multipolar

Herausgegeben von Stefan Korinth,
Paul Schreyer und Ulrich Teusch

Announcing an attack

On July 9 and 10, 2021, the World Economic Forum held its third Cyber Polygon exercise, an exercise designed to simulate a hacker attack with serious global consequences. Klaus Schwab and other players publicly place cyberattacks high on their list of serious threats – even before the coronavirus crisis. They speak, quite literally, of an impending "cyber pandemic." Also striking is the involvement of Russia in Cyber Polygon. As in previous years, the Russian state-affiliated Sberbank is the host and initiator of the simulation.

STEFAN KORINTH, 19. Juli 2021, *0 Kommentare*

Note: *This article ist also available in German.*

Ever since the simulation exercise Event 201, which acted out a global coronavirus pandemic from the perspective of decision-makers in October 2019, these exercises and "warnings" from the World Economic Forum (WEF) need to be taken extremely seriously. In his opening address at last year's Cyber Polygon 2020 simulation, Klaus Schwab, the WEF's founder and chairman, stressed that the coronavirus crisis would be only "a small disturbance" compared to a successful global cyberattack – and he may well be taken seriously.

Schwab described the dimensions of such a hacker attack, which, as a massive blackout, could dwarf any lockdown: Power plants would fail, the transportation system would collapse, hospitals would barely be able to operate – indeed, our entire global society would be paralyzed.

From July 9 to 10, this is exactly what was again rehearsed at Cyber Polygon 2021. Cyber Polygon is an annual IT security event organized under the umbrella of the WEF. However, it should be clear that when the WEF talks about "cybersecurity," it means the security of corporations and, with some exceptions, government institutions. Nothing else.

The event, which was livestreamed, has two parallel elements. The first is an online conference where "senior officials from international organisations and leading corporations" make their statements and engage in debates on cybersecurity – but more on that later. In the second, Cyber Polygon is touted by the WEF as the "world's largest technical training exercise for corporate teams." Among the participants are mainly companies from the financial and IT sectors, but also food companies and universities.

Attack on digital and analog supply chains

This time, a "targeted supply chain attack on a corporate ecosystem" was simulated. In digital information technology, a supply chain attack is defined as follows: Malicious computer code is injected into software (from an IT vendor) that users trust, and which, through the regular distribution (supply chain) of that software into operating systems, apps, and updates, finds its way into the digital devices of numerous users, including corporate customers and public institutions. Malicious software can cause very different types of damage to the target and, as a result, the real, physical supply chain of a business sector is disrupted.

The recent supply chain attack on US software provider Kaseya on July 2 hinted at how this might look in practice. Its remote maintenance program, VSA, was hacked, and anonymous perpetrators were subsequently able to encrypt the data and systems of up to 1,500 Kaseya corporate customers, demanding a "ransom." Such extortion attacks are known as ransomware attacks. For example, the Swedish supermarket chain Coop, a Kaseya customer, had to close all of its 800 stores at short notice because its checkout systems were blocked. German companies were also affected. It was "a colossal and devastating supply chain attack," said an IT security expert from US firm Huntress.

Current cyberattacks: The ideal template for WEF warnings

The WEF warns that due to the current high level of digital networking, a cyberattack could trigger a chain reaction that could ultimately paralyze the global infrastructure. A single vulnerable chain link is enough to bring down the entire system. In other words, one effective hack, and suddenly supermarkets, gas stations, banks, government offices, train stations, airports, and others can no longer operate. All at the same time.

Several recent cyberattacks on US facilities – such as attacks on a gasoline pipeline, a meat producer and two government departments – lend particular weight to this warning in the run-up to Cyber Polygon 2021. An article in Heise had this to say of the hacking attack on Kaseya:

> *"This will not have been the last attack via supply chains. Nor will it be the worst. This is because the multipliers so far affected, including SolarWinds Orion or Kaseya VSA, were small fish that almost no-one had heard of before these incidents. But what will happen when one of the really big players, whose software is used by many millions of companies or end users, is hit? It's hard to imagine what the consequences would be if a supply chain attack hit Microsoft, Apple or Google."*

This, then, would be exactly the kind of major attack that Cyber Polygon is "warning" about. The timing and prevalence of supply-chain attacks is strikingly convenient to the WEF's concerns. After the Kaseya attack, it promptly published an article with its own requirements. The alarmism around the run-up to the Cyber Polygon simulation could hardly be more appropriate.

Cyber Polygon as a digital battle arena

In Russian, the term polygon represents a military maneuver and test zone. Cyber Polygon is therefore not to be understood as a harmless "online training" event, as some media portray it, but literally as a virtual battlefield where attackers and defenders test their strategies and techniques against each other. The combat troops here, however, are not state armies, but rather the IT security teams of the participating companies.

As in classic NATO Cold War military maneuvers, for Cyber Polygon there is an attacking team in red and a defending team in blue. In the German Bundeswehr, incidentally, this is still called "Rotland gegen Blauland" (Redland against Blueland) – i.e. Russia against NATO. The attackers at Cyber Polygon 2021 are, appropriately enough, the Russian company BI.ZONE, which, in real life, is responsible for the IT security of the Russian Sberbank and is a co-organizer of the event.

This role reversal illustrates that when it comes to digital security, any defender could practically also become an attacker. Ultimately, the same principle as in bioweapons research can be applied: There is no alternative to being simultaneously offensive and defensive. Anyone who wants to simulate attacks by a hypothetical enemy in order to develop countermeasures cannot avoid acquiring these attacking capabilities themselves.

Each group participating in Cyber Polygon, including Deutsche Bank, for example, provides a defense team that must fend off attacks from a red team within the provided training infrastructure. The cloud infrastructure for this is provided by Cyber Polygon's "technology partner," IBM. Independent participants are prohibited from taking part.

In the first scenario, a so-called large-scale attack takes place, which the defenders must combat in real time for four hours. In the second scenario, on July 10, the blue teams must retroactively investigate a cyberattack that has already occurred to identify vulnerabilities and analyze the attacker's modus operandi. More details on the scenarios can be found on the Cyber Polygon website. According to BI.ZONE, the number of last year's 120 participants was surpassed, with around 200 teams from nearly 50 countries taking part in this year's exercise. Many of the participants remain anonymous.

Conference debates: The interpretive framework is set

The online conference, which was broadcast live on the Cyber Polygon website, ran parallel to the first scenario involving the IT specialists. As in 2020, Sberbank's chairman, Herman Gref (who also sits on the WEF Board of Trustees), Russian Prime Minister Mikhail Mishustin, and WEF CEO Klaus Schwab opened the event with their introductory statements. This was followed by discussion panels and interviews, where the most notable participants included Apple co-founder, Steve Wozniak, and the head of IT security, Yevgeny Kaspersky. The discussion panels featured various chairmen and other high-ranking representatives from INTERPOL, Microsoft, Visa, Mastercard, IBM, and the Russian authorities, among others.

In setting the topics for the panels, it is clear how the WEF organizers want to see the issue of cybersecurity interpreted. At last year's Cyber Polygon, for example, a debate with journalists focused on "fake news," and a conversation with former British Prime Minister Tony Blair focused on how the coronavirus has changed people's attitudes toward digitization.

The agenda of the 2021 conference included the future of digital citizenship and the topic of digital currencies. Representatives of the Red Cross and UNICEF, symbolic of the humanitarian and charitable side, were given the opportunity to explain why cybersecurity would also benefit children and war victims. Even astronauts from the International Space Station were directly linked in. The cybersecurity of corporations is, apparently, to be given likeable faces that require protection.

The titles of the debates, on the other hand, show exactly which direction the WEF thinks the political journey should be taking: "International regulations on the web – it’s necessary, but is it possible?" or "New world – new currency." The latter is not even a question.

What is the great significance of Cyber Polygon?

Conferences and exercises involving international organizations are frequently held – so why should this particular event receive special attention? The answer to this is based on experience gained from previous developments. US journalists Johnny Vedmore and Whitney Webb of Unlimited Hangout write:

> *"When the world’s most powerful people, such as members of the WEF, desire to make radical changes, crises conveniently emerge—whether a war, a plague, or economic collapse—that enable a 'reset' of the system, which is frequently accompanied by a massive upward transfer of wealth. In recent decades, such events have often been preceded by simulations that come thick and fast before the very event they were meant to 'prevent' takes place. Recent examples include the 2020 US election and COVID-19. … The forum’s current agenda and its past track record of hosting prophetic simulations demands that the exercise [Cyber Polygon 2021] be scrutinized."*

According to Vedmore and Webb, the WEF's warnings of the consequences of a global cyberattack sound almost exactly like their warnings (at the October 2019 simulation exercise, Event 201) of a global pandemic. The WEF's proposed solutions also sound somewhat identical. In particular, the call for increased "public-private partnership" stands out again and again. Ultimately, a rather euphonious term for the increasing merger of state institutions and private corporations – in other words, a monopolization of power, capital, and rights of intervention.

Pandemic Framing

The vocabulary that Klaus Schwab and others involved in Cyber Polygon use in connection with a major cyberattack is also reminiscent of the coronavirus pandemic and, quite penetratingly, shows how the WEF wants to see the whole issue interpreted. Since 2020, the organizers have literally been talking about an impending "cyber pandemic." The coronavirus vocabulary, which has, in the meantime, been successfully integrated into ordinary language, is used purposefully by the exercise organizers, with both events (the "coronavirus pandemic" and the "cyber pandemic") being equated again and again.

A targeted "virus" or other malware could "infect" increasing numbers of computers. In this context, WEF business chief Jeremy Jurgens speaks of "exponential growth." The WEF is encouraging entrepreneurs to "vaccinate" their companies against a cyber pandemic and to ensure "cyber hygiene." There is also talk of "waves." In a video from early 2021, the WEF speaks of a "cyberattack with COVID-like characteristics."

This framing is bearing fruit: In December 2020, several media – including the Süddeutsche Zeitung – referred to the supply chain attack on the US company SolarWinds as an "attack of the super-spreader."

Will the simulation enable subsequent hacking by participants?

Both elements of Cyber Polygon – the hacking exercise and the conference where the elite deliver their statements – raise concerns. Just as in a military exercise, Cyber Polygon 2021 could be used as a cover or springboard for a real attack. Indeed, many companies' IT security teams were involved in the defensive exercise on the day, revealing their capabilities and defensive strategies to informed professionals. Interested stakeholders could draw conclusions about their competencies and behavior during a real cyberattack. Johnny Vedmore and Whitney Webb note the following:

> *"BI.ZONE's gaining knowledge of global institutional weaknesses through cyberdefense training could be useful intelligence for their parent company, Sberbank, and in turn the largest shareholder of Sberbank, the Russian government."*

Each team's performance is evaluated against a set of points, which are then compared against the others. Cyber Polygon thus provides the characteristics of a game or competition for the participating IT professionals. This "gamification" of the exercise should make critical observers sit up and take notice. After all, such competitive incentives in modern information technology serve primarily as bait to draw out specific behavior and information from those concerned.

Agenda-setting by the superrich

Yet another threat is the political agenda-setting that the WEF is pursuing through this event. After the great pandemic, the next global threat has been publicly defined, presented and mentally anchored here by Klaus Schwab and company. In addition, the correct political approach to a major cyberattack, from the WEF's perspective, is being explained again and again. The hundreds of high-ranking Cyber Polygon participants are thus not only transmitters, but also receivers of the WEF messages.

Consequently, when this previously-announced global cyberattack actually happens, everyone will already know what to do. This worked in the same way for the pre-2020 message that was repeated over and over again in the planning exercises: Only vaccination could end a pandemic. After the coronavirus crisis began taking its course at the beginning of 2020, no alternative solutions to vaccinating the world's population have even been discussed.

Because it accelerated digitization to such an extent, Klaus Schwab has described the coronavirus "pandemic" as an event with a "catalyzing effect." At Cyber Polygon 2020, he said the following: "In a couple of months, we have achieved such advancements in digital transformation that would have taken, otherwise, two, maybe three, maybe even more years."

This creates an interesting situation: The WEF would actually have to be very much in favor of the very catastrophic events it "warns" about, as this would allow its political-economic ideas to be implemented all the more quickly and with almost no resistance. And all the better if the rebuilding plans are already in the drawer. Vedmore and Webb write:

> *"If the destabilizing events simulated at Cyber Polygon do come to pass, it will likely be similarly welcomed by the WEF, given that a critical failure in the current global financial system would allow the introduction of new public-private "digital ecosystem" monopolies such as those being built in Russia by Sberbank."*

Russia's role

Cyber Polygon is hosted and organized by Sberbank, Russia's largest financial institution. In both 2019 and 2020, the exercise took place at its "security operations center" in Moscow. The bank's main shareholder is the Russian government. Sberbank's focus is the digital market, including areas that have nothing to do with financial services at all. In recent years, it has purchased numerous Russian companies offering online services – including a media portal, a navigation service, a real estate platform, a music streaming service, a health service, and a data center.

And it plans to issue Russia's first digital currency (Sbercoin) before the end of the year, as soon as the Russian regulator gives the green light, according to a bank announcement in April. Sbercoin will be pegged to the ruble. This would make Sberbank the first bank in the world to issue a cryptocurrency.

This could be a crucial position of power for them in the future. The bank, or rather the Russian government behind it, appears to be aiming for a monopoly on digital financial services in Russia. And from this perspective, the bank would have even more power potential in its hands through the control of a de facto state-owned digital currency. The merging of state and private sector appears to be becoming a reality within the bank itself.

In addition to Sberbank, as mentioned earlier, numerous Russian interlocutors from business, government, and politics, up to and including the prime minister, were participants at Cyber Polygon. Furthermore, the Russian state news agency TASS was a media partner at the event.

Are Russian hackers not the bad guys this time?

All of this is unusual: Russia has always been considered the bad guy, even in matters of online security. For years, Western politicians and media have blamed Russian hacker groups close to the state, including those from the intelligence service, for almost every cyberattack. This was also the case with the latest supply chain attacks on the U.S. company SolarWinds in December 2020, on the Irish hospital service HSE in May 2021, or on the IT company Kaseya in July 2021.

At Cyber Polygon, on the other hand, there is only ever talk of anonymous criminals in the context of potential perpetrators. In this way, the organizers bypass the narrative entirely. Vedmore and Webb write:

> *"The complete absence of the 'Russian hacker' narrative at Cyber Polygon as well as Russia's leadership role at the event suggests either that a geopolitical shift has taken place or that the Russian hacker narrative commonly deployed by intelligence agencies in the US and Europe is mainly meant for the general public and not for the elite figures and policymakers in attendance at Cyber Polygon."*

The reasons for this could be that the Western power elites need both Russia and China to implement the Great Reset that was announced by the WEF. This could only work in a global context. According to the two US authors, Russia and China also have an interest in this and therefore participate in both the official coronavirus narrative as well as the allegedly imminent "cyber pandemic." Cyber Polygon could therefore be a kind of "Russian charm offensive," and Sberbank, as a Russian pioneer, would be the ideal host.

Anonymous hacker attack – an unbeatable wild card

The anticipated collapse of the international financial system and the introduction of digital currencies could be ideally justified through an anonymous hacker attack, Vedmore and Webb suspect. It is likely that the collapse will be controlled so that the power elites retain their power. Anonymous hackers would be ideal perpetrators, not only because the superrich, who are organized, among others, in the WEF, could thus reject responsibility for the collapse of the financial system, but also because, according to the two authors of Unlimited Hangout, any potential enemy could be blamed: from North Korea to Iran to so-called domestic terrorists.

It should be added that Russian hackers could also be named as perpetrators – if it fits geopolitically. Perhaps by maliciously exploiting Cyber Polygon? The simulation would then prove to be a trap for the host. According to a video (minute 26:00) from the Express newspaper, one could even imagine that the power circle around the WEF would not shy away from carrying out the cyberattack itself.

Moreover, virtually no one would be able to verify the reliability of the hacking allegations, since these attacks take place in sensitive, secretive economic spheres and cannot be understood without expert IT knowledge anyway. Another advantage of a large-scale anonymous cyberattack would be that recalcitrant companies, or even entire states, could be shut down or brought into line in parallel – a digital form of a protection racket. Interestingly, the Western-backed coup attempt in Belarus, which was exposed in April, would also have involved a hacker attack on the country's power grid.

Allegedly inevitable

Ultimately, the WEF's messages build upon themselves. First, the coronavirus is forcing both globally uniform ways of reacting and the comprehensive digitalization of life. Second, the threat of cyberattacks requires the establishment of a common global security architecture of states and corporations. And, since everything in the digital world is, in principle, hackable, as the BI.ZONE company itself points out in this video, access rights of the security services would have to be maximum, comprehensive and deep.

The entire crisis could be used not only to expand the access rights of states and companies as well as introduce digital central bank currencies, but also to enforce a mandatory digital biometric identity (ID) that Britain’s ex-prime minister Tony Blair promoted at Cyber Polygon 2020. Digital vaccination passports could also be integrated. Tony Blair said that the introduction of a digital ID was inevitable. "Absolutely inevitable!"

Inevitable was one of the crucial words that kept coming up at Cyber Polygon 2020. The ever-advancing digitalization was inevitable, the global crisis was inevitable, a major cyberattack was inevitable. The use of the term is among the main obfuscating strategies of the whip-crackers of modern surveillance capitalism, noted economist Shoshana Zuboff in her recent book on the subject (The Age of Surveillance Capitalism):

"The image of technology as an autonomous force whose actions and consequences are inevitable has been used for centuries to erase the fingerprints of power and absolve it of any responsibility. It was the monster who did it, not Victor Frankenstein."