multipolar

Herausgegeben von Stefan Korinth,
Paul Schreyer und Ulrich Teusch

Angriff mit Ansage

Am 9. und 10. Juli veranstaltet das Weltwirtschaftsforum zum dritten Mal die Übung „Cyber Polygon“, die einen Hacker-Angriff mit schwerwiegenden globalen Folgen simulieren soll. Klaus Schwab und weitere Akteure platzieren Cyber-Attacken öffentlich ganz weit oben auf der Liste schwerwiegender Bedrohungen – noch vor Corona. Wörtlich sprechen sie von einer drohenden „Cyber-Pandemie“. Auffällig ist zudem die Einbindung Russlands bei Cyber Polygon. Wie in den Jahren zuvor ist auch diesmal die staatsnahe Sberbank Gastgeber und Initiator des Planspiels.

STEFAN KORINTH, 9. Juli 2021, *5 Kommentare*

Hinweis: *Dieser Artikel ist auch auf Englisch verfügbar.*

Spätestens seit dem Planspiel „Event 201“, das im Oktober 2019 eine weltweite Corona-Pandemie aus Sicht der Entscheidungsträger durchspielte, müssen Simulationen und „Warnungen“ des Weltwirtschaftsforums (WEF) äußerst ernst genommen werden. So darf man Klaus Schwab – den Gründer und Vorsitzenden des WEF – durchaus ernst nehmen, wenn er betont, die Corona-Krise wäre „nur eine kleine Störung“ im Vergleich zu einer gelungenen globalen Cyber-Attacke. Dies betonte er in seiner Eröffnungsansprache zum letztjährigen Planspiel *Cyber Polygon 2020*.

Damit zeigte Schwab die Dimension eines solchen Hackerangriffs auf, der als monströser Blackout jeden Lockdown in den Schatten stellen könnte. Kraftwerke würden ausfallen, das Transportsystem zusammenbrechen, Krankenhäuser kaum noch betrieben werden können – ja unsere gesamte (globale) Gesellschaft wäre gelähmt, erläuterte Schwab im vergangenen Jahr.

Vom 9. bis 10. Juli soll genau das beziehungsweise die Verteidigung gegen solch einen Angriff bei *Cyber Polygon 2021* wieder geübt werden. Cyber Polygon ist eine unter dem Dach des WEF jährliche organisierte Veranstaltung zur IT-Sicherheit. Klar sollte dabei sein, wenn das WEF von „Cyber-Sicherheit" spricht, ist damit die Sicherheit von Konzernen, und mit Abstrichen die von staatlichen Einrichtungen, gemeint. Nichts anderes.

Die per Livestream übertragene Veranstaltung besteht aus zwei parallelen Strängen. Zum einen gibt es eine Online-Konferenz, in der sich „hochrangige Vertreter internationaler Organisationen und führender Unternehmen" in Stellungnahmen und Debatten zum Thema Cybersicherheit äußern – dazu später mehr. Zum anderen wird Cyber Polygon vom WEF als „weltweit größte technische Trainingsübung für Unternehmensteams" vorgestellt. Unter den Teilnehmern finden sich vor allem Unternehmen aus dem Finanz- und IT-Bereich, aber auch Nahrungsmittelkonzerne oder Universitäten.

Angriff auf digitale und analoge Lieferkette

Konkret simuliert werde diesmal eine „targeted supply chain attack on a corporate ecosystem", heißt es, also ein gezielter Angriff auf die digitale Lieferkette eines Unternehmensgeflechts. Unter einer „supply chain attack" wird in der digitalen Informationstechnologie Folgendes verstanden: Bösartiger Computercode wird in eine Software (eines IT-Anbieters) eingeschleust, der die Nutzer vertrauen, und gelangt durch die reguläre Verteilung (Lieferkette) dieser Software in Betriebssysteme, Apps und Updates auf digitale Geräte zahlreicher Nutzer – etwa Firmenkunden und öffentliche Einrichtungen. Die bösartige Software kann am Ziel ganz unterschiedliche Arten von Schaden anrichten. Infolgedessen ist dann auch die reale, materielle Lieferkette eines Wirtschaftssektors betroffen.

Wie so etwas praktisch aussehen könnte, deutete der kürzlich erfolgte Lieferkettenangriff auf den US-Softwareanbieter Kaseya am 2. Juli an. Dessen Fernwartungsprogramm VSA wurde gehackt, woraufhin die anonymen Täter die Daten und Systeme von bis zu 1500 Kaseya-Firmenkunden verschlüsseln konnten und „Lösegeld" forderten. Solche Angriffe mit sogenannten „Erpressungs-Trojanern" werden als Ransomware-Attacken bezeichnet. Die schwedische Supermarktkette Coop, die Kundin von Kaseya ist, musste beispielsweise alle 800 Filialen kurzfristig schließen, da ihre Kassensysteme blockiert waren. Auch deutsche Firmen sind betroffen. "Das ist ein riesiger und verheerender Angriff auf Lieferketten", erklärte ein IT-Sicherheitsexperte der US-Firma Huntress.

Aktuelle Cyberattacken: Ideale Vorlagen für WEF-Warnung

Durch die starke digitale Vernetzung könne ein Hackerangriff eine Kettenreaktion auslösen, die letztlich sogar die weltweite Infrastruktur lahmlegt, so die Warnung des WEF. Ein einziges verwundbares Kettenglied genüge, um das gesamte System zum Einsturz zu bringen. Das heißt: Ein effektiver Hack und plötzlich können Supermärkte, Tankstellen, Banken, Ämter, Bahnhöfe, Flughäfen und andere nicht mehr arbeiten. Und zwar alle gleichzeitig.

Mehrere kürzlich erfolgte Cyber-Attacken auf US-Einrichtungen – etwa Angriffe auf eine Benzin-Pipeline, einen Fleischkonzern und zwei Ministerien – verleihen dieser Warnung im zeitlichen Vorfeld von Cyber Polygon 2021 besonderen Nachdruck. In einem Artikel bei *Heise* heißt es zum Hackerangriff auf Kaseya:

> *„Das wird nicht der letzte Angriff über Lieferketten gewesen sein. Und auch nicht der schlimmste. Denn die bislang betroffenen Multiplikatoren wie Solarwind Orion oder Kaseya VSA waren eher kleine Fische, die vor diesen Vorfällen kaum jemand kannte. Doch was passiert, wenn es einen der wirklich großen Player trifft, deren Software viele Millionen von Firmen oder auch Endanwender einsetzen? Man kann sich kaum vorstellen, was es bedeutet, wenn ein solcher Supply-Chain-Angriff Microsoft, Apple oder Google trifft.“*

Das wäre dann genau der große Angriff vor dem Cyber Polygon „warnt“. Der Zeitpunkt und die Häufung der supply-chain-attacks kommt den Anliegen des WEF auffällig gelegen. Nach dem Kaseya-Angriff lancierte es zeitnah einen Artikel mit den eigenen Forderungen. Der Alarmismus im Vorfeld des Planspiels Cyber Polygon könnte kaum geeigneter sein.

Cyber Polygon als digitale Kampfarena

Der Begriff Polygon (Vieleck) steht im Russischen für ein militärisches Manöver- und Testgelände. Cyber Polygon ist demnach nicht als harmloses „Online-Training“ zu begreifen, als welches es manche Medien darstellen, sondern wörtlich zu verstehen als virtueller Kampfplatz, auf dem Angreifer und Verteidiger ihre Strategien und Techniken gegeneinander ausprobieren. Kampftruppen hierbei sind jedoch keine staatlichen Armeen, sondern die IT-Sicherheitsteams beteiligter Unternehmen.

Wie auch in klassischen NATO-Militärmanövern nach Schema des Kalten Krieges gibt es bei Cyber Polygon ein angreifendes Team Rot und ein verteidigendes Team Blau. Bei der Bundeswehr heißt das übrigens bis heute „Rotland gegen Blauland“ – sprich Russland gegen NATO. Die Angreifer bei Cyber Polygon 2021 stellt passenderweise das russische Unternehmen BI.Zone, das im echten Leben für die IT-Sicherheit der russischen Sberbank zuständig und Mitorganisator der Veranstaltung ist.

Dieser Rollentausch verdeutlicht, dass in Sachen digitaler Sicherheit jeder Verteidiger praktisch auch zum Angreifer werden kann. Hier gilt letztlich dasselbe Prinzip wie in der Biowaffenforschung: Sie kann gar nicht anders als immer offensiv und defensiv gleichzeitig zu sein. Wer Angriffe eines hypothetischen Feindes simulieren will, um Gegenmaßnahmen zu entwickeln, kommt nicht umhin, sich diese Angriffsfähigkeiten selbst anzueignen.

Jeder an Cyber Polygon teilnehmende Konzern, darunter beispielsweise auch die Deutsche Bank, stellt ein Verteidigungsteam, dass jedes für sich die Angriffe von Team Rot in einer bereitgestellten Trainingsinfrastruktur abwehren muss. Die Cloud-Infrastruktur dafür liefert Cyber-Polygon-„Technologiepartner“ IBM. Unabhängige Teilnehmer sind nicht erlaubt.

Im ersten Szenario erfolgt eine sogenannte Large-Scale-Attack, die die Verteidiger vier Stunden lang in Echtzeit bekämpfen müssen. Im zweiten Szenario müssen die blauen Teams am 10. Juli einen bereits erfolgten Cyberangriff nachträglich untersuchen, um Schwachstellen zu identifizieren und die Vorgehensweise des Angreifers zu analysieren. Näheres zu den Szenarien findet sich auf der Cyber-Polygon-Website. Nach 120 Teilnehmern im vergangenen Jahr, beteiligen sich laut Bi.Zone an der diesjährigen Übung bereits 200 Teams aus fast 50 Ländern. Viele davon bleiben anonym.

Konferenzdebatten: Interpretationsrahmen wird festgezurrt

Parallel zum ersten Szenario der IT-Spezialisten läuft die Online-Konferenz, die live auf der Cyber-Polygon-Website übertragen wird. Wie bereits im vergangenen Jahr werden der Sberbank-Vorsitzende Herman Gref (sitzt auch im WEF-Kuratorium), der russische Ministerpräsident Michail Mischustin und WEF-Chef Klaus Schwab die Veranstaltung mit Statements eröffnen. Es folgen Diskussionsrunden und Interviews, deren namhafteste Teilnehmer der Apple-Mitbegründer Steve Wozniak und der Chef des IT-Sicherheitsdienstes Jewgeni Kaspersky sind. Die Diskussionsrunden sind durchweg besetzt mit Vorsitzenden und weiteren hochrangigen Vertretern unter anderem von Interpol, Microsoft, Visa, Mastercard, IBM und russischen Behörden.

Bei der Themensetzung der Diskussionsrunden wird deutlich, wie die WEF-Organisatoren das Thema Cyber-Sicherheit interpretiert sehen wollen. Beim letztjährigen Cyber Polygon ging es in einer Debatte mit Journalisten beispielsweise um „Fake News“ und in einem Gespräch mit dem früheren britischen Premierminister Tony Blair um die durch Corona veränderte Einstellung der Menschen zur Digitalisierung.

Bei der Konferenz 2021 stehen die Zukunft des digitalen Staatsbürgers und das Thema digitale Währungen auf der Agenda. Vertreter des Roten Kreuz und von Unicef dürfen als Vertreter der humanitär-karitativen Seite erklären, warum Cybersicherheit auch Kindern und Kriegsopfern nützt. Sogar Kosmonauten von der Internationalen Raumstation werden direkt zugeschaltet. Die Cyber-Sicherheit von Konzernen soll offenbar sympathische, schutzbedürftige Gesichter bekommen.

Die Titel der Debatten zeigen hingegen ganz direkt, wohin die politische Reise nach Ansicht des WEF gehen sollte: „Internationale Vorschriften im Internet – notwendig, aber auch möglich?“ oder „Neue Welt – neue Währung“. Letzteres ganz ohne Fragezeichen.

Worin liegt die große Bedeutung von Cyber Polygon?

Konferenzen und Übungen internationaler Organisationen gibt es häufiger – warum also sollte gerade diese Veranstaltung besondere Aufmerksamkeit erfahren? Die Antwort basiert auf einem gewissen Lerneffekt aus vorangegangenen Entwicklungen. Die US-Journalisten Johnny Vedmore und Whitney Webb von *Unlimited Hangout* schreiben:

> *„Wenn die mächtigsten Menschen der Welt, wie zum Beispiel die Mitglieder des WEF, radikale Veränderungen vornehmen wollen, tauchen bequemerweise Krisen auf – sei es ein Krieg, eine Seuche oder ein wirtschaftlicher Zusammenbruch –, die einen "Reset" des Systems ermöglichen, der häufig von einem massiven Transfer von Wohlstand nach oben begleitet wird. In den letzten Jahrzehnten sind solchen Ereignissen oft Simulationen vorausgegangen, die sich häufen, bevor genau das Ereignis eintritt, das sie "verhindern" sollten. Jüngste Beispiele sind die US-Wahl 2020 und COVID-19. (…) Die aktuelle Agenda des Forums und seine bisherige Erfolgsbilanz bei der Ausrichtung prophetischer Simulationen verlangen, dass die Übung [Cyber Polygon 2021] genau unter die Lupe genommen wird.“*

Die WEF-Warnungen vor den Folgen einer weltweiten Cyber-Attacke klingen fast genau wie die WEF-Warnungen (beim Planspiel *Event 201* im Oktober 2019) vor einer weltweiten Pandemie, schreiben Vedmore und Webb. Auch die Lösungsvorschläge des WEF klingen identisch. Vor allem der Ruf nach einer verstärkten „public-private partnership“ sticht immer wieder hervor. Letztlich ein wohlklingender Begriff für die zunehmende

Verschmelzung von staatlichen Einrichtungen und privaten Konzernen – also einer Monopolisierung von Macht, Kapital und Durchgriffsrechten.

Pandemie-Framing

Auch das Vokabular, dass Klaus Schwab und andere an Cyber Polygon beteiligte Akteure, im Zusammenhang mit einem großen Cyberangriff benutzen, erinnert an Corona und zeigt geradezu penetrant, wie das WEF das ganze Thema interpretiert sehen will. Seit 2020 sprechen die Organisatoren wortwörtlich von einer bevorstehenden „Cyber-Pandemie". Das mittlerweile erfolgreich in die Umgangssprache integrierte Corona-Vokabular wird von den Übungsveranstaltern gezielt verwendet, beide Ereignisse („Corona-Pandemie" und „Cyber-Pandemie") immer wieder gleichgesetzt.

Ein gezielt eingesetztes „Virus" oder andere Schadprogramme könnten immer mehr Rechner „infizieren". WEF-Busines-Chef Jeremy Jurgens spricht in dem Zusammenhang von „exponentiellem Wachstum". Das WEF wirbt bei Unternehmern dafür, ihre Firmen gegen eine Cyber-Pandemie zu „impfen" und für „Cyber-Hygiene" zu sorgen. Auch von „Wellen" ist die Rede. In einem Video von Anfang 2021 spricht das WEF von einer „Cyberattacke mit covid-ähnlichen Eigenschaften".

Das Framing trägt Früchte: Im Dezember 2020 bezeichneten mehrere Medien – so etwa die Süddeutsche Zeitung – den Lieferkettenangriff auf die US-Firma Solarwinds als „Angriff mit dem Superspreader".

Ermöglicht das Planspiel späteres Hacking der Teilnehmer?

Beide Stränge von Cyber Polygon – das Hacking-Manöver und die Eliten-Statements – geben Anlass zur Sorge. Wie eine militärische Übung könnte auch Cyber Polygon 2021 als Tarnung oder Sprungbrett für einen echten Angriff verwendet werden. Tatsächlich sind Teile der IT-Sicherheitsteams zahlreicher Unternehmen an diesem Tag in der Abwehrübung gebunden und geben für informierte Fachleute erkennbar ihre Fähigkeiten und Verteidigungsstrategien preis. Interessierte Akteure können hieraus Rückschlüsse auf deren Kompetenzen und Verhaltensweisen bei realen Cyber-Angriffen ziehen. Johnny Vedmore und Whitney Webb merken an,

> *„dass das Wissen, das BI.ZONE durch Cyberdefense-Training über die Schwachstellen globaler Institutionen erlangt hat, eine nützliche Information für die Muttergesellschaft, die Sberbank, und damit für den größten Aktionär der Sberbank, die russische Regierung, sein könnte."*

Die Leistungen der einzelnen Teams werden anhand eines festgelegten Punktekatalogs bewertet und anschließend verglichen. Cyber Polygon bietet demnach einen Spiel- und Wettbewerbscharakter für die teilnehmenden IT-Profis. Diese „Gamification" der Übung sollte kritische Beobachter aufhorchen lassen. Dienen solche Wettbewerbsanreize in der modernen Informationstechnologie doch vor allem als Köder, um bei Betroffenen bestimmte Verhaltensweisen und Informationen zum Vorschein zu bringen.

Agenda-Setting der Superreichen

Auf eine andere Art bedrohlich ist die politische Themensetzung, die das WEF mit der Veranstaltung inhaltlich betreibt. Nach der großen Pandemie wird von Klaus Schwab und Co. hier die nächste globale Bedrohung öffentlich als solche definiert, präsentiert und mental verankert. Dazu wird auch immer wieder der aus Sicht

des WEF richtige politische Umgang mit einem großen Hacker-Angriff erklärt. Die hunderten hochrangigen Teilnehmer von Cyber Polygon sind damit nicht nur Sender, sondern auch Empfänger der WEF-Botschaften.

Sobald die angekündigte globale Cyber-Attacke tatsächlich kommt, wissen alle schon, was nun zu tun ist. Ähnlich funktionierte dies mit der vor 2020 in Planspielen immer wiederholten Botschaft, dass nur die Impfung eine Pandemie beenden könne. Seit die Corona-Krise Anfang 2020 ihren Lauf nahm, werden gar keine anderen Lösungsansätze mehr diskutiert als die „Impfung" der Weltbevölkerung.

Klaus Schwab bezeichnete die Corona-„Pandemie" als Ereignis mit „katalytischem Effekt", weil es die Digitalisierung so dermaßen beschleunigt habe. „In ein paar Monaten haben wir solche Fortschritte in der digitalen Transformation gemacht, die sonst zwei, drei oder noch mehr Jahre gedauert hätten", sagte er bei Cyber Polygon 2020.

Damit entsteht die interessante Situation, dass das WEF genau die katastrophalen Ereignisse, vor denen es im Vorhinein „warnt", tatsächlich sehr befürworten müsste, da seine politisch-ökonomischen Vorstellungen dadurch umso schneller und nahezu widerstandslos umgesetzt werden können. Umso besser, wenn die Umbaupläne schon in der Schublade liegen. Vedmore und Webb schreiben:

> *„Sollten die bei Cyber Polygon simulierten destabilisierenden Ereignisse tatsächlich eintreten, wird dies vom WEF wahrscheinlich ähnlich begrüßt werden, da ein kritisches Versagen des derzeitigen globalen Finanzsystems die Einführung neuer öffentlich-privater "digitaler Ökosystem"-Monopole ermöglichen würde, wie sie in Russland von der Sberbank aufgebaut werden."*

Russlands Rolle

Gastgeber und Organisator von Cyber Polygon ist mit der Sberbank das größte russische Finanzinstitut. Bereits 2019 und 2020 fand die Übung in deren „Security Operations Center" in Moskau statt. Hauptaktionär der Bank ist die Russische Regierung. Die Sberbank hat sich auf den digitalen Markt fokussiert und zwar auch auf Bereiche, die gar nichts mit Finanzdienstleistungen zu tun haben. In den letzten Jahren kaufte sie zahlreiche russische Unternehmen auf, die Onlinedienste anbieten – darunter ein Medienportal, einen Navigationsdienst, eine Immobilienplattform, einen Musikstreamingdienst, einen Gesundheitsdienst und ein Rechenzentrum.

Und noch für das laufende Jahr ist die Ausgabe der ersten russischen Digitalwährung („Sbercoin") geplant. Dies geschehe, sobald die russische Regulierungsbehörde grünes Licht dazu gebe, teilte die Bank im April mit. Sbercoin soll an den Rubel gebunden sein. Die Sberbank wäre damit die erste Bank weltweit, die eine Kryptowährung ausgibt.

Dabei könnte es sich um eine entscheidende Machtposition der Zukunft handeln. Die Bank, beziehungsweise die russische Regierung dahinter, scheint eine Monopolstellung für digitale Finanzdienstleistungen in Russland anzustreben. Perspektivisch hätte die Bank mit der Kontrolle einer de facto staatlich digitalen Währung sogar noch weitaus mehr Machtpotenzial in der Hand. Die Verschmelzung von Staat und privatem Sektor scheinen in der Bank selbst Realität zu werden.

Neben der Sberbank sind wie bereits erwähnt zahlreiche russische Gesprächspartner aus Wirtschaft, Verwaltung und Politik bis hoch zum Premierminister bei Cyber Polygon dabei. Zudem beteiligt sich die staatliche russische Nachrichtenagentur TASS als Medienpartner an der Veranstaltung.

Russische Hacker diesmal nicht der Bösewicht?

Dies alles ist insofern ungewöhnlich, da Russland bisher auch in Sachen Online-Sicherheit immer als der Bösewicht gilt. Von westlichen Politikern und Medien werden staatsnahe russische Hackergruppen, etwa aus dem Geheimdienst, seit Jahren für nahezu jeden Cyberangriff verantwortlich gemacht. So auch bei den letzten Lieferkettenangriffen auf die US-Firma Solarwinds im Dezember 2020, auf den irischen Krankenhausdienst HSE im Mai 2021 oder auf die Firma Kaseya im Juli 2021.

Bei Cyber Polygon hingegen ist im Zusammenhang mit potenziellen Tätern immer nur die Rede von anonymen Kriminellen. Die Organisatoren umgehen das Narrativ also komplett. Vedmore und Webb schreiben:

> *„Das völlige Fehlen des Narrativs "russischer Hacker" bei Cyber Polygon sowie die führende Rolle Russlands bei der Veranstaltung lassen darauf schließen, dass entweder eine geopolitische Verschiebung stattgefunden hat oder dass das von den Geheimdiensten in den USA und Europa verbreitete Narrativ "russischer Hacker" hauptsächlich für die breite Öffentlichkeit und nicht für die bei Cyber Polygon anwesenden Eliten und politischen Entscheidungsträger gedacht ist.“*

Hintergrund könnte sein, dass die westlichen Machteliten Russland und auch China brauchen, um den vom WEF ebenfalls angekündigten großen Umbruch (Great Reset) umzusetzen. Dieser könne nur global funktionieren. Auch Russland und China hätten Interesse daran und beteiligten sich deswegen am offiziellen Corona-Narrativ wie auch an der angeblich bevorstehenden „Cyber-Pandemie“, vermuten die beiden US-Autoren. Cyber Polygon könnte demnach eine Art „russische Charmeoffensive“ sein. Und die Sberbank als Vorreiter Russlands der ideale Gastgeber.

Anonymer Hackerangriff – ein unschlagbarer Joker

Der erwartete Zusammenbruch des internationalen Finanzsystems und die Einführung digitaler Währungen könnten mit einem anonymen Hackerangriff ideal begründet werden, vermuten Vedmore und Webb. Wahrscheinlich werde der Kollaps kontrolliert durchgeführt, damit die Machteliten ihre Macht auch behalten. Anonyme Hacker seien hierbei ideale Täter, nicht nur weil die Superreichen, die unter anderem im WEF organisiert sind, so ihre Verantwortung für den Zusammenbruch des Finanzsystems weit von sich weisen könnten. Sondern auch, weil jedes mögliche Feindbild damit bedient werden könnte: von Nordkorea über Iran bis hin zu sogenannten inländischen Terroristen, schreiben die beiden Autoren von *Unlimited Hangout*.

Ergänzt werden müsste, dass auch russische Hacker als Täter benannt werden könnten – wenn es geopolitisch wieder passt. Vielleicht, indem sie Cyber Polygon arglistig ausgenutzt hätten? Das Planspiel würde sich dann als Falle für den Gastgeber erweisen. Man könne sich sogar vorstellen, dass der Machtzirkel rund um das WEF nicht davor zurückschrecken würde, die Cyber-Attacke selbst durchzuführen, heißt es in einem Video (Minute 26:00) der Express Zeitung.

Zudem könnte so gut wie niemand den Wahrheitsgehalt von Hackingvorwürfen prüfen, da diese Angriffe in sensiblen, geheimgehaltenen Wirtschaftssphären stattfinden und ohne IT-Expertenwissen sowieso nicht zu verstehen sind. Weiterer Vorteil eines großen anonymen Cyberangriffs wäre, dass widerspenstige Unternehmen oder ganze Staaten dadurch parallel ausgeschaltet oder auf Linie gebracht werden könnten –

eine digitale Form der Schutzgelderpressung. Interessanterweise war für den im April aufgeflogenen westlichen Putschversuch in Weißrussland auch ein Hackerangriff auf das Stromnetz des Landes vorgesehen.

Angeblich unvermeidbar

Letztlich bauen die Botschaften des WEF aufeinander auf. Erstens: Corona erzwinge global-einheitliche Reaktionsweisen und die umfassende Digitalisierung des Lebens. Zweitens: Drohende Cyber-Angriffe erforderten die Einrichtung einer gemeinsamen globalen Sicherheitsarchitektur von Staaten und Konzernen. Und da in der digitalen Welt prinzipiell alles hackbar ist, wie die Firma BI.Zone in diesem Video selbst darlegt, müssten die Zugriffsrechte der Sicherheitsdienste maximal, umfassend und tiefgehend sein.

Die gesamte Krise könnte nicht nur dazu benutzt werden, Zugriffsrechte von Staaten und Unternehmen auszuweiten sowie digitale Zentralbankwährungen einzuführen, sondern auch die verpflichtende digitale biometrische Identität (ID) durchzusetzen, für die der britische Ex-Premier Tony Blair bei Cyber Polygon 2020 geworben hat. Auch digitale Impfpässe könnten integriert werden. Tony Blair sagte, die Einführung einer digitalen ID sei unvermeidbar. „Absolut unvermeidbar!“

Unvermeidbar war bei Cyber Polygon 2020 eines der entscheidenden Wörter, das immer wieder fiel. Die ständig voranschreitende Digitalisierung sei unvermeidbar, die globale Krise sei unvermeidbar, ein großer Cyberangriff sei unvermeidbar. Die Verwendung des Begriffs gehört zu den verschleiernden Hauptstrategien der Einpeitscher des modernen Überwachungskapitalismus, stellte die Ökonomin Shoshana Zuboff in ihrem aktuellen Buch zum Thema (Seite 260) fest:

> *„Das Bild von Technologie als autonomer Kraft, deren Handlungen und Folgen unvermeidbar seien, wird seit Jahrhunderten dazu eingesetzt, die Fingerabdrücke der Macht zu verwischen und sie von jeder Verantwortung zu befreien. Das Monster war’s, nicht Victor Frankenstein.“*