steuern ihre Schadsoftware über eine derartige C2-Infrastruktur aus der Ferne und nutzen die Systeme auch zur automatisierten Verbreitung von Phishing-Mails und für andere Komponenten von Cyber-Operationen.

Zwei Wochen später wurde berichtet, dass die vermutlich russische APT Sandworm mittels ASUS-Routern ein neues Botnet (genannt Cyclops Blink) aufbaute, vermutlich ebenfalls als C2-Infrastruktur für eine neue Angriffswelle. Sandworm wird dem russischen Militärgeheimdienst G(R)U zugeschrieben und griff in der Vergangenheit auch westliche Ziele an. Dies kulminierte schließlich in der Warnung von US-Präsident Joe Biden am 21. März, dass man »aktuelle Informationen« habe, dass Russland Optionen für Cyber-Angriffe gegen den Westen prüfe. Am 31. März tauchte schließlich ein Bericht in ungarischen Medien auf, welcher von einer umfassenden Kompromittierung des ungarischen Außenministeriums durch russische Spionagekampagnen sprach. Diese Kompromittierung gehe teils Jahre zurück, da es Ungarn aufgrund fehlender Kompetenzen und politischem Willen nicht gelang, die Angreifer permanent aus den Netzwerken zu werfen. Ungarische Insider berichten von erhöhter Aktivität der Angreifer im Januar. Sie hätten über das ukrainische Außenministerium Fernzugriff auf sensible Datenkanäle der EU und NATO bekommen, während zeitgleich diverse NATO- und EU-Krisenkonferenzen im Hinblick auf den bevorstehenden Krieg in der Ukraine tagten.

Diese gezielteren Aktivitäten russischer Nachrichtendienste entsprechen ungefähr dem, was man auch in der Vergangenheit, etwa mit Hacks gegen diverse Außenministerien (darunter auch das deutsche), beobachten konnte. Diese Angriffe sind eher leise und auf wenige Ziele fokussiert, aber dafür auf dauerhaften Zugang ausgelegt. Nur dadurch lassen sich wertvolle nachrichtendienstliche Informationen extrahieren. Da Russland Informationen über die westliche Positionierung innerhalb der EU und NATO, etwa bei der Unterstützung von Sanktionen oder Waffenlieferungen sucht, ist Cyber-Spionage das Mittel der Wahl. Das Ziel dürfte mittel- bis langfristig sein, Keile zwischen die westlichen Staaten zu treiben, um die Sanktionen oder die Militärhilfe der Ukraine zurückzufahren. Darin dürfte der größte Wert von Cyber-Spionage im Kontext des Krieges in der Ukraine liegen.

Cyber-Scharmützel

Neben verborgener staatlicher Aktivität ist die digitale Dimension des Ukraine-Krieges von einer Vielzahl kleinerer Scharmützel zwischen pro-russischen und pro-ukrainischen Hacktivist:innen gekennzeichnet. Weltweit schlossen sich IT-Expert:innen und Hacker:innen dem ukrainischen Aufruf zur Bildung einer IT-Army an. Mittlerweile haben sich um die 70 Hacktivist:innengruppen, von GhostSec, Anonymous, Network Battalion 65, aber auch Cyberkriminelle wie Ransomware-Gruppen auf die ukrainische Seite geschlagen. Es gibt aber auch Gruppen, die Russland unterstützen wie Conti, KillDisk oder Xaknet, die bereits Cyber-Angriffe auf westliche Ziele gestartet haben. Der Begriff Hacktivist beschreibt den losen Zusammenhang global verteilter Hacker:innen, die sich ad hoc für gemeinsame Aktivitäten verbünden, aber nicht zentral gesteuert werden.

Ein Großteil ihrer Aktivität ist insbesondere durch zahlreiche Distributed Denial of Service-Angriffe (DDoS) gekennzeichnet. Immer wieder werden russische Websites wie vom Kreml, von Ministerien, Botschaften, von Geheimdiensten wie dem FSB, Banken, aber auch russischen Staatsmedien temporär überlastet. DDoS-Angriffe dauern meist nur kurz an und sind reversibel. Sie werden auch immer wieder gegen ukrainische Internetdienstanbieter (ISP) gerichtet, was teilweise zu partiellen Konnektivitätsverlusten in einzelnen Regionen führt. Daneben gibt es auch zahlreiche Website-Defacement-Angriffe, bei denen Anti-Kriegsbotschaften und die berühmte »Guy Fawkes«-Maske auf Websites platziert werden.

Daneben wenden Hacktivist:innen eine Hack & Leak-Strategie gegen Russland an. In Netzwerke und Server von Ministerien, Behörden und Unternehmen wird eingebrochen, deren Daten gestohlen und zum Download zur Verfügung gestellt. Hacktivist:innen behaupten unter anderem in die folgenden Institutionen eingebrochen zu sein: die russische Zentralbank, die russische Weltraumbehörde, Gazprom, Rosneft Deutschland (das BKA ermittelt), Transneft, die Medienregulationsanstalt Roskomnadzor, Rüstungsunternehmen wie Rostec, Tetraedr und Kronshtadt, Nuklearforschungsinstitute sowie Medien. Diese Leaks beinhalten auch wertvolle strategische Informationen: so wurden die Namen und Dienstnummern von den über 120.000 russischen Soldat:innen in der Ukraine veröffentlicht. Zudem wurden detaillierte Informationen über 620 Agenten des russischen Geheimdienstes FSB veröffentlicht. Diese Daten sind für westliche und weitere Nachrichtendienste ein Fundus und dürften allesamt übersetzt und ausgewertet werden, um nachrichtendienstliche Vorteile zu erlangen. Ein Beispiel hierfür ist die Enttarnung von Geheimdienstagenten durch die Korrelation von Handydaten und Essensbestellungen bei Lieferdiensten durch die NGO Bellingcat.

Daneben gibt es noch eine ganze Reihe von Hacks mit diversen Zielen, etwa um die russische Internetzensur zu umgehen und der russischen Bevölkerung ein anderes Bild des Krieges zu zeigen. Ziel solcher »Informationsoperationen« ist es, die Informationshoheit der Staatspropaganda in Russland zu durchbrechen. So hackte Anonymous mit dem Internet verbundene Drucker, um Anti-Kriegsflugblätter zu drucken. Überwachungskameras wurden gehackt und in ihre Videofeeds Anti-Kriegsbotschaften eingebettet. Das russischsprachige soziale Netzwerk VK wurde angeblich gehackt, um ähnliche Informationen zu verbreiten. Vieles lässt sich nur schwer verifizieren. Zur Umgehung von Staatspropaganda in Russland werden zudem auch andere Mittel genutzt wie zum Beispiel Email-Spam an russische Email-Adressen, SMS- und WhatsApp-Spam über ein eigens von Hacktivist:innen entwickeltes Tool, sowie klassische Anrufe bei russischen Telefonnummern, um vom Krieg zu berichten. Es gibt zudem Berichte, dass Live-Streams von russischen Fernsehsendern gehackt wurden, um pro-ukrainische Botschaften zu zeigen. Wie erfolgreich diese Initiativen sind, ist schwer abzuschätzen.

Es gibt zudem erste Berichte, dass auch Ransomware eingesetzt wird. Ransomware verschlüsselt Daten auf Zielsystemen und macht sie für ihre Besitzer:innen unbrauchbar. Ransomware ist ein weitverbreitetes Mittel von Cyber-Kriminellen, um Lösegeld zur Wiederfreigabe der verschlüsselten Daten zu erpressen. Die Systeme der russischen Firma Miratorg, einem der größten Fleischproduzenten des Landes, wurden angeblich verschlüsselt, ohne dass eine Lösegeldzahlung abgesetzt wurde. Zudem behauptete die »Belarussian Cyber Guerilla«, das Logistiknetzwerk der belarusischen Eisenbahn mit Ransomware lahmgelegt zu haben, um die Verlegung russischer Truppen in Belarus zu verhindern. Allerdings gab es auch physische Sabotageakte entlang der belarusischen Eisenbahnlinien, so dass unklar ist, ob Schadsoftware oder brennende Kabelschächte die Ausfälle auslösten. Diverse Ransomware-Gruppen, darunter Stormous oder auch Conti sind auf russischer Seite in den Konflikt eingestiegen. Conti behauptet etwa für einen Ransomware-Angriff auf das deutsche Windenergieunternehmen Nordex im April 2022 verantwortlich zu sein. Conti war in der Vergangenheit für über 800 Ransomware-Vorfälle weltweit verantwortlich, die meisten in den USA. Die Gruppe wurde aber selbst Opfer eines Datenlecks: einer ihrer Mitarbeitenden war Ukrainer und veröffentlichte große Teile der internen Jabber-Kommunikation der Gruppe, aus der Kontakte zum russischen FSB sowie diverse Managementprobleme sichtbar wurden. Dieses Datenleck allein erlaubt einen einmaligen Einblick in das verborgene Geschäftstreiben von Cyber-Kriminellen.

Zusammenfassend kann man sagen, dass all diese Vorfälle eher kleinere Störungen sind, eine recht unkoordinierte Taktik der tausend Nadelstiche. Sie beeinflussen die Ereignisse am Boden nicht wirklich. Allerdings können die zahlreichen Datenlecks mittel- bis langfristig Russland schaden. Die schiere Summe der veröffentlichten Daten dürften ein Fundus für Nachrichtendienste weltweit darstellen und seltene Einblicke in das Innenleben des geheimniskrämerischen russischen Staates geben. Für sich genommen erzielt die Vielzahl der Vorfälle aber kaum militärische Effekte und beeinflusst Geschehnisse auf dem physischen Schlachtfeld kaum.

Erklärungsversuche

In der akademischen Community entbrannte eine Diskussion hinsichtlich der Frage, wie diese Befunde einzuordnen sind. Warum ist der große Cyber-Krieg ausgeblieben? Warum gab es bisher keine größeren Stromausfälle? Es gibt eine Reihe konkurrierender Hypothesen.

Erstens scheint plausibel, dass die ukrainische Cyber-Abwehr sehr erfolgreich arbeitet und bisher das Schlimmste verhindern konnte. So konnte das ukrainische Computer Emergency Response Team (CERT) am 8. April einen Stromausfall verhindern, indem eine Schadsoftware namens Industroyer2 rechtzeitig identifiziert und unschädlich gemacht wurde. Industroyer2 basiert auf einer Schadsoftware, die bereits 2016 in Kyjiw kurz den Strom ausschaltete. Ukrainische Cyber-Spezialist:innen studierten diesen Angriff intensiv und lernten daraus, was letztlich sinnvoll für die Vorbereitung gewesen sein dürfte. Die Ukraine gilt seit 2014 als »Testgebiet für Cyber-Krieg« und hat seitdem, wohl wie kein zweites Land auf der Welt, praktische Erfahrung in der Abwehr von Cyber-Angriffen machen können. Zudem erhält die ukrainische Cyber-Abwehr schlagkräftige Unterstützung von weltweiten IT-Sicherheitsunternehmen wie ESET und Microsoft, welche ihre Informationen zu laufenden Angriffskampagnen mit der Ukraine teilen. Auch die USA und die NATO (über das Cyber-Kompetenzzentrum in Tallinn) teilen sogenannte »threat intelligence« (taktische Informationen zu laufenden Operationen) mit der Ukraine, um besser gegen laufende Angriffe gewappnet zu sein.

Zweitens ist anzunehmen, dass wir das wahre Ausmaß der bisherigen Cyber-Angriffe durch den »Nebel des Krieges« nicht wahrnehmen können. Russland kommuniziert in der Regel eigene Cyber-Operationen bzw. Cyber-Vorfälle im eigenen Land nicht. Außerdem gibt es, anders als in westlichen Ländern, auch keine Berichtspflichten für Unternehmen. Insofern ist es möglich, dass größere Cyber-Sicherheitsvorfälle im Hintergrund stattfanden und bisher nicht öffentlich wurden.

Eine dritte Hypothese, die insbesondere in der akademischen Cyber-Konfliktforschung vertreten wird, ist, dass die Erwartung eines desaströsen Cyber-Angriffs schlichtweg auf einer Fehlcharakterisierung von »Cyber War« in westlichen Ländern basiert. In der akademischen Literatur wird schon lange der Mythos entzaubert, dass Cyber-Angriffe eine Revolution der Kriegsführung bedeuten. Das hypothetische »Cyber-Pearl Harbor«-Szenario, ein Industrieland aus der Ferne auszuschalten, hat wenig mit der operativen Wirklichkeit von Cyber-Operationen zu tun. Cyber-Angriffe unterliegen zahlreichen Einschränkungen wie langen Vorbereitungszeiten, einer gewissen Fehlerrate sowie der Ungewissheit von Effekten. Generell ist es sehr schwierig und zeit- und ressourcenintensiv, physische Effekte wie einen landesweiten Stromausfall auszulösen. Deswegen sind derartige, hochintensive Cyber-Angriffe extrem selten. Die Charakteristika von Cyber-Vorfällen haben trotz ihres militärischen »Framings« als »Cyber-Angriff« wenig mit Krieg zu tun. Krieg ist durch massive Gewalt, Tod und Zerstörung gekennzeichnet. Die meisten Cyber-Angriffe sind in ihren Effekten weitaus niedrigschwelliger und vor allem reversibel. Temporäre Störungen etwa durch Ransomware oder DDoS Angriffe, Cyber-Kriminalität, Hack & Leak-Operationen und Spionage bestimmen das Cyber-Konfliktbild. Und dies repräsentiert auch die Mehrzahl der dokumentierten Cyber-Vorfälle um den Ukrainekrieg.

Die vierte Hypothese leitet sich daraus ab: Es ist schwierig, mit Cyber-Angriffen physische Effekte hervorzurufen. Einfacher ist es, dies mit konventionellen Mitteln zu tun. Da Russland ohnehin mit konventionellen Truppen in der Ukraine präsent ist, können Strom oder Internetausfälle auch einfach durch Raketenbeschuss oder das Kappen von Leitungen hervorgerufen werden. Das ist einfacher, billiger und schneller. Aber vor allem ist die Erfolgswahrscheinlichkeit verglichen mit einer Cyber-Operation höher. Insofern argumentieren einige Forschende, dass Cyber-Operationen im Kontext eines Bodenkrieges eher ungeeignet sind. Stattdessen eignen sie sich weitaus besser für den Wettbewerb zwischen Nachrichtendiensten. Cyber-Operationen haben viel mehr Ähnlichkeiten mit dem subversiven Vorgehen von Geheimdiensten, das etwa auf die verborgene Beschaffung von Information und die subversive Beeinflussung von Diskursen in anderen Gesellschaften durch sogenannte »aktive Maßnahmen« abzielt. Dies ist im Übrigen auch die primäre Charakterisierung von Cyber-Aktivitäten in autoritären Regimen wie China und Russland: Dort wird nicht von Cyber-Krieg gesprochen, sondern vom übergeordneten Konzept des Informationskrieges. Cyber-Operationen sind darin nur eine Subkategorie und damit nur ein Werkzeug von vielen, was dem Ziel der Informationsüberlegenheit und Kontrolle dienen soll.

Eine fünfte Hypothese ist, dass die wechselseitige Interdependenz von vernetzten Systemen über das Internet zu Zurückhaltung auf staatlicher Seite führt. Staaten schrecken vor destruktiven Cyber-Angriffen mit langan-

haltenden Schäden zurück, weil sie selbst abhängig und verwundbar sind. Die meisten Staaten nutzen ähnliche Hard- und Software (zum Beispiel Windows-Betriebssysteme, Android- oder iPhone-Smartphones oder Open-Source-Bibliotheken in Webservern). Es werden immer wieder Schwachstellen veröffentlicht, die ein Großteil aller mit dem Internet verbundenen Systeme betreffen, wie etwa Heartbleed (2014) oder Log4J (2021). Darüber sind alle Staaten, die entsprechende Software nutzen, gleichermaßen angreifbar. Wenn Russland kritische Infrastrukturen im Ausland mit einer Schadsoftware angreift, die zum Beispiel die Log4J-Schwachstelle ausnutzt, ist zu befürchten, dass etwa die USA in Russland Ähnliches tun könnten. Russland beschwerte sich in der Vergangenheit, dass das United States Cyber Command in russischer kritischer Infrastruktur aktiv ist. Auch Russlands Bemühungen im Bereich der IT souverän zu werden und somit auf westliche Dienste zu verzichten, sind in diesem Licht zu interpretieren. Es existiert also bei destruktiven Cyber-Angriffen hoher Intensität eine Art Gleichgewicht des Schreckens, zumindest zwischen der NATO und Russland.

Zudem ist es nicht unwahrscheinlich, dass ein schwerwiegender Cyber-Angriff gegen westliche Staaten rechtlich als »bewaffneter Angriff« interpretiert werden könnte und den NATO-Verteidigungsfall nach Artikel 5 auslöst. Das dürfte nicht in Russlands Interesse sein. Zurückhaltung wird auch durch die schwere Kontrollierbarkeit von Cyber-Angriffen befördert: Ein außer Kontrolle geratener Angriff könnte auch Drittparteien in den Konflikt ziehen. Die Effekte von Cyber-Angriffen gegen weitverbreitete Systeme sind mitunter schwer zu kontrollieren und können wie ein Bumerang wirken, der ungeplante Kaskadeneffekte auch in eigenen Systemen auslöst. Der russische Not-Petya-Angriff löschte weltweit Daten, darunter auch russischer Firmen, obwohl er sich ursprünglich gegen ukrainische Systeme gerichtet hatte. Im konkreten Falle von Russlands Krieg gegen die Ukraine gibt es Evidenz für diese Interdependenzthese: Es gibt etwa Hinweise, dass die russische Militärkommunikation teils unverschlüsselt über öffentliche Netze wie das Internet oder auch das Mobilfunknetz läuft. Wenn Russland diese Dienste per Cyber-Angriff ausschalten würde, könnte es selbst nicht mehr kommunizieren.

Fazit

Der brutale Krieg in der Ukraine tobt nun schon seit mehr als zwei Monaten. Insofern ist es zu früh für weitreichende Schlussfolgerungen. Cyber-Operationen sind letztlich Werkzeuge staatlichen Handelns, die an politische Ziele angepasst werden müssen. Ändert sich der Fokus und das Ziel des Krieges, so ist auch eine Veränderung in der Nutzung von Cyber-Operationen wahrscheinlich. Vieles deutete darauf hin, dass Russland einen kurzen Enthauptungsfeldzug plante und dass folglich Cyber-Operationen auf dieses Ziel hin angepasst wurden. Darauf deutet die koordinierte, taktische Verwendung von Wipern in der Frühphase des Krieges hin. Ändert sich das Kriegsziel zu einem langwierigen und strategischen Zermürbungskrieg, der sich auch gegen Zivilist:innen wendet, dann dürften auch Cyber-Operationen vermehrt diesem Zweck folgen. Insofern sind größere, strategische Cyber-Operationen etwa gegen Stromnetze in der Ukraine nicht mehr auszuschließen. Es gibt zudem vermehrt Hinweise, dass Russland auch Cyber-Operationen gegen den Westen ausweitet, etwa gegen kritische Infrastrukturen im Energiesektor wie Windenergie-Betreiber. Wenn Deutschland und Europa die Abhängigkeit vom russischen Gas mithilfe von Windenergie reduzieren wollen, dann dürften diese Industrien somit auch in den Fokus russischer Attacken geraten. Auch die amerikanische Cyber-Behörde CISA (Cybersecurity and Infrastructure Security Agency) warnte jüngst erneut, dass sich russische Hacker:innen für industrielle Steuerungsanlagen im Bereich Energieversorgung interessieren und dafür Schadsoftware entwickeln. Insofern ist es wahrscheinlich, dass sich der Westen auf einen länger anhaltenden Cyber-Konflikt mit Russland einstellen muss und dass das vormals ukrainische Testlabor von Cyber-Aktivitäten nun auch auf westliche Staaten ausgeweitet wird.
Stand: 25. April 2022

Über den Autor
Dr. *Matthias Schulze* ist der stellvertretende Leiter der Forschungsgruppe Sicherheitspolitik der Stiftung Wissenschaft und Politik. Er forscht zu Cyber-Konflikten, Spionage und Cyber-Kriminalität. Er betreibt einen Blog und Podcast zum Thema unter www.percepticon.de.

Lesetipps

- David Sanger (2018) The perfect weapon, War, sabotage, and fear in the cyber age, New York, Melbourne, London, Crown Publishers; Scribe.
- Andy Greenberg (2019) Sandworm, A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers, New York, Doubleday, 2019.
- Nicu Popescu & Stanislav Secrieru (2019) Hacks, leaks and disruptions. Russian cyber strategies. Challiot Paper No. 148, October 2018, European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

- Matthias Schulze (2020) Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations, in: Jančárková, T./Lindström, L./Signoretti M./Tolga G. Visky (Eds), 2020 12th International Conference on Cyber Conflict, NATO CCDCOE Publications, Tallinn. https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf.
- Lennart Maschmeyer (2021) "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations", International Security, Vol. 46, No. 2, 2021, 51–90.
- Microsoft (2022) Special report Ukraine. An overview of Russia's cyberattack activity in Ukraine. 27.04.2022, abrufbar unter https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

DOKUMENTATION

Cybervorfälle im Verlauf von Russlands Krieg gegen die Ukraine (Februar bis April 2022)

Tabelle 1: Cybervorfälle im Verlauf von Russlands Krieg gegen die Ukraine (Februar bis April 2022)

Datum des Cybervorfalls	Kurzbeschreibung des Cybervorfalls
14.01.2022	Die Websites des ukrainischen Regierungskabinetts, von sieben Ministerien und des nationalen Notfallservice sind vorübergehend nicht erreichbar. Eine Botschaft wird platziert: »Habt Angst und erwartet das Schlimmste«.
17.02.2022	Website des Außenministeriums Russlands ist vorübergehend offline.
17.02.2022	Sabotage von Glasfaserleitungen in dem von der Ukraine kontrollierten Gebiet der Region Luhansk reduziert die Leistungsfähigkeit des Mobilfunknetzwerkes von Vodafone um 70 Prozent.
18.02.2022	Dutzende von Computern in zwei Regierungsbehörden der Ukraine wurden mit Whispergate-Schadsoftware gelöscht.
23.02.2022	Bericht von Trend Micro zu einem neuen Botnet, genannt Cyclops Blink. Hauptzweck des Botnets ist es, eine Infrastruktur für weitere Angriffe auf hochwertige Ziele in der Ukraine aufzubauen.
23.02.2022	Die IT-Firma ESET entdeckte eine neue Wiper-Malware (Hermetic Wiper), die in der Ukraine verwendet wurde. ESET-Telemetrie zeigt, dass sie auf Hunderten von Geräten im Land installiert wurde.
23.02.2022	Die Websites der Verteidigungs-, Außen- und Innenministerien der Ukraine wurden mit DDoS Angriffen überlastet. Darüber hinaus löschte Hermetic Wiper Daten auf Hunderten von Computern in der Ukraine, Lettland und Litauen.
25.02.2022	Das Anonymous-Kollektiv ist offiziell in den Cyberkrieg gegen die russische Regierung eingetreten.
26.02.2022	Hacktivst:innen von DDoSecrets veröffentlichen 200 GB an Daten des belarusischen Verteidigungsunternehmens Tetraedr.
26.02.2022	Die Ukraine rekrutiert Hacktivist:innen (IT-Armee der Ukraine) und definiert Ziellisten von Domains, die über »alle Vektoren und mit DDoS« angegriffen werden sollen.
27.02.2022	Das Anonymous-Network Battalion 65 veröffentlicht Dateien des russischen Instituts für Nuklearforschung.
28.02.2022	Das Ghostsec Kollektiv behauptet, es verfügt über einen Remote-Zugriff auf den NICA-Teilchenbeschleuniger des russischen Kernforschungsinstituts.
01.03.2022	Microsoft meldet, dass ukrainische Einrichtungen kurz vor der Invasion mit Foxblade Wiper angegriffen wurden.
01.03.2022	ESET-Forscher:innen entdecken einen neuen Wiper, der ukrainische Organisationen befällt (IsaacWiper).
01.03.2022	Die Ukrainska Prawda veröffentlicht Daten von 120.000 russischen Soldat:innen, die in der Ukraine kämpfen.
01.03.2022	Sberbank, eine russische staatliche Bank, wurde gehackt. Webserver-Daten wurden veröffentlicht.

Fortsetzung auf der nächsten Seite

Tabelle 1: Cybervorfälle im Verlauf von Russlands Krieg gegen die Ukraine (Februar bis April 2022) (Fortsetzung)

Datum des Cybervorfalls	Kurzbeschreibung des Cybervorfalls
02.03.2022	Flüchtlingsmanagementsysteme von NATO-Ländern wurden möglicherweise von der Ghostwriter APT angegriffen.
03.03.2022	Der niederländische Militärgeheimdienst informiert über eine Phishing-Kampagne der Sandworm-Gruppe, die auf Internetroutern von kleinen und mittelständigen Unternehmen abzielte.
03.03.2022	Ein Leak des Quellcodes der Schadsoftware Trickbot deutet darauf hin, dass diverse kriminelle Cyber-Gruppen (Wizard Spiders, Maze, Conti, Diavol, Ryuk) mit dem russischen Geheimdienst FSB kooperieren.
04.03.2022	Der deutsche Verfassungsschutz warnt vor vermehrter Phishing-Aktivität.
06.03.2022	Das Hackerkollektiv Ghostsec behauptet, Serverdateien vom russischen Institut für Nuklearforschung gestohlen zu haben.
07.03.2022	Forscher:innen von Googles Threat Analysis Group registrieren eine Zunahme von Spionage- und Phishing-Kampagnen von Bedrohungsakteuren wie Fancy Bear / APT 28 (GRU) und Ghostwriter / UNC1151 (Belarus)
08.03.2022	Eine Gruppe von Hacktivist:innen sagt, dass sie auf über 400 Überwachungskamera-Feeds in Russland zugreifen kann und Antikriegsbotschaften platziert hat.
10.03.2022	DDoSecrets veröffentlicht 360.000 Dateien von Roskomnadsor, der russischen Agentur, die für die Überwachung und Kontrolle russischer Massenmedien verantwortlich ist.
10.03.2022	Kaspersky meldet, dass die Gamaredon APT-Gruppe seit Anfang Februar zunehmend aktiver geworden ist.
13.03.2022	Rosneft Deutschland GmbH wurde gehackt, dabei wurden 20 TB Daten gestohlen. Das BKA ermittelt.
14.03.2022	CaddyWiper löscht Daten in ukrainischen Netzwerken.
14.03.2022	Squad303 behauptet, automatisiert 20 Millionen SMS und WhatsApp-Nachrichten sowie E-Mails an zufällig ausgewählte Russ:innen geschickt zu haben.
16.03.2022	Ein Video wurde über Facebook, VK, Telegram und YouTube geteilt, in dem eine seltsam bewegungslose Version von Selenskyj ukrainische Truppen bat, die Waffen niederzulegen. Es handelte sich dabei um ein mittels Algorithmen manipuliertes Deepfake-Video.
17.03.2022	Eine neue Variante des Cyclops-Blink-Botnets wird entdeckt. Hauptzweck des Botnets ist es, eine Infrastruktur für weitere Angriffe auf hochwertige Ziele aufzubauen. Cyclops-Blink wird mit der APT-Sandworm in Verbindung gebracht, die wiederum mit dem russischen G(R)U assoziiert wird.
17.03.2022	DDoSecrets hat 79 Gigabyte E-Mails von Omega, der Forschungs- und Entwicklungsabteilung von Transneft, Russlands staatlich kontrolliertem Pipeline-Unternehmen, veröffentlicht.
17.03.2022	In das Node-IPC JavaScript-Modul für die Interprozess-Kommunikation, das Millionen von Entwickler:innen beim Entwickeln von Software verwenden, wurde ein manipulierter Code eingefügt. Der neue Code löscht alle Dateien auf Entwicklersystemen, die in Russland und Belarus genutzt werden.
18.03.2022	Chinesische Staatshacker:innen haben es auf die ukrainische Regierung abgesehen. APT31/ Mustang Panda hat auch Phishing-Angriffe gegen europäische Organisationen platziert.
21.03.2022	Der US-amerikanische Präsident Biden warnt, dass Russland Optionen für neue Cyber-Angriffe sondiert.
22.03.2022	Das russische Fleischproduktionsunternehmen Miratorg wurde von einem Cyber-Angriff betroffen. Die IT-Systeme des Unternehmens wurden verschlüsselt.
24.03.2022	Das Anonymous-Kollektiv hat die Zentralbank Russlands gehackt. Mehr als 28 GB an Daten wurden veröffentlicht.
25.03.2022	Laut einem Bericht des Computer Emergency Response Team der Ukraine (CERT-UA) wurden im Zeitraum zwischen dem 15. und 22. März insgesamt 60 Cyber-Angriffe auf staatliche und lokale Behörden, den Finanz-, Energie-, Sicherheits- und Verteidigungssektor sowie kommerzielle Organisationen entdeckt.
26.03.2022	Die Gruppen Killnet und Xaknet behaupten, die polnische Investitions- und Handelsagentur gehackt und 20 GB an Daten gestohlen zu haben.
27.03.2022	Cyber-Angriffe gegen NATO-Länder, die von chinesischen IP-Adressen stammen, haben um 116 Prozent zugenommen, so ein Bericht der Firma Checkpoint.
28.03.2022	Der ukrainische Militärgeheimdienst veröffentlicht eine Liste mit 620 russischen FSB-Mitarbeitenden.
28.03.2022	Das ukrainische CERT warnt davor, dass die mit Belarus in Verbindung gebrachte Ghostwriter APT-Gruppe staatliche Einrichtungen in der Ukraine angreift.
28.03.2022	Anonymous hackt das Rüstungsunternehmen Rostproekt und veröffentlicht dessen Emails.
29.03.2022	Die Hacking-Gruppe Network Battalion 65 beansprucht die Verantwortung für einen Cyberangriff gegen MOSEKSPERTIZA.
29.03.2022	Das russische Außenministerium prangert die Cyber-Aggression des »kollektiven Westens« an und droht mit Vergeltung.

Fortsetzung auf der nächsten Seite

Tabelle 1: Cybervorfälle im Verlauf von Russlands Krieg gegen die Ukraine (Februar bis April 2022) (Fortsetzung)

Datum des Cybervorfalls	Kurzbeschreibung des Cybervorfalls
30.03.2022	Russische Hacker:innen konnten sich Zugang zum internen Netzwerk des ungarischen Außenministeriums verschaffen.
30.03.2022	Das Satellitenkommunikationsunternehmen Viasat gibt am 24. Februar eine Erklärung in Bezug auf den Hack von KA-SAT-Satelliten ab. Eine Bodenstation wurde falsch konfiguriert, um manipulierte Befehle auszugeben, was zu einer Abschaltung von Satellitenmodems führte.
30.03.2022	Die Threat Analysis Group von Google schreibt, dass immer mehr Bedrohungsakteure Russlands Krieg gegen die Ukraine ausnutzen, um die osteuropäischen und NATO-Länder, einschließlich der Ukraine, mit Phishing- und Malware-Angriffen zu belegen.
31.03.2022	Das Xaknet-Team veröffentlicht Daten aus dem ukrainischen Außenministerium. Sie bekräftigen damit, dass sie die russische Regierung unterstützen.
02.04.2022	Der deutsche Windkraftanlagenhersteller Nordex wurde am 31. März von einem Cyber-Angriff betroffen. Das Eindringen wurde früh erkannt. Systeme wurden heruntergefahren, um die Ausbreitung zu vermeiden.
02.04.2022	Die Blue Hornet-Gruppe veröffentlicht Daten von APT-28, insbesondere zu dessen Mitgliedern, Namen, E-Mail-Adressen, Kennwörter, Konten bei sozialen Medien, Telefonnummern und Aliase.
04.04.2022	Anonymous veröffentlicht Dienstränge und Passdetails der russischen Soldat:innen, die in der 64. Motorisierten Schützenbrigade dienen, die den Kyjiwer Vorort Butscha vor dem 31. März besetzt hielt.
04.04.2022	Die IT-Firma Sektrio verzeichnet eine gesteigerte russische Cyberaktivität: IT-Sicherheitsprogramme (sog. Honeypots) verzeichnen in Westeuropa mehr Tätigkeiten, insbesondere im Bereich Energieunternehmen, Ölpipeline-Unternehmen, erneuerbare Energien, industrielle Fertigung & Verteidigung.
04.04.2022	Anonymus behauptet, für die Veröffentlichung von Daten von 120.000 russischen Soldat:innen verantwortlich zu sein, die im März von Ukrainska Prawda veröffentlicht wurden. Anonymous veröffentlicht dabei weitere Details.
05.04.2022	Das ukrainische CERT entdeckt eine neue Angriffskampagne der Armageddon APT gegen ukrainische Staatseinrichtungen.
05.04.2022	Die Stormous Ransomware Gruppe droht Frankreich mit Angriffen aufgrund seiner Äußerungen gegen Russland.
06.04.2022	Das FBI erlangt Zugriff auf ein Cyclops Blink-Botnetz, indem es physisch auf die Command-and-Control-Infrastruktur zugreift. Infizierte PCs werden bereinigt. Das Botnetz wird der Gruppe Sandworm zugeschrieben.
07.04.2022	Microsoft blockiert Cyber-Angriffe gegen ukrainische Einrichtungen, die von der russischen APT Strontium (G(R)U) ausgehen.
08.04.2022	Das Anonymus-Kollektiv erlangt nach eigenen Angaben Zugang zum Überwachungskamerasystem des Kremls.
08.04.2022	Es werden Cyber-Angriffe und Sabotage gegen belarusische Eisenbahninfrastruktur registriert, um die Bewegung russischer Truppen und militärischer Ausrüstung in die Ukraine zu stören.
08.04.2022	CaddyWiper-Schadsoftware wurde bei einem ukrainischen Energieversorger platziert und später entdeckt.
09.04.2022	Das russische Raumfahrtprogramm zur Erkundung des Mondes Luna-Glob (Roskosmos) wurde gehackt. Daten über dessen Umlaufbahn wurden veröffentlicht.
12.04.2022	Das CERT-UA meldet, dass ein Cyber-Angriff gegen eine Umspannanlage des elektrischen Versorgungsnetzes verhindert wurde. Der Industroyer2 genannte Angriff weist Ähnlichkeiten zu früheren Vorfällen (etwa dem im Jahr 2016) auf und wurde zudem mit CaddyWiper kombiniert, um die Wiederherstellung der Systeme zu erschweren.
13.04.2022	Denial-of-Service-Attacken sorgen während einer Rede des ukrainischen Präsidenten Selenskyj für Störungen bei finnischen Regierungswebseiten. Der Ausfall ereignete sich gleichzeitig mit Erwägungen eines finnischen NATO-Betritts am selben Tag.
13.04.2022	Die IT-Firma Mandiant warnt vor Cyber-Angriffen gegen industrielle Steuerungssysteme der Firma Schneider Electric mittels der Pipedream-Schadsoftware.
14.04.2022	Die Ransomware-Gruppe Conti hat die Verantwortung für den zuvor von NORDEX offengelegten »Cyber-Sicherheitsvorfall« übernommen.
15.04.2022	Cyber-Angriff gegen das deutsche Unternehmen Windtechnik AG in Bremen. Alle Systeme wurden heruntergefahren, um den Vorfall einzudämmen.
16.04.2022	Russische Fernseh- und Radiosender wurden gehackt.
17.04.2022	Das Ghostsec-Hacking-Team veröffentlicht 140 MB an Daten des größten Domain-Anbieter (.ru) in Russland.

Fortsetzung auf der nächsten Seite

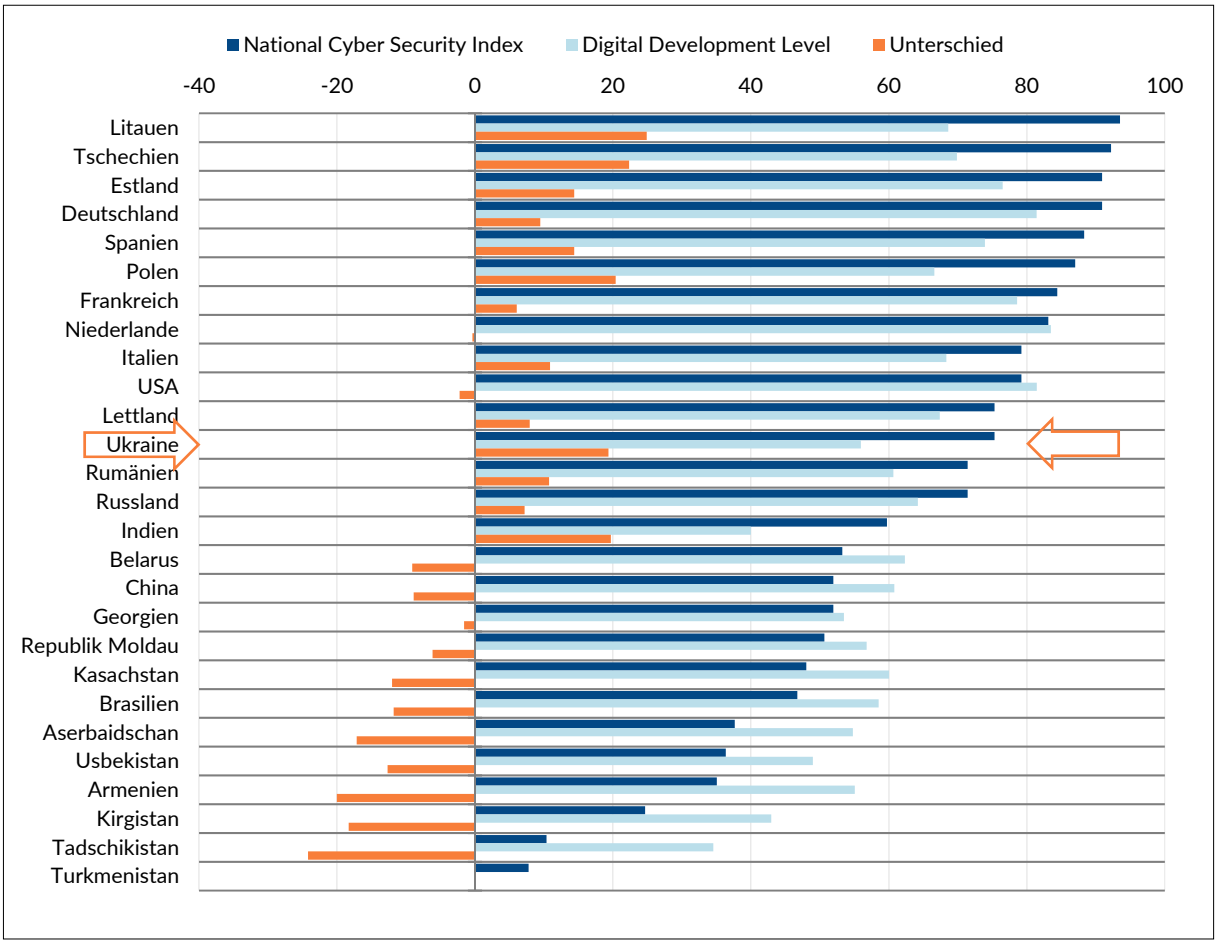
Tabelle 1: Cybervorfälle im Verlauf von Russlands Krieg gegen die Ukraine (Februar bis April 2022) (Fortsetzung)

Datum des Cybervorfalls	Kurzbeschreibung des Cybervorfalls
17.04.2022	Die russische Hacktivist:innen-Gruppe Killnet behauptet, das US-amerikanische Energieunternehmen Devon Energy mit Revil Ransomware angegriffen zu haben.
18.04.2022	Das ukrainische Computer Emergency Response Team (CERT) warnt vor einer neuen Angriffskampagne.
19.04.2022	Anonymous hat über die Onlineplattform Ddosecrets 87.500 neue E-Mails (107 GB) des Ingenieurunternehmens Neocom Geoservice veröffentlich. Neocom Geoservice spezialisiert sich auf die Erkundung von Öl- und Gasfeldern und bietet Unterstützung bei Bohrungen an.
22.04.2022	Die Nachrichtendienste der Five Eyes-Länder veröffentlichen eine gemeinsame Warnung, dass russische Angreifer sich für kritische Infrastrukturen in der Ukraine interessieren.

Quelle: Eigene Zusammenstellung durch Matthias Schulze, SWP Berlin.

National Cyber Security Index

Grafik 1: National Cyber Security Index



Quelle: NCSI (o.J.): National Cyber Security index. https://ncsi.ega.ee/ncsi-index/?order=-isd.

Anmerkung: Der Nationale Cybersicherheitsindex (NCSI) misst die Bereitschaft der Länder, Cyberbedrohungen zu verhindern und Cybervorfälle zu bewältigen. Drei verschiedene Bedrohungsarten werden identifiziert: Denial of e-services – Dienste sind nicht zugänglich, die Verletzung der Datenintegrität und die Verletzung der Vertraulichkeit von Daten. Um gegen diese Cyber-Bedrohungen gewappnet zu sein, muss ein Land über angemessene Kapazitäten für die Cybersicherheit verfügen, die der NCSI anhand von 46 Indikatoren misst. Der NCSI-Score gibt den Prozentsatz an, den das Land vom Maximalwert der Indikatoren erhalten hat. Das Digital Develpoment Level (DDL) wird anhand des ICT Development Index (IDI) und des Networked Readiness Index (NRI) berechnet. Das DDL ist der durchschnittliche Prozentsatz, den das Land vom Höchstwert beider Indizes erhalten hat.

Tabelle 1: National Cyber Security Index

Land	National Cyber Security Index	Digital Development Level	Unterschied
Armenien	35,06	55,06	−20
Aserbaidschan	37,66	54,78	−17,12
Belarus	53,25	62,33	−9,08
Brasilien	46,75	58,53	−11,78
China	51,95	60,81	−8,86
Tschechien	92,21	69,86	22,35
Estland	90,91	76,51	14,4
Frankreich	84,42	78,59	6,07
Georgien	51,95	53,5	−1,55
Deutschland	90,91	81,43	9,48
Indien	59,74	40,02	19,72
Italien	79,22	68,33	10,89
Kasachstan	48,05	60,04	−11,99
Kirgistan	24,68	42,96	−18,28
Lettland	75,32	67,38	7,94
Litauen	93,51	68,61	24,9
Republik Moldau	50,65	56,79	−6,14
Niederlande	83,12	83,48	−0,36
Polen	87,01	66,61	20,4
Rumänien	71,43	60,67	10,76
Russland	71,43	64,22	7,21
Spanien	88,31	73,92	14,39
Tadschikistan	10,39	34,56	−24,17
Turkmenistan	7,79		
Ukraine	75,32	55,95	19,37
USA	79,22	81,44	−2,22
Usbekistan	36,36	49	−12,64

Quelle: NCSI (o.J.): National Cyber Security index. https://ncsi.ega.ee/ncsi-index/?order=-isd.

Anmerkung: Der Nationale Cybersicherheitsindex (NCSI) misst die Bereitschaft der Länder, Cyberbedrohungen zu verhindern und Cybervorfälle zu bewältigen. Drei verschiedene Bedrohungsarten werden identifiziert: Denial of e-services – Dienste sind nicht zugänglich, die Verletzung der Datenintegrität und die Verletzung der Vertraulichkeit von Daten. Um gegen diese Cyber-Bedrohungen gewappnet zu sein, muss ein Land über angemessene Kapazitäten für die Cybersicherheit verfügen, die der NCSI anhand von 46 Indikatoren misst. Der NCSI-Score gibt den Prozentsatz an, den das Land vom Maximalwert der Indikatoren erhalten hat. Das Digital Develpoment Level (DDL) wird anhand des ICT Development Index (IDI) und des Networked Readiness Index (NRI) berechnet. Das DDL ist der durchschnittliche Prozentsatz, den das Land vom Höchstwert beider Indizes erhalten hat.

Cyber-Operationen gegen die Ukraine

Tabelle 2: Ein Vergleich von fünf Cyberangriffen von Russland gegen die Ukraine

	Geschwindigkeit	Intensität	Kontrolle	Strategischer Nutzen
Wahlein-mischung (2014)	3 Monate	geringer Umfang, hohe Reichweite	keine vorzeitige Entdeckung; störende Wirkung auf das Ziel wird teilweise erzeugt; störende Wirkung wird innerhalb von 20 Stunden neutralisiert, wodurch Auswirkungen verhindert werden	unbedeutend
Stromnetz I (2015)	19 Monate	hoher Umfang, hohe Reichweite	vorzeitige Entdeckung; störende Wirkung auf das Ziel erzeugt; störende Wirkung innerhalb von 6 Stunden neutralisiert	unbedeutend
Stromnetz II (2016)	31 Monate	hoher Umfang, höchste Reichweite	vorzeitige Entdeckung; störende Wirkung auf das Ziel teilweise erzeugt; störende Wirkung inner-halb von 75 Minuten neutralisiert	unbedeutend
»Not Petya« (2017)	6 Monate	höchster Umfang, mittlere Reichweite	vorzeitige Entdeckung; störende Wirkung auf Ziele erzeugt	messbar, signifikante Aus-wirkungen auf das Stromnetz
»Bad Rabbit« (2017)	12 Monate	geringer Umfang, geringe Reichweite	keine vorzeitige Entdeckung; störende Wirkung auf das Ziel wurde erzeugt; kontrollierte Pro-liferation	unbedeutend

Quelle: Maschmeyer, L. (2018): The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. International Security, 46:2, S. 72.

Tabelle 3: Akteure und Ziele von Cyberangriffen in der Ukraine

Pro-Kyjiw	Akteur/ Ziel	Frequenz (%)	Pro-Rebellen (selbsternannte Donezker und Luhansker »Volksrepubliken«)	Akteur/ Ziel	Frequenz (%)
Anonymous Ukraine	Akteur/ Ziel	6(<1)	CyberBerkut	A	134 (7)
Ukrainian Cyber Forces	Akteur/ Ziel	1,392 (76)	Cyber Riot Novorossiya	A	41 (2)
Regierungseinheiten und Offizielle	A/T	3(<1)/326 (18)	Green Dragon	A	1 (<1)
Ukrainische Armeeeinheiten	T	1(<1)	Quedagh	A	1 (<1)
Westliche Regierungen und Organisationen	T	15(1)	Regierungsbeamt:innen der Krim	T	6 (<1)
Westliche nicht-staatliche Akteure	T	7(<1)	Russische Armeeeinheiten	A/T	1 (<1)/14 (1)
Nicht-staatliche Unterstützung	T	91 (5)	Nicht-staatliche Unterstützung	T	444 (24)
			Rebellengruppen	A/T	2 (<1)/926 (50)
			Russische staatliche Einheiten und Regierungsbeamt:innen	A/T	2 (<1)/14 (1)
			Staatlich unterstützte russische Gruppen	A	237 (13)
Insgesamt		1.841 (100)			1.841 (100)

Quelle: Kostyuk, N. & Zhukov, Y. M. (2019): Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? Journal of Conflict Resolution, 63:2, S. 325.

Tabelle 4: Arten von Cyberoperationen in der Ukraine

Propaganda	Ukraine (%)	Störungen	Ukraine (%)	Beides	Ukraine (%)
PPI – Veröffentlichung von Daten der Mitglieder der Konfliktparteien online	47 (2)	AVG – Sammeln von Audio-, Video- und Geodaten	423 (23)	WDT – Verunstalten von Webseiten	51 (3)
PRM/PUM – Posts online	54 (3)/5 (<1)	CPI – Sammeln von privaten Daten über offene Quellen	13 (<1)		
UWP – Update von Websiten	6 (<1)	DDoS – distributed denial-of-service attack	499 (27)		
		ODS – andere Attacken zur Störung oder Spionage	9 (1)		
		SPE – Spear-Phishing-E-Mail	234 (13)		
		STM – Versenden von Nachrichten oder Anrufen	40 (2)		
		WBG – Blockieren von Webseiten	257 (14)		
		WFC – Zugang zu Internetzugriffspunkten erlangen	31 (<2)		
Insgesamt	1.841 (100)		1.841 (100)		1.841 (100)

Quelle: Kostyuk, N. & Zhukov, Y. M. (2019): Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? Journal of Conflict Resolution, 63:2, S. 327.

ANALYSE

Zur persönlichen Einstellung von Beschäftigten des öffentlichen Sektors gegenüber aktuellen eGovernment-Initiativen in der Ukraine

Olha Popelyshyn (Tallinn University of Technology), Florian Lemke (Capgemini Deutschland) und Konstantin Ehrhardt (HEC Paris und Freie Universität Berlin)

DOI: 10.31205/UA.267.02

Zusammenfassung
Die Beschäftigten des öffentlichen Sektors in der Ukraine sehen sich im Zuge der digitalen Transformation des Staates neuen Herausforderungen gegenübergestellt. Zunehmende Endnutzer:innenorientierung und die digitale Transformation von Strukturen und Prozessen verändern die Arbeitswelt der Mitarbeitenden. Eine Befragung von Staatsbediensteten gibt Aufschluss über deren wahrgenommene Partizipation sowie Gründe und Ursachen für Motivation und Frustration im Kontext der Digitalisierung der Erbringung von staatlichen Dienstleistungen.

Einleitung
Die Beschäftigten des öffentlichen Sektors sind mit Veränderungen ihrer Arbeitsweise und insbesondere mit den Erwartungen von Bürger:innen und Unternehmen konfrontiert. Durch die zunehmende gesellschaftliche Technisierung entsteht externer Druck auf Staatsbedienstete, sich auf veränderte Anforderungen in Bezug auf effizientere und bürgernahe Dienstleistungen ein-

zustellen. Durch die Verabschiedung von Gesetzen und Vorschriften wird die Modernisierung von Verwaltungsprozessen und die Einführung von eGovernment weiter vorangetrieben. In mehreren Ländern Europas wurden digitale Initiativen ins Leben gerufen, auch um auf veränderte Erwartungen von Endnutzer:innen zu reagieren. Der Wandel von einer bürokratie- zu einer dienstleistungsorientierten öffentlichen Verwaltung bringt jedoch aus Sicht der Beschäftigten des öffentlichen Sektors auch Unsicherheiten mit sich: So ist eGovernment nicht als bloße Digitalisierung von Dienstleistungen zu verstehen. Sie verändert auch die Prozesse und Strukturen in der öffentlichen Verwaltung nachhaltig. Infolgedessen sehen sich die Beschäftigten des öffentlichen Sektors vielfach erheblichen Veränderungen in ihrem Arbeitsumfeld ausgesetzt.

Eine Betrachtung öffentlicher Bediensteter als Rezipient:innen des digitalen Wandels würde aber zu kurz greifen, da diese nicht nur von Digitalisierung betroffen sind, sondern diese im Rahmen ihrer Tätigkeit mit ausgestalten (können). In den letzten Jahrzehnten hat sich die Verwaltungsforschung zu Beschäftigten des öffentlichen Sektors weitgehend auf deren Arbeitsmotivation konzentriert, wobei die Rolle einzelner öffentlich Bediensteter im organisationalen Wandel nur punktuell erforscht wurde.

Insbesondere im Kontext von eGovernment-Initiativen hat diese zudem wenig Beachtung gefunden. Bisherige Untersuchungen deuten auf potenzielle Hindernisse für die erfolgreiche Umsetzung von eGovernment hin: Einerseits haben Wissenschaftler:innen in den vergangenen zehn Jahren festgestellt, dass Beschäftigte des öffentlichen Sektors risikoscheuer und skeptischer gegenüber organisatorischen Veränderungen sind und diese aus Angst vor Arbeitsplatzverlust ablehnen, was ein Haupthindernis für die Umsetzung digitaler Initiativen darstellt.

Andererseits kann auch die Wahrnehmung eines unzureichenden prozessualen Einbezugs zum Scheitern von Veränderungsbemühungen beitragen. Insgesamt wird öffentlichen Bediensteten damit eine hybride Rolle zuteil: Sie sind sowohl Empfänger:innen als auch Vermittler:innen digitaler Transformation. Ein tiefergehender Blick auf einzelne Beschäftigte des öffentlichen Sektors ist also lohnend und trägt zum Verständnis bei, unter welchen Bedingungen eGovernment-Initiativen erfolgreich sein können und/oder auf Hindernisse stoßen.

Bestrebungen zur Digitalisierung der Verwaltung in der Ukraine

Die Ukraine will die Digitalisierung der eigenen Staatsverwaltung bis 2024 abschließen. Die eGovernment-Bewegung in der Ukraine begann 2014, aber eine der ersten Anordnungen des ukrainischen Ministerkabinetts »*On the Approval of the Concept of E-Services System Development in Ukraine*« wurde erst 2016 verabschiedet. Im Gegensatz zur deutschen Vorgehensweise bei der Einführung von elektronischen Dienstleistungen sind in der Ukraine verschiedene nichtstaatliche Akteure beteiligt. Vor allem zivilgesellschaftliche Organisationen sind als Motoren der Innovation auf den Plan getreten, auch weil es Regierungsbeamt:innen oft an IT-Fachwissen und einem unterstützenden Umfeld fehlt. Insgesamt lässt sich der ukrainische Weg zur Umsetzung von eGovernment als ein Prozess beschreiben, der stark von nichtstaatlichen Akteuren getrieben und insgesamt fragmentiert ist. Bei der Entwicklung einer staatlichen Digitalisierungspolitik wurde ein Multi-Stakeholder-Ansatz verfolgt. Dies bedeutet, dass der Zweck einer staatlichen Stelle darin besteht, die Anforderungen der Beteiligten (z. B. NGOs, Bürger:innen, Verwaltung) zu ermitteln, diese zu harmonisieren und umzusetzen. Insgesamt zielt die Digitalisierungsstrategie in der Ukraine darauf ab, die Verwaltung des öffentlichen Sektors an das Niveau anderer europäischer Länder anzugleichen. Dies soll unter anderem durch die Einbeziehung verschiedener gesellschaftlicher Gruppen in die Planung und Umsetzung von Maßnahmen erreicht werden, was zu einer allumfassenden Digitalisierung des öffentlichen Sektors führen soll. Da die Ukraine kein EU-Mitglied ist, bestehen diese Interessen vorrangig seitens der Ukraine und werden nicht durch die EU eingefordert. Bis zum Krieg im Februar 2022 bestand keine strategische Ausrichtung seitens der EU-Staaten, eine Anbindung ukrainischer eGovernment Systeme zu ermöglichen. Im Hinblick der Flüchtlingsbewegungen findet seither jedoch ein Paradigmenwechsel statt, der eine interoperable Anbindung ukrainischer Authentifizierungslösungen vorantreibt. Zur Steigerung der Effizienz wird durch die Zivilgesellschaft und von NGOs, die im Bereich der Verwaltungsdigitalisierung aktiv sind, erwartet, dass sich jede staatliche Einrichtung auf die jeweiligen gesellschaftlichen Erwartungen konzentriert und ein hohes Maß an Rechenschaftspflicht aufrechterhält, so das Ministerkabinett im Jahr 2019. Die Weltbank schreibt in ihrer eGovernment-Bewertung dem ukrainischen Ministerkabinett eine führende Rolle zu. Die ministerielle Hauptaufgabe besteht jedoch darin, Strategien zu genehmigen, während die staatliche eGovernment-Agentur des Ministeriums für Digitale Transformation die Ausgestaltung und Umsetzung koordiniert. Die Entscheidungen des Ministeriums für Digitale Transformation sind für die Ausführung durch staatliche, regionale und lokale Behörden sowie für Unternehmen verbindlich. Die staatliche eGovernment-Agentur hat verschiedene Funktionen wie das Einbringen neuer Gesetzesvorschläge, die Bereitstellung

methodischer und rechtlicher Informationen, die organisatorische Unterstützung beteiligter Akteure und die internationale Zusammenarbeit (bspw. USAID (The United States Agency for International Development); UKAID (The UK Department for International Development); SIDA (The Swedish International Development Cooperation Agency); SDC (Swiss Agency for Development and Cooperation) sowie die East Europe Foundation). Die Liste der Funktionen ist somit breit gefächert und umfasst sowohl die Politikgestaltung als auch die Umsetzung, was Bedenken hinsichtlich der Kapazität der staatliche eGovernment-Agentur aufkommen lässt. Seit dem Beginn des Digitalisierungsprozesses hat die Ukraine von EU-Berater:innen und internationalen staatlichen Initiativen Unterstützung erhalten. Die eGovernance-Akademie Estlands half bei der Entwicklung von Strategien und Leitlinien für lokale eGovernment-Initiativen. Darüber hinaus hat die Ukraine nach dem Vorbild der estnischen Datenaustauschplattform, X-tee (früher X-Road), mit Trembita eine Lösung für den sicheren Datenaustausch entwickelt, welche das Rückgrat des eGovernment-Systems bildet. Das System harmonisiert die IT-Standards für neue elektronische Dienste, bietet das erforderliche Sicherheitsniveau und erleichtert einheitliche Interaktionen zwischen IT-Systemen, lässt aber gleichzeitig genügend Spielraum für Flexibilität. Der Prozess der Einführung elektronischer Dienstleistungen in der Ukraine ist ebenfalls dezentralisiert. Die meisten eGovernment-Initiativen auf lokaler Ebene entstehen in Zusammenarbeit mit ukrainischen Organisationen der Zivilgesellschaft und ausländischen Förderern wie USAID (United States Agency for International Development), UKAID (UK Department for International Development) und der East Europe Fundation. Auch die staatliche eGovernment-Agentur profitiert von internationaler Unterstützung. Eines der vielversprechenden Projekte, welches das Ergebnis der Zusammenarbeit zwischen der ukrainischen Regierung, der staatlichen eGovernment-Agentur, zivilgesellschaftlichen Organisationen und ausländischen Förderorganisationen ist, ist das Online-Portal und die mobile Anwendung für öffentliche Dienstleistungen DIIA (vom ukrainischen Wort »Дія« – Aktion). Das Projekt hat das ehrgeizige Ziel, bis 2024 alle öffentlichen Dienstleistungen für die Bürger:innen der Ukraine digital zugänglich zu machen.

Rahmenbedingungen für Beschäftigte im öffentlichen Sektor

Die Reform der öffentlichen Verwaltung, die im Jahr 2018 gestartet wurde, konzentriert sich auf die Verbesserung und Modernisierung der Auswahlverfahren und -kriterien für Beschäftigte des öffentlichen Sektors, wobei digitale Kompetenzen, analytische und kommunikative Fähigkeiten sowie Englischkenntnisse stärkere Gewichtung erfuhren. Es gibt jedoch keinen Aktionsplan, wie die Qualifikationen der derzeit beschäftigten Beamt:innen verbessert werden könnten. Entsprechend bleiben diese vielfach im Transformationsprozess zurück. Mangelnde Fähigkeiten, um mit dem Tempo der Einführung neuer elektronischer Dienstleistungen Schritt zu halten, können zu Effizienzverlusten und Verwirrung bei der Erbringung öffentlicher Dienstleistungen führen. Die Beschäftigten des öffentlichen Sektors erhalten nicht die erforderliche Ausbildung und können daher die elektronische Erbringung öffentlicher Dienstleistungen für die Bürger:innen nur bedingt erleichtern. Dadurch wird der Wert ihrer Arbeit geschmälert und die Wahrnehmung der eigenen Rolle im Prozess verzerrt. Ein weiteres entscheidendes Problem ist der Mangel an Personal, das für die Wartung der IT-Infrastrukturen ausreichend qualifiziert ist. Aufgrund der im Vergleich zum Privatsektor geringen Vergütung ist die Fluktuation unter den Angestellten hoch. Ungeachtet des schnellen Wachstums digitaler Services und der gut durchdachten technischen Gestaltung neuer elektronischer Dienstleistungen wird deutlich, dass Faktoren wie die Einbeziehung und Weiterentwicklung von Verwaltungsbeschäftigten von zentraler Bedeutung für eine erfolgreiche Digitalisierung der Verwaltung sind.

Aktuelle Herausforderungen für Beschäftigte in der ukrainischen Verwaltung

Die für diese Analyse durchgeführte qualitative Befragung wurde vom 04. Februar 2020 bis zum 14. Februar 2020 mit 32 Teilnehmenden aus der Ukraine durchgeführt. Die Befragung hatte zum Ziel, zumeist subjektive Einstellungen der Befragten zu erfassen und deren Überschneidungen und Mehrfachnennungen zum zuvor fest definierten Rahmen der Befragung zu erörtern. Mithilfe der Codierung von Aussagen offener Fragestellungen sowie der Auswertung von Fragen mit gradueller Antwortskala, auf der die Befragten ihre Einstellung zu einer bestimmten Aussage darlegten, entwickelte sich ein breites Bild zur persönlichen Einstellung von Beschäftigten des öffentlichen Sektors gegenüber aktuellen eGovernment-Initiativen in der Ukraine. Bei den Befragten wurde auf eine durchschnittliche Verteilung von Alter, Geschlecht, der Verortung im politischen System sowie der Verantwortlichkeit im Rahmen der Verwaltungsdigitalisierung geachtet. Freilich ermöglicht eine Befragung von $n = 32$ keine repräsentativen Aussagen. Die Befragung war in vier Unterabschnitte gegliedert, um die Fragen thematisch zu bündeln. Zunächst wurden allgemeine Informationen von den Befragten erhoben. Im zweiten und dritten Teil wurden die Teilnehmenden zu ihren Eindrücken von der digitalen Transformation, ihre

Berührungspunkte mit entsprechenden Initiativen und Prozessen und persönlichen Motiven und Zielen befragt. Der letzte Abschnitt konzentrierte sich auf den Bereich der persönlichen Motivation und die Ergebnisse, die mit der digitalen Transformation erzielt werden sollten. Die Mehrheit der befragten Personen waren Beschäftigte des öffentlichen Sektors. Zudem waren Respondent:innen in Nichtregierungsorganisationen und anderen zivilgesellschaftlichen Institutionen tätig.

Die Ergebnisse der Umfrage haben zunächst gezeigt, dass die Vergütung und das soziale Sicherungsnetz für Verwaltungsbeschäftigte ihre Motivation wesentlich prägen. Die Beschäftigten ukrainischer NGOs oder der Zivilgesellschaft hingegen ziehen ihre Motivation aus der Sichtbarkeit der erzielten Ergebnisse bei einzelnen Vorhaben und dem Gesamtzielbild einer funktionsfähigen digitalen Verwaltung. Die Motivation der Beschäftigten ukrainischer NGOs oder der Zivilgesellschaft speist sich hauptsächlich daraus, mit neuen Ideen zur Nutzung digitaler Technologien nutzerfreundlichere öffentliche Dienstleistungen und ein günstigeres politisches Umfeld zu schaffen. Diese persönliche Einstellung zeigt sich zugleich in der in Grafik 1 auf S. 18 aufgeführten Übersicht der Antworten zur Auffassung der digitalen Transformation im öffentlichen Sektor. Eine Bedienstete einer NGO antwortete, sie sei motiviert durch die »Möglichkeit, am Projektmanagement [digitaler Initiativen] von Anfang bis Ende beteiligt zu sein; durch die Vorstellung, das Endergebnis des Produkts oder der Dienstleistung zu sehen.« Die Ergebnisse der offenen Fragen trugen dazu bei, die Hauptursachen für Frustrationen und Hindernisse bei der Einführung elektronischer Dienste zu umreißen. Eine davon ist das Festhalten an traditionellen oder eher veralteten Arbeitsmethoden, hierarchischen Organisationsstrukturen und das Denken in Abteilungsstrukturen, sogenannten »Silos«. Sie sind Hindernisse für die Übernahme neuer digitaler Initiativen und verlangsamen den Veränderungsprozess erheblich. Als weitere Hindernisse wurden die Komplexität und die dringend erforderliche Rechtssicherheit für elektronische Behördendienste genannt. Die ukrainischen Befragten aus Staat und Zivilgesellschaft betonten auch den Mangel an Ressourcen (z. B. moderne Hardware, hochwertige Internetverbindungen und Gehälter). Die zivilgesellschaftlichen Akteure hoben hierbei auch die mangelnde Unterstützung durch die Regierung bei der Schaffung neuer digitaler öffentlicher Dienste hervor. Große Übereinstimmung fand sich bei dem Punkt, dass die Einstellung von Regierungsbeamt:innen geändert werden müsse, damit diese eine treibende Kraft des digitalen Wandels werden können.

Abschließend wurden die Eindrücke zu den bisher erreichten Meilensteinen analysiert. Die Gruppe der Befragten, welche eher negative Eindrücke von den Veränderungen teilen, beklagen einen Mangel an Fachwissen, Koordination zwischen den Abteilungen und Transparenz. Einer der Befragten erklärte, dass »der Prozess dezentralisiert ist und viele Dienstleistungen ohne Absprache zwischen den verschiedenen Verantwortlichen und Entwicklern von diesen Dienstleistungen erscheinen.« Eine weitere Sorge dieser Gruppe ist die geringe Beteiligung der Endnutzer:innen. Die Umfrage wurde mit einer offenen Frage abgeschlossen, bei der die Befragten ihre Ideen zur Veränderung hinsichtlich der Strategie sowie der prozessualen Umsetzung bei der Einführung einer neuen digitalen Initiative auf nationaler Ebene mitteilen konnten. Eine allgemeine Übersicht zur Auffassung der Befragten in Bezug darauf, welchen Einfluss die Einführung von elektronischen Dienstleistungen auf die eigene Arbeitswelt hat, ist in Grafik 2 auf S. 19 aufgeführt. Das Gros der Befragten war sich einig, dass die Strategie, die externe Kommunikation, die Zusammenarbeit zwischen verschiedenen Abteilungen bzw. Einrichtungen sowie die Qualifikation der Beschäftigten des öffentlichen Sektors verbessert und ein Bewusstsein für die Veränderungen geschaffen werden muss. Des Weiteren wurde die Notwendigkeit von Personalschulungen vor der Einführung neuer elektronischer Dienstleistungen hervorgehoben und ein verstärkter Einbezug von qualifizierten Fachleuten als Berater:innen in Entscheidungsprozessen gewünscht. Der Einbezug und Umgang mit den Anforderungen verschiedener Gruppen von Nutzer:innen sollte dazu beitragen, elektronische Dienstleistungen bedarfsgerecht anzupassen und mögliche Probleme auf der Grundlage ihrer Erfahrungen zu vermeiden.

Resümee

Die Einführung von eGovernment in der Ukraine hat etablierte Strukturen der öffentlichen Verwaltung in einen transformativen Veränderungsprozess geführt, der auch die öffentlichen Beschäftigten direkt betrifft. Der öffentliche Sektor wurde dazu angehalten, sich digital zu transformieren, um den neuen Anforderungen von Bürger:innen und Unternehmen gerecht zu werden.

Der Krieg in der Ukraine hat die Entwicklung neuer und die Verbesserung bestehender öffentlicher elektronischer Dienste gefördert. Dies lässt sich durch die dringende Notwendigkeit erklären, die öffentliche Dienstleistungen in kritischen Zeiten stark zu beschleunigen, diese zu sichern und zu optimieren. Die Hauptplattform DIIA ermöglicht den Ukrainer:innen nicht nur den Online-Zugang zu Dokumenten, sondern vereinfacht auch die Erbringung der wichtigsten öffentlichen Dienstleistungen wie zum Beispiel die Registrierung eines neuen Wohnsitzes (für Bürger:innen, die aufgrund des Krieges binnenvertrieben wurden), die Beantragung von Sozialhilfen oder den Zugriff auf digitale Bildungs-

dienste. Darüber hinaus hat die DIIA Plattform seit Beginn des Krieges eine Reihe von kriegsbezogenen elektronischen Dienstleistungen zur Verfügung gestellt. So können Bürger:innen beispielsweise Berichte über die Zerstörung ihres Eigentums im Verlauf des Krieges einreichen, die später zur Schätzung der entsprechenden Entschädigung herangezogen werden. Aufgrund der Kriegshandlungen ergeben sich schnelle Entscheidungsprozesse, die auf eine Stabilisierung der digitalen Infrastruktur abzielen. So wurde in kürzester Zeit ein Gesetz über die Nutzung von Cloud-Technologien im öffentlichen Sektor verabschiedet.

Noch vor dem Krieg haben die im Rahmen unserer Forschung Befragten auf bekannte Mängel im Digitalisierungsprozess hingewiesen, die für den öffentlichen Sektor in der Ukraine typisch sind, wie zum Beispiel mangelhafte Kommunikation und Zusammenarbeit zwischen Abteilungen und Institutionen, die zu Unstimmigkeiten bei der Umsetzung digitaler Initiativen führen. Nach Meinung der Befragten gibt es keine realisierbaren und umfassenden Digitalisierungsstrategien auf nationaler Ebene. Aufgrund mangelnder Transparenz in den Digitalisierungsprozessen haben die Beschäftigten des öffentlichen Sektors nur begrenzte Möglichkeiten, einen Beitrag zu leisten oder ihr Wissen und ihre Erfahrung weiterzugeben, was ihren Wert in diesem Prozess mindert. Den Beschäftigten des öffentlichen Sektors mangelt es an digitalen Kompetenzen und an Klarheit über die neuen Prozesse, was sich auf ihr Vertrauen und ihre Produktivität bei der Arbeit mit kürzlich eingeführten elektronischen Diensten auswirkt.

Auf der Grundlage der Analyse der Rückmeldungen haben die Autor:innen erste Handlungsempfehlungen abgeleitet. Diese richten sich insbesondere an Führungskräfte im öffentlichen Sektor und sollen diese bei zukünftigen Entscheidungsprozessen unterstützen. Zunächst ist eine ebenenübergreifende Kommunikation und eine Inklusion aller Beteiligten und Betroffenen notwendig, um von Prozessbeginn für eine passende Formierung von Initiativen und der Entwicklung digitaler Dienste zu sorgen. Die Einbindung, die Beteiligung und das Interesse kann auch durch regelmäßige und transparente Berichterstattung über Projektfortschritte und das Erreichen von Meilensteinen gefördert werden. Zweitens ist eine Anpassung der Schulungsinhalte von größter Bedeutung, um wettbewerbsfähig zu bleiben und eine weitgehende Unabhängigkeit von Beratungsunternehmen zu ermöglichen. Hier ist die Durchführung tool-spezifischer Schulungen und die Einrichtung von zentralen Ansprechpartner:innen in den Abteilungen nach der Einführung neuer Prozesse und Software von grundlegender Bedeutung. Schließlich bildet die Möglichkeit zur Mitgestaltung einen wichtigen Baustein. Es ist wichtig, die Beschäftigten des öffentlichen Sektors in den Entscheidungsprozess bei der Einführung neuer elektronischer Dienste oder Rechtsvorschriften einzubeziehen. Diese Empfehlungen machen deutlich, wie notwendig die Einbindung der öffentlichen Bediensteten in jeder Phase der digitalen Transformation ist. Die Beschäftigten müssen insbesondere bei der Ausarbeitung digitaler Strategien und Gesetze für digitale Programme einbezogen werden. Die Beschäftigten wünschen sich klare Maßnahmen, um mögliche Lösungen zur Verbesserung der Arbeitsweise im Rahmen der digitalen Transformation aufzuzeigen.

Über die Autor:innen

Olha Popelyshyn ist eine ukrainische Business Data Analystin, die in Wien lebt. Sie hat eGovernment in Estland studiert und forscht zu Open Data im öffentlichen Sektor.

Florian Lemke ist Senior Business Analyst bei Capgemini in Berlin und promoviert zu Zukunftsthemen des eGovernment in Deutschland, der EU und Asien. Er hat eGovernment in Estland studiert und lehrt dies an der Hochschule für Wirtschaft und Recht in Berlin.

Konstantin Ehrhardt ist Masterstudierender im Doppelabschlussprogramm »Public Policy & Management« an der École des Hautes Études Commerciales de Paris (HEC Paris) und der Freien Universität Berlin.

Hinweis

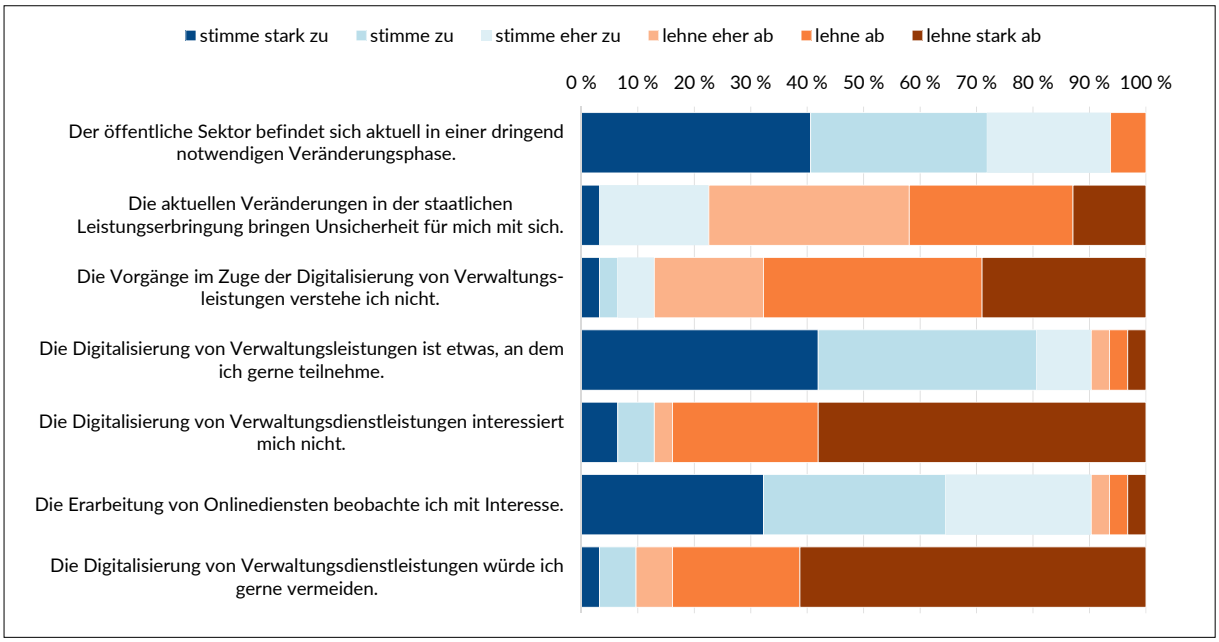
Der vorliegende Beitrag basiert auf einer vergleichenden Fallstudie zu Deutschland und der Ukraine, die erstmals 2021 in der Zeitschrift dms – der moderne staat veröffentlicht wurde:

Lemke, F., Ehrhardt, K., Popelyshyn, O. (2021). Support and Resistance of Public Officials Towards Current eGovernment Initiatives – A Case Study on Ukraine and Germany. dms – der moderne staat – Zeitschrift für Public Policy, Recht und Management, 14(1-2021), 61–80. https://doi.org/10.3224/dms.v14i1.08

UMFRAGEN

Digitalisierung im öffentlichen Sektor: Ergebnisse einer nicht-repräsentativen Umfrage

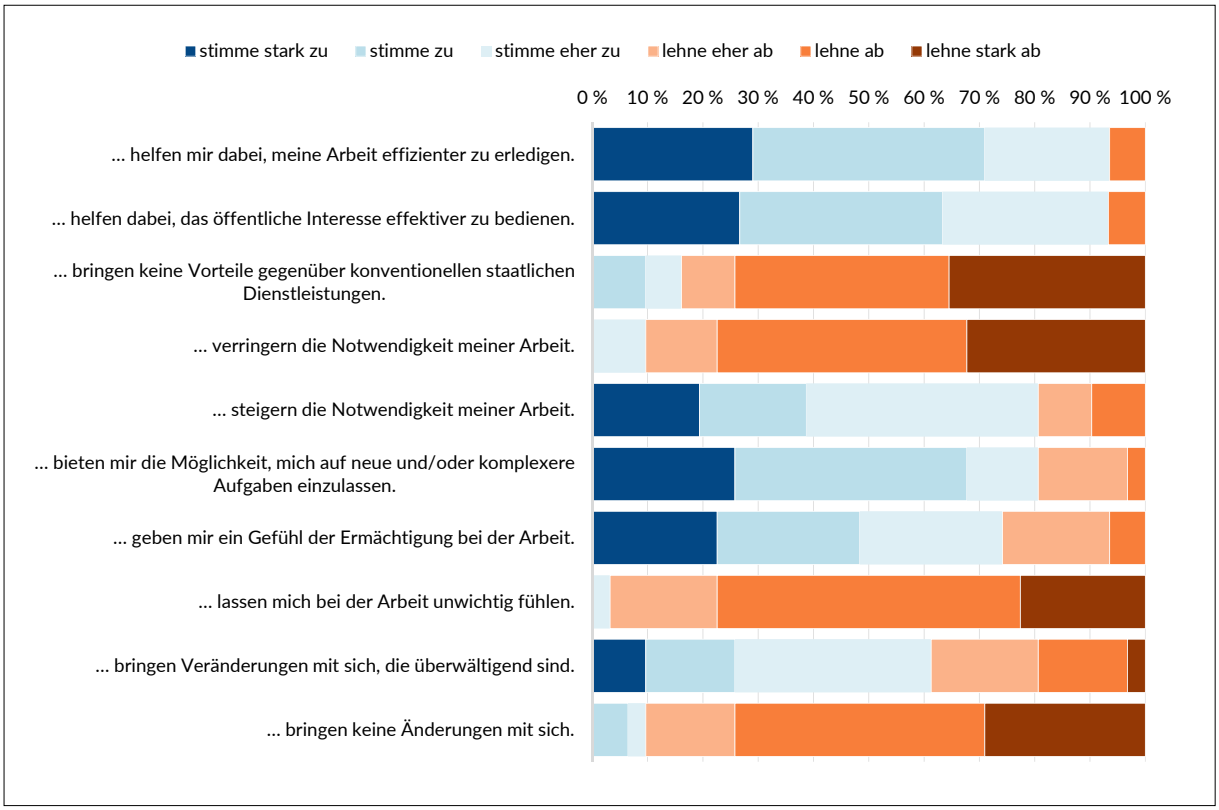
Grafik 1: Bitte legen Sie Ihre Einstellungen gegenüber der digitalen Transformation im öffentlichen Sektor dar:



	stimme stark zu	stimme zu	stimme eher zu	lehne eher ab	lehne ab	lehne stark ab
Der öffentliche Sektor befindet sich aktuell in einer dringend notwendigen Veränderungs-phase.	13	10	7	0	2	0
Die aktuellen Veränderungen in der staatlichen Leistungser-bringung bringen Unsicherheit für mich mit sich.	1	0	6	11	9	4
Die Vorgänge im Zuge der Digitalisierung von Ver-waltungsleistungen verstehe ich nicht.	1	1	2	6	12	9
Die Digitalisierung von Ver-waltungsleistungen ist etwas, an dem ich gerne teilnehme.	13	12	3	1	1	1
Die Digitalisierung von Ver-waltungsdienstleistungen interessiert mich nicht.	2	2	0	1	8	18
Die Erarbeitung von Online-diensten beobachte ich mit Interesse.	10	10	8	1	1	1
Die Digitalisierung von Ver-waltungsdienstleistungen würde ich gerne vermeiden.	1	2	0	2	7	19

Quelle: Lemke, F., Ehrhardt, K., Popelyshyn, O. (2021): Support and Resistance of Public Officials Towards Current eGovernment Initiatives – A Case Study on Ukraine and Germany. dms – der moderne staat – Zeitschrift für Public Policy, Recht und Management, 14(1-2021), 61–80. https://doi.org/10.3224/dms.v14i1.08

Grafik 2: E-Government Services…



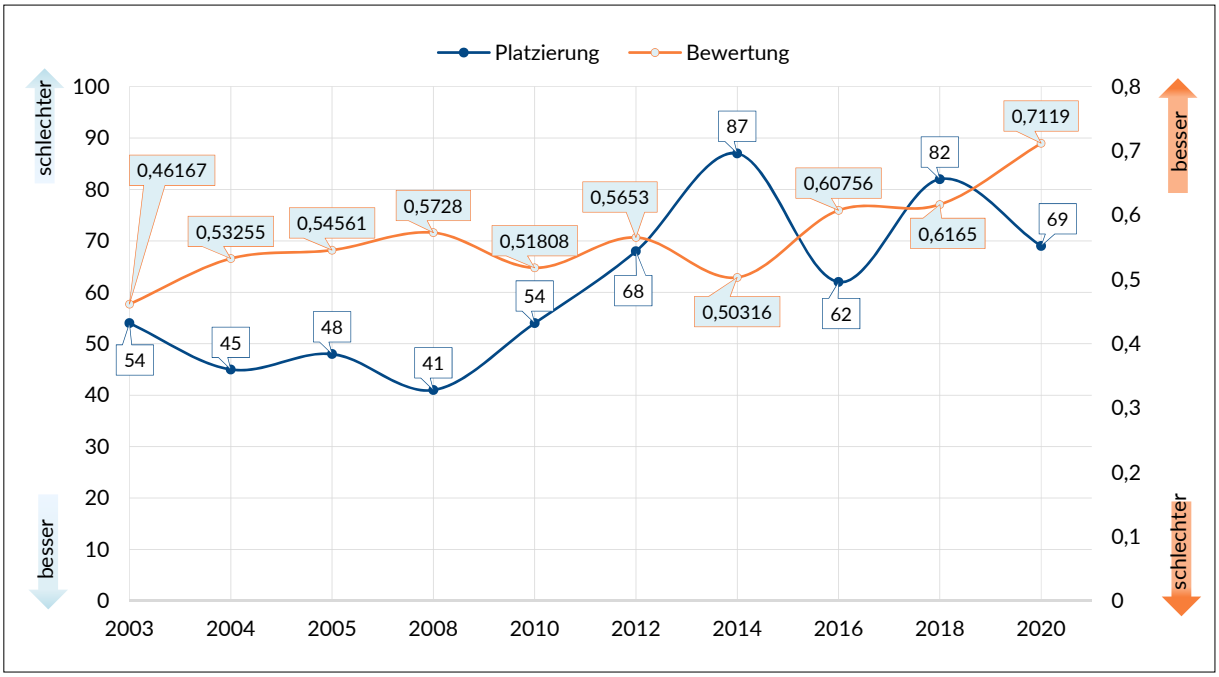
	stimme stark zu	stimme zu	stimme eher zu	lehne eher ab	lehne ab	lehne stark ab
… helfen mir dabei, meine Arbeit effizienter zu erledigen.	9	13	7	0	2	0
… helfen dabei, das öffentliche Interesse effektiver zu bedienen.	8	11	9	0	2	0
… bringen keine Vorteile gegenüber konventionellen staatlichen Dienstleistungen.	0	3	2	3	12	11
… verringern die Notwendigkeit meiner Arbeit.	0	0	3	4	14	10
… steigern die Notwendigkeit meiner Arbeit.	6	6	13	3	3	0
… bieten mir die Möglichkeit, mich auf neue und/oder komplexere Aufgaben einzulassen.	8	13	4	5	1	0
… geben mir ein Gefühl der Ermächtigung bei der Arbeit.	7	8	8	6	2	0
… lassen mich bei der Arbeit unwichtig fühlen.	0	0	1	6	17	7
… bringen Veränderungen mit sich, die überwältigend sind.	3	5	11	6	5	1
… bringen keine Änderungen mit sich.	0	2	1	5	14	9

Quelle: Lemke, F., Ehrhardt, K., Popelyshyn, O. (2021): Support and Resistance of Public Officials Towards Current eGovernment Initiatives – A Case Study on Ukraine and Germany. dms – der moderne staat – Zeitschrift für Public Policy, Recht und Management, 14(1-2021), 61–80. https://doi.org/10.3224/dms.v14i1.08

STATISTIK

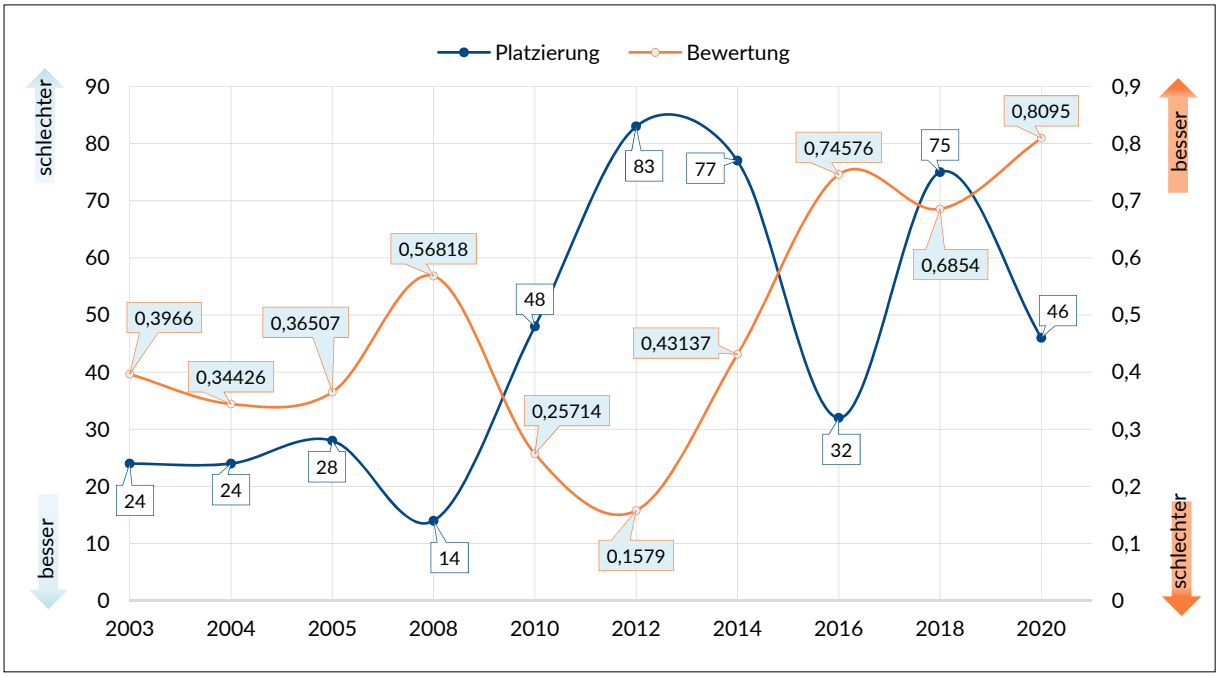
Digitalisierung in der Ukraine

Grafik 3: Die Ukraine im E-Government Development Index



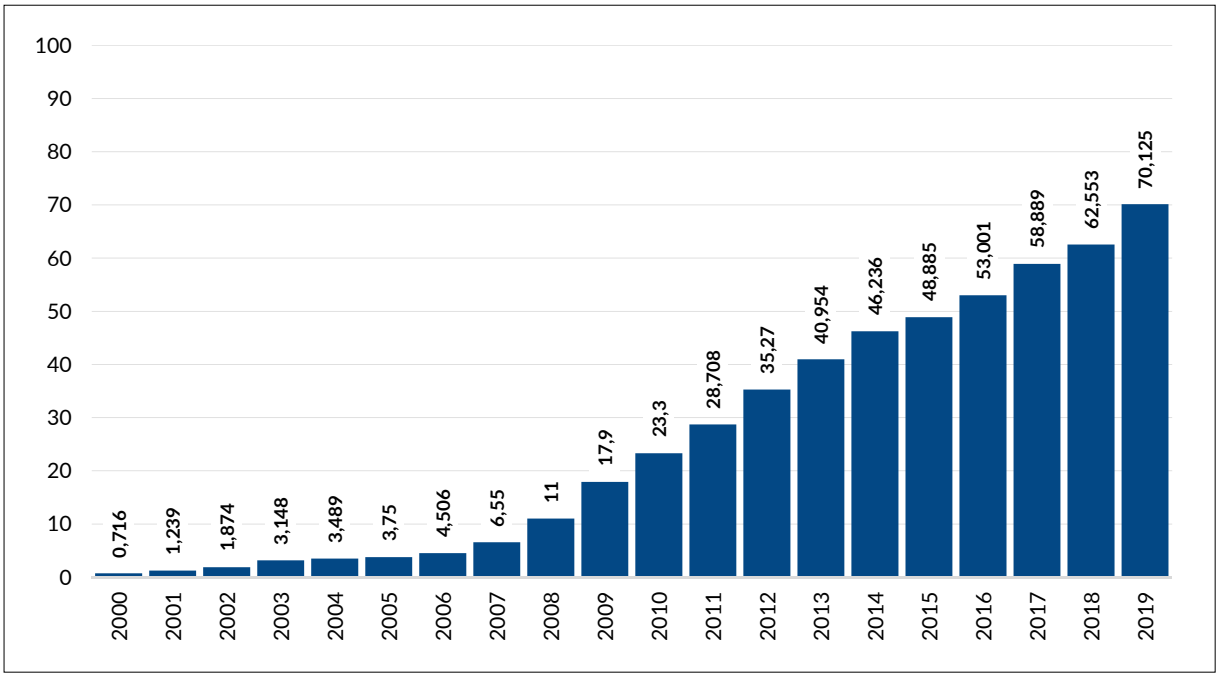
Quelle: UN E-Government Knowledgebase (2020): Ukraine. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine

Grafik 4: Die Ukraine im E-Participation Index



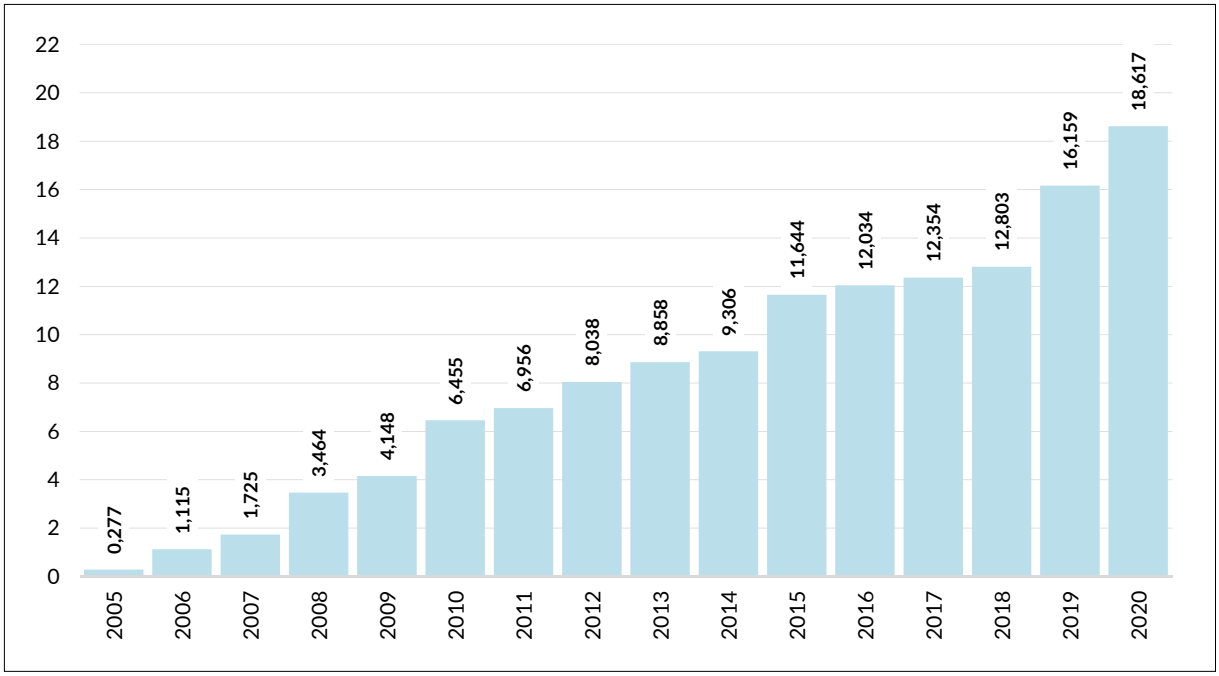
Quelle: UN E-Government Knowledgebase (2020): Ukraine. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine

Grafik 5: Internetnutzer:innen in der Ukraine (in %)



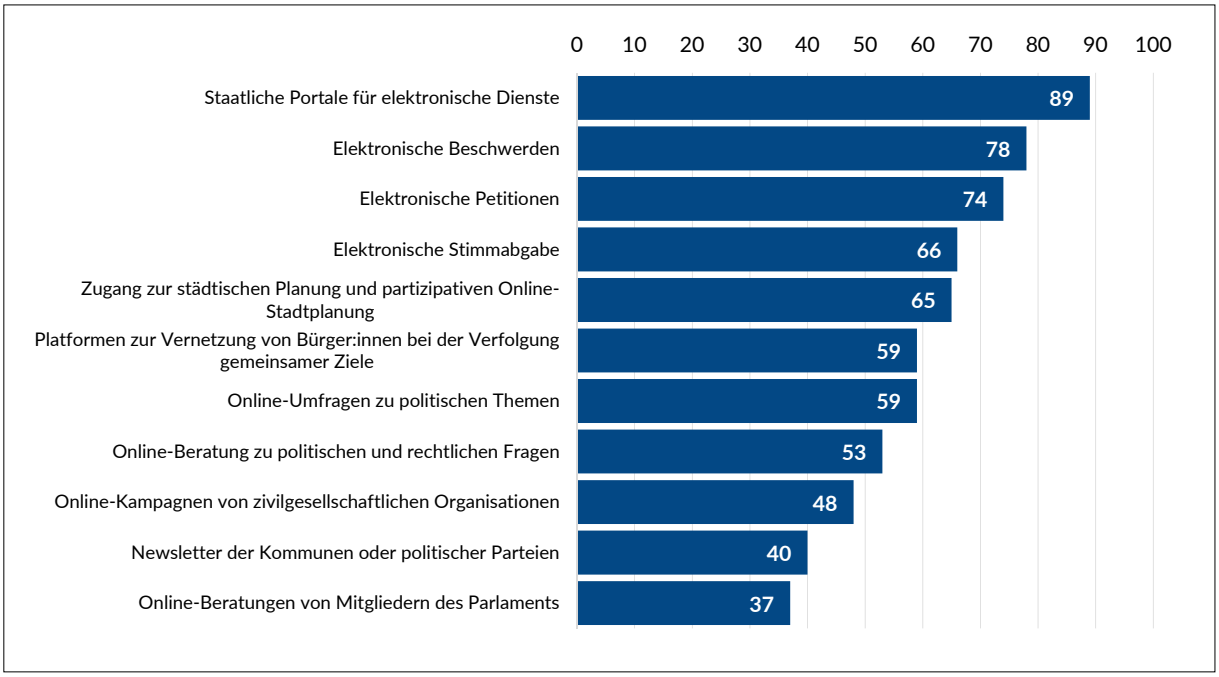
Quelle: Weltbank (2019): Individuals using the Internet (% of population) – Ukraine. https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2019&locations=UA&start=1990&view=chart&year=2019

Grafik 6: Breitbandabonnements pro 100 Menschen



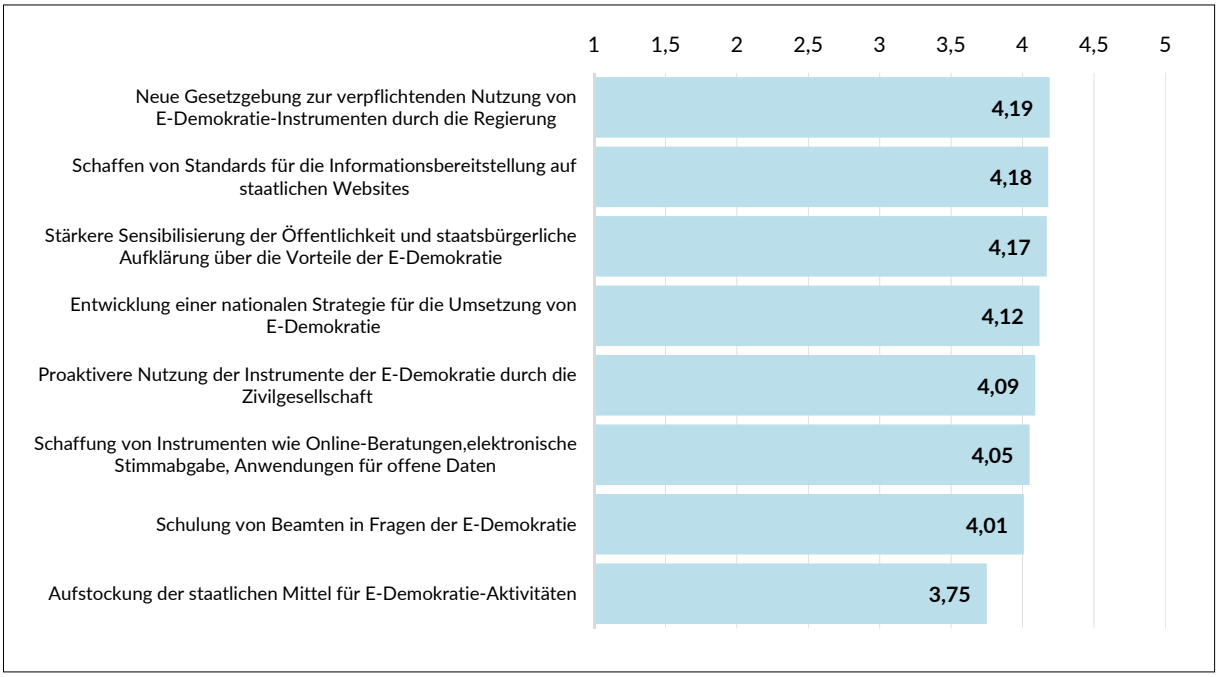
Quelle: Weltbank (2020): Fixed broadband subscriptions (per 100 people) – Ukraine. https://data.worldbank.org/indicator/IT.NET.BBND.P2?view=chart&locations=UA

Grafik 7: Welche der folgenden E-Demokratie-Instrumente würden Sie am ehesten nutzen? (in %)



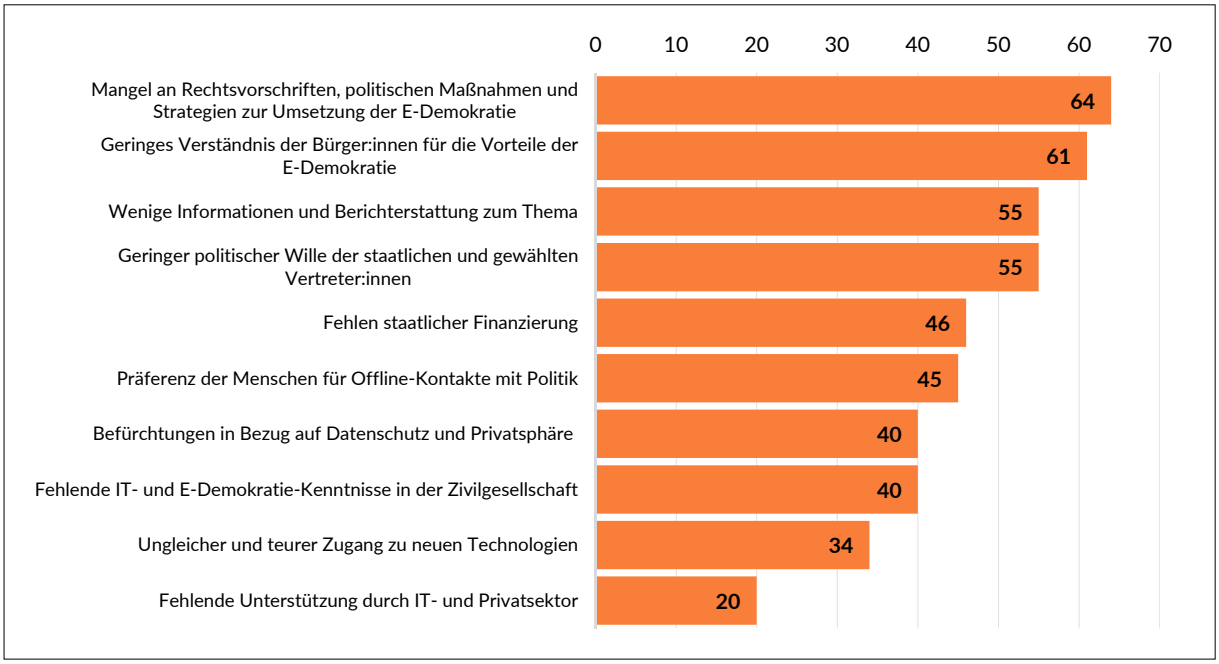
Quelle: Tomkova, J. [Hrsg.] (2016): eDEMOCRACY IN UKRAINE Citizens' & Key Stakeholders' Perspectives. Kiyv: EGAP Program. S. 14.

Grafik 8: Welche Prioritäten sollten den folgenden Maßnahmen gegeben werden, um das demokratische Leben in der Ukraine zu verbessern? (Skala von 1 niedrigste Priorität bis 5 höchste Priorität)



Quelle: Tomkova, J. [Hrsg.] (2016): eDEMOCRACY IN UKRAINE Citizens' & Key Stakeholders' Perspectives. Kiyv: EGAP Program. S. 15.

Grafik 9: Was sind Ihrer Meinung nach die Haupthindernisse für eine optimale Nutzung der Informations- und Kommunikationstechnologien zur Stärkung der E-Demokratie in der Ukraine? (in %)



Quelle: Tomkova, J. [Hrsg.] (2016): eDEMOCRACY IN UKRAINE Citizens' & Key Stakeholders' Perspectives. Kiyv: EGAP Program. S. 16.

DOKUMENTATION

Top-10-Vorschläge aus der ukrainischen Zivilgesellschaft für das Ministerium für digitale Transformation für 2021–22

Basierend auf den Ergebnissen der öffentlichen Diskussion über die Prioritäten der Digitalpolitik am 26. März 2021.

1. **Verbesserung der digitalen Kompetenzen von Informationsmanager:innen und Bürger:innen:** Durchführung von Schulungen zum Umgang mit offenen Daten, elektronischen Dienstleistungen und Instrumenten der elektronischen Demokratie.
2. **Veröffentlichung staatlicher Daten:** Stärkung der Zusammenarbeit des Ministeriums mit dem Menschenrechtsbeauftragten des Parlaments bei der Verfolgung von Verstößen gegen die Veröffentlichung staatlicher Daten und im Zusammenhang mit Instrumenten der E-Demokratie.
3. **Gewährleistung der automatischen Integration offener Daten:** Anwendung eines einheitlichen Prinzips der Offenheit, Interoperabilität und automatischen Integration offener Daten bei der Entwicklung neuer Dienste.
4. **Transparenz von staatlichen offenen Daten:** Digitalisierung der Prozesse und Gewährleistung der automatischen Veröffentlichung offener Daten.
5. **Weiterführung der Dezentralisierung der Verwaltungsdienstleistungen und ihre maximale Überführung in das elektronische Format:** Überführung einer maximalen Anzahl von Dienstleistungen an die Verwaltungsdienstleistungszentren, vor allem der Registerdienste.
6. **Einrichtung eines Datenverwaltungssystems:** Entwicklung klarer Algorithmen für die Erfassung und Veröffentlichung von Daten durch autorisierte Personen.

7. **Ausarbeitung und Genehmigung des Aktionsplans für die Umsetzung des Konzepts zur Entwicklung der E-Demokratie in der Ukraine für die Jahre 2021–2022:** Konsolidierung der Maßnahmen zur Entwicklung von E-Demokratie-Instrumenten, der Fristen und der für ihre Umsetzung zuständigen Personen auf der Ebene der normativen Regulierung.
8. **Vereinheitlichung und Umsetzung der nationalen und regionalen Bürgerhaushalte:** Verwendung von Online-Tools, die als Impuls für die Entwicklung des Sozialkapitals und des Zusammenhalts dienen.
9. **Entwicklung der E-Demokratie auf lokaler Ebene:** Bereitstellung von Subventionen aus dem Staatshaushalt für die Gebietskörperschaften, Förderung der Einwerbung von Zuschüssen und anderen Mechanismen zur Unterstützung des Funktionierens von E-Demokratie-Instrumenten auf lokaler Ebene.
10. **Stärkung der Interaktion der Regierung mit der interessierten Öffentlichkeit:** Schaffung einer Online-Plattform für die Interaktion der Behörden mit Einrichtungen der Zivilgesellschaft, öffentlichen Räten und anderen Beratungsgremien, mit elektronischen Dienstleistungen für Online-Sitzungen, Abstimmungen usw.

Quelle: Reanimation Package of Reforms (2021): Top 10 proposals for the Government of Ukraine for 2021-22 from citizens. https://rpr.org.ua/en/news/top-10-proposals-for-the-government-of-ukraine-for-2021-2022-from-citizens/

CHRONIK

11. März – 09. April 2022

11.03.2022	Der Direktor der Internationalen Atomenergiebehörde (IAEA) Rafael Mariano Grossi teilt mit, ein ukrainisches Team habe mit der Reparatur der beschädigten Stromleitung bei dem ehemaligen Atomkraftwerk Tschernobyl begonnen, das derzeit von der Stromversorgung abgeschnitten ist.
11.03.2022	Nach Angaben lokaler Behörden werden die Städte Dnipro sowie die Flughäfen in der Nähe von Iwano-Frankiwsk und Luzk in der Westukraine bei russischen Luftangriffen getroffen. Aus Charkiw und Mykolajiw werden Angriffe auf Wohngebiete gemeldet.
11.03.2022	Die humanitäre Lage in Mariupol spitzt sich zu. Laut dem Bürgermeister Wadym Bojtschenko können Hilfslieferungen die Stadt nicht erreichen und die Einrichtung von Fluchtkorridoren scheitert aufgrund fortwährenden Beschusses.
11.03.2022	Das Ministerkabinett richtet eine Koordinierungsstelle für den Umgang mit russischen Kriegsgefangenen ein, um ein korrektes Vorgehen bei den Kriegsgefangenen sicherzustellen.
11.03.2022	Auf einem EU-Gipfel einigen sich die Staats- und Regierungschefs auf weitere 500 Millionen Euro an Militärhilfen für die Ukraine, nachdem schon Ende Februar ein erstes Paket über die gleiche Summe bewilligt worden war.
12.03.2022	In einer Videobotschaft fordert der ukrainische Präsident Wolodymyr Selenskyj die Freilassung des Bürgermeisters von Melitopol Iwan Fedorow, der am Vortrag mutmaßlich von russischen Besatzer:innen entführt worden war.
12.03.2022	Mit der Unterzeichnung eines Memorandums billigt US-Präsident Joe Biden die Freigabe weiterer 200 Millionen US-Dollar für Waffenlieferungen an die Ukraine. Bereits Ende Februar hatte Biden Militärhilfen im Umfang von 350 Millionen US-Dollar freigegeben.
13.03.2022	Nach Angaben lokaler Behörden werden bei russischen Angriffen ein Ausbildungsstützpunkt, der etwa 20 Kilometer von der polnischen Grenze in der Nähe von Lwiw liegt, sowie den zweiten Tag in Folge der Luftwaffenstützpunkt in Iwano-Frankiwsk beschossen.
13.03.2022	Laut Angaben des Stadtrats steigt die Zahl der zivilen Todesopfer in der von russischen Truppen belagerten Hafenstadt Mariupol auf 2.187. Etwa 400.000 Zivilist:innen sitzen noch in der Stadt fest, während ihre Evakuierung über Fluchtkorridore blockiert wird.
14.03.2022	Die Stadt Charkiw wird von russischer Seite mit Artillerie beschossen, dort sind laut Bürgermeister Ihor Terechow schon mehr als 600 Häuser, Schulen und medizinische Einrichtungen beschädigt oder zerstört worden.
14.03.2022	Laut einer Umfrage der »European Business Association« haben 42 Prozent der Kleinunternehmen in der Ukraine den Betrieb vollständig, 31 Prozent vorübergehend eingestellt. Außerdem beabsichtigen laut der Umfrage etwa 51 Prozent der Befragten, die staatliche Finanzhilfe über 6.500 UAH (ca. 200 Euro) zu beantragen.

14.03.2022	Die EU-Mitgliedsstaaten einigen sich auf ein neues Sanktionspaket gegen Russland, das unter anderem Sanktionen gegen den russischen Oligarchen Roman Abramowitsch und ein Exportverbot für Luxusgüter umfasst.
14.03.2022	Der Gouverneur der Region Sumy, Dmytro Schywyzkyj, teilt mit, dass Einwohner:innen von Trostjanez von russischen Soldat:innen in vorgetäuschte Fluchtkorridore gebracht, ihrer Handys entledigt und als menschliche Schutzschilde missbraucht werden.
15.03.2022	Bei mehreren Angriffen auf die Hauptstadt Kyjiw von russischer Seite werden unter anderem ein Wohngebäude in dem zentralen Stadtteil Podil getroffen sowie die Fassade der Metrostation Lukjaniwska beschädigt. Auch in den Vororten Irpin, Hostomel und Butscha gibt es weitere Angriffe, in der Oblast Odesa wird die Küste von russischen Kriegsschiffen aus beschossen.
15.03.2022	Die Regierungschefs von Polen, Tschechien und Slowenien reisen mit dem Zug nach Kyjiw, um dort den ukrainischen Präsidenten Wolodymyr Selenskyj sowie Premierminister Denys Schmyhal zu treffen und ein Zeichen der Solidarität mit der Ukraine zu setzen.
15.03.2022	Auf Initiative von Präsident Wolodymyr Selenskyj verlängert das ukrainische Parlament das Kriegsrecht um einen Monat bis zum 25. April 2022.
15.03.2022	Laut dem Gouverneur der Oblast Donezk Pawlo Kyrylenko dringen russische Truppen in ein Krankenhaus in Mariupol ein und nehmen Patient:innen sowie medizinisches Personal als Geiseln.
15.03.2022	Präsident Wolodymyr Selenskyj äußert sich vor Vertretern der »Joint Expeditionary Force« ernüchtert über die Perspektive eines NATO-Beitritts, der in der Ukraine ein Verfassungsziel ist: »Jahrelang haben wir von offenen Türen gehört, aber jetzt haben wir auch gehört, dass wir dort nicht eintreten dürfen, und das müssen wir einsehen.«
15.03.2022	Laut Angaben des stellvertretenden Leiters des ukrainischen Präsidentenamtes, Kyrylo Tymoschenko, verlassen etwa 20.000 Zivilist:innen in Privatautos die Hafenstadt Mariupol über einen Fluchtkorridor. Bisher waren größere Evakuierungen aus der von russischen Truppen belagerten Stadt gescheitert.
16.03.2022	Nach Angaben des ukrainischen Außenministeriums wird von russischer Seite ein Theater in Mariupol bombardiert, in dem mehrere hundert Zivilist:innen Schutz gesucht hatten. Satellitenbilder zeigen, dass das russische Wort für »Kinder« auf den Vorplatz geschrieben worden war.
16.03.2022	Der Bürgermeister von Melitopol Iwan Fedorow wird gegen neun kriegsgefangene russische Soldat:innen getauscht. Der Bürgermeister war einige Tage zuvor von russischen Besatzer:innen entführt und festgehalten worden.
16.03.2022	Nach einer per Video übertragenden Rede des ukrainischen Präsidenten Wolodymyr Selenskyj vor dem US-Kongress, in der er für die Einrichtung einer Flugverbotszone plädiert, sichert US-Präsident Joe Biden der Ukraine weitere Militärhilfen in Höhe von 800 Millionen US-Dollar zu und nennt den russischen Präsidenten Wladimir Putin einen »Kriegsverbrecher«.
16.03.2022	Der internationale Gerichtshof in Den Haag ordnet an, dass Russland den Krieg gegen die Ukraine sofort beenden muss, und gibt damit einer Dringlichkeitsklage der Ukraine statt.
17.03.2022	Nach einer per Video übertragenen Rede des ukrainischen Präsidenten Wolodymyr Selenskyj vor dem Deutschen Bundestag, in der er Deutschland eine Mitschuld an Verzögerungen bei der NATO- und EU-Integration gibt und sich mit den Worten »reißen Sie die Mauer nieder« direkt an den deutschen Bundeskanzler Olaf Scholz wendet, sichert dieser in einer Pressekonferenz der Ukraine weitere Unterstützung zu.
18.03.2022	Das Koordinationsbüro für Humanitäre Angelegenheiten der Vereinten Nationen teilt mit, dass ein erster Konvoi mit Hilfsgütern für die Versorgung von etwa 35.000 Menschen die Stadt Sumy im Nordosten der Ukraine erreicht hat.
18.03.2022	Laut Angaben des Bürgermeisters von Lwiw, Andrij Sadowyj, wird eine Flugzeugwerkstatt in der Nähe der Stadt von mehreren Raketen getroffen. Der stellvertretende Bürgermeister von Mariupol, Serhij Orlow, teilt mit, dass das Stahlwerk »Asowstal« durch Luftangriffe zerstört worden sei. Bei russischen Angriffen auf Kyjiw, Charkiw, Mariupol, Tschernihiw, Mykolajiw und weitere Städte werden zahlreiche Zivilist:innen getötet und verletzt.
19.03.2022	Ein Sprecher des russischen Verteidigungsministeriums erklärt, Russland habe eine Hyperschallrakete eingesetzt und damit ein unterirdisches Munitionslager in der Region Iwano-Frankiwsk zerstört.
19.03.2022	Nach Angaben der Stadtverwaltung von Berdjansk stoppen russische Truppen einen Konvoi zur Evakuierung von Menschen aus Mariupol.
19.03.2022	Die Nationale Agentur für Korruptionsprävention erstellt eine Datenbank mit potenziellen Kollaborateuren im Krieg gegen Russland, darunter Beamte, die russische Propaganda verbreiten und die Verteidigungsfähigkeit und Souveränität der Ukraine untergraben.
19.03.2022	Laut Schätzung des ukrainischen Finanzministers Serhij Martschenko ist die ukrainische Wirtschaft seit Beginn des Krieges um ein Drittel geschrumpft, was er an den sinkenden Steuereinnahmen festmacht.

20.03.2022	Nach Angaben der Stadtverwaltung bombardieren russische Streitkräfte eine Kunstschule in Mariupol, in der mehrere hundert Menschen Zuflucht gesucht haben. In der Nähe der nordwestlichen Stadt Riwne wird ein Truppenübungsplatz beschossen.
20.03.2022	Die Ukraine lehnt die russische Forderung nach Aufgabe der Stadt Mariupol ab. In einem Schreiben des russischen Verteidigungsministeriums vom 20. März 2022 heißt es, dass Russland nur dann einen humanitären Korridor einrichten werde, wenn Mariupol kapituliert; die Ukraine fordert die sofortige Einrichtung eines solchen Korridors.
21.03.2022	Die Ukraine beschuldigt Russland, Kinder aus dem besetzten Donbas zu entführen. Nach Angaben des ukrainischen Außenministeriums seien 2.389 Kinder illegal nach Russland verschleppt worden.
21.03.2022	Bei einem Bombenangriff in Charkiw wird der 96-jährige Holocaust-Überlebende Boris Romantschenko getötet.
22.03.2022	Nach Regierungsangaben kapern die russischen Besatzer:innen einen Konvoi, der zur Evakuierung von Menschen aus Mariupol unterwegs gewesen sei, und nehmen Mitarbeiter:innen des Katastrophenschutzes sowie Fahrer:innen gefangen.
23.03.2022	Die USA werfen Russland offiziell Kriegsverbrechen in der Ukraine vor. Es gebe »zahlreiche glaubwürdige Berichte über wahllose Angriffe« auf Zivilist:innen, auf Wohnhäuser, Schulen und Krankenhäuser, heißt es in einer Erklärung des US-Außenministers Antony Blinken.
23.03.2022	Laut Angaben des Bürgermeisters von Irpin, Oleksandr Markuschkin, setzen die russischen Streitkräfte in den Kyjiwer Vororten Irpin und Hostomel Phosphorbomben ein. Der Einsatz solcher Waffen gegen Zivilist:innen ist nach der Genfer Konvention verboten. Aus Charkiw und Mariupol werden weitere schwere Angriffe gemeldet. Laut dem Bürgermeister von Melitopol, Iwan Fedorow, missbrauchen russische Streitkräfte die Einwohner:innen seiner Stadt als lebende Schutzschilde.
23.03.2022	Der ukrainische Oligarch Rinat Achmetow erklärt gegenüber dem Wall Street Journal, dass seine Metallwerke »Asowstal« und »Iljitsch«, die vorübergehend geschlossen sind, unter russischer Besatzung nicht mehr in Betrieb gehen werden.
24.03.2022	Nach eigenen Angaben zerstören ukrainische Streitkräfte im Hafen von Berdjansk das russische Landungsschiff »Orsk«.
24.03.2022	Der stellvertretenden Premierministerin Iryna Wereschtschuk zufolge wurden zehn russische gegen zehn ukrainische Kriegsgefangene ausgetauscht, wobei es sich um den »ersten echten Austausch von Kriegsgefangenen« seit Beginn des Krieges gehandelt habe.
24.03.2022	Der Gouverneur der Oblast Charkiw, Oleh Synjehubow, teilt mit, dass russische Streitkräfte die Innenstadt von Charkiw mit vom Schwarzen Meer aus abgefeuerten Raketen angreifen. Seinen Angaben zufolge ist Charkiw täglich Ziel zahlreicher Angriffe.
24.03.2022	Bei einem NATO-Sondergipfel bittet der ukrainische Präsident Wolodymyr Selenskyj, der per Video zugeschaltet ist, um die Freigabe von einem Prozent der bündniseigenen Kampfjets und Panzer. Die NATO beschließt, ihre Truppen an der Ostflanke angesichts der russischen Invasion in der Ukraine massiv aufzustocken und warnt Russland davor, Chemiewaffen einzusetzen.
25.03.2022	Laut eigenen Angaben gewinnen die ukrainischen Streitkräfte die Kontrolle über die Gebiete nordöstlich von Kyjiw zurück, von wo sich Einheiten der russischen Truppen nach einem beobachteten Verlust von mehr als der Hälfte ihrer Soldaten hinter die russische Grenze zurückgezogen haben.
25.03.2022	Aus Augenzeugenberichten geht hervor, dass bei dem Angriff russischer Truppen auf ein Theater in Mariupol etwa 300 Menschen getötet worden sein könnten, wie es in einer Erklärung des Stadtrats von Mariupol heißt. Zuvor hatte der Stadtrat einen Hilferuf veröffentlicht, da die Einwohner:innen zu verhungern drohen. Nach Angaben der Leiterin der UN-Beobachtungsmission für Menschenrechte legen Satellitenbilder die Existenz von Massengräbern in der belagerten Stadt nahe.
25.03.2022	Nach Polizeiangaben werden bei einem russischen Angriff auf eine medizinische Einrichtung in Charkiw sieben Menschen verletzt, vier von ihnen sterben. Die Weltgesundheitsorganisation (WHO) zählt in einer Erklärung mindestens 70 russische Angriffe auf Krankenhäuser, Krankenwägen und Ärzte seit Beginn des russischen Krieges in der Ukraine.
25.03.2022	Nach Angaben des ukrainischen Verteidigungsministeriums zielen russische Streitkräfte mit Raketen auf das Gebiet des Luftwaffenkommandos in der zentralwestlichen Stadt Winnyzja, wobei mehrere Gebäude beschädigt werden. In Charkiw wird nach Angaben des Gouverneurs der Oblast, Oleh Synjehubow, der Flughafen beschossen.
26.03.2022	In der Stadt Dubno (Gebiet Riwne) gerät ein Öllager durch russische Raketenangriffe in Brand.

26.03.2022	Zum 26. März sind zehn humanitäre Korridore vereinbart worden. Sie sollen die Evakuierung der Bürger:innen aus einigen Siedlungen in den Regionen Donezk, Kyjiw und Luhansk ermöglichen. Zudem will Frankreich gemeinsam mit Griechenland und der Türkei eine »humanitäre Operation« starten, um alle Menschen, die Mariupol verlassen wollen, zu evakuieren.
26.03.2022	Abgeordnete der Opposition im ukrainischen Parlament bringen zwei Gesetzesvorschläge ein, um ein Verbot der Ukrainischen Orthodoxen Kirche, die dem Moskauer Patriarchat untersteht, zu erwirken. Es handele sich bei dieser Kirche um eine religiöse Organisation, deren leitendes Zentrum sich außerhalb der Ukraine in einem Staat befindet, der gegen die Ukraine Krieg führe und einen Teil des Landes besetzt hält.
26.03.2022	Russische Truppen dringen in die Stadt Slawutytsch in der Region Kyjiw ein und besetzen das Krankenhaus der Stadt. Der Bürgermeister Jurij Fomitschew wird entführt, später jedoch wieder freigelassen. Im Zentrum der Stadt findet eine pro-ukrainische Demonstration gegen die Okkupation statt, welche die russischen Truppen versuchen, auseinander zu treiben.
26.03.2022	Der ukrainische Präsident Wolodymyr Selenskyj spricht per Videokonferenz auf einem katarischen Forum in Doha. Er fordert eine Reform der UNO und Katar dazu auf, die Energieproduktion zu steigern.
26.03.2022	Die Stadt Tschernihiw hat seit Beginn des Krieges mehr als die Hälfte ihrer Einwohner:innen verloren. Dies berichtet der Bürgermeister der Stadt, Wladyslaw Atroschenko. Hatte die Stadt vor dem Krieg knapp 290.000 Einwohner:innen, liegt die Zahl heute bei 120.000–130.000. Russland zerstöre weiterhin vorsätzlich zivile Einrichtungen wie Schulen, Krankenhäuser, Stadien, Bibliotheken usw. Seit Beginn des Krieges sind laut Angaben des Ministers für Kommunale und Territoriale Entwicklung, Oleksij Tschernyschew, etwa 4.500 Wohnhäuser, 100 Unternehmen, 400 Bildungseinrichtungen und 150 Gesundheitseinrichtungen durch den russischen Angriff zerstört worden.
26.03.2022	In einer Videokonferenz mit dem polnischen Präsidenten Andrzej Duda zeigt sich der ukrainische Präsident Wolodymyr Selenskyj enttäuscht darüber, dass, entgegen ihrer erklärten Bereitschaft, einige osteuropäische Länder, darunter auch Polen, Flugzeuge aus sowjetischer Produktion noch immer nicht an die Ukraine übergeben hätten.
27.03.2022	Die ukrainische Eisenbahngesellschaft bietet zusätzliche Evakuierungszüge aus Charkiw, Dnipro, Kramatorsk und Odesa an.
27.03.2022	Der Bürgermeister der südukrainischen Stadt Mariupol, Wadym Bojtschenko, schätzt, dass von den 540.000 Menschen, die vor dem Krieg in Mariupol lebten, etwa 50 Prozent die Stadt verlassen haben. Er schätzt zudem, dass 20–30 Tausend Menschen nach Russland zwangsumgesiedelt wurden. In Mariupol wurden durch den Beschuss und die Bombardierung durch russische Truppen 90 Prozent des Wohnungsbestands – 2.600 Häuser – beschädigt.
27.03.2022	Die Ukraine vereinbart zwei humanitäre Korridore zur Evakuierung von Menschen aus den Regionen Donezk und Luhansk.
27.03.2022	Das britische Verteidigungsministerium meldet, dass Russland weiterhin auf Langstreckenraketen oder Bomben von russischem Luftraum aus setzt, um den ukrainischen Luftabwehrkräften die Möglichkeit zu nehmen, russische Flugzeuge zu treffen.
27.03.2022	In Dubno (Gebiet Riwne) ist das Öllager, das am 26. März durch Raketenangriffe in Brand geraten war, inzwischen vollständig zerstört.
27.03.2022	Die Behörden in der selbsternannten »Luhansker Volksrepublik« teilen mit, sie wollen in absehbarer Zeit ein »Referendum« über die Zugehörigkeit des Gebiets zu Russland abhalten. Das ukrainische Außenministerium erklärt daraufhin, dass Referenden in den vorübergehend besetzten und international nicht anerkannten Gebieten keine rechtliche Bindung haben.
27.03.2022	Das britische Verteidigungsministerium verkündet, es habe der Ukraine eine Reihe von tragbaren Starstreak-Luftabwehrsystemen übergeben.
28.03.2022	Eine weitere Verhandlungsrunde zwischen der ukrainischen und der russischen Delegation soll am 29. März in der Türkei stattfinden. Die ukrainischen Unterhändler:innen sind bereits auf dem Weg.
28.03.2022	Infolge eines Raketenangriffs der russischen Besatzungstruppen bricht Feuer in einem Öllager in der Region Riwne aus, das Öllager wird vollständig zerstört. Bereits am 27. März hatte es einen Raketenangriff auf ein Öldepot in der Region Wolhynien gegeben. Zuvor waren bereits Öldepots in Lwiw und Dubno (ebenfalls in der Region Riwne) mit Raketen beschossen worden.
28.03.2022	In der Region Sumy überfährt ein russischer Militäroffizier absichtlich eine Familie, die in Richtung eines Konvois mit russischem Militärgerät lief. Ein 15-jähriger Junge und seine Mutter werden verletzt, ein 33-jähriger Mann erliegt im Krankenhaus seinen Verletzungen.

28.03.2022	Der Bürgermeister von Charkiw, Ihor Terechow, meldet, dass infolge des russischen Beschusses und der Luftangriffe in Charkiw bereits 1.177 Wohnhäuser zerstört worden seien. In der Stadt sind insgesamt 1.410 Gebäude zerstört worden, darunter 53 Kindergärten, 69 Schulen und 15 Krankenhäuser.
29.03.2022	Seit Beginn der russischen Invasion sind bereits mehr als 510.000 Bürger:innen in die Ukraine zurückgekehrt, etwa 75–80 Prozent davon sind Männer. Gleichzeitig haben in dieser Zeit mehr als 3,8 Millionen Menschen das Land verlassen.
29.03.2022	In Istanbul findet eine weitere Runde der ukrainisch-russischen Friedensverhandlungen statt. Die ukrainische Delegation teilt Russland ihre Vorstellungen von internationalen Sicherheitsgarantien für die Ukraine mit, ohne jedoch, dass es zu einem Durchbruch kommt.
29.03.2022	Der ukrainische Präsident Wolodymyr Selenskyj verkündet auf Telegram, Italien habe sich bereit erklärt, Sicherheitsgarant für die Ukraine zu werden.
29.03.2022	Die Nachrichtenagentur Reuters berichtet, dass russische Soldaten mit ihren gepanzerten Fahrzeugen ohne Strahlenschutz in der Sperrzone um den stillgelegten Atomreaktor Tschernobyl gefahren seien und dort radioaktive Staubwolken aufgewirbelt haben. Ein Arbeiter aus Tschernobyl spricht von »Selbstmord«, weil der radioaktive Staub, den sie dadurch einatmeten, eine innere Strahlenbelastung in ihrem Körper verursachen könne.
29.03.2022	Der Rat der Europäischen Union hat einen 10-Punkte-Plan zur Unterstützung von Ukrainer:innen gebilligt, die aufgrund des Krieges gezwungen sind, das Land zu verlassen. Z. B. geht es um den Austausch von Registrierungsinformationen für alle ankommenden Personen.
29.03.2022	Einzelne Einheiten der russischen Streitkräfte werden aus den Regionen Kyjiw und Tschernihiw abgezogen, nachdem die russische Armee die beiden Städte nach mehr als einem Monat des Krieges nicht einnehmen konnte und bei den Gefechten hohe Verluste erlitt.
30.03.2022	Das am 28. März ausgebrochene Feuer in einem Öllager in der Region Riwne konnte nach drei Tagen gelöscht werden.
30.03.2022	In der Region Charkiw werden Antipersonenminen und Sprengminen gefunden, die von den russischen Besatzungstruppen gelegt wurden. Der Einsatz solcher Minen ist nach dem Ottawa-Abkommen über das Verbot von Antipersonenminen nicht zulässig. In Marinka, Region Donezk, setzen die Besatzer Phosphorgranaten ein. Als Folge des Beschusses kommt es zu mehreren Bränden, wie der Leiter der militärischen Administration der Oblast Donezk, Pawlo Kyrylenko, berichtet.
30.03.2022	Im Parlament findet die erste Lesung über den Gesetzentwurf Nr. 7198 statt. Dieser soll Entschädigungszahlungen für Betroffene gewährleisten, deren Häuser während des Krieges beschädigt oder zerstört wurden.
30.03.2022	Über drei vereinbarte humanitäre Korridore erreichen 1.530 Menschen Saporischschja in ihren eigenen Fahrzeugen. Darunter sind 812 Personen aus Mariupol und 718 Bewohner:innen der Region Saporischschja. Die ukrainische Vize-Regierungschefin Iryna Wereschtschuk teilt außerdem mit, dass russische Truppen immer noch Hilfsgüter auf dem Weg nach Saporischschja blockieren würden.
30.03.2022	Die USA beabsichtigen, der ukrainischen Regierung im Zuge der russischen Invasion direkte Haushaltshilfen in Höhe von 500 Millionen US-Dollar zu gewähren. Dies sagte der Präsident der USA, Joe Biden, dem ukrainischen Präsidenten Wolodymyr Selenskyj in einem Telefongespräch zu.
30.03.2022	In dem Kyjiwer Vorort Irpin, der teilweise von russischen Truppen besetzt ist, wurden nach vorläufigen Angaben der örtlichen Behörden bis zu 300 Zivilist:innen und bis zu 50 Soldat:innen getötet.
31.03.2022	Der Generalstab der Streitkräfte der Ukraine berichtet, dass die russischen Besatzungstruppen in der von ihnen besetzten Region Cherson mit den Vorbereitungen für ein »Referendum« zur Gründung einer »Volksrepublik Cherson« beginnen.
31.03.2022	Die russischen Truppen haben sich laut Angaben der ukrainischen »Agentur zur Verwaltung der Sperrzone« vollständig vom Gebiet des stillgelegten Atomreaktors Tschernobyl zurückgezogen.
31.03.2022	Russland blockiert die Verlängerung des Mandats der OSZE-Sonderbeobachtermission in der Ukraine (OSZE SMM). Die OSZE SMM war 2014 auf Ersuchen der ukrainischen Regierung durch einen Konsensbeschluss aller 57 OSZE-Staaten eingerichtet worden und kontrollierte bis zur russischen Invasion im Februar 2022 die Kämpfe im Donbas.
31.03.2022	Der Präsident der Ukraine Wolodymyr Selenskyj teilt nach Gesprächen mit dem türkischen Präsidenten Recep Tayyip Erdogan auf Twitter mit, dass die Türkei bereit sei, ein Garant für die Sicherheit der Ukraine zu werden.
31.03.2022	Der russische Präsident Wladimir Putin sagt in einem Telefongespräch mit dem italienischen Ministerpräsidenten Mario Draghi, die Bedingungen für einen Waffenstillstand in der Ukraine seien »noch nicht erfüllt«.

31.03.2022	Laut Angaben der ukrainischen Vize-Regierungschefin Iryna Wereschtschuk wurden aus der Stadt Mariupol, die seit drei Wochen von russischen Truppen belagert wird, insgesamt 75.000 Menschen evakuiert. Weitere 100.000 Menschen müssten noch evakuiert werden. Etwa 45.000 Ukrainer:innen seien nach Russland zwangsdeportiert worden.
31.03.2022	Der Sprecher des ukrainischen Präsidenten, Mychajlo Podoljak, spricht sich gegen ein Verbot der Ukrainischen Orthodoxen Kirche – Moskauer Patriarchat aus. Diese habe sich während des aktuellen Krieges eindeutig pro-ukrainisch positioniert.
01.04.2022	Der ukrainische Präsident Wolodymyr Selenskyj erkennt dem ehemaligen Leiter der Hauptdirektion des Inlandsgeheimdienstes SBU, Andrij Naumow, und dem ehemaligen SBU-Chef für die Region Cherson, Serhij Kryworutschko, wegen Landesverrats die Generalsränge ab.
01.04.2022	Georgien erklärt, sich den internationalen Sanktionen gegen Russland anzuschließen.
01.04.2022	Ukrainische Streitkräfte haben 11 Siedlungen in der Region Cherson sowie die Stadt Butscha in der Nähe von Kyjiw wieder unter ihre Kontrolle gebracht. Die Administration der Region Tschernihiw meldet, dass sich die russischen Besatzungstruppen aus der Region zurückziehen.
01.04.2022	Die Präsidentin des Europäischen Parlaments, Roberta Metsola, reist nach Kyjiw, wo sie mit ukrainischen Beamten über die europäische Integration der Ukraine und neue Sanktionen gegen Russland spricht.
01.04.2022	Die Abgeordneten der Werchowna Rada verabschieden einen Gesetzentwurf, der vorsieht, dass in bestimmten Fällen Eigentum von russischen Staatsbürger:innen und Kollaborateur:innen zugunsten des ukrainischen Staates beschlagnahmt werden kann.
02.04.2022	Russische Truppen führen in der Nacht Angriffe auf die Region Dnipropetrowsk durch. Raketen zerstören vor allem Infrastruktureinrichtungen. Zwei Personen werden verletzt. Auch aus anderen Regionen werden nächtliche Angriffe gemeldet. In Charkiw werden Wohngebiete beschossen.
02.04.2022	Pentagon-Sprecher John Kirby verkündet, dass die USA der Ukraine weitere Militärhilfen im Umfang von 300 Millionen US-Dollar zur Verfügung stellen werden, einschließlich gepanzerter Fahrzeuge.
02.04.2022	Die Ukraine vereinbart sieben humanitäre Korridore für die Evakuierung aus den Regionen Donezk, Saporischschja und Luhansk. Ein Evakuierungskonvoi, der am 1. April Melitopol in Richtung Saporischschja verließ, steht mit mehr als 400 Fahrzeugen am Kontrollpunkt in Wassiliwka und wird nicht durchgelassen.
02.04.2022	Das ukrainische Verteidigungsministerium meldet, dass die gesamte Region Kyjiw von den russischen Besatzungstruppen befreit ist.
02.04.2022	Russische Besatzungstruppen durchtrennen eine Gaspipeline in der Nähe von Sjewjerodonezk. Fast die gesamte Oblast Luhansk bleibt dadurch ohne Gas, das vor allem zum Heizen benutzt wird.
03.04.2022	Der Bürgermeister der Stadt Butscha, Anatolij Fedoruk, meldet, dass in mehreren Massengräbern in der Stadt bereits 280 Menschen gefunden worden seien. Nach der Befreiung der Stadt wird das Ausmaß der starken Zerstörung von Butscha sichtbar. Die Straßen seien übersät mit Leichen von Zivilist:innen, die während der Okkupation von russischen Soldat:innen ermordet worden sein sollen.
03.04.2022	Der britische Premierminister Boris Johnson besteht laut Angaben der Zeitung »Times« darauf, dass die Ukraine Anti-Schiffs-Raketen benötigt, um ihre Küste gegen Beschuss vom Meer aus verteidigen zu können.
03.04.2022	Nachdem die Region Kyjiw von den russischen Besatzungstruppen befreit wurde, beginnen ukrainische Einheiten mit der Minenräumung. In den Siedlungen entlang der Schytomyr-Autobahn waren von russischen Truppen zahlreiche Minen ausgelegt worden.
03.04.2022	Der Bürgermeister der Stadt Isjum in der Region Charkiw meldet, dass Russische Truppen rund 80 Prozent der Wohngebäude in der Stadt zerstört haben. Die Kämpfe dauern unvermindert an.
03.04.2022	Die Ukraine erhält aus den USA 150 Tonnen Medikamente, Ausrüstung und einen Krankenwagen. Am Vortag war die humanitäre Fracht in Polen gelandet und von dort weitergeleitet worden.
03.04.2022	Die Medienagentur Ukraine Media Center meldet, Russlands groß angelegter Einmarsch in der Ukraine habe bereits 23.000 Kilometer öffentlicher Straßen zerstört, was 13 Prozent aller Straßen des Landes entspricht.
03.04.2022	Nach Angaben der Vereinten Nationen wurden seit Beginn des russischen Einmarsches in der Ukraine mindestens 1.417 Zivilist:innen getötet und weitere 2.038 verwundet.
04.04.2022	In der Nacht feuerten russische Truppen Raketen auf eine Einrichtung in Odesa und beschossen am Morgen Mykolajiw im Süden der Ukraine. In den vergangenen 24 Stunden wurden in der Region Mykolajiw 49 Menschen, darunter ein Kind, durch Granatenbeschuss verletzt. Die große Mehrheit der Verletzten waren Zivilist:innen.
04.04.2022	Die größte russische Nachrichtenagentur, RIA Novosti, veröffentlicht einen Artikel mit dem Titel »Was Russland mit der Ukraine tun sollte«. Darin wird dazu aufgerufen, die Ukraine zu »entnazifizieren« und, damit einhergehend, zu »entukrainisieren«. Die Ukraine dürfe kein souveräner Staat mehr sein.

04.04.2022	Russland fordert eine Dringlichkeitssitzung des UN-Sicherheitsrates. Nach dem Bekanntwerden der brutalen Morde an Zivilist:innen durch russische Truppen in Butscha bei Kyjiw behauptet Russland, dass es sich dabei um eine »Provokation durch Radikale« handeln soll. Die Einberufung der Sitzung wird abgelehnt. Das US-Unternehmen Maxar Technologies veröffentlichte zuvor Satellitenbilder von der Stadt Butscha. Die Fotos zeigen erste Anzeichen für die Aushebung eines Massengrabs auf dem Gelände einer Kirche bereits am 10. März, als die Stadt von russischen Truppen besetzt war.
04.04.2022	Laut der Vize-Regierungschefin der Ukraine, Iryna Wereschtschuk, befinden sich derzeit etwa 600 russische Kriegsgefangene in der Ukraine.
04.04.2022	Seit Beginn des Krieges ist in der Ukraine ein erheblicher Anstieg der Lebensmittelpreise zu verzeichnen. Insbesondere zwischen dem 23. Februar und dem 4. April stiegen die Preise für Buchweizen um 25,5 Prozent und für Nudeln um 24,5 Prozent.
05.04.2022	Präsident Wolodymyr Selenskyj beruft eine ukrainische Delegation ein, die einen Entwurf für ein Abkommen über Sicherheitsgarantien für die Ukraine entwerfen und mit Russland vereinbaren soll.
05.04.2022	Das russische Militär kündigt eine Feuerpause für die Städte Mariupol und Wolnowacha an. Zivilist:innen sollen so die beiden eingekesselten Städte verlassen können. Laut Angaben der Stadtverwaltung von Mariupol stand die Stadt mehr als 40 Stunden unter Beschuss. Auch Krankenhäuser und Schulen seien dabei getroffen worden. Im Laufe des Tages wird die angekündigte Feuerpause immer wieder gebrochen. In Mariupol leben nach Angaben der Stadtverwaltung weiterhin etwa 130.000 Zivilist:innen, die die Stadt aufgrund des Beschusses durch die russische Armee nicht verlassen können.
05.04.2022	Nach ersten Schätzungen müssen bereits 80.000 Quadratkilometer ukrainischen Territoriums aufgrund von Minen und Kontamination durch explosive Überreste geräumt werden. Laut der UNO ist die Ukraine eines der am stärksten verminten Länder der Welt.
05.04.2022	Das Razumkov-Zentrum veröffentlicht die Ergebnisse einer soziologischen Umfrage, der zufolge 79 Prozent der Ukrainer:innen, die ihre Heimat wegen des Krieges verlassen haben, planen, nach Beendigung des Krieges wieder zurückzukehren. Aus einer weiteren Umfrage des Umfrageinstituts »Rating« geht hervor, dass inzwischen 91 Prozent der Ukrainer:innen für einen EU-Beitritt sind, vor der russischen Invasion waren es 68 Prozent. Die Zahl derjenigen, die der NATO beitreten wollen, liegt bei 68 Prozent und damit etwas niedriger als vor der russischen Invasion.
05.04.2022	Die Kyjiwer Metro gibt neue Fahrtzeiten bekannt. Ab dem 6. April wird die Kyjiwer Metro von 7:30 – 19:00 Uhr verkehren. Die U-Bahnhöfe sollen weiterhin rund um die Uhr als Schutzräume zur Verfügung stehen.
06.04.2022	In einem Interview mit dem Rundfunksender »Deutsche Welle« berichtet der Bürgermeister von Butscha, Anatolij Fedoruk, dass nach aktuellem Stand in der Stadt 320 Zivilist:innen während der russischen Besetzung ums Leben gekommen seien. Die Zahl der entdeckten Leichen steige von Tag zu Tag.
06.04.2022	Aus der Region Cherson werden weiterhin Kämpfe gemeldet, ebenso Kämpfe an den Grenzen der Regionen Mykolajiw und Dnipropetrowsk. Die meisten Siedlungen im Kriegsgebiet stehen am Rande einer humanitären Katastrophe, da viele Dörfer und Siedlungen ohne Licht und Wasser sind.
06.04.2022	Der irische Premierminister, Micheál Martin, versichert im irischen Parlament, Irland unterstütze den Beitritt der Ukraine zur EU und werde dies auch weiterhin tun.
06.04.2022	Die ukrainische Vize-Regierungschefin Iryna Wereschtschuk fordert die Bevölkerung dazu auf, Teile von Charkiw sowie die Regionen Donezk und Luhansk zu verlassen, da dies kaum möglich sein würde, sobald die russische Armee eine neue Offensive startet.
06.04.2022	Der Gesamtukrainische Rat der Kirchen und religiösen Organisationen ruft alle Länder der Welt auf, die Kriegsverbrechen Russlands in der Ukraine als Völkermord am ukrainischen Volk anzuerkennen. Dem Rat gehört auch die Ukrainische Orthodoxe Kirche an, welche zum Moskauer Patriarchat gehört.
07.04.2022	Die russischen Besatzungstruppen haben in der besetzten Stadt Enerhodar in der Region Saporischschja damit begonnen, eigene Verwaltungsbehörden einzurichten und die bisherigen Mitarbeiter:innen der ukrainischen Behörden zu entlassen.
07.04.2022	Der Bürgermeister der ostukrainischen Stadt Dnipro, Boris Filatow, empfiehlt Einwohner:innen, die die Stadt verlassen haben, vorerst nicht zurückzukehren. Frauen, Kindern, älteren Menschen und Personen, die nicht in der Industrie oder der kritischen Infrastruktur tätig sind, wird empfohlen, die Stadt zu verlassen.
07.04.2022	Die UN-Vollversammlung setzt die Mitgliedschaft Russlands im UN- Menschenrechtsrat aus. Als Grund dafür werden Berichte über grobe und systematische Menschenrechtsverletzungen in der Ukraine genannt. Daraufhin erklärt Russland seine Tätigkeit in dem Gremium für beendet.

07.04.2022	Die ukrainische Eisenbahngesellschaft gibt für den Tag Evakuierungszüge aus den Gebieten Donezk und Charkiw bekannt. Drei Evakuierungszüge aus Kramatorsk und Slowjansk werden infolge eines russischen Luftangriffs blockiert.
07.04.2022	Die Kreditanstalt für Wiederaufbau (KfW) unterzeichnet im Auftrag der Bundesregierung einen Kreditvertrag über 150 Mio. Euro mit dem ukrainischen Finanzministerium. Dieser soll bei der Unterstützung des ukrainischen Mittelstands und zur Abfederung der Kriegsfolgen helfen.
07.04.2022	Der litauische Botschafter Valdemar Sarapin nimmt seine Arbeit in Kiew wieder auf. Er ist einer der ersten diplomatischen Vertreter, der nach seiner Evakuierung die Arbeit in der ukrainischen Hauptstadt wieder aufnimmt.
07.04.2022	Der ukrainische Präsident Wolodymyr Selenskyj bittet Griechenland um Hilfe bei einer humanitären Mission zur Rettung der Einwohner:innen von Mariupol.
08.04.2022	Über 50 Prozent der ukrainischen Bevölkerung spricht sich für ein Verbot der Ukrainischen Orthodoxen Kirche, die zum Moskauer Patriarchat gehört, auf dem Gebiet der Ukraine aus. Dies ergab eine Umfrage des Umfrageinstituts »Rating«.
08.04.2022	Laut Angaben des örtlichen Gouverneurs Pawlo Kyrylenko sind in der ostukrainischen Stadt Kramatorsk bei einem Raketenangriff auf den Bahnhof mehr als 50 Personen getötet worden. Viele Menschen warteten auf dem Bahnhof auf ihre Evakuierung aus der umkämpften Region.
08.04.2022	EU-Kommissionspräsidentin Ursula von der Leyen besucht die Ukraine. Bei einer gemeinsamen Ansprache mit dem ukrainischen Präsidenten Wolodymyr Selenskyj sagt von der Leyen, die Ukraine »gehöre zur europäischen Familie«. Die Ukraine hatte kurz nach Beginn des russischen Angriffs die EU-Mitgliedschaft beantragt, den die EU-Kommission aktuell prüft. Die EU-Kommissionspräsidentin besucht noch am gleichen Tag den Kyjiwer Vorort Butscha, wo russische Truppen schwere Kriegsverbrechen an Zivilist:innen verübt haben sollen.
08.04.2022	Sechs Wochen nach dem Ausbruch des Krieges eröffnet die Europäische Union wieder ihr Büro in Kyjiw.
08.04.2022	Das Staatliche Statistikamt der Ukraine meldet, dass der Anstieg der Verbraucherpreise in der Ukraine sich im März 2022 auf 4,5 Prozent beschleunigte, nach 1,6 Prozent im Februar und 1,3 Prozent im Januar.
08.04.2022	Nach Angaben des »Rating«-Instituts hat sich in den letzten Monaten die Zahl derer, die die Wiederherstellung freundschaftlicher Beziehungen zwischen Ukrainer:innen und Russ:innen für unmöglich halten, um das Anderthalbfache erhöht.
09.04.2022	Die russischen Truppen setzen den intensiven Beschuss und die teilweise Blockade der Stadt Charkiw in Richtung Sloboschanske fort. In Charkiw wurde in den letzten zwei Tagen der Einsatz eines neuartigen Geschosses registriert, das mit Fallschirmen auf die Stadt abgeworfen wurde. Der Bürgermeister, Ihor Terechow, fordert die Menschen in der Stadt auf, wenn möglich in Schutzräumen, Bunkern und U-Bahnhöfen zu bleiben.
09.04.2022	Österreichs Kanzler Karl Nehammer reist zu politischen Gesprächen nach Kyjiw und übergibt 20 Rettungsfahrzeuge und zehn Tanklöschfahrzeuge. Am Folgetag plant er einen Besuch des Kyjiwer Vororts Butscha.
09.04.2022	Der Stadtrat von Ternopil beschließt, ein Denkmal für den russischen Dichter und Schriftsteller Alexander Puschkin abzureißen. Bürgermeister Serhij Nadal begründet dies mit den Worten, dass »alles Russische demontiert werden sollte«.
09.04.2022	Der britische Premierminister Boris Johnson reist ohne mediale Vorankündigung nach Kyjiw, wo er zu Gesprächen mit dem ukrainischen Präsidenten Wolodymyr Selenskyj zusammentrifft. Nach dem Treffen kündigt Johnson ein neues Finanz- und Militärhilfepaket für die Ukraine an.
09.04.2022	Der stellvertretende polnische Ministerpräsident Jarosław Kaczyński kritisiert den ungarischen Ministerpräsidenten Viktor Orbán. Dieser unterhalte trotz des russischen Krieges in der Ukraine weiterhin gute Beziehungen zu Russland und sehe den ukrainischen Präsidenten Wolodymyr Selenskyj als seinen »Rivalen«. Kaczyński betont, dass eine weitere Zusammenarbeit zwischen Polen und Ungarn unmöglich sei, wenn Orban seine Haltung gegenüber der russischen Aggression in der Ukraine nicht ändere.

Die Chronik wird zeitnah erstellt und basiert ausschließlich auf im Internet frei zugänglichen Quellen. Die Redaktion bemüht sich, bei jeder Meldung die ursprüngliche Quelle eindeutig zu nennen. Aufgrund der großen Zahl von manipulierten und falschen Meldungen kann die Redaktion der Ukraine-Analysen keine Gewähr für die Richtigkeit der Angaben übernehmen.

Zusammengestellt von Almuth Müller, Dr. Martin Buchholz

Sie können die gesamte Chronik seit Februar 2006 auch auf http://www.laender-analysen.de/ukraine/ *unter dem Link »Chronik« lesen.*

Herausgeber:
Forschungsstelle Osteuropa an der Universität Bremen
Deutsche Gesellschaft für Osteuropakunde e.V.
Deutsches Polen-Institut
Leibniz-Institut für Agrarentwicklung in Transformationsökonomien
Leibniz-Institut für Ost- und Südosteuropaforschung
Zentrum für Osteuropa- und internationale Studien (ZOiS) gGmbH

Redaktion:
Dr. Fabian Burkhardt (verantwortlich)
Assistenz: Leonie Eckl, Florian Kübler
Chronik: Almuth Müller, Dr. Martin Buchholz
Satz: Matthias Neumann

Wissenschaftlicher Beirat:
Dr. Kseniia Gatskova, Leibniz-Institut für Ost- und Südosteuropaforschung Regensburg
Prof. Dr. Guido Hausmann, Leibniz-Institut für Ost- und Südosteuropaforschung Regensburg
Dr. Susan Stewart, Stiftung Wissenschaft und Politik, Berlin
Dr. Susann Worschech, Europa-Universität Viadrina, Frankfurt/O.

Ukraine-Analysen-Layout: Cengiz Kibaroglu, Matthias Neumann und Michael Clemens
Alle Ausgaben der Ukraine-Analysen sind mit Themen- und Autorenindex archiviert unter www.laender-analysen.de
Die Ukraine-Analysen werden im Rahmen eines Lizenzvertrages in das Internetangebot der Bundeszentrale für politische Bildung (www.bpb.de) aufgenommen.
ISSN 1862-555X
Forschungsstelle Osteuropa • Länder-Analysen • Klagenfurter Str. 8 • 28359 Bremen • Telefon: +49 421-218-69600 • Telefax: +49 421-218-69607
e-mail: laender-analysen@uni-bremen.de • Internet-Adresse: http://www.laender-analysen.de/ukraine/

LÄNDER–ANALYSEN

Belarus–Analysen | Polen–Analysen | Russland–Analysen | Ukraine–Analysen | Zentralasien–Analysen

CSS ETH Zurich | DGO Deutsche Gesellschaft für Osteuropakunde e.V. | Deutsches Polen Institut | Forschungsstelle Osteuropa | iamo Leibniz-Institut für Agrarentwicklung in Transformationsökonomien | IOS Leibniz-Institut für Ost- und Südosteuropaforschung | ZOIS Zentrum für Osteuropa- und internationale Studien

@laenderanalysen

Kostenlose E-Mail-Dienste: Länder-Analysen

Die Länder-Analysen bieten regelmäßig im kostenlosen Abonnement kompetente Einschätzungen aktueller politischer, wirtschaftlicher, sozialer und kultureller Entwicklungen in Ostmitteleuropa und der GUS. Alle Länder-Analysen verstehen sich als Teil eines gemeinsamen Projektes, das der wissenschaftlich fundierten, allgemeinverständlich formulierten Analyse der Entwicklungen im östlichen Europa, der Offenheit für verschiedene inhaltliche Positionen und der kostenlosen und nicht-kommerziellen Information einer breit verstandenen interessierten Öffentlichkeit verpflichtet ist. Autor/innen sind internationale Fachwissenschaftler/innen und Expert/innen. Die Redaktionen der Länder-Analysen bestehen aus Wissenschaftler/innen mit langjähriger Forschungserfahrung.

Die deutschsprachigen Länder-Analysen werden gemeinsam von der Forschungsstelle Osteuropa an der Universität Bremen, dem Zentrum für Osteuropa- und internationale Studien, der Deutschen Gesellschaft für Osteuropakunde, dem Deutschen Polen-Institut, dem Leibniz-Institut für Agrarentwicklung in Transformationsökonomien und dem Leibniz-Institut für Ost- und Südosteuropaforschung herausgegeben. Die englischsprachigen Länder-Analysen erscheinen in Kooperation der Forschungsstelle Osteuropa mit dem Center for Security Studies (CSS) der ETH Zürich.

Die Länder-Analysen bieten regelmäßig Kurzanalysen zu aktuellen Themen, ergänzt um Grafiken und Tabellen sowie Dokumentationen. Zusätzlich gibt es eine Chronik aktueller Ereignisse.

Belarus-Analysen
Erscheinungsweise: zweimonatlich
Abonnement unter: http://www.laender-analysen.de/belarus/

Caucasus Analytical Digest
In englischer Sprache. Erscheinungsweise: zweimonatlich
Abonnement unter: http://www.css.ethz.ch/en/publications/cad.html

Polen-Analysen
Erscheinungsweise: zweimal monatlich
Abonnement unter: http://www.deutsches-polen-institut.de/newsletter/polen-analysen/

Russland-Analysen
Erscheinungsweise: zweimal monatlich
Abonnement unter: http://www.laender-analysen.de/russland/

Russian Analytical Digest
In englischer Sprache. Erscheinungsweise: zweimal monatlich
Abonnement unter: http://www.css.ethz.ch/en/publications/rad.html

Ukraine-Analysen
Erscheinungsweise: zweimal monatlich
Abonnement unter: http://www.laender-analysen.de/ukraine/

Zentralasien-Analysen
Erscheinungsweise: zweimonatlich
Abonnement unter: http://www.laender-analysen.de/zentralasien/