



Samstag, 19. Februar 2022, 15:59 Uhr
~22 Minuten Lesezeit

Menschen kontrollieren

Das Weltwirtschaftsforum und die russische Sberbank haben im Juli 2021 zum dritten Mal in Folge die jährliche Übung Cyber Polygon veranstaltet.

von Stefan Korinth
Foto: REDPIXEL.PL/Shutterstock.com

200 IT-Teams internationaler Firmen und Institutionen nahmen an der Übung Cyber Polygon teil, doch nur wenige von ihnen konnten den simulierten Hackerangriff abwehren. Die Live-Veranstaltung wurde währenddessen von realen Hackern attackiert. Im öffentlichen Teil der Konferenz verzichtete WEF-Gründer Klaus Schwab diesmal auf apokalyptische Ankündigungen – trotzdem verschaffte die Veranstaltung einen Einblick in einige Vorhaben der Architekten der angestrebten digitalen Kontrollwelt.

„Wer glaubt, den Wandel einer freien Gesellschaft zur Totalität aussitzen zu können und dabei sein kleines privates Glück zu bewahren, wird in Kürze in einer bargeldlosen, digitalen Impf- und Klimaschutz-Kontrollwelt aufwachen, die in alle privaten Bereiche vorgedrungen ist.“

Raymond Unger (1)

Cyber Polygon – die laut WEF „weltweit größte technische Trainingsübung für Unternehmensteams“ – geriet zuletzt auf den Schirm der kritischen Öffentlichkeit, nachdem WEF-Gründer Klaus Schwab bei der Eröffnung der Veranstaltung 2020 in dramatischen Worten vor einer großangelegten Cyber-Attacke **gewarnt hatte** (<https://www.youtube.com/watch?v=EOvz1Flfrfw&t=426s>).

Gelinge solch ein katastrophaler Hackerangriff auf die kritische Infrastruktur (wie Strom-, Wasser- und Nahrungsversorgung), wäre die gesamte Gesellschaft lahmgelegt. Die Corona-Krise würde dagegen nur wie „eine kleine Störung“ wirken, prophezeite Schwab damals und **mahnte** (<https://youtu.be/EOvz1Flfrfw?t=144>) einmal mehr einen globalen Neustart – einen „Great Reset“ – an.

Zudem nährte die Ankündigung der Organisatoren, bei Cyber Polygon 2021 einen Angriff auf die digitale Lieferkette von Wirtschaftssektoren zu simulieren, bei Kritikern einen Verdacht: Hier könnte es sich um ein elitäres Planspiel handeln, das genau das vorwegnimmt, was währenddessen oder kurz darauf tatsächlich **passieren soll** (<https://multipolar-magazin.de/artikel/angriff-mit-ansage>). Hintergrund und Vorbild dieser Befürchtungen unter anderem: **Event 201** (<https://www.centerforhealthsecurity.org/event201/about>), ein Planspiel des WEF und der Bill-und-Melinda-Gates-Stiftung, das im Oktober 2019 eine Corona-Pandemie simulierte.

Konzerne und Behörden arbeiten zusammen

Cyber Polygon ist eines von mehreren Projekten, die das WEF in Kooperation mit internationalen Konzernen, aber auch mit vielen staatlichen Einrichtungen zu digitaler Sicherheit von Unternehmen betreibt. Die verschiedenen Initiativen sind seit 2018 in einem Centre for Cybersecurity **versammelt** (<https://www.weforum.org/platforms/the-centre-for-cybersecurity>). Dabei geht es nicht nur darum, Politiker und Strafverfolgungsbehörden in die Mitverantwortung für die digitale Sicherheit privater Konzerne zu nehmen, sondern Zweck ist auch, zivilen und staatlichen Vertretern die Mantras des Weltwirtschaftsforums permanent einzuimpfen.

Die wichtigste dieser Botschaften, die bei den Cybersicherheits-Projekten des WEF teils explizit, teils implizit ausgesprochen wird, lautet: Hacking sei ein globales Problem, das Staaten aufgrund der allgegenwärtigen Digitalisierung in ihren Grundfesten erschüttern könne. Dieser Gefahr könnten Regierungen und Behörden letztendlich nur begegnen, indem sie gemeinsam mit den Konzernen der Superreichen die digitale Überwachung auf sämtliche Lebensbereiche ausdehnen.

Cyber Polygon und die Sberbank

Bei Cyber Polygon spielt die staatsnahe russische Sberbank eine Hauptrolle. Deren IT-Sicherheitsdienstleister BI.Zone liefert das organisierende Fachpersonal für die Übung und aus den entsprechend aufgepeppten IT-Räumlichkeiten der Bank in Moskau wird der öffentliche Teil der jährlichen Cyber-Polygon-Veranstaltung in die Welt gesendet. Zudem holt Sberbank-Chef Herman Gref, der auch eine wichtige Rolle beim WEF spielt,

hochrangige russische Staatsvertreter wie den Ministerpräsidenten Michail Mischustin an Bord der Konferenz.

Die Veranstaltung besteht aus zwei voneinander unabhängigen Elementen: Ein **öffentlicher Teil**

(<https://cyberpolygon.com/gallery/>) mit Stellungnahmen und Talkrunden zugeschalteter Konzern- und Staatsvertreter.

Meinungsverschiedenheiten gibt es in diesen Gesprächen in der Regel nicht, da alle Beteiligten auf Linie des WEF liegen. Der andere Teil der Veranstaltung ist eine zweitägige Übung in digitaler Unternehmenssicherheit, wobei die Zuschauer nur wenig Einblick erhalten. Lediglich für wenige Minuten berichten Teilnehmer von BI.Zone im Livestream zwischen den Talkrunden vom Fortgang der Übung. Auch der **schriftliche Abschlussbericht** (https://cyberpolygon.com/upload/media/Cyber_Polygon_2021_Report_EN.pdf) bleibt in dieser Hinsicht schmallippig.

Nur eine Handvoll Teilnehmer kann die Angriffe abwehren

Bei Cyber Polygon 2021 traten nach Angaben der Veranstalter diesmal 200 Teams von IT-Spezialisten an, um unabhängig voneinander simulierte Hackerangriffe auf eine vorbereitete virtuelle Struktur abzuwehren und anschließend forensisch aufzuklären. Die Teilnehmerzahl des Formats stieg über die Jahre stark an. Mehr als 1.200 IT-Teams hatten sich diesmal für die begrenzten Plätze angemeldet, heißt es im Abschlussbericht. Bei der nächsten Veranstaltung im Sommer 2022 soll die Kapazität unbegrenzt sein.

Die Teams gehörten zu Unternehmen unter anderem aus den Sektoren Finanzen, Informationstechnologie und Beratung sowie zu öffentlichen Einrichtungen aus den Bereichen Strafverfolgung,

Verwaltung, Wissenschaft oder Gesundheit. Die Teilnehmer blieben mehrheitlich anonym. Die Organisatoren verraten im Abschlussbericht nur so viel: Die meisten Teams kamen aus Russland, den USA, Großbritannien und Kasachstan (je über zehn). Auch aus der Schweiz und aus Deutschland waren jeweils fünf bis zehn Unternehmen dabei. Namentlich erwähnt wurde davon nur die Deutsche Bank.

Mehr als die Hälfte aller Teilnehmer bei Cyber Polygon 2021 wurde von IT- und Finanzunternehmen entsendet. Teams solcher Unternehmen waren dann laut Abschlussbericht auch die besten der Übung. Allerdings konnten nur „fünf oder sechs“ der 200 Teilnehmer alle verwundbaren Stellen der Manöver-Software in der vorgegebenen Zeit sichern, erläutert (<https://youtu.be/7E00PocVkys?list=PL LH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=19004>) einer der Organisatoren von BI.Zone, der zum Angriffsteam der Übung gehörte.

Dieses verheerende Ergebnis wurde von den Akteuren im Livestream jedoch ungerührt hingenommen und im Abschlussbericht nicht mal erwähnt. Dort ist zu lesen, 15 Prozent der Teilnehmer konnten im ersten Szenario gar keinen Punkt erzielen, was aber dennoch eine deutliche Verbesserung zur Übung Cyber Polygon 2020 sei. Im zweiten Szenario schnitten die Teilnehmer diesmal hingegen um 13 Prozent schlechter ab als im Vorjahr. Die praktischen Konsequenzen solch ernüchternder Ergebnisse thematisieren die Cyber-Polygon-Organisatoren nicht öffentlich.

Angeblicher Angriff auf Cyber Polygon selbst

Nach gut 90 Minuten der fast sechsstündigen, per Livestream übertragenen Sendung **behauptete** (<https://youtu.be/7E00PocVkys?list=PL LH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=5910>) Moderator Alexander Tushkanov, Cyber Polygon sei „gerade vor 15 Minuten“ per **DDOS-Attacke** (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html) von echten Hackern angegriffen worden.

„Man muss immer bereit sein, auch während des Trainings. Unnötig zu sagen, dass der Angriff abgewehrt wurde.“

Wie glaubwürdig das ist, bleibt dahingestellt, jedoch passt solch eine Nachricht hervorragend in das permanent wiederholte Bedrohungsmantra des WEF.

Nur wenige Tage vor Cyber Polygon fand ein sogenannter Lieferkettenangriff („supply chain attack“) auf den US-Softwareanbieter Kaseya große internationale Aufmerksamkeit. Erpresserische Verschlüsselungsprogramme gelangten am 2. Juli über die digitale Lieferkette des Unternehmens in die IT-Systeme von bis zu 1.500 Kaseya-Kunden – darunter die schwedische Eisenbahn, neuseeländische Schulen und deutsche Mittelständler – die daraufhin nicht mehr in ihre Computersysteme gelangen, ohne Lösegeld zu zahlen. Auf einem Lieferkettenangriff basierten auch die Übungsszenarien bei Cyber Polygon 2021.

Geopolitische Begleitmusik: Kaseya-Angriff beschäftigt Putin und Biden

Hier lohnt sich ein kurzer Exkurs: Der Kaseya-Angriff unmittelbar

im Vorfeld von Cyber Polygon ging nach offiziellen Angaben von der Hackergruppe „REvil“ aus. Von dieser werde vermutet, dass sie in Russland sitze, da sie nie Ziele in ehemaligen sowjetischen Ländern angreife, heißt es in angelsächsischen Medien. REvil hatte im Frühling auch den weltgrößten Fleischkonzern JBS Foods gehackt.

Die angegriffene Firma Kaseya erhielt allerdings nur drei Wochen später einen digitalen Generalschlüssel zur Entsperrung der blockierten Daten. Zuerst sei unklar gewesen, woher die Firma den Schlüssel bekommen hatte. Manche Medien **vermuteten** (<https://www.n-tv.de/wirtschaft/Kaseya-Kein-Loesegeld-fuer-Schluessel-gezahlt-article22706130.html>), Kaseya habe das geforderte Lösegeld von 70 Millionen Dollar an REvil bezahlt. Das bestritten die Firmenverantwortlichen jedoch und **sagten** (<https://www.bbc.com/news/technology-57946117>), sie hätten den Schlüssel von einer „vertrauenswürdigen dritten Partei“ erhalten.

Laut Washington Post

(https://www.washingtonpost.com/national-security/ransomware-fbi-revil-decryption-key/2021/09/21/4a9417d0-f15f-11eb-a452-4da5fe48582d_story.html) handelt es sich dabei um das FBI, das sich den Schlüssel durch Zugriff auf den REvil-Server selbst besorgt habe. Die Zeitung geht dieser Behauptung nicht weiter nach, doch auch hier darf an der Erklärung aus anonymen Kreisen Washingtons durchaus gezweifelt werden. Jeder, der den Schlüssel besitzt, kann selbst der Angreifer gewesen sein.

Dass das Ganze wie ein geopolitisches Blame-Game wirkt, erhält zudem Nahrung dadurch, dass der Kaseya-Vorfall zeitnah Thema in einem Gespräch zwischen den Präsidenten Joe Biden und Wladimir Putin war. Resultat: Punktsieg Biden. Denn REvil verschwand nur wenige Tage nach der Attacke aus dem Darknet. US-Medien **stellen es so dar** (<https://edition.cnn.com/2021/07/13/tech/revil-ransomware-disappears/index.html>), als sei dies eine Folge von

Bidens Ermahnungen gegenüber Putin, dieser solle etwas gegen russische Hacker tun, ansonsten werde Biden die US-Dienste anweisen, die Sache selbst in die Hand zu nehmen.

Wie dem auch sei, Kaseya-Chef Fred Voccolla wurde im August 2021 trotz des verheerenden Lieferkettenangriffs auf sein Unternehmen und dessen Kunden nicht entlassen, sondern für erfolgreiche Unternehmensleistung und Produktstärke **ausgezeichnet** (<https://www.kaseya.com/press-release/kaseya-ceo-fred-voccolla-selected-as-a-top-50-saas-ceo-for-second-year-in-a-row/>). Die Hackergruppe REvil tauchte im September wieder auf und führte weitere Erpressungen durch, bevor sie in den folgenden Monaten durch internationale Ermittler endgültig zerschlagen wurde. Verdächtige wurden in Rumänien, Polen, den USA und Südkorea **festgenommen** (<https://www.zeit.de/digital/internet/2021-11/europol-ransomwaregruppe-revil-festnahmen-fbi-loesegeld>). Der Täter im Kaseya-Fall sei ein Ukrainer, wurde gemeldet. Im Januar 2022 **verhafteten** (<https://www.spiegel.de/netzwelt/web/revil-russland-nimmt-mutmassliche-mitglieder-beruechtigter-hacker-gruppe-fest-a-92c10cfa-20f9-4e78-bb18-43233c52d0bb>) russische Behörden bei Razzien 14 weitere Verdächtige.

Russische Regierung ist Ziel von hochkomplexen Hackerangriffen

Zurück zu Cyber Polygon: Genau solche geopolitischen Verwicklungen und instrumentellen Täterspekulationen beim Thema Hacking bilden den Hintergrund eines der interessantesten Gespräche bei Cyber Polygon 2021. Es handelt sich um die **Diskussion** (<https://www.youtube.com/watch?v=P2LwnKjyvqA&list=PL LH6GxQM05JZ1eIqyaATpIef9TrYi6W03&index=10>) des leitenden Microsoft-Sicherheitsberaters Roger Halbheer

mit Igor Lyapunov, dem Vizepräsidenten für Informationssicherheit der russischen Telekom.

In diesem Interview gibt es eine für westliche Ohren eher seltene Information. Lyapunov **berichtet** (<https://youtu.be/P2LwnKjyvqA?list=PLH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=766>) über Cyber-Attacken gegen die russische Regierung. Moskau habe mit hochkomplexen Angriffen zu tun, die versuchen, die Kontrolle über digitale Regierungssysteme zu erlangen. Seine Organisation schätzt die Kosten einer einzigen solchen Attacke auf 1,5 Millionen Dollar, erläutert der russische Experte. Die Angriffe seien sehr schwierig festzustellen und werden von IT-Sicherheitssystemen gar nicht bemerkt. Auf eine neue Ressource unter der Regierungsdomain gov.ru begann bereits fünf Tage, nachdem diese online ging, ein ausgefeilter Angriff.

Die Täterfrage spart Lyapunov zwar aus, aber unter Berücksichtigung von Ziel und offensichtlich vorhandenen Ressourcen ist es eher unwahrscheinlich, dass diese Angriffe von privaten Hackern ausgehen. Allein die indirekte Andeutung, dass westliche Regierungen und Geheimdienste beachtliche Mittel in Hackerangriffe gegen Russland investieren, ruft den Moderator und früheren CNN-Mann Ryan Chilcote auf den Plan, der hier nicht vertiefend nachfragt, sondern wie als Retourkutsche das Narrativ von russischen Hackern ins Spiel bringt, die im Auftrag des Kreml westliche Infrastruktur angreifen.

Microsoft kennt nur anti-westliche Hacker

Dieses in westlichen Debatten zum Thema Hacking dominante Narrativ („Russische Hacker greifen unsere Demokratien an“) kommt bei Cyber Polygon sonst in der Regel nicht zur Sprache — sei

es, um die russischen Gastgeber nicht zu verärgern, sei es, weil diese Erzählung sowieso nur als Theaterdonner für die westliche Medienöffentlichkeit, nicht aber für elitäre Entscheidungsträger gedacht ist, wie die Journalisten Whitney Webb und Johnny

Vedmore **vermuteten**

[\(https://unlimitedhangout.com/2021/02/investigative-reports/from-event-201-to-cyber-polygon-the-webs-simulation-of-a-coming-cyber-pandemic/\)](https://unlimitedhangout.com/2021/02/investigative-reports/from-event-201-to-cyber-polygon-the-webs-simulation-of-a-coming-cyber-pandemic/).

Den Machern des WEF passt das Narrativ offensichtlich nicht ins Konzept. Geht es um die Identität der Angreifer, ist bei Cyber Polygon lediglich die Rede von anonymen „bad guys“, von kriminellen Hackern, die ausschließlich finanziell motiviert zu sein scheinen. Hier in diesem Gespräch ist es kurzzeitig anders.

Microsoft-Mann Halbheer erwähnt zwei Gruppen namentlich:

Nobelium (aus Russland) und Hafnium (aus China). Beide

Gruppierungen sind in diesem **Schaubild**

<https://1gew6o3qn6vx9kp3s42ge0y1-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/5/2021/10/Sample-Nation-State-Actors-scaled.jpg>) des Microsoft-Sicherheitsberichts von 2021 aufgezählt. Der **Bericht** (<https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/>) bezeichnet alle aufgezählten Hackergruppen wie chemische Elemente.

Mehr als die Hälfte aller von Microsoft festgestellten Hackerangriffe seien laut Bericht von Russland ausgegangen. Viele IT-Attacken stammten zudem aus Nordkorea, dem Iran und China. Westliche Hacker kennt der Microsoft-Report überhaupt nicht. Halbheer

bezeichnet

<https://twitter.com/rhalbheer/status/1446142448758099972>) das Papier als "must read".

Hacker versuchen, russischen Finanzmarkt zu destabilisieren

Im Cyber-Polygon-Gespräch beschwichtigt Lyapunov, indem er betont, Cyberkriminalität habe keine Nationalität. Er wirbt für Informationsaustausch und zwischenstaatliche Zusammenarbeit gegen Hacker. Dieselbe Art Angriffe wie gegen staatliche Stellen Russlands gebe es auch auf andere Teile der russischen Infrastruktur, sagt er.

Jedoch schwächt das nicht gerade den Verdacht geheimdienstlicher Täter. Russische Medien berichteten in den Wochen nach Cyber Polygon über massive Angriffe auf russische Banken seit Sommer 2021. In der Zeitung Kommersant hieß es (<https://www.kommersant.ru/doc/4985218>) Mitte September:

„Mehr als 150 Angriffe auf russische Finanzinstitute wurden im letzten Monat aufgedeckt, eine Verdreifachung des Vorjahresrekords (...). Dabei sind die Betrüger von gezielten Angriffen auf einzelne Unternehmen zu massiven Angriffen übergegangen. (...) ,Nach der Hartnäckigkeit und dem Einfallsreichtum der Cyberkriminellen zu urteilen, können wir sagen, dass wir es mit einer komplexen geplanten Aktion zu tun haben, die darauf abzielt, zumindest den russischen Finanzmarkt zu destabilisieren‘.“

Schwab: Mehr Digitalisierung erfordert mehr Sicherheit

Die geheimdienstlich-geopolitische Komponente des Hacking-Themas, und damit die einzige Quelle für Dissens bei Cyber Polygon, tauchte nur noch einmal kurz auf. (2) Ansonsten vermittelten die Vertreter der Konzerne und staatlichen

Einrichtungen in trauter Einigkeit die Botschaften des Weltwirtschaftsforums. Diese öffentlichen Gespräche liefern den Zuschauern aber immerhin einen bemerkenswerten Einblick in einige Vorhaben und Argumentationsweisen derjenigen, die am Aufbau einer digitalen Kontroll- und Überwachungswelt arbeiten.

Die Grundargumentation, die auch Klaus Schwabs 13-minütiges **Grußwort** (<https://youtu.be/DnwtG1VDvh0?t=666>) für Cyber Polygon 2021 durchzieht, geht so: Alle Lebensbereiche werden immer stärker digitalisiert. Corona war der Katalysator dieser Entwicklung. Durch die umfassende Digitalisierung sind jedoch ganz neue Angriffsflächen entstanden. Alles und jeder könne Opfer einer Hacker-Attacke werden. Alles könne von Hackern zur Waffe umfunktioniert werden – sogar Sicherheitsupdates wie bei Lieferkettenangriffen – und jeder könne von Hackern – etwa durch Identitätsdiebstahl – zum Täter gemacht werden. Deshalb müsse auch alles und jeder permanent kontrolliert werden. Letztere Aussage wird von den Akteuren allerdings in wohlklingende oder technische Formulierungen verpackt.

Die „Sicherheit“ soll nach den Vorstellungen des WEF durch Staaten und Konzerne gemeinsam gewährleistet werden. Klaus Schwab **unterstreicht** (<https://youtu.be/DnwtG1VDvh0?t=1065>) in seiner Begrüßungsansprache, dass zwar Regierungen für die Cybersicherheit verantwortlich seien, die fachliche Expertise jedoch häufig im Privatsektor liege. Hieraus leitet er seine Behauptung von zunehmend nötiger Zusammenarbeit von Behörden und Konzernen („Public-private Partnership“) ab – eine Kernforderung des WEF in allen Themenbereichen.

Schwab verzichtete im Gegensatz zum Vorjahr zwar auf apokalyptische Warnungen. Doch nutzt er erneut das Corona-Vokabular, um Hacker-Attacken mit Pandemien zu vergleichen. Masken seien nicht genug gegen das Virus, es müssten Impfungen her.

So müsse man auch bei der IT-Sicherheit weg vom einfachen Schutz hin zur Immunisierung. Schwab spricht von „digitalen Antikörpern“, die bereits in das System eingebaut sein müssten. Konkreter wird er nicht.

Cyber-Immunität und Zero Trust

IT-Unternehmer Jewgeni Kaspersky, Chef der russischen Softwarefirma Kaspersky Lab, benutzt das Vokabular ebenfalls. Er **berichtet** (<https://youtu.be/S9dZsCITfaw?list=PLLH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=2399>) bei Cyber Polygon, dass seine Firma eine Strategie der „Cyber-Immunität“ entwickle. Jedes Modul eines IT-Systems werde hierbei von den anderen „isoliert“ und bekomme eine klare Definition von vertrauenswürdigem Verhalten („trusted behaviour“). Das digitale Sicherheitssystem werde derzeit für Industriesysteme und für das Internet der Dinge entwickelt.

Was klingt wie die digitale Umsetzung von Quarantäne- und AHA-Regeln sei das Zukunftskonzept für kritische Infrastruktur. Es könne Lieferkettenangriffe verhindern, sagt Kaspersky, denn ein infizierter Teil würde andere Teile dann nicht mehr anstecken.

In einem **Expertenvortrag** (<https://www.youtube.com/watch?v=kOjR0T3mVUY>) bei Cyber Polygon wurde zudem von einem Microsoft-Sicherheitsverantwortlichen das Konzept „Zero Trust“ (Null Vertrauen) vorgestellt.

„Dieses Sicherheitskonzept setzt voraus, dass jeder Benutzer oder jedes Gerät seine Anmeldedaten jedes Mal vorlegen muss, wenn er Zugang zu einer Ressource innerhalb oder außerhalb des Netzes anfordert.“

Auch dies klingt, als habe man die 2G-Regel auf die virtuelle Welt

übertragen. Nutzer sollen durch permanentes Ausweisen die eigene Ungefährlichkeit bescheinigen.

Ein weiteres Sicherheitskonzept, das bei Cyber Polygon anklang, ist die biometrische Authentifizierung. Der oben bereits zitierte Schweizer Microsoft-Berater Roger Halbheer **ist überzeugt** (<https://youtu.be/P2LwnKjyvqA?list=PL LH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=705>), dass man sich bald nicht mehr über Passwörter, sondern über biometrische Identifizierung wie Fingerabdruck, Gesichts- oder Iris-Scan in seine Online-Konten einloggt.

Kaspersky: Angriffe auf Lieferketten werden zunehmen

Warum diese extremen Konzepte? Halbheer sagt, in der IT-Sicherheit sei es entscheidend, Identitäten zu schützen, um Daten zu schützen. Kaspersky **erklärt** (<https://youtu.be/S9dZsCITfaw?list=PL LH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=715>), die Zahl der professionellen Hacker-Banden steige schnell an. Sie teilten Informationen untereinander, arbeiteten zusammen und würden immer besser. Diese Argumentation ist für IT-Sicherheitsunternehmer nicht überraschend, gleichwohl passen die Warnungen gut in das Schema des WEF.

Kaspersky befürchtet in Zukunft viel mehr Angriffe auf digitale Lieferketten, da in Zeiten umfassender Digitalisierung nahezu alles zum potenziellen Angriffsziel werden kann. Die EU räumt dem Problem übrigens ebenfalls Priorität ein und führt seit Mitte Januar eine sechswöchige **Übungssimulation** (<https://www.bloomberg.com/news/newsletters/2022-01-13/supply-chain-latest-eu-cyberattack-drills-to-test-supply-chains>) einer großangelegten Cyber-Attacke auf Lieferketten durch.

Auch die nächste bundesweite länder- und ressortübergreifende Katastrophenschutzübung in Deutschland (**LÜKEX 22** (https://www.bbk.bund.de/DE/Themen/Krisenmanagement/LUEKEX/Aktuell/aktuell_node.html)) hat einen Cyberangriff auf Regierung und kritische Infrastruktur zum Thema.

Die Angriffe über digitale Lieferketten der vergangenen Jahre zeigen: Durch Hacker bedroht sind in erster Linie Konzerne, aber dadurch auch die **kritische Infrastruktur** (https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html) in Staaten, die häufig durch private Unternehmen betrieben wird. Kaspersky erläutert, die Sicherheits- und Risikobewertung kritischer Infrastruktur unterscheidet sich stark von der einer normalen Firma. In ersterem Falle ist der Umfang des Risikos nicht vorherzusehen. Schäden seien nahezu unbegrenzt möglich. Wenn ein Kraftwerk angegriffen werde, gehe es eben nicht nur um die Kosten einer Turbine, sondern um die Folgewirkungen auf Wirtschaft, Staat und Gesellschaft, weil die Stromversorgung zusammenbricht.

Die grundsätzliche Frage, ob die Durchdigitalisierung sämtlicher Lebensbereiche angesichts derartiger Risiken tatsächlich noch ein positives Kosten-Nutzen-Verhältnis aufweist, bleibt bei der gesamten Veranstaltung jedoch außen vor. Stattdessen **kündigt** (<https://youtu.be/DnwtG1VDvh0?t=297>) der russische Ministerpräsident Michail Mischustin bei Cyber Polygon an, dass auf Weisung Wladimir Putins bis Anfang 2024 alle „sozial signifikanten“ Regierungs- und Behördendienste Russlands in nutzerfreundliche digitale Formate umgewandelt werden.

Überwachung und Beschränkung: Digitales Zentralbankgeld kommt

Fortgeschritten sind in Russland auch die Planungen zur Einführung des digitalen Rubel. In einem Gespräch mit dem Titel „**Neue Welt – neue Währung** (<https://www.youtube.com/watch?v=FMptufdosIO&list=PLLH6GxQM05JZ1eIqyaATpIef9TrYi6W03&index=6>)“ gab Alexey Zabolotkin, eine Führungskraft der russischen Zentralbank, bei Cyber Polygon 2021 Einblicke in das politische Vorhaben. Er **sagt** (<https://youtu.be/FMptufdosIO?list=PLLH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=1157>), der digitale Rubel werde sich von Bargeld und Giralgeld dahingehend unterscheiden, dass er in unverwechselbaren, identifizierbaren Einheiten vorliegen werde. Dies verbessere die Verfolgbarkeit des Geldflusses. Im Klartext: Mit digitalem Zentralbankgeld wird die behördliche Dokumentation und Überwachung jedes Zahlvorgangs möglich.

Noch mehr in sich hat es seine anschließende Aussage:

„Wir untersuchen die Möglichkeit, Bedingungen für die zulässige Verwendung einer bestimmten Währungseinheit festzulegen.“

Das heißt konkret, die Zentralbank möchte entscheiden können, was mit einer Geldeinheit gekauft werden darf und was nicht. Zu den gewaltigen Kontroll- und Lenkungspotenzialen, die solch ein Instrument Regierungen und Zentralbanken gegenüber der Bevölkerung in die Hände legen würde, sagt Zabolotkin nichts. Der russische Banker erklärt die Überlegungen stattdessen am Beispiel von Taschengeld, das Eltern ihren Kindern in digitalen Rubel geben, und dabei etwa ausschließen könnten, dass die Kinder das Geld für Fast Food ausgeben.

Was Zabolotkin nur andeutet: Mit staatlich programmierbarem Geld könnte auch jede andere Verwendung beschränkt oder an die Erfüllung bestimmter Vorbedingungen geknüpft werden. Digitales Zentralbankgeld wäre ein Schlüssel zur Einführung eines effektiven staatlichen Bonussystems.

Ersetzt digitales Zentralbankgeld das Bargeld?

Ein Schritt auf diesem Weg ist die Abschaffung des Bargeldes, da es eine Ausweichmöglichkeit darstellt. Während die russische Zentralbank solch ein Ziel hinter dem digitalen Rubel auf ihrer Website bis heute noch **dementiert**

(https://cbr.ru/eng/analytics/d_ok/dig_ruble/) („Will a digital ruble replace cash? No.“), klingt dies bei Zabotkin schon anders. Im Cyber-Polygon-Gespräch kündigt er beiläufig an: Der (russische) Bürger werde in Zukunft zwischen Giralgeld und digitalem Rubel wählen können, so wie er heute zwischen Giralgeld und Bargeld wähle. Demzufolge würde der digitale Rubel das Bargeld ersetzen.

Die kommerziellen Banken und Zahlungsdienstleister blieben auch beim digitalen Rubel als Akteure zwischen Zentralbank und Bürger geschaltet, beruhigt Zabotkin die Gesprächspartner. Das unterscheidet digitale Zentralbankwährungen (CBDC) von freien Kryptowährungen und ist gerade für die großen Geschäftsbanken und die namhaften Zahlungsdienstleister, die im WEF versammelt sind, von besonderer Bedeutung. Immerhin arbeiten auch westliche Länder an CBDCs.

Seit dem 19. Januar 2022 wird der digitale Rubel in Russland real genutzt. Die Zentralbank startete die erste Testphase in Zusammenarbeit mit zwölf russischen Finanzinstituten – darunter auch die Sberbank. **Zuerst erprobt** (<https://tass.ru/ekonomika/13465621>) werden nun zwei Jahre lang Zahlungen von Bürger zu Bürger. Digitales Zentralbankgeld kann auch ohne Internetverbindung von Smartphone zu Smartphone überwiesen werden. Nach dieser Pilotphase sollen auch Transaktionen zwischen Unternehmen und Konsumenten, zwischen Unternehmen untereinander sowie zwischen Unternehmen und Regierung getestet werden.

China als Vorreiter, EU an Erfahrungsaustausch interessiert

In China sind diese Testphasen noch weiter fortgeschritten. Nach Tests in zehn großen Regionen des Landes, inklusive der bekannten Metropolen, steht die App für den digitalen Yuan seit Jahresanfang für alle Bürger **bereit**

(<https://www.wienerzeitung.at/nachrichten/wirtschaft/international/2134454-China-praesentiert-den-Digital-Yuan.html>). Der E-Yuan soll nach offiziellen Aussagen das Bargeld teilweise ersetzen. Auch die zweckgebundene Programmierung von Geldeinheiten ist bei der chinesischen Digitalwährung möglich.

Der damalige Bundesbankpräsident Jens Weidmann und andere Verantwortliche der Eurozone seien in Hinsicht auf einen digitalen Euro sehr an einem Erfahrungsaustausch mit China interessiert, **berichtete** (<https://www.faz.net/aktuell/finanzen/e-yuan-und-digitaler-euro-deutschland-will-von-china-lernen-17536648.html>) die Frankfurter Allgemeine.

Das Thema hat neben den Aspekten Überwachung und Bargeldabschaffung noch eine bedeutende geopolitische Komponente, die Chinas und Russlands Vorreiterrolle hierbei erklären könnte: Digitale Zentralbankwährungen erleichtern den Ausstieg aus dem westlich dominierten Zahlungssystem SWIFT, da sie internationale Zahlungen unabhängig von US-Sanktionen **ermöglichen**

(<https://www.handelsblatt.com/meinung/kolumnen/asia-technomics/kolumne-asia-technomics-chinas-e-yuan-ist-innovativ-und-reaktionaer-zugleich/27268298.html>).

Kryptowährungen unerwünscht

Es ist ein starkes Indiz für die Bedeutsamkeit des Themas digitale Währungen, dass die Organisatoren des WEF es auch bei Cyber Polygon auf die Tagesordnung setzten. Hacking spielte in dem Gespräch, an dem auch hochrangige Vertreter von Visa und Mastercard teilnahmen, jedenfalls keine Rolle.

Die Vertreter der Kreditkartenkonzerne bestätigen in dem Talk, dass die Corona-Krise ihrem Geschäft einen starken Schub gegeben habe. Mark Barnett von Mastercard sagt, in fünf Monaten Pandemie habe man einen Fortschritt bei der elektronischen Bezahlung gesehen, der ansonsten fünf Jahre gedauert hätte. Matthew Dill (Visa) betont, Covid-19 habe eine bleibende Verhaltensänderung im Bezahlverhalten der Menschen hervorgerufen.

Freie Kryptowährungen wie Bitcoin, die anonym genutzt werden können, sollen nach den Vorstellungen der Cyber-Polygon-Gäste aber besser keine Rolle spielen. Zentralbanker Alexey Zabolotkin erklärt, dass Russland keine Kryptowährungen als Zahlungsmittel im Land akzeptieren werde. Seine Zentralbank **forderte** (<https://invezz.com/de/news/2022/01/22/bank-of-russia-fordert-vollstandiges-krypto-verbot/>) kürzlich ein vollständiges Verbot. In China sind Kryptowährungen bereits illegal.

In einem anderen Gespräch **bezeichnet** (<https://youtu.be/ofDHAy-CHkA?list=PLH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=1402>) Michael Daniel von der Lobbygruppe Cyber Threat Alliance Kryptowährungen als „Treibstoff“ der Ransomware-Industrie — also der Hacker, die wie bei dem Angriff auf Kaseya andere IT-Systeme verschlüsseln und diese erst nach Lösegeldzahlungen in Bitcoin wieder freigeben.

Michael Daniel ist nicht irgendein Lobbyist, sondern war vor seiner **aktuellen Tätigkeit** (https://www.cyberthreatalliance.org/team_member/michael-daniel/) jahrelang Koordinator und Berater für Cybersicherheit von

US-Präsident Barack Obama. (3) Hacking sei heute nicht mehr nur eine kriminelle Handlung, sondern „eine Bedrohung der nationalen Sicherheit und der öffentlichen Gesundheit“, **betont** (<https://youtu.be/ofDHAy-CHkA?list=PLLH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=523>) er in dem Talk ebenfalls.

Drehtüreffekt: Vom staatlichen Posten zum Großkapital

Nicht nur an Michael Daniel, sondern auch am Blick in die Lebensläufe zahlreicher Cyber-Polygon-Teilnehmer zeigt sich, wie weit das Weltwirtschaftsforum mit seinem Vorhaben der Public-private Partnership praktisch schon vorgedrungen ist. Beispielhaft verdeutlicht der **Werdegang** (<https://www.weforum.org/people/troels-oerting-jorgensen-de140be2-a9c3-4f21-9251-c6d281ce9720>) von Cyber-Polygon-Initiator Troels Oerting, wie stark die Kompetenzen und Interessen von Behörden und Konzernen bereits verschmolzen sind. Oerting **moderierte** (<https://www.youtube.com/watch?v=S9dZsCITfaw&list=PLLH6GxQM05JZ1eIqyaATpIef9TrYi6W03&index=14>) auch eine der Gesprächsrunden.

Er **arbeitete**

(https://web.archive.org/web/20150329035019/http://www.bka.de/nn_193484/DE/Publikationen/Herbsttagungen/2014/Programm/ht2014OertingVita.html) seit den 1990er Jahren auf verschiedenen Leitungsposten bei der dänischen Polizei und beim dänischen Inlandsgeheimdienst. Von dort wechselte er 2009 zu Europol, wo er seit 2013 das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) leitete. 2015 ging Oerting in die Privatwirtschaft – nämlich als Chef für Informationssicherheit zur britischen Großbank Barclays. 2018 heuerte er schließlich beim WEF

als Leiter des Centre for Cybersecurity an. Mittlerweile hat er sein eigenes IT-Unternehmen namens Bullwall.

Mit Jürgen Stock und Craig Jones — beide von Interpol — sind noch zwei weitere (allerdings aktive) Repräsentanten internationaler Polizeiorganisationen bei Cyber Polygon beteiligt. In ihren Aussagen vertreten sie bei dieser Veranstaltung nahezu eins zu eins die Positionen des WEF, als wären die Interessen von öffentlicher Strafverfolgung und superreichen Konzerneigentümern identisch. Auch Stock, bis 2014 Vizepräsident des Bundeskriminalamtes, spricht von „Cyber-Hygiene“ und betont in seiner Rede durchgängig, dass Online-Kriminalität vom privaten und öffentlichen Sektor zusammen bekämpft werden müsse. Die Cybersicherheit-Industrie bezeichnet er als Alliierten von Interpol.

Solche Polizeikräfte wirken wie Idealtypen der Public-private Partnership, die sich die Macht- und Finanzeliten des WEF wünschen. Auch Interpol selbst wird inzwischen nicht mehr allein von den rund 190 Mitgliedsstaaten, sondern auch durch Konzerne **finanziert** (<https://www.tageblatt.lu/headlines/wer-finanziert-interpol-polizei-organisation-stoesst-auf-kritik-aus-luxemburg/>) — unter anderem durch die **Pharmaindustrie** (<https://www.zeit.de/2013/42/internationale-polizeiorganisation-interpol-pharmaindustrie>).

Ausblick: Daten sammeln, Menschen kontrollieren

Der Generalverdacht, der mit Corona erstmals umfassend in die analoge Welt getragen wurde — jeder sei ein potenzielles Sicherheitsrisiko —, soll offensichtlich auf die digitale Welt übertragen werden. Veranstaltungen wie Cyber Polygon sind Teil der WEF-Strategie, dieses Mantra in der Öffentlichkeit zu

verankern. Setzt sich diese Argumentation durch, könnte Cyberkriminalität in Zukunft dieselben politischen Funktionen erfüllen wie der Terrorismus in den Jahren nach 9/11 oder wie Corona aktuell: ein allgegenwärtiger Angstmacher und eine Universalrechtfertigung für Gesetzesverschärfungen.

Die permanent bei Cyber Polygon beschworene Parallelität von Pandemie und Hacking ist ein Zeichen für diese Absicht. Klaus Schwab und Co. haben seit einigen Jahren das Hacking als Thema mit großem Potenzial zur politischen Instrumentalisierung ausgemacht. Angriffe auf Krankenhäuser (**Beispiel Uniklinik Düsseldorf** (<https://www.welt.de/vermishtes/article215908784/Hacker-Angriff-auf-Uniklinik-Duesseldorf-Patientin-stirbt-nach-Verlegung.html>)) oder Kraftwerke (**Beispiel Stadtwerke Pirna** (<https://www.mdr.de/nachrichten/sachsen/dresden/freital-pirna/cyberangriff-stadtwerke-pirna-100.html>)), wie sie bei Cyber Polygon besprochen wurden, eignen sich für interessierte Akteure hervorragend, um die beängstigende Dimension möglicher Hackerangriffe aufzuzeigen. Wer würde sich nicht vor einem anhaltenden Blackout fürchten? Wer könnte gegen Schutzmaßnahmen sein?

Solchen Initiativen des Großkapitals werde immer ein wohlwollender, menschenfreundlicher Mantel umgehängt, von dem man sich nicht täuschen lassen sollte, argumentiert der Journalist Norbert Häring in seinem aktuellen Buch „Endspiel des Kapitalismus“. Dort schreibt er: Die großen Konzerne, die unter anderem im WEF versammelt sind, träumen von einer „totalüberwachten, neofeudalen Welt“ in der Menschen „praktisch nichts mehr tun können, ohne digitale Spuren zu hinterlassen“ (4).

Alle Bürger der Erde sollen demnach bis 2030 mit einer biometrisch unterlegten, digitalen Identität versehen sein, wenn es nach der Initiative ID2020 geht, die unter anderem von Microsoft und der

Impfallianz Gavi **betrieben wird** (<https://id2020.org/alliance>) und sich auf die nachhaltigen Entwicklungsziele (SDG) der Vereinten Nationen beruft. (5) Der gemeinsame Nenner zahlreicher Projekte, Planspiele und Initiativen der Superreichen und ihrer Stiftungen ist laut Häring

„das Ziel der umfassenden, automatisierbaren Sammlung und Speicherung verlässlicher Daten über das Tun und Lassen der Weltbevölkerung. Denn wer die Daten hat, hat die Macht, sowohl in kommerzieller als auch in politischer Hinsicht.“

Nahezu alle bei Cyber Polygon besprochenen Aspekte vom Schutz vor Hacking bis zur digitalen Zentralbankwährung laufen auf dieses Ziel zu.

Redaktionelle Anmerkung: Dieser Beitrag erschien zuerst unter dem Titel „**Menschen kontrollieren**“ (<https://multipolar-magazin.de/artikel/menschen-kontrollieren>) bei Multipolar.

Quellen und Anmerkungen:

(1) Raymond Unger: Das Impfbuch. Über Risiken und Nebenwirkungen einer COVID-19-Impfung (**Scorpio-Verlag** (<https://www.scorpio-verlag.de/Buecher/415/DasImpfbuch.html>), München, 2021), Seite 190

(2) Im Gespräch zu widerstandsfähigen Lieferketten sagt der IT-Sicherheitsunternehmer Jewgeni Kaspersky, das System müsse so gebaut sein, dass ein Hack für die Angreifer teurer wäre als der

Schaden, den sie damit anrichten könnten. Der frühere Europoldirektor und dänische Geheimdienstleiter Troels Oerting **ergänzt** (<https://youtu.be/S9dZsCITfaw?list=PL LH6GxQM05JZ1eIqyaATpIef9TrYi6W03&t=2496>) kurz darauf: Gegen normale Kriminelle sei das eine wirkungsvolle Strategie. Aber staatliche Angriffe würden dadurch nicht verhindert. Da spielten die Kosten keine Rolle. Oerting bestätigt damit indirekt die Vermutung, dass es sich bei den teuren Angriffen auf russische Regierungsinfrastruktur um staatliche Angriffe handelt.

(3) Michael Daniel gehörte allerdings nicht zu den anti-russischen Falken. Nach einem vermeintlichen russischen Hackerangriff auf das Weiße Haus **rechtfertigte**

(https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html) er die Entscheidung, keine Sanktionen

gegen Russland als Strafmaßnahme einzuführen, mit den bemerkenswert offenen Worten: „Es ging [bei dem mutmaßlich russischen Hack] um das Sammeln von Informationen, wie es Nationalstaaten — auch die Vereinigten Staaten — tun. Aus unserer Sicht war es wichtiger, sich auf die Stärkung der Abwehrkräfte zu konzentrieren.“

(4) Norbert Häring: Endspiel des Kapitalismus. Wie die Konzerne die Macht übernahmen und wie wir sie zurückholen. (Quadriga, Köln, 2021), Seite 254

(5) Norbert Häring: Endspiel des Kapitalismus. Seite 242



Stefan Korinth, Jahrgang 1983, ist freiberuflicher Journalist. Er lebt und arbeitet als Autor und Redakteur

in Hannover. Dort studierte er Politikwissenschaften und Soziologie. Für seine Abschlussarbeit forschte er in der Ukraine. Seine journalistischen Arbeitsschwerpunkte sind politische und historische Themen sowie der Ukraine-Konflikt. Er schreibt für mehrere unabhängige Online-Medien und eine Nachrichtenagentur.

Gemeinsam mit Ulrich Teusch und Paul Schreyer gründete er das Magazin **Multipolar** (<https://multipolar-magazin.de/>).

Dieses Werk ist unter einer **Creative Commons-Lizenz (Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International** (<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>)) lizenziert.

Unter Einhaltung der Lizenzbedingungen dürfen Sie es verbreiten und vervielfältigen.