multipolar

Herausgegeben von Stefan Korinth,
Paul Schreyer und Ulrich Teusch

Citizen Control

In July 2021, the World Economic Forum (WEF), together with Russia's Sberbank, hosted the Cyber Polygon exercise for the third year in a row. Two hundred IT teams from international companies and institutions took part, but only a few of them were able to fend off the simulated hacker attack. Meanwhile, the live event was attacked by real hackers. In the public part of the conference, WEF founder Klaus Schwab this time refrained from apocalyptic announcements – nevertheless, the event provided a glimpse into the intentions of the architects of an envisioned digital world of control.

STEFAN KORINTH, 12. Februar 2022, 0 Kommentare

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

„Those who think they can sit out the transformation of a free society to totality while preserving their little private happiness will soon wake up to a cashless, digital vaccination and climate-protected controlled world that has penetrated every private sphere." – Raymond Unger (1)

Cyber Polygon – according to the WEF, the "world's largest technical exercise for corporate teams" – recently came under critical public scrutiny after WEF founder, Klaus Schwab, warned of a large-scale cyberattack in quite dramatic terms at the opening of the 2020 event. If such a catastrophic hacking attack on critical infrastructure (electricity, water, and food supplies) were to be successful, our entire society would be paralyzed. The coronavirus crisis, in comparison, would appear as a mere "minor disruption," Schwab predicted at the time, and once again called for a global reboot – a Great Reset.

Simultaneously, the organizers announced that Cyber Polygon 2021 would simulate an attack on the digital supply chains of economic sectors. This aroused suspicion among critics that this could be an elitist simulation game that anticipates precisely what will actually happen during or shortly after the event. The background and model for these fears include Event 201, a simulation exercise jointly organized by the WEF and the Bill and Melinda Gates Foundation, that in October 2019 played out a fictitious coronavirus pandemic.

Corporations and authorities working together

Cyber Polygon is one of several projects on the digital security of companies that the WEF organizes in cooperation with international corporations as well as with many government institutions. Since 2018, the various initiatives have been brought together in a Centre for Cybersecurity. The goal is not only to ensure that politicians and law enforcement agencies are jointly responsible for the digital security of private corporations, but also to permanently inculcate the mantras of the WEF into society and government representatives.

The most important of these messages, which in the WEF's cybersecurity projects are sometimes explicit and sometimes implicit, is that hacking is a global problem that can shake countries to their core due to the universal shift toward digitalization. Ultimately, governments and authorities can only counter this danger by working together with the corporations of the superrich to extend digital surveillance into all areas of life.

Cyber Polygon and Sberbank

Russia's state-affiliated Sberbank plays a leading role at Cyber Polygon. Its IT security service provider, BI.ZONE, supplies the technical staff that organize the exercise, and the public event of the annual Cyber Polygon conference is broadcast to the world from the bank's appropriately spruced-up IT premises in Moscow. In addition, Sberbank CEO, Herman Gref, who also plays an important role at the WEF, brings high-ranking Russian state officials, such as Prime Minister Mikhail Mishustin, on board for the conference.

The conference consists of two independent elements. The first is a public event that includes commentaries and talk sessions by corporate and state representatives involved in the event. In these talks, there are usually no disagreements, as all participants are in line with the WEF. The other part of the event is a two-day exercise in digital enterprise security, into which viewers get little insight – BI.ZONE participants report on the progress of the exercise during the livestream for only for a few minutes between the talk sessions. The written final report also reveals little in this respect.

Only a handful of participants could defend themselves against the attacks

According to the organizers, 200 teams of IT specialists competed at Cyber Polygon 2021 to independently defend themselves against simulated hacker attacks on a given virtual structure and then forensically investigate them. The number of participants in the format has risen sharply over the years. More than 1,200 IT teams signed up for the limited seats for this event, the final report states. At the next event in the summer of 2022, capacity is expected to be unlimited.

The teams were from companies in sectors including finance, IT, and consulting, as well as from public agencies in law enforcement, government, academia, and health. The majority of participants chose to remain anonymous. The organizers reveal only this much in the final report: Most teams came from Russia, the US, Great Britain, and Kazakhstan (more than ten each). There were also between five and ten companies from each of Switzerland and Germany. Only the Deutsche Bank is mentioned by name.

More than half of all the participants at Cyber Polygon 2021 came from IT and financial concerns. Teams from these companies were also the best in the exercise, according to the final report. However, only "five or six" of the 200 participants were able to secure all of the vulnerable sections of the maneuver software in the allotted time, explains one of the organizers of BI.Zone, who was part of the exercise's attack team.

This devastating result, however, was accepted with indifference by the presenters in the livestream broadcast and was not mentioned at all in the final report. The report reveals that 15 percent of the participants failed to score any points at all in the first scenario, but that this was a marked improvement over the exercise in Cyber Polygon 2020. In the second scenario, on the other hand, the participants performed worse than last year by 13 percent. The Cyber Polygon organizers have not publicly discussed the practical consequences of such sobering results.

Alleged attack on Cyber Polygon itself

After a good 90 minutes of the nearly six-hour, livestreamed broadcast, host Alexander Tushkanov made a claim that Cyber Polygon had been attacked by real hackers "just 15 minutes ago" through a DDoS attack.

> *"You always need to be ready, even more so during the training. Needless to say, the attack was stopped and deflected."*

Although it remains to be seen how credible this is, this kind of news fits perfectly into the WEF's continuously repeated threat mantra.

Just days before Cyber Polygon, a so-called supply chain attack on US software provider Kaseya received widespread international attention. On July 2, 2021, blackmailing encryption programs entered the IT systems of up to 1,500 Kaseya customers –including the Swedish rail network, New Zealand schools, and German SMEs – via the company's digital supply chain. As a result, these customers were unable to access their computer systems without paying a ransom. The simulation exercises at Cyber Polygon 2021 were also based on a supply chain attack.

Geopolitical accompaniment: Kaseya attack preoccupies Putin and Biden

A short digression is useful here: According to official information, the Kaseya attack immediately before Cyber Polygon was carried out by the hacker group REvil. This group is suspected of being based in Russia, since, according to the Anglo-Saxon media, it has never targeted former Soviet countries. REvil was also responsible for hacking the world's largest meat company, JBS Foods, in the spring.

The target company, Kaseya, however, received a digital master key to unlock the blocked data just three weeks after the attack. At first, it was unclear where the company had obtained the key. Some media suspected that Kaseya had paid the requested ransom of $70 million to REvil. However, company officials denied this, saying they had received the key from a "trusted third party."

According to the Washington Post, this trusted party was the FBI, which had obtained the key itself by accessing the REvil server. The newspaper does not investigate this claim further, but again, the explanation from anonymous Washington circles may well be held in doubt. Anyone who has the key could, themselves, have been the attacker.

The fact that the whole incident looks like a geopolitical blame game is reinforced by the fact that the Kaseya incident was the subject of a conversation between Presidents Joe Biden and Vladimir Putin. The outcome was a victory for Biden. REvil disappeared from the darknet only a few days after the attack and the US media presented this as if it was a consequence of Biden's exhortations to Putin to address the problem of the Russian hackers, or else Biden would instruct the US services to take matters into their own hands.

Be that as it may, Kaseya CEO, Fred Voccola, was not fired in August 2021 despite the devastating supply chain attack on his company and its customers. Instead, he was awarded for the successful performance of the company and the strength of its products. The REvil hacking group resurfaced in September, carrying out further extortions before being finally dismantled by international investigators in the following months. Suspects were arrested in Romania, Poland, the US, and South Korea. The perpetrator in the Kaseya case was said to be a Ukrainian. And in January 2022, Russian authorities arrested 14 more suspects in raids.

Russian government target of highly complex hacking attacks

Back to Cyber Polygon: It is precisely these kinds of geopolitical entanglements and politically usable culprit speculation in hacking that provided the background to one of the most interesting conversations at Cyber Polygon 2021. This was the discussion between senior Microsoft security advisor Roger Halbheer and Igor Lyapunov, vice president for information security at Russia's Rostelekom.

In this interview, there is piece of information that is usually rather rare for Western ears. Lyapunov tells of cyberattacks against the Russian government. He said Moscow is dealing with highly complex attacks attempting to gain control of digital government systems. The Russian expert explained that his organization has estimated the cost of a single attack of this nature at $1.5 million. He added that these cyberattacks are very difficult to detect and often go unnoticed by IT security systems. Just five days after it went online, a new resource under the government domain gov.ru experienced a sophisticated attack.

Although Lyapunov did not address the question of the identity of the perpetrator, he suggested that by taking into account the target and the obvious resources involved, it is unlikely that these attacks were the work of private hackers. This indirect suggestion that Western governments and intelligence agencies are investing considerable resources in hacking attacks against Russia was enough for the moderator and former CNN reporter, Ryan Chilcote, to interrupt and, although he did not ask any in-depth questions here, as if in retaliation, he brought into play the narrative of Russian hackers attacking Western infrastructure on behalf of the Kremlin.

Microsoft only knows of anti-Western hackers

This dominant narrative in Western debates on hacking ("Russian hackers are attacking our democracies") does not usually come up at Cyber Polygon – either to avoid upsetting the Russian hosts, or because this narrative is only intended as theatrical media thunder for the Western public anyway and not for elite decision-makers at the event, as journalists Whitney Webb and Johnny Vedmore suspect.

The influential WEF players obviously do not like this narrative. When it comes to the identity of the attackers, Cyber Polygon speaks only of anonymous "bad guys," criminal hackers who appear to be motivated solely by financial gain. For a brief moment in this conversation, it was different.

Microsoft's Halbheer mentions two groups by name – Nobelium (from Russia) and Hafnium (from China). Both of these groups are listed in this chart from the 2021 Microsoft Digital Defense Report. The report defines the hacker groups through the use of chemical element names.

According to the report, more than half of all the hacking attacks detected by Microsoft originated in Russia. This was followed by North Korea, Iran, and China. Western hackers are not identified at all in the Microsoft report. Halbheer calls the paper a "must read."

Hackers attempt to destabilize Russian financial market

In the Cyber Polygon interview, Lyapunov tries to appease by emphasizing that cybercrime is nationless. He promotes information sharing and interstate cooperation in the defense against hackers. He says that the same kind of attacks employed against Russia's state agencies are also employed against other parts of Russia's infrastructure.

However, this does not necessarily weaken the presumptions of the intelligence-hacking perpetrators. In the weeks after Cyber Polygon, the Russian media reported massive attacks on Russian banks since the summer of 2021, with the newspaper Kommersant reporting in mid-September:

> *"More than 150 attacks on Russian financial institutions were uncovered last month, a threefold increase from last year's record … In the process, the fraudsters have moved from targeted attacks on individual companies to massive attacks. … 'Judging by the persistence and ingenuity of the cybercriminals, we can say that we are dealing with a complex planned operation aimed at destabilizing at least the Russian financial market'."*

Schwab: Increased digitalization requires more security

The intelligence service-geopolitical component of the hacking issue, the only source of dissent at Cyber Polygon, surfaced briefly only once more. (2) Otherwise, representatives of corporations and governmental institutions conveyed the WEF's messages in comfortable unison. These public conversations do, however, at least provide viewers with an insight into some of the plans and reasoning of those who are working to build a world of digital control and surveillance.

The basic argument, which also runs through Klaus Schwab's 13-minute greeting message, follows these lines: All areas of life are becoming increasingly digitalized. The coronavirus pandemic was the catalyst for this development. However, comprehensive digitalization has created entirely new areas of attack. Everything and everyone are potential victims of a hacker attack. Anything can be weaponized by hackers – even security updates, as in supply chain attacks – and anyone can be turned into a perpetrator by hackers – through, for example, identity theft. Thus, everything and everyone needs to be permanently controlled. This last statement, however, is neatly packaged by the actors in euphonious or technical formulations.

According to the WEF's vision, "security" is to be guaranteed jointly by states and corporations. In his welcome address at Cyber Polygon 2021, Klaus Schwab emphasized that, while governments are responsible for cybersecurity, the technical expertise often lies in the private sector. From this, he derives his assertion of an increasingly necessary cooperation between public authorities and corporations (public-private partnerships) – a core demand of the WEF in all subject areas.

In contrast to the previous year, Schwab refrained from issuing apocalyptic warnings. But he again uses the Covid vocabulary to compare hacker attacks to pandemics. Masks are inadequate protection against the virus and vaccinations are needed; in IT security, too, we need to move away from simple protection and toward “immunization.” Schwab talks about digital “antibodies” that need to be built into the system. He is not more specific than that.

Cyber immunity, zero trust

IT entrepreneur Yevgeny Kaspersky, head of the Russian software company Kaspersky Lab, also uses this vocabulary. At Cyber Polygon, he tells how his company is developing a strategy for cyber “immunity”. Each module of an IT system is “isolated” from the others and assigned a level of trusted behavior. This digital security system is currently being developed for industrial systems and the Internet of Things.

What sounds like a digital implementation of quarantine and AHA rules (The German Covid rules of physical distancing, hygiene, and face masks) is the future concept for critical infrastructure, he said. According to Kaspersky, this could prevent supply chain attacks because any infected part would then no longer infect other parts.

In an expert presentation at Cyber Polygon, the concept of zero trust was also introduced by one of Microsoft’s security executives.

> *“This security concept requires any user or device to present their credentials every time they request access to a resource inside or outside the network.”*

Again, this sounds like the 2G rule (the German Covid rule requiring an individual to prove their status of being either recovered or vaccinated) has been applied to the virtual world. Users are required to certify their own harmlessness by permanently identifying themselves.

Another security concept that resonated at Cyber Polygon is biometric authentication. Roger Halbheer, the Swiss Microsoft consultant quoted above, is convinced that people will soon no longer log into their online accounts via passwords but rather via biometric identifications like fingerprints and facial or iris scans.

Kaspersky: Attacks on supply chains will increase

Why these extreme concepts? Halbheer says that in IT security it is crucial to protect identities in order to protect data. Kaspersky explains that the number of professional hacker gangs is growing rapidly. They share information and work together, and are getting better and better. This reasoning is not surprising to IT security entrepreneurs. Nevertheless, the warnings fit well into the WEF’s scheme.

Kaspersky fears there will be many more attacks on digital supply chains in the future – in times of extensive digitalization almost everything can become a potential target. Incidentally, the EU is also prioritizing the problem by conducting a six-week simulation exercise of a large-scale cyberattack on supply chains starting in mid-January 2022. The next national civil protection exercise in Germany (LÜKEX 22) will also focus on a cyberattack on government and critical infrastructure.

Attacks via digital supply chains in recent years show that corporations are primarily threatened by hackers, but, through them, critical infrastructure in countries, which is often operated by private companies, is also at risk. Kaspersky explained that the security and risk assessment of critical infrastructure is very different from that of a normal company. In the case or critical infrastructure, the extent of the risk is unpredictable. Damage, he says, can be almost unlimited. If a power plant is attacked, it is not just a question of the cost of a turbine, but of the consequences for the entire economy, the state, and society, because the power supply collapses.

However, the fundamental question of whether the digitalization of all areas of life really still has a positive cost-benefit ratio in view of such risks is not addressed at all during the event. Instead, Russian Prime Minister Mikhail Mishustin announces at Cyber Polygon that, as instructed by Vladimir Putin, all of Russia's "socially significant" government and official services will be converted to user-friendly digital formats by the beginning of 2024.

Surveillance and restriction: digital central bank money is on its way

Advanced plans are also underway in Russia to introduce the digital ruble. In a conversation titled "New world - new currency", Alexey Zabotkin, an executive at Russia's central bank, provided insight into the policy plan at Cyber Polygon 2021. According to Zabotkin, the digital ruble will differ from cash and fiat money in that it will be in distinctive, identifiable units. This will improve the traceability of the flow of money. In plain language, digital central bank money will make it possible for the authorities to document and monitor every payment transaction.

His subsequent statement is even more compelling:

> *"We explore the possibility of setting conditions on the permitted terms of use of a given unit of currency."*

In concrete terms, this means that the central bank would like to be able to decide what may and may not be purchased with a monetary unit. Zabotkin says nothing about the enormous control and steering potential that such an instrument would place in the hands of governments and central banks vis-à-vis the population. Instead, the Russian banker explains it using the example of pocket money that parents give their children in digital ruble form. This condition could then, for example, be used to prevent the children from spending their money on fast food.

What Zabotkin is only hinting at is that with state-programmable money, any other use could also be restricted or linked to the fulfillment of certain preconditions. Digital central bank money would be a key to introducing an effective state bonus system.

Will digital central bank money replace cash?

One step along this path is the abolition of cash, as cash represents a fallback option. While the Russian central bank still denies this as their goal behind the digital ruble on its website ("Will a digital ruble replace cash? No."), Zabotkin's message already sounds different. In the Cyber Polygon interview, he casually announces: "[In the future] it will be up to the users [Russian citizens] to choose between the electronic bank money or the digital ruble as today they choose between the electronic bank money and cash." Accordingly, the digital ruble would replace cash.

Zabotkin reassures the other speakers that the commercial banks and payment service providers will remain as facilitators between the central bank and the citizens, even with the digital ruble. This will distinguish central bank digital currencies (CBDCs) from the free cryptocurrencies and is particularly important for the large commercial banks and well-known payment service providers who are convened at the WEF. After all, Western countries are also working on CBDCs.

The digital ruble has been in actual use in Russia since January 19, 2022. The central bank launched its first test phase in cooperation with twelve Russian financial institutions – including Sberbank. Two years of citizen-to-citizen payments will be the first to be tested. Digital central bank money can also be transferred, without an Internet connection, from smartphone to smartphone. After this pilot phase, transactions between companies and consumers, between different companies, and between companies and the government will also be tested.

China as pioneer; EU interested in exchanging experience

In China, these test phases are at an even more advanced stage. Following tests in ten major regions of the country, including the well-known metropolises, the app for the digital yuan has been available to all citizens since the beginning of the year. According to official statements, the e-CNY (digital yuan) is intended to partially replace cash. The earmarked programming of monetary units is also possible with the Chinese digital currency.

The Frankfurter Allgemeine reported that the German Bundesbank President and other eurozone officials have also expressed interest in exchanging experiences with China with regard to a digital euro.

In addition to the aspects of surveillance and the abolition of cash, the topic also has a significant geopolitical component that could explain the pioneering role of China and Russia in this regard: Digital central bank currencies facilitate an exit from the Western-dominated SWIFT payment system as they enable international payments independent of US sanctions.

Cryptocurrencies are unwelcome

A strong indication of the importance of the topic of digital currencies is that the WEF organizers put it on the agenda at Cyber Polygon. Furthermore, hacking did not play a role in this discussion, which was also attended by high-ranking representatives of Visa and Mastercard.

In the discussions, the representatives of the credit card companies confirmed that the coronavirus crisis had given their business a strong boost. Mark Barnett of Mastercard said that, in five months of the pandemic, they saw progress in electronic payments that would otherwise have taken five years. Matthew Dill of Visa pointed out that Covid-19 has created a lasting behavioral change in people's payment patterns.

However, according to the Cyber Polygon participants, free cryptocurrencies like bitcoin, which can be used anonymously, are better off not playing a role. Central banker Alexey Zabotkin explained that Russia would not accept cryptocurrencies as a means of payment in the country. The Russian central bank recently called for a complete ban. In China, cryptocurrencies are already illegal.

In another interview, Michael Daniel of the lobby group Cyber Threat Alliance calls cryptocurrencies the “fuel” of the ransomware industry – that is, the hackers who, as in the attack on Kaseya, encrypt other IT systems and release these only after receiving a ransom in bitcoin.

Michael Daniel is not just any lobbyist. Prior to his current job, he was cybersecurity coordinator and advisor to US President Barack Obama for some years. (3) Hacking today is no longer merely a criminal act, but, as he emphasizes in his talk, also “a national security and public health and safety threat.”

The revolving door effect: From state appointments to big business

A look at Michael Daniel’s curricula vitae, as well as those of numerous other Cyber Polygon participants, shows how far the WEF has already advanced with its public-private partnership project. The career of Cyber Polygon initiator Troels Oerting demonstrates the extent to which the competences and interests of government agencies and private corporations have already merged. Oerting was also the moderator of one of the discussion rounds.

Since the 1990s, Oerting worked in various management positions with the Danish police and the Danish Security and Intelligence Service. From there, he moved to Europol in 2009, where he headed the European Cybercrime Centre (EC3) from 2013. In 2015, Oerting moved to the private sector – as head of information security at the major British bank Barclays. In 2018, he was employed at the WEF as head of the Centre for Cybersecurity. He has subsequently started his own IT company called BullWall.

Jürgen Stock and Craig Jones – both from Interpol – are two other (albeit active) representatives of international police organizations involved in Cyber Polygon. In their statements at the event, they represented the WEF’s position almost one-for-one, as if the interests of public law enforcement and those of the superrich owners of corporate organizations were identical. Stock, who was vice president of the German Federal Criminal Police Office until 2014, also talks about “cyber hygiene” and throughout his talk emphasizes that online crime must be fought by the private and public sectors together. He calls the cybersecurity industry an ally of Interpol.

These types of police forces seem like ideal candidates for the private-public partnerships that the power and financial elites at the WEF would like to see. Even Interpol itself is now no longer funded solely by its 190 or so member states, but also by corporations, including corporations from the pharmaceutical industry.

Outlook: Collect data, control the people

The general suspicion that was first comprehensively carried into the analog world with the coronavirus crisis – i.e., that everyone is a potential security risk – is obviously to be transferred to the digital world. Events like Cyber Polygon are part of the WEF strategy to reinforce this mantra among the public. If this intention prevails, cybercrime could fulfill the same political functions in the future as terrorism did in the years after 9/11, or as the coronavirus crisis currently does: an omnipresent scaremonger and a universal justification for tightening the law.

The parallelism between pandemic and hacking, which is repeatedly invoked at Cyber Polygon, is an indication of this intention. Klaus Schwab and his associates have, over the past years, identified hacking as a topic with great potential for political instrumentalization. Attacks on hospitals (e.g., the Uniklinik Düsseldorf) or power plants (e.g., Stadtwerke Pirna), as discussed at Cyber Polygon, are perfect for those interested players to highlight the frightening dimension of possible hacking attacks. Who is not afraid of a prolonged blackout? Who could possibly be against the protective measures?

But these initiatives by big business are always cloaked in a benevolent, philanthropic mantle that should not deceive us, argues journalist Norbert Häring in his current book, Endspiel des Kapitalismus (Endgame of Capitalism). He writes that the big corporations gathered at the WEF, among others, dream of a "wholly monitored, neo-feudal world" in which people "can do practically nothing without leaving a digital trace." (4)

According to the ID2020 initiative, run by Microsoft and Gavi, the vaccination alliance, among others, and based on the Sustainable Development Goals (SDGs) of the United Nations, all citizens of the world should have a biometric digital identity by 2030. (5) According to Häring, the common denominator of numerous projects, business games, and initiatives by the superrich and their foundations is:

> *"the goal of comprehensive, automatable collection and storage of reliable data on the activities of the world's population. Because whoever has the data has the power, both commercially and politically."*

Nearly all aspects discussed at Cyber Polygon, from protection against hacking to digital central bank currencies, converge on this goal.

Notes

(1) Raymond Unger: Das Impfbuch. Über Risiken und Nebenwirkungen einer COVID-19-Impfung (The Vaccination Book. About the Risks and Side Effects of COVID-19 Vaccinations). Scorpio-Verlag, Munich, 2021, p. 190.

(2) Talking about resilient supply chains, IT security entrepreneur Yevgeny Kaspersky says the system must be built in such a way that a hack would be more expensive for the attackers than the damage they could do with it. Former Europol director and Danish intelligence chief Troels Oerting adds shortly after this that against normal criminals, this is an effective strategy; but it would not prevent state attacks. In this case, costs would not play a role. Oerting thus indirectly confirms the assumption that the expensive attacks on Russian government infrastructure are state attacks.

(3) Michael Daniel, however, was not one of the anti-Russian hawks. After an alleged Russian hacking attack on the White House, he justified the decision not to impose sanctions on Russia as a punitive measure, saying remarkably candidly, "It [the alleged Russian hack] was information collection, which is what nation states – including the United States – do. From our perspective, it was more important to focus on shoring up defenses."

(4) Norbert Häring: Endspiel des Kapitalismus. Wie die Konzerne die Macht übernahmen und wie wir sie zurückholen (Endgame of Capitalism. How the Corporations Took Power and How We Are Taking It Back). Quadriga, Cologne, 2021, p. 254.

(5) Norbert Häring: Endspiel des Kapitalismus (Endgame of Capitalism). p. 242.

Editorial Note: *The Multipolar editorial team has decided to place this article under a Creative Commons license (CC BY-NC-ND 4.0). This means that the article can be republished by other media and users in compliance with the terms of the license, i.e. unedited, for non-commercial purposes and with attribution to the author and source Multipolar.*

Further article on the topic:

- **Announcing an attack** (Stefan Korinth, 19.7.2021)