Vom „Event 201“ zum „Cyber-Polygon“: Die Simulation einer kommenden „Cyber-Pandemie“ durch das WEF

- uncut-news.ch
- Februar 12, 2021

Letztes Jahr hat sich das Weltwirtschaftsforum mit der russischen Regierung und globalen Banken zusammengetan, um eine hochkarätige Cyberangriffssimulation durchzuführen, die auf die Finanzindustrie abzielte, ein tatsächliches Ereignis, das den Weg für einen „Reset“ der Weltwirtschaft ebnen würde. Die Simulation mit dem Namen Cyber Polygon war möglicherweise mehr als eine typische Planungsübung und weist Ähnlichkeiten mit der vom WEF gesponserten Pandemie-Simulation Event 201 auf, die kurz vor der COVID-19-Krise stattfand.

Am Mittwoch kündigte das Weltwirtschaftsforum (WEF) zusammen mit der russischen Sberbank und ihrer Cybersecurity-Tochter BI.ZONE an, dass im kommenden Juli eine neue globale Cyberangriffssimulation stattfinden wird, um die Teilnehmer in der „Entwicklung sicherer Ökosysteme“ zu unterweisen, indem ein Cyberangriff auf die Lieferkette simuliert wird, ähnlich dem jüngsten SolarWinds-Hack, der die „Cyber-Resilienz“ der Übungsteilnehmer bewerten soll. Auf der neu aktualisierten Veranstaltungswebsite warnt die Simulation mit dem Namen Cyber Polygon 2021 unheilvoll davor, dass angesichts der Digitalisierungstrends, die vor allem durch die COVID-19-Krise vorangetrieben wurden, „ein einziges verwundbares Glied ausreicht, um das gesamte System zum Einsturz zu bringen, genau wie der Dominoeffekt“, und fügt hinzu, dass „ein

sicherer Ansatz für die digitale Entwicklung heute die Zukunft der Menschheit für die nächsten Jahrzehnte bestimmen wird.“

Die Übung kommt einige Monate, nachdem das WEF, die „internationale Organisation für öffentlich-private Zusammenarbeit“, die die reichste Elite der Welt zu ihren Mitgliedern zählt, offiziell ihre Bewegung für einen Great Reset angekündigt hat, der den koordinierten Übergang zu einer globalen Wirtschaft der vierten industriellen Revolution beinhalten würde, in der menschliche Arbeitskräfte zunehmend irrelevant werden. Diese Revolution, deren größter Befürworter WEF-Gründer Klaus Schwab ist, stellte die WEF-Mitglieder und -Organisationen bisher vor ein großes Problem: Was wird mit den Massen von Menschen geschehen, die durch die zunehmende Automatisierung und Digitalisierung der Arbeitswelt arbeitslos werden?

Neue Wirtschaftssysteme, die digital basieren und entweder mit Zentralbanken zusammenarbeiten oder von diesen geleitet werden, sind ein wichtiger Teil des Great Reset des WEF, und solche Systeme wären Teil der Antwort auf die Kontrolle der Massen der kürzlich arbeitslos gewordenen Menschen. Wie andere bemerkt haben, würden diese digitalen Monopole, nicht nur bei Finanzdienstleistungen, denen, die sie kontrollieren, erlauben, einer Person das Geld und den Zugang zu Dienstleistungen „abzuschalten“, wenn diese Person bestimmte Gesetze, Mandate und Vorschriften nicht einhält.

Das WEF hat solche Systeme aktiv gefördert und geschaffen und nennt sein bevorzugtes Modell neuerdings „Stakeholder-Kapitalismus“. Obwohl es als eine „inklusivere“ Form des Kapitalismus beworben wird, würde der Stakeholder-Kapitalismus im Wesentlichen den öffentlichen und den privaten Sektor verschmelzen und ein System schaffen, das Mussolinis korporatistischem Stil des Faschismus viel ähnlicher ist als alles andere.

Doch um dieses neue und radikal andere System einzuführen, muss das aktuelle korrupte System irgendwie in seiner Gesamtheit zusammenbrechen, und sein Ersatz muss den Massen erfolgreich als irgendwie besser als sein Vorgänger vermarktet werden. Wenn die mächtigsten Menschen der Welt, wie z.B. 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 Reichtum 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. Eines dieser Ereignisse, Event 201, wurde im Oktober 2019 vom Weltwirtschaftsforum mitveranstaltet und simulierte eine neuartige Coronavirus-Pandemie, die sich weltweit ausbreitet und große Störungen in der Weltwirtschaft verursacht und das nur wenige Wochen bevor der erste Fall von

COVID-19 auftrat. Cyber Polygon 2021 ist nur die jüngste derartige Simulation, die vom Weltwirtschaftsforum mitfinanziert wird. Die aktuelle Agenda des Forums und seine bisherige Erfolgsbilanz bei der Durchführung prophetischer Simulationen verlangen, dass die Übung genau unter die Lupe genommen wird.

Obwohl Cyber Polygon 2021 noch Monate entfernt ist, ging Cyber Polygon 2020 voraus, eine ähnliche, vom WEF gesponserte Simulation, die im vergangenen Juli stattfand und in der Redner vor einer kommenden tödlichen „Pandemie“ von Cyberangriffen warnten, die hauptsächlich zwei Wirtschaftssektoren, das Gesundheitswesen und das Finanzwesen, betreffen würden. Cyber Polygon 2020 wurde offiziell als „internationales Online-Training zur Erhöhung der globalen Cyber-Resilienz“ beschrieben und involvierte viele der weltweit größten Tech-Unternehmen und internationalen Behörden, von IBM bis INTERPOL. Es gab auch viele überraschende Teilnehmer bei der Veranstaltung, von denen einige traditionell als Gegner westlicher imperialer Interessen angesehen werden. Zum Beispiel war die Person, die ausgewählt wurde, um das Cyber Polygon Event zu eröffnen, der Premierminister der Russischen Föderation, Mikhail Mishustin, und der Hauptveranstalter, BI.ZONE, war eine Tochtergesellschaft der von der russischen Regierung kontrollierten Sberbank. Dies deutet darauf hin, dass das überstrapazierte „russische Hacker“-Narrativ sich dem Ende zuneigt oder bald gegen einen anderen Buhmann ausgetauscht wird, der angesichts der aktuellen politischen Realitäten besser geeignet ist.

Neben Mishustin nahmen auch WEF-Exekutivdirektor Klaus Schwab und der ehemalige britische Premierminister Tony Blair an der Veranstaltung Cyber Polygon 2020 teil, die jährlich wiederholt werden soll und viele Ähnlichkeiten mit dem Event 201 von 2019 aufweist. Anstatt sich auf eine mögliche medizinische Pandemie vorzubereiten, konzentrierte sich Cyber Polygon 2020 auf die Vorbereitung auf eine „Cyberpandemie“, von der Mainstream-Medien wie der New Yorker behaupten, sie sei „bereits im Gange“. Angesichts der jüngsten Simulationen des WEF scheinen mächtige Milliardärsunternehmer und Banker bereit zu sein, sowohl physische als auch digitale Pandemien zu nutzen, um unsere Gesellschaften nach ihrem eigenen Entwurf und zu ihrem eigenen Vorteil zu reformieren.

Die Architekten von Cyber Polygon

Nach Angaben der russischen Cybersecurity-Firma BI.ZONE nahmen 120 Organisationen aus 29 Ländern an den beiden Szenarien teil, die bei Cyber Polygon 2020 simuliert wurden, wobei angeblich fünf Millionen Menschen in über 57 Ländern den Livestream verfolgten. Wie viele Veranstaltungen im Jahr 2020 wurden auch die Cyber Polygon-Simulationen aufgrund der COVID-19-Beschränkungen online durchgeführt. Zusammen mit dem World Economic Forum leitet BI.ZONE, eine Tochtergesellschaft der Sberbank, das Cyber Polygon Projekt. Der größte Anteilseigner der Sberbank ist seit letztem Jahr die

russische Regierung, weshalb sie von englischsprachigen Medien oft als staatlich kontrollierte Bank bezeichnet wird.

Die Veranstaltung 2020 wurde mit einer Ansprache des russischen Premierministers Mischustin eröffnet, der schon vor seinem Eintritt in die Politik westliche Tech-Unternehmen umworben hat. 1989 schloss Mischustin sein Studium an der Moskauer Staatlichen Technologischen Universität (allgemein bekannt als Stankin) mit einem Abschluss in Systemtechnik ab. In den 1990er Jahren arbeitete er beim International Computer Club, einer gemeinnützigen Organisation, die sich zum Ziel gesetzt hat, „westliche fortschrittliche Informationstechnologien“ nach Russland zu holen. Zwischen 1996 und 1998 war Mishustin Vorstandsvorsitzender des ICC, doch das Unternehmen wurde 2016 aufgelöst. Zwischen 2010 und 2020 diente er als Leiter des Föderalen Steuerdienstes der Russischen Föderation. Obwohl er nie zuvor politische Ambitionen gezeigt hatte, wurde er am 16. Januar 2020 durch einen Erlass von Präsident Putin zum Premierminister der Russischen Föderation ernannt.

Während Mischustins Begrüßungsrede auf dem Cyber Polygon 2020 des WEF warnte der russische Premierminister vor der Notwendigkeit, eine öffentliche Politik zu schaffen, um „die digitale Sicherheit kritischer Aktivitäten zu stärken, ohne die Vorteile der digitalen Transformation in kritischen Sektoren zu untergraben, die die Nutzung und Offenheit digitaler Technologie unnötig einschränken würde.“ Die Erklärung legt nahe, dass „unnötige Einschränkungen“ mit der Zeit als notwendig angesehen werden könnten.

Mischustin erklärt weiter, dass Russlands wirtschaftlicher Aufschwung nach dem COVID auf der „zunehmenden Digitalisierung der Wirtschaft und der Regierung“ basieren wird und fügt hinzu, dass „wir die Anzahl der verfügbaren digitalen öffentlichen Dienstleistungen drastisch erhöhen und grundlegend neue Unterstützungsmaßnahmen für digitale Unternehmen einführen werden.“ Er erklärte auch, dass „Russland ein gemeinsames nationales System zur Identifizierung und Verhinderung von Cyberangriffen entwickelt hat, in das die Informationssysteme der Regierungsbehörden eingebunden sind.“ Er sprach vor dem Cyber Polygon-Publikum auch darüber, dass die internationale Gemeinschaft zusammenkommen muss, um eine „globale Cyberbetrugs-Pandemie“ zu verhindern.

Die Sberbank, das größte russische Bankinstitut und ehemalige sowjetische Sparmonopol, das ursprünglich von Nikolaus I. gegründet wurde, war neben dem Weltwirtschaftsforum offizieller Gastgeber der Cyber Polygon 2020 Veranstaltung. Wie der Economist im Januar 2021 berichtete, hat der russische Bankenriese damit begonnen, sein Geschäft neu zu gestalten, um zu einem Giganten der Verbrauchertechnologie zu werden. Die Sberbank hat rund 2 Milliarden Dollar für Technologie und Akquisitionen ausgegeben, darunter die Übernahme des Internet-Medienkonzerns Rambler, den sie 2020 vollständig übernommen hat. Erst am 30. Dezember 2020 erwarb die Sberbank Doma.ai,

das sich selbst als „eine bequeme Immobilienverwaltungsplattform“ beschreibt. Am 15. Juni 2020 kaufte die Sberbank 2GIS, ein Karten-, Navigations- und Branchenverzeichnis mit über 42 Millionen monatlich aktiven Nutzern. Zu den zweiundzwanzig Investitionen der Sberbank, elf davon als Hauptinvestor, gehören einige der meistgenutzten Dienste in Russland, und es ist ihre klare Absicht, ein digitaler One-Stop-Shop für alle Dienstleistungen zu werden. Die Bank wurde auch Eigentümerin eines der größten Rechenzentren in Europa, als das Rechenzentrum South Port im November 2011 eröffnet wurde und die bestehenden sechsunddreißig regionalen Rechenzentren ersetzte. Die Sberbank wird die erste Bank der Welt sein, die im März dieses Jahres ihre eigene Kryptowährung Sbercoin und ein digitales Finanz-„Ökosystem“ einführt. Sie kündigte den kommenden Sbercoin, einen „Stablecoin“, der an den russischen Rubel gebunden ist, nur wenige Wochen nach der Cyber Polygon 2020 Übung an.

Die Allianz der Sberbank mit dem WEF und ihre Prominenz bei Cyber Polygon 2020 wurde bei der Veranstaltung während der Begrüßungsrede von Klaus Schwab hervorgehoben. Schwab bedankte sich besonders bei Herman Gref, einem Mitglied des Kuratoriums des Weltwirtschaftsforums und CEO der Sberbank, und sprach eine eindringliche Warnung aus:

Wir alle kennen das Schreckensszenario eines umfassenden Cyberangriffs, der die Stromversorgung, den Transport, die Krankenhausversorgung, unsere Gesellschaft als Ganzes zum Erliegen bringen würde, aber wir schenken ihm noch zu wenig Beachtung. Die COVID-19-Krise wäre in dieser Hinsicht als eine kleine Störung im Vergleich zu einem großen Cyberangriff zu sehen. Wir müssen uns in einer solchen Situation fragen, wie wir so etwas zulassen konnten, obwohl wir alle Informationen über die Möglichkeit und Schwere eines Risikoangriffs hatten. Cyberkriminalität und globale Zusammenarbeit sollten ganz oben auf der globalen Agenda stehen.

Ähnliche Warnungen wurden bei einer ebenfalls vom Weltwirtschaftsforum mitgesponserten Simulation für 2019, Event 201, ausgesprochen. Event 201, das nur wenige Monate vor der COVID-19-Krise eine globale Pandemie simulierte, warnte in seiner offiziellen Dokumentation vorausschauend: „Die nächste schwere Pandemie wird nicht nur große Krankheiten und Verluste an Menschenleben verursachen, sondern könnte auch große kaskadenartige wirtschaftliche und gesellschaftliche Folgen auslösen, die stark zu den globalen Auswirkungen und dem Leid beitragen könnten.“ Im Gegensatz zu ähnlichen Simulationen, die in der Vergangenheit durchgeführt wurden, setzte sich Event 201 für einen „Public-Private-Partnership“-Ansatz zur Bekämpfung von Pandemien ein, mit dem Fokus auf der Einbindung „des privaten Sektors in die Epidemie- und Ausbruchsvorbereitung auf nationaler oder regionaler Ebene“. Das WEF ist unter anderem ein großer Befürworter der Verschmelzung von öffentlichem und privatem Sektor auf globaler Ebene und bezeichnet sich selbst

als „internationale Organisation für privat-öffentliche Zusammenarbeit“. Es ist daher nicht überraschend, dass ihre neueste Katastrophensimulation, die sich auf Cyberangriffe konzentriert, genau diese Agenda fördert.

Die Redner bei Cyber Polygon 2020

Neben Schwab und Mishustin nahmen zwanzig weitere Referenten an Cyber Polygon 2020 teil, darunter einige große Namen aus der politischen Führungsriege. Zunächst diskutierte Herman Gref mit dem ehemaligen britischen Premierminister Tony Blair, der sich seit Jahrzehnten für digitale Identitätssysteme einsetzt. Blair sagte dem CEO der Sberbank ohne Umschweife, dass biometrische digitale Identitätssysteme „zwangsläufig“ die Werkzeuge sein werden, die die meisten Regierungen einsetzen werden, um mit zukünftigen Pandemien umzugehen. Blair, der mit Gref über die Coronavirus-Pandemie diskutierte, sprach sich für die härtesten Abriegelungsmaßnahmen aus und sagte, die einzige Alternative zu biometrischen digitalen Identitäten sei es, „die Wirtschaft abzuriegeln“.

Als nächstes diskutierte Sebastian Tolstoy, Ericssons Generaldirektor für Osteuropa, Zentralasien und Russland und derzeitiger Vorsitzender der Tolstoy Family Foundation in Schweden, mit Alexey Kornya. Kornya ist Präsident, CEO und Vorsitzender der Geschäftsführung von Mobile TeleSystems. Zuvor arbeitete er für PricewaterhouseCoopers und AIG-Brunswick Capital Management bei North-West Telecom. Tolstoy und Kornya präsentierten auf der Cyber Polygon 2020 ein Segment mit dem Titel „Building a Secure Interconnected World: What Is the Role of the Telecom Sector?“, in dem sie die Bedeutung der digitalen Kommunikation und Konnektivität für unsere moderne Lebensweise diskutierten.

Im nächsten Segment sprach Nik Gowing, BBC World News-Moderator zwischen 1996 und 2014 und Gründer und Direktor von Thinking the Unthinkable, mit Vladimir Pozner, Journalist und Rundfunksprecher, über das Thema „Fake News“ in einem Gespräch, das in seinen Argumenten und seinem Ansatz tatsächlich etwas erfrischend war.

Stéphane Duguin, der CEO des CyberPeace Institute, einer in Genf ansässigen Firma, die sich selbst als „Bürger, die Frieden und Gerechtigkeit im Cyberspace suchen“ beschreibt, hielt anschließend einen Vortrag vor den Millionen von Zuschauern, die die Simulation verfolgten. Das CyberPeace Institute, das unter anderem von Microsoft, Facebook, Mastercard und der Hewlett Foundation finanziert wird, behauptet, seinen Kunden dabei zu helfen, „die digitale Widerstandsfähigkeit und die Fähigkeit zu erhöhen, auf Cyberangriffe zu reagieren und sich von ihnen zu erholen“. Die Hauptunterstützer des CyberPeace Institute gehören auch zu den Top-Unterstützern der Global Cyber Alliance, die den öffentlichen Sektor der USA, Großbritanniens und Frankreichs mit multinationalen Unternehmen und geheimdienstlichen Cybersecurity-Firmen

vereint und „einen koordinierten Ansatz und eine nicht-traditionelle Zusammenarbeit“ anwendet, um „Cyber-Risiken zu reduzieren.“

Duguin, der auch im Beirat des Global Forum on Cyber Expertise sitzt, hat kürzlich die Initiative Cyber4Healthcare ins Leben gerufen, einen „kostenlosen“ Cybersecurity-Service für Gesundheitsdienstleister im Kampf gegen die COVID-19-Pandemie. Die Cyber4Healthcare-Initiative umfasst als Hauptpartner BI.ZONE sowie Microsoft und die Global Cyber Alliance. Dies ist ein weiterer verdächtiger, mit Microsoft verbundener, kostenloser Cybersicherheitsdienst, der derzeit Gesundheitsdienstleistern auf der ganzen Welt angeboten und von ihnen angenommen wird – und das zu einer Zeit, in der die Warnungen vor einem kommenden Cyberangriff auf die Gesundheitssysteme weltweit immer öffentlicher werden.

Dhanya Thakkar, Senior Vice President AMEA bei Trend Micro, der sich selbst online als Top ASEAN LinkedIn „Cybersecurity Influencer“ bewirbt, und Wendi Whitmore, Vice President IBM X-Force Threat Intelligence, diskutierten als nächstes das Thema „Know Your Enemy: How Is the Crisis Changing the Cyberthreat Landscape?“ Die Anwesenheit von IBM ist aufgrund der langjährigen Beziehung des Unternehmens zur CIA bemerkenswert, die bis in den frühen Kalten Krieg zurückreicht. Das Unternehmen ist so fest verwurzelt, dass die CIA kürzlich ihren Chief Information Officer direkt von IBM Federal rekrutierte. Bevor er zu IBM kam, war Whitmore in leitenden Positionen bei den kalifornischen Cybersicherheitsunternehmen CrowdStrike und Mandiant tätig, wobei letzteres von FireEye in einem Aktien- und Bargeld-Deal im Wert von über 1 Milliarde US-Dollar übernommen wurde. Whitmore war für den Bereich „Professional Services“ verantwortlich. Bemerkenswert ist, dass sowohl CrowdStrike als auch Mandiant/FireEye die wichtigsten Organisationen sind, die die Ermittlungen zum jüngsten SolarWinds-Hack leiten, den der US-Geheimdienst einem „russischen Hacker“ zuschreibt, ohne Beweise zu liefern. Whitmore begann ihre Karriere als Spezialagentin, die beim Air Force Office of Special Investigations Untersuchungen zu Computerkriminalität durchführte.

Jacqueline Kernot, die australische „Partnerin für Cybersicherheit“ bei Ernst and Young, und Hector Rodriguez, Senior Vice President und Regional Risk Officer bei Visa, diskutierten anschließend, wie man sich auf Cyberattacken vorbereiten kann. Kernot arbeitete über fünfundzwanzig Jahre lang als Militäroffizier für das Australian Intelligence Corps und verbrachte zwei Jahre bei IBMs Defence|Space|Intelligence für Tivoli Software in Großbritannien mit „internationaler Verantwortung innerhalb des britischen Verteidigungsministeriums, der Defence Primes und der NATO.“ Ernst and Young und Visa sind neben anderen WEF-verbundenen Unternehmen wie Salesforce im exklusiven Rat für inklusiven Kapitalismus des Vatikans gut vertreten. Der Rat, wie auch das WEF, fordert den Umbau des Wirtschaftssystems, um „nachhaltiger“, „inklusiver“ und „dynamischer“ zu werden, indem „die Macht des privaten Sektors genutzt wird.“

Troels Ørting Jørgensen , Vorsitzender des Beirats des Zentrums für Cybersicherheit des Weltwirtschaftsforums, und Jürgen Stock, der dänische Generalsekretär von INTERPOL, sprachen ebenfalls gemeinsam bei Cyber Polygon über die Veränderungen der globalen Cyberkriminalität im Laufe des vergangenen Jahres. Einige Monate nach seinem Auftritt bei Cyber Polygon gab die dänische Finanzaufsichtsbehörde in einer offiziellen Erklärung bekannt, dass „Troels Ørting das Wirtschaftsministerium darüber informiert hat, dass er aus dem Vorstand der dänischen Finanzaufsichtsbehörde ausscheidet.“ Unter Berufung auf ungenannte Quellen berichtete der dänische Finanznachrichtendienst FinansWatch, dass Ørting in der Zeit zwischen 2015 und 2018, als er als Sicherheitschef bei der Barclays Bank angestellt war, eine Schlüsselfigur bei der Jagd nach einem Whistleblower gewesen sei, der dieselben kriminellen Aktivitäten aufgedeckt hatte, gegen die Ørting bei Cyber Polygon gewettert hatte.

Der Mann, der neben Ørting spricht, Jürgen Stock, ist ein ehemaliger deutscher Polizeibeamter, Kriminologe und Rechtsanwalt. Er wurde 2019 für eine zweite Amtszeit als Generalsekretär von INTERPOL gewählt, eine Amtszeit, die normalerweise fünf Jahre dauert. Craig Jones, der Direktor für Cyberkriminalität bei INTERPOL, nahm ebenfalls an der Diskussion bei Cyber Polygon 2020 teil. Der Neuseeländer war siebenundzwanzig Jahre lang in der Strafverfolgung tätig und gilt als Experte für Ermittlungen im Bereich Cyberkriminalität. Zuvor hatte er mehrere leitende Positionen in der britischen Strafverfolgung inne, zuletzt bei der National Crime Agency.

Petr Gorodov und John Crain wurden auf der Cyber Polygon 2020 Veranstaltung kurz interviewt. Gorodov ist Leiter der Generaldirektion für internationale Beziehungen und Rechtshilfe der Generalstaatsanwaltschaft der Russischen Föderation und sitzt auch in der Kommission für die Kontrolle der Akten von INTERPOL. Er ist Mitglied der Requests Chamber von INTERPOL, die Anträge auf Datenzugang sowie Anträge auf Korrektur und/oder Löschung von Daten, die im INTERPOL-Informationssystem verarbeitet werden, prüft und entscheidet. John Crain ist Chief Security, Stability und Resiliency Officer bei ICANN, der gemeinnützigen Gesellschaft für Internetsicherheit. Er ist derzeit für die Verwaltung des L-Root-Servers verantwortlich, einem der dreizehn Root-Server des Internets, was seine Teilnahme an der Simulation besonders bemerkenswert macht. Bei Cyber Polygon 2020 warb er für eine „langfristige Lösung der Zusammenarbeit in der Cybersicherheits-Community“.

Das letzte Wort bei Cyber Polygon 2020 hatte Stanislav Kuznetsov, stellvertretender Vorstandsvorsitzender der Sberbank. Er ist auch Vorstandsmitglied der Sberbank-Wohltätigkeitsstiftung „Contribution to the Future“, einem Projekt, das russische Schüler von der siebten bis zur elften Klasse für KI (künstliche Intelligenz), maschinelles Lernen und Datenanalyse begeistern und ihnen helfen soll, Mathematik- und Programmierkenntnisse zu

entwickeln. Kuznetsov studierte am Juristischen Institut des Innenministeriums der Russischen Föderation.

Das Hauptereignis: Betreten Sie das Polygon

Bei der Simulationskomponente von Cyber Polygon 2020 nahmen 120 Teams aus neunundzwanzig Ländern an der technischen Cybersecurity-Simulation teil. Während der Online-Veranstaltung „übten[d] die Teilnehmer die Aktionen des Reaktionsteams bei einem gezielten Angriff, der darauf abzielte, vertrauliche Daten zu stehlen und damit den Ruf des Unternehmens zu schädigen.“ Zwei Teams, das Rote und das Blaue, traten in den Simulationen gegeneinander an, wobei das Rote Team, bestehend aus den Trainingsorganisatoren von BI.ZONE, Cyberangriffe simulierte und die Mitglieder des Blauen Teams versuchten, ihre Segmente der Trainingsinfrastruktur zu schützen. Die eigentliche Simulation bestand aus zwei Szenarien, in denen die verschiedenen Untergruppen der Teams Punkte sammeln konnten.

Im ersten Szenario, genannt Defence, übten die Cyber Polygon Teilnehmer die Abwehr eines aktiven APT (Advanced Persistent Threat) Cyberangriffs. Als Ziel des Szenarios wurde angegeben, „Fähigkeiten zur Abwehr von gezielten Cyberangriffen auf ein geschäftskritisches System zu entwickeln“. Die virtuelle Infrastruktur des fiktiven Unternehmens umfasste einen Dienst, der vertrauliche Kundendaten verarbeitet. Dieser Dienst wurde zum Gegenstand des Interesses einer APT-Gruppe, die plante, vertrauliche Benutzerdaten zu stehlen und sie im „Darknet“ weiterzuverkaufen, um daraus finanziellen Nutzen zu ziehen und den Ruf des Unternehmens zu schädigen. Die APT-Gruppe untersuchte das Zielsystem im Vorfeld und entdeckte mehrere kritische Sicherheitslücken. Im Szenario plant die Cyber-„Gang“ einen Angriff am Tag der Übung. Die beteiligten Teilnehmer wurden nach ihrer Fähigkeit beurteilt, den Angriff so schnell wie möglich zu bewältigen, die Menge der gestohlenen Informationen zu minimieren und die Verfügbarkeit der Dienste aufrechtzuerhalten. Die Teilnehmer des Blue Teams konnten beliebige Anwendungen und Tools zum Schutz der Infrastruktur einsetzen und durften auch Systemschwachstellen durch Verbesserung des Service-Codes beheben.

Im zweiten Szenario, genannt Response, mussten die Teams den Vorfall mit „klassischen Forensik- und Threat-Hunting-Techniken“ untersuchen. Anhand der gesammelten Informationen mussten die Teilnehmer ein Dossier zusammenstellen, das den Strafverfolgungsbehörden bei der Suche nach den Verbrechern helfen sollte. Das zweite Szenario hatte zum Ziel, Fähigkeiten in der Untersuchung von Vorfällen zu entwickeln, wobei das Szenario verwendet wurde, in dem Cyberkriminelle durch einen erfolgreichen Phishing-Angriff Zugang zu einem privilegierten Konto erhielten.

Als das BI.ZONE-Team die Ergebnisse der Simulation veröffentlichte, vermieden sie es absichtlich, die echten Namen der Organisationen zu nennen, um „keinen

Wettbewerb zwischen den Teilnehmern auszulösen und ihre Ergebnisse vertraulich zu halten“. Allerdings konnten die Teams später ihre Ergebnisse mit den anderen vergleichen, indem sie ein einfaches Scoreboard verwendeten, und die Gastgeber konnten die entscheidenden Daten analysieren, die verschiedene organisatorische Schwächen jedes der teilnehmenden Teams/Institutionen aufzeigten.

Im Abschlussbericht heißt es, die Ergebnisse zeigten, dass „Banken und Unternehmen aus der IT-Branche die höchste Resilienz zeigten. Das Fachwissen zur Sicherheitsbewertung ist in diesen Sektoren recht gut entwickelt, wobei klassische Forensik und Threat Hunting weit verbreitet sind.“ Laienhaft ausgedrückt, schienen die Teams aus Banken und der IT-Industrie besser auf die Untersuchung und Jagd nach Bedrohungen vorbereitet zu sein als die meisten anderen Branchen. Allerdings erwiesen sich alle beteiligten Teams als weniger gut, wenn es um die erste Abwehr eines Cyberangriffs ging. Der BI.ZONE-Bericht stellt fest: „27% der Teams hatten Schwierigkeiten, Punkte für das erste Szenario zu sammeln, was uns zu dem Schluss kommen lässt, dass einige der Teammitglieder keine oder nur unzureichende Kenntnisse in der Sicherheitsbewertung und dem Schutz von Webanwendungen haben.“ Zum Thema „Threat Hunting“ heißt es im Bericht weiter: „21 % der Teams konnten in der zweiten Runde des zweiten Szenarios keinen einzigen Punkt erzielen. Dies wurde darauf zurückgeführt, dass ‚Threat Hunting‘ ein relativ neuer Ansatz ist und die Mehrheit der Organisationen keine Erfahrung mit der Anwendung dieser Techniken in der Praxis hat.“

Die Cyber Polygon 2020-Veranstaltung hat die Schwäche der von Menschen geführten Abwehrmaßnahmen und der Widerstandsfähigkeit in Bezug auf Cyberdefense offenbart. Dieses Ergebnis ist praktisch für Hightech-Cybersecurity-Unternehmen wie BI.ZONE, die die Überlegenheit von KI-gesteuerten Cybersecurity-Produkten im Vergleich zu „ineffizienten“ menschlichen Mitarbeitern hervorheben wollen. Darüber hinaus ist anzumerken, dass das Wissen, das BI.ZONE durch Cyberdefense-Training über die Schwachstellen globaler Institutionen erlangt, eine nützliche Information für die Muttergesellschaft, die Sberbank, und damit für den größten Aktionär der Sberbank, die russische Regierung, sein könnte.

Holt Russland aus der Kälte?

Obwohl die Behörden der Russischen Föderation daran gewöhnt sind, sowohl politisch als auch physisch im Abseits zu stehen, scheint es eine Veränderung in der üblichen Ordnung der Nationen zu geben. Die Einbeziehung Russlands in eine so wichtige globale Cybersicherheitsinitiative ist etwas überraschend, vor allem nachdem Russland seit mehreren Jahren der Sündenbock für alle Cyberangriffe auf westliche Mächte ist, zuletzt beim SolarWinds-Hack in den USA. Dennoch gab es im Westen keinen Aufschrei über Cyber Polygon 2020, bei dem ein Unternehmen, das sich mehrheitlich im Besitz der russischen

Regierung befindet, durch die Ausrichtung der Übung direktes Wissen über die Schwachstellen der Cyberabwehr von großen globalen Institutionen, Banken und Unternehmen erlangen konnte.

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.

Eine andere Möglichkeit, dass Russland nicht mehr als der ewige Feind des Cyberspace behandelt wird, ist, dass es sowohl mit dem offiziellen Coronavirus-Narrativ als auch mit der angeblich bevorstehenden Cyberpandemie voll und ganz einverstanden ist. Cyber Polygon 2020 schien zum Teil eine russische Charmeoffensive zu sein, die von der Machtelite begrüßt wurde. Tony Blair, der einst Oberst Gaddafi im Namen der internationalen Gemeinschaft die Hand zur falschen Versöhnung reichte, war in den Jahren seit seinem Ausscheiden aus dem öffentlichen Dienst oft an diesen Übungen der internationalen Diplomatie im Namen der Eliten beteiligt. Seine Beteiligung an der Übung könnte dazu gedacht gewesen sein, die Unterstützung unter den westlichen WEF-verbündeten Regierungen für eine noch größere Einbeziehung Russlands in den Großen Reset zu erleichtern. Ein Teil davon ist auf die WEF-geführten Bemühungen zurückzuführen, BRICS-Nationen wie China und Russland in den Schoß des Great Reset zu bringen, weil dies für den Erfolg ihrer Agenda auf globaler Ebene wesentlich ist. Nun ist Russland Vorreiter dieses neuen Modells von angeblich nationalen Finanzsystemen, das das WEF durch die Schaffung eines digitalen Monopols der Sberbank nicht nur für Finanzdienstleistungen, sondern für alle Dienstleistungen innerhalb der Russischen Föderation unterstützt.

Cyber Polygon 2020 war sowohl eine Werbung für pro-russische Beziehungen als auch eine Werbeübung für Klaus Schwab und den Great Reset des Weltwirtschaftsforums. Einige der Personen, die an der Cyber Polygon-Veranstaltung teilnahmen und sie unterstützten, sind auf den höchsten Ebenen der Cyber-Intelligenz tätig; einige mögen sogar inoffizielle Vertreter ihres nationalen staatlichen Geheimdienstapparates gewesen sein. Die Entscheidungen mehrerer nationaler Regierungen, sich direkt an dem vom WEF geleiteten Great Reset zu beteiligen, ist keine „Verschwörungstheorie“. Zum Beispiel schickte die neue Biden-Regierung ihren Klimabeauftragten John Kerry zum WEF-Jahrestreffen im letzten Monat, wo Kerry das Engagement der USA für die Great Reset-Agenda und die damit verbundene Vierte Industrielle Revolution unterstrich, die darauf abzielt, die meisten Jobs, die derzeit von Menschen ausgeführt werden, zu automatisieren. Mit den Regierungen von Russland, China, den USA, Großbritannien, Israel, Kanada und Indien, unter anderem, an Bord mit dieser transnationalen Agenda, wird es zutiefst

beunruhigend, dass hochrangige Agenten sowohl im öffentlichen als auch im privaten Sektor dem WEF beigetreten sind, um eine Krisensimulation durchzuführen, die eindeutig die Great Reset Agenda begünstigen würde.

Wie bereits erwähnt, hat das WEF eine Simulation einer Coronavirus-Pandemie nur wenige Monate vor dem tatsächlichen Ereignis mitgesponsert. Kurz nachdem die COVID-19-Krise im März letzten Jahres ernsthaft begann, bemerkte Schwab, dass die Pandemiekrise genau das war, was benötigt wurde, um den Great Reset zu starten, da sie als bequemer Katalysator diente, um mit der Überholung der Wirtschaft, der Regierungsführung und der sozialen Gesellschaft im globalen Maßstab zu beginnen. Sollten die bei Cyber Polygon simulierten destabilisierenden Ereignisse tatsächlich eintreten, wird dies vom WEF wahrscheinlich ähnlich begrüßt werden, da ein kritisches Versagen des aktuellen globalen Finanzsystems die Einführung neuer öffentlich-privater „digitaler Ökosystem"-Monopole ermöglichen würde, wie sie in Russland von der Sberbank aufgebaut werden.

Dieses Bestreben der Sberbank, den Zugang zu allen privaten und öffentlichen Dienstleistungen sowohl zu digitalisieren als auch zu monopolisieren, mag für einige aufgrund seiner offensichtlichen Bequemlichkeit verlockend sein. Es wird jedoch auch sinnbildlich für das sein, was wir von Schwabs „Great Reset" erwarten können – Monopole aus verschmolzenen Unternehmen des öffentlichen und privaten Sektors, getarnt unter dem Begriff „Stakeholder-Kapitalismus". Was die breite Öffentlichkeit noch nicht weiß, ist, dass sie selbst nicht zu diesen „Stakeholdern" gehören wird, da der Great Reset von den Bankern und der reichen Elite für die Banker und die reiche Elite entworfen wurde.

Was das Cyber-Polygon 2020-Ereignis betrifft, so wird uns die kommende Cyberpandemie prophetisch ins Gesicht geworfen, genau wie die Pandemie-Übung vor dem Auftreten der tatsächlichen Krankheit. Solche prophetischen Warnungen kommen aber nicht nur vom WEF. Zum Beispiel warnte der Leiter des israelischen Nationalen Cyber-Direktorats, Yigal Unna, letztes Jahr, dass ein „Cyber-Winter" von Cyber-Angriffen „kommt und zwar schneller, als selbst ich vermutet habe". Im Cyber-Direktorat arbeitet Unna eng mit israelischen Geheimdiensten zusammen, darunter die berüchtigte Einheit 8200, die auf eine lange Geschichte elektronischer Spionage gegen die USA und andere Länder zurückblicken kann und für mehrere verheerende Hacks verantwortlich war, darunter der Stuxnet-Virus, der das iranische Atomprogramm beschädigte. Der israelische Geheimdienst wird aufgrund der Stärke des israelischen Hi-Tech-Sektors zu den größten Nutznießern des Great Reset gehören. Im vergangenen Monat folgte die Zentralbank der Vereinigten Arabischen Emirate dem Beispiel von Cyber Polygon und führte in Zusammenarbeit mit dem privaten Finanzsektor der Emirate ihre allererste Cyberangriffssimulation durch. Die Unternehmensmedien ihrerseits begannen dieses Jahr mit der Behauptung,

dass „Cyberattacken die nächste Krise für Banken auslösen könnten“ und am 1. Februar, dass „die nächste Cyberattacke bereits im Gange ist“.

Einige werden sagen, dass eine „Cyberpandemie“ eine unvermeidliche Folge der sich schnell entwickelnden High-Tech-Welt ist, in der wir leben, aber es ist dennoch fair, darauf hinzuweisen, dass 2021 das Jahr ist, das viele für die finanzielle Zerstörung großer Institutionen vorausgesagt haben, die zu neuen Wirtschaftssystemen führen wird, die mit dem Großen Reset übereinstimmen. Der unvermeidliche Zusammenbruch des globalen Bankensystems, der aus der seit Jahrzehnten grassierenden Korruption und dem Betrug resultiert, wird wahrscheinlich durch einen kontrollierten Zusammenbruch erfolgen, der es reichen Bankern und Eliten, wie denen, die an Cyber Polygon beteiligt waren, erlauben würde, der Verantwortung für ihre wirtschaftliche Ausplünderung und kriminellen Aktivitäten zu entgehen.

Dies gilt insbesondere für den Cyber Polygon-Teilnehmer Deutsche Bank, dessen unvermeidlicher Zusammenbruch aufgrund der extremen Korruption, des Betrugs und des massiven Engagements in Derivaten der Bank seit Jahren offen diskutiert wird. Ende 2019, Monate vor Beginn der COVID-19-Krise, warnte der CEO der Deutschen Bank, dass die Zentralbanken nicht mehr über Instrumente verfügen, die auf die nächste „Wirtschaftskrise“ angemessen reagieren können. Es ist sicherlich bezeichnend, dass völlig neue Bankensysteme, wie das bald startende digitale Geldmonopol der Sberbank, gerade zu dem Zeitpunkt zu entwickeln begannen, als öffentlich anerkannt wurde, dass die traditionellen Mittel der Zentralbanken, auf wirtschaftliche Katastrophen zu reagieren, nicht mehr tragfähig waren.

Ein massiver Cyberangriff, wie er bei Cyber Polygon 2020 simuliert wurde, würde es ermöglichen, gesichtslose Hacker für den wirtschaftlichen Zusammenbruch verantwortlich zu machen und so die wirklichen Finanzkriminellen von der Verantwortung zu entbinden. Darüber hinaus kann aufgrund der schwierigen Natur der Untersuchung von Hacks und der Fähigkeit von Geheimdiensten, andere Nationalstaaten für Hacks zu beschuldigen, die sie in Wirklichkeit selbst begangen haben, jeder Boogeyman der Wahl beschuldigt werden, ob eine „inländische Terrorgruppe“ oder ein Land, das nicht mit dem WEF verbündet ist (zumindest im Moment), wie Iran oder Nordkorea. Zwischen den gut platzierten Warnungen, Simulationen und dem klaren Nutzen für die globale Elite, die auf einen Great Reset aus ist, scheint Cyber Polygon 2020 nicht nur seinem öffentlich erklärten Zweck gedient zu haben, sondern auch seinen eigenen Hintergedanken.

QUELLE: FROM “EVENT 201” TO “CYBER POLYGON”: THE WEF’S SIMULATION OF A COMING “CYBER PANDEMIC”

Quelle: https://uncutnews.ch/vom-event-201-zum-cyber-polygon-die-simulation-einer-kommenden-cyber-pandemie-durch-das-wef/
20210506 DT (https://stopreset.ch)