BRASIDAS
GROUP

Stable Instability

Newsletter-December 2021

Contents

Introduction

With 2021 coming to a close, Brasidas' newsletter reflects a year of instability and uncertainty in global markets and geopolitics. While the COVID-19 pandemic rages on with no end in sight and new variants emerging constantly, the US withdrawal from Afghanistan offers to shake up power dynamics of an already volatile region, tensions have renewed between East and West, and emerging technologies continue to influence the evolution of statecraft.

In April of 2021, US President Joe Biden announced that US Forces would be out of Afghanistan by September 2021, exactly two decades after the 11 September 2001 terror attacks. This announcement confirmed the Trump policy of withdrawal and closed the chapter on the longest war in US history. The message was clear, that the unstable Afghan government would be on its own, and left to its own devices to fight off the Taliban insurgency. As the withdrawal began ramping up, the first provincial capital fell to the Taliban on 6 August 2021, while US intelligence assessments predicted that the Afghan Security Forces could hold out for months, within 11 days the Afghan Security Forces fled from the battlefield and ceased to exist. The country had collapsed and fallen back into the hands of the Taliban.

What the US withdrawal means for Afghanistan going forward remains unclear. Any hopes the international community had of a western-style democracy in the country departed with the last NATO troops out of Hamid Karzai International Airport. The US will face a set of new security challenges as traditional adversaries vie for position vis a vis the new regime. Not just traditional adversaries such as the Islamic Republic of Iran are looking to cooperate with the new regime, but also traditional allies like Turkey are evaluating their future position in Afghanistan.

On the frontiers of the European Union, there is growing contention between Brussels and Moscow. Belarus has launched a campaign against the European Union by employing elements of hybrid warfare against Poland. Daily updates are revealing the scope of the Belarussian KGB's involvement in stoking tensions online and trucking in migrants by the hundreds to the border with Poland. While the term hybrid warfare may have fallen out of vogue with think tanks in the West, it is alive and well throughout the globe.

At the time of writing, Ukraine has assessed that the Russian Armed Forces has amassed more than 90,000 troops along the Ukrainian border. Fears are growing in the West that the Kremlin is posturing for an invasion of Ukraine. In recent weeks both sides have shown an unwillingness to de-escalate as NATO has threatened Moscow with a "high price" for any aggression, and Russian President Putin warned NATO not to cross its red line for fear of its new hypersonic weapons. A one-to-one phone call between Biden and Putin did little to alleviate fears of a coming conflict. And whether the Kremlin is posturing to pressure Brussels away from Kiev remains to be seen.

The COVID-19 pandemic has only increased the threat of digital actors creating chaos. Cyber-attacks have sharply risen during the pandemic, by an FBI estimated 400%. Unfortunately, these attacks are not just targeting financial institutions, but increasingly alarming for decision-makers, as these attacks are targeting critical infrastructure and energy sites.

A recent ransomware attack on the Colonial Pipeline has given hope to some, that mainstream acceptance of cryptocurrencies and law enforcement's technical means to monitor cryptocurrency are dashing criminals' hopes that crypto could be a means to avoid the loss of their ill-gotten gains.

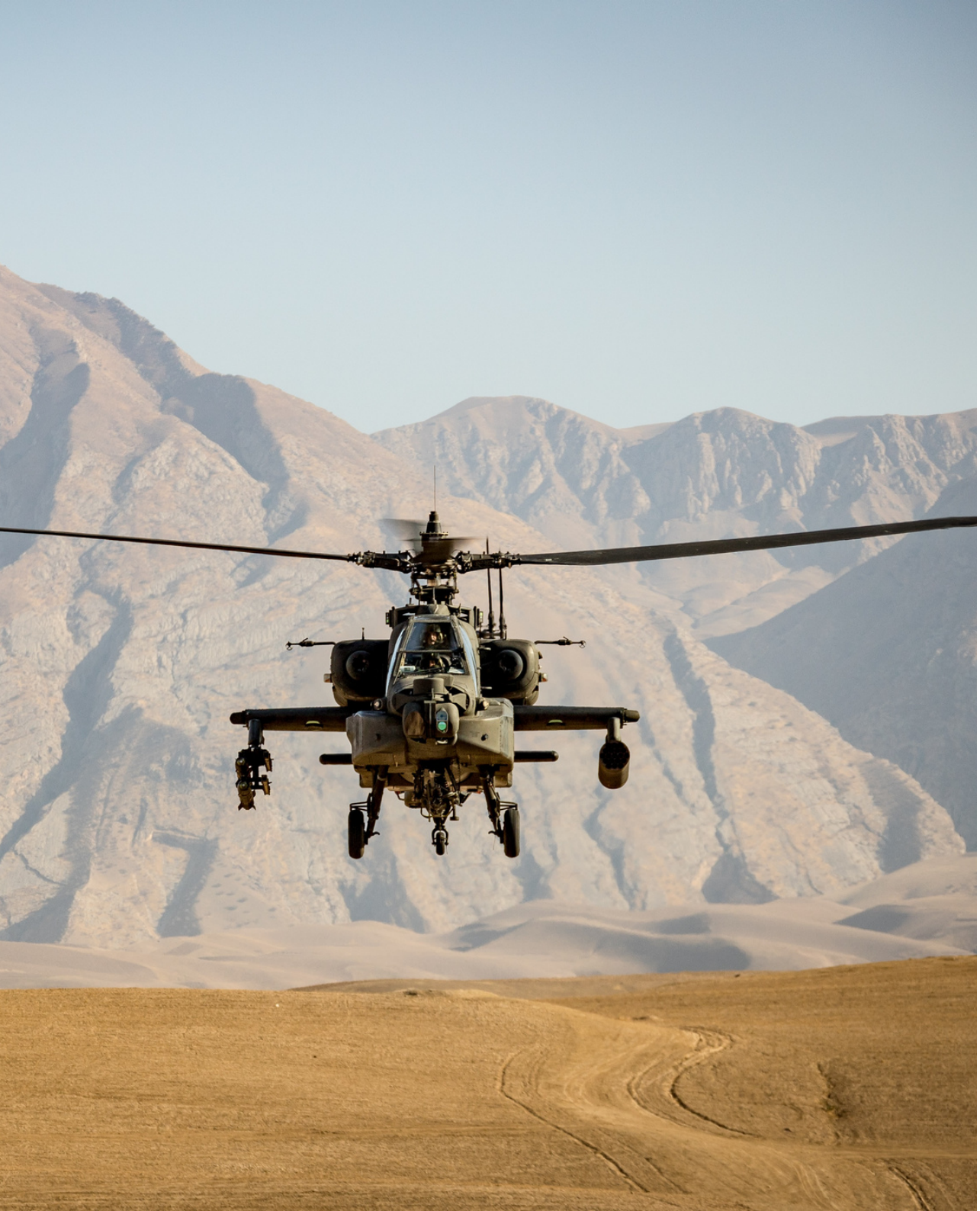
Alongside increased law enforcement capabilities, certain regulators like the EU are increasing the legislative tools at their disposal to strengthen their ability to combat money laundering. With the issuance of the EU's 6th AML directive, there are measures to increase cooperation among Member States' Financial Intelligence Units (FIUs).

While the West is strengthening its measures to combat money laundering and cybercriminals, China is attempting to tackle a whole new issue, minors increasing addiction to video games. While the employment of facial recognition software and other tools to curb this trend among China's youth might alarm some, investors might have to admit its game over for China's promising e-gaming market.

Wherever this instability and uncertainty find you this year, we hope that you find this newsletter insightful and informative, as our goal is always to maximize awareness and minimize risk. We look forward to continuing to help you navigate this uncertainty in 2022 and beyond to provide you with the intelligence to inform your decisions.

From all of us at the Brasidas family, we hope that you have a happy holiday season.

Brasidas Group AG 2021
Contact: info@brasidas.ch



US Withdrawal from Afghanistan Reintroduces a Familiar Security Dilemma for the US

US withdrawal from Afghanistan and the subsequent decline of their power in the region has provided an opportunity to strengthen an anti-American alliance in Central Asia. The ascendant Taliban regime in Afghanistan is rapidly becoming more of a challenge to the US than prior to the US invasion in 2001. Simultaneously, US failure in the country will reverberate beyond Afghanistan and stain US credibility as a global leader of the democratic world. The US withdrawal has left a power vacuum in the country and a cabal of US adversaries is posturing to fill the void. A new "Great Game" has kicked off in the region, and Washington's adversaries are off and running.

Tehran and its regional allies cautiously welcomed the new regime in Afghanistan. Despite disagreements over theology and mutual distrust, Iranian leadership openly embraced the Taliban takeover as an example of obsolete US foreign policy in the region. Strategists in Tehran have been emboldened by US failure in Afghanistan and are hopeful it could be a harbinger of similar setbacks across the region.

However, Tehran is reluctant to establish lasting partnerships with the Taliban regime, primarily due to the Taliban's systematic targeting of Afghanistan's Shi'a population, regardless of any promises. Nevertheless, the Taliban takeover in Afghanistan opened new geopolitical opportunities for Iran. Iran is presenting itself as the only reliable actor in opposition to US leadership and economic cooperation between the two has already grown since the US withdrawal. This economic cooperation has been dubbed by both a "resistance economy."

China and Beijing's increased support for the Taliban remains a concern for US policymakers. Beijing's interest in Central Asia remains primarily economic and is related to its Belt and Road Initiative. With the withdrawal of Western funding, China is seeking to strengthen Afghanistan's economic dependency on Beijing. An economic partnership is also in the interests of the Taliban, who are desperate to supplant Western funds (which accounted for 80% of the country's income) with stable alternatives. China is a perfect partner for the Taliban, as Beijing will not question the Taliban on human rights issues, but a flashpoint for the relationship could present itself if the Taliban voice opposition to China's treatment of the Uyghur community or export religious extremism into the Xinjiang province.

Russia has also been emboldened by the US withdrawal to regain some of its lost influence in the region. Foreign Minister Sergei Lavrov has already offered Russian support building a stable and "inclusive" government in Afghanistan. On the other hand, Moscow will not tolerate the exportation of religious extremism from Afghanistan and will quickly react to threats to its Central Asian partners. Following the US withdrawal, Russia was quick to stage a military exercise in Tajikistan to signal to the Taliban their resolve to combat any further incursions.

Continuing narratives about the decline of US global power will only further enhance the confidence of its primary challengers in Central Asia. US withdrawal from Afghanistan has multiplied security concerns in the region and weakened the US ability to confront them while strengthening adversarial actors.

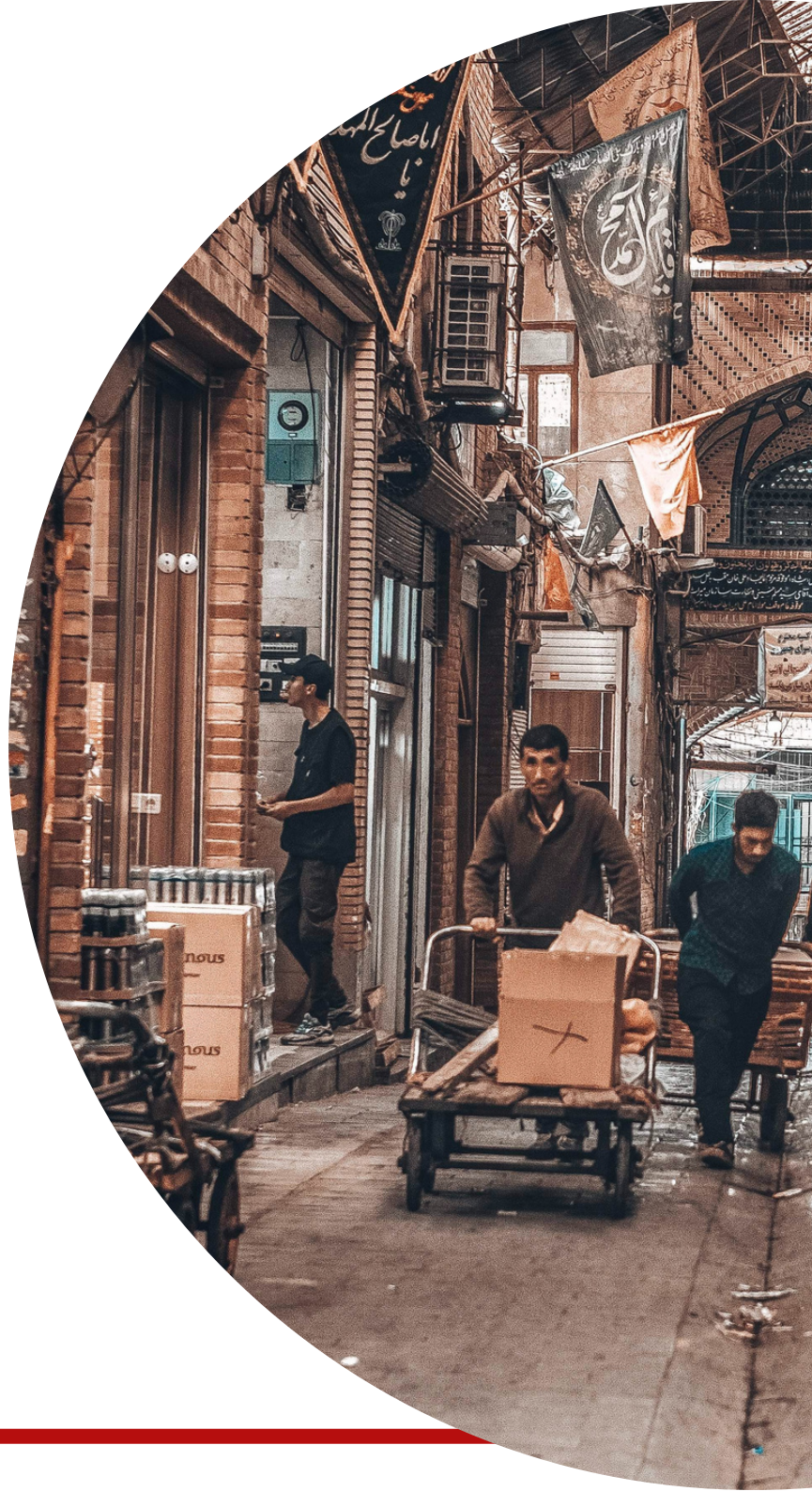
TALIBAN TAKEOVER OF AFGHANISTAN: IMPACT ON CROSS-BORDER TRADE WITH IRAN

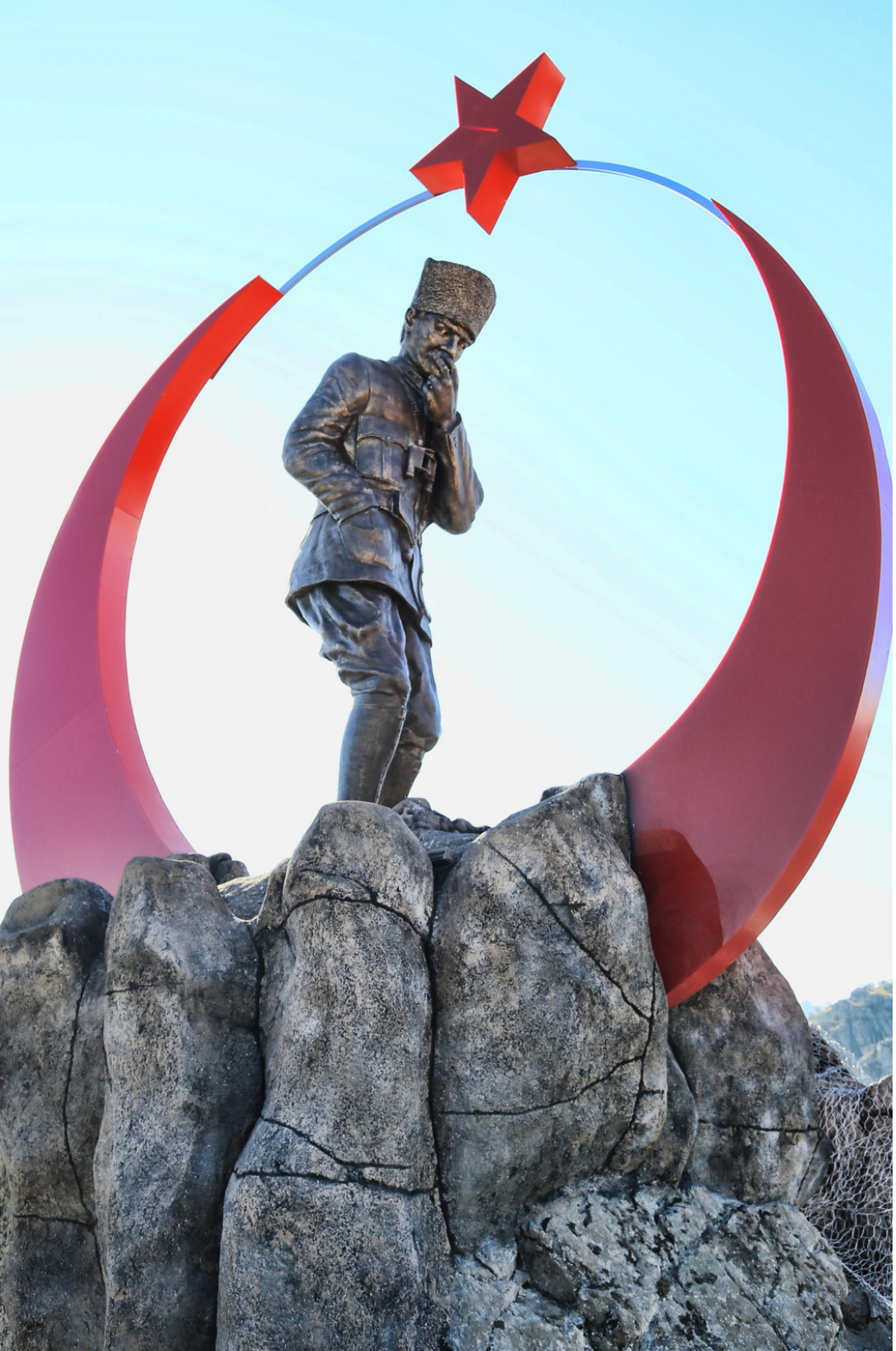
In the wake of US and coalition forces' withdrawal from Afghanistan, the Taliban rapidly took back control of the country, which implies numerous changes. At first glance, the prospects of a Taliban-led government presented the Islamic Republic of Iran with an opportunity to expand its interests in the region. Despite the historically hostile relationship between Tehran and the Islamist militant group, the two have seemingly found common ground based on the ancient proverb "the enemy of my enemy is my friend." Having faced a litany of economic sanctions imposed by the United States since the Islamic revolution in 1979, Iran has primarily relied on neighboring countries as its main trading partners, and the ties between Kabul and Tehran appear to be strengthening.

The two countries voiced their intentions to elevate their partnership in October 2021, when Tehran and the new regime in Kabul committed to negotiating a bilateral trade agreement, pledging to strengthen their economic ties and lower obstacles to the movement of goods. It is important to note that Iran is currently Afghanistan's largest import partner, primarily regarding petroleum products. However, the trade between the two transcends petroleum, as Afghanistan relies heavily on Iran for other materials as well. Afghanistan imported around USD 2.3 billion worth of non-oil Iranian goods, an estimated third of the country's non-oil imports. Thus, Tehran believes that by improving infrastructure and lowering tariffs, it can expand and solidify its economic activity in Afghanistan.

Given the extremely fragile state of Afghanistan's economy, it is highly contestable whether Iran can reliably depend on Afghanistan as a viable trading partner. Furthermore, the dire state of the Afghan economy is already deteriorating under Taliban rule. Economists predict that the power shift in Afghanistan will result in reduced access to hard currency for Tehran. Additionally, stoppages in international aid and cash deliveries in Afghanistan will lead to a drop in quality of life and a rise in inflationary pressures. These factors are expected to drastically reduce the demand for Iranian goods, and consequently diminish Iran's long-term economic development, which is heavily reliant on the political and economic landscape of the region.

Furthermore, there is a growing concern of Afghani-produced opium crossing the Iranian border as prices are surging. Members of Iranian Security forces, particularly the Basij paramilitary force, have reportedly been engaged in this illicit activity for some time, but with the Taliban return to power in Afghanistan, this activity is expected to increase. Additionally, a deterioration in Afghanistan's economic circumstances already leads thousands to join this trade every year. Given the Taliban takeover has brought increased economic hardships, there is a realistic fear from policy-makers that this could increase the amount of opium trade worldwide, as Iran has served as a transit point in the past. Furthermore, even though the future economic situation of Afghanistan is yet to be witnessed, growing illegal trade and subsequent economic fluctuations can lead to internal conflict and further destabilize the region.





CAN TURKEY FILL THE POWER VACUUM IN AFGHANISTAN?

As the Taliban rapidly seized control of Afghanistan this past August, global powers like the US and the UK pulled out of the country after nearly two decades, leaving behind them a power vacuum that different regional players have been vying to fill since. Among them, Turkey has emerged as a key mediator between the new government in Kabul and the international community, taking advantage of Afghanistan's power void to move closer to its own geostrategic goals. In this context, Turkish presence in Afghanistan is only the most recent example of Ankara's efforts to expand its soft power in the region and establish itself as a key political power.

Following NATO's withdrawal from Afghanistan, the Taliban have requested Turkey's help in running the Hamid Karzai International Airport in Kabul. Having no land border with Afghanistan, by assisting the Taliban in this regard, Turkey hopes to gain a stepping stone to Central Asia. While the Taliban have requested only technical assistance from Turkey and do not want the Turkish Armed Forces or any other foreign military at the airport, Ankara has been working on a compromise. Namely, instead of using its military, Turkey is considering engaging SADAT Inc. International Defense Consultancy, a private Turkish military, and security contractor.

By gaining access to Kabul's airport, Turkey is simultaneously seen securing further economic expansion in the region. For example, opening economic relations with the Taliban could be an opportunity for Turkish goods to find their way to the Afghan market. Furthermore, warmer relations with the Taliban appear to have opened a door for Turkish construction companies to enter Afghanistan and work on projects to repair the war-torn country's infrastructure. In fact, during the Taliban-Turkey high-level talks in Ankara in October 2021, the Taliban welcomed Turkey's participation in infrastructure projects and economic investment programs in the country. Finally, as it is already hosted by over 3.7 million Syrian refugees, gaining a foothold in Afghanistan could help prevent an additional flow of Afghan refugees to Turkey. Averting an influx of Afghan refugees fleeing the Taliban is seen as a priority of Ankara's given that accepting additional refugees would undermine the government's popularity at home.

What differentiates Turkey from other players competing to fill the regional power vacuum are the country's extensive religious, cultural, and political ties to Afghanistan, as well as its status as an ally to Pakistan, the Taliban's main backer. Additionally, Turkey's presence in Afghanistan in a non-combatant role means the country is not perceived as an invader, unlike other NATO states.

Should it continue to refrain from the use of hard power, Turkey's ambitions in Afghanistan are likely to deliver results and Ankara is set to cement its position as a mediator between the Taliban and the international community.

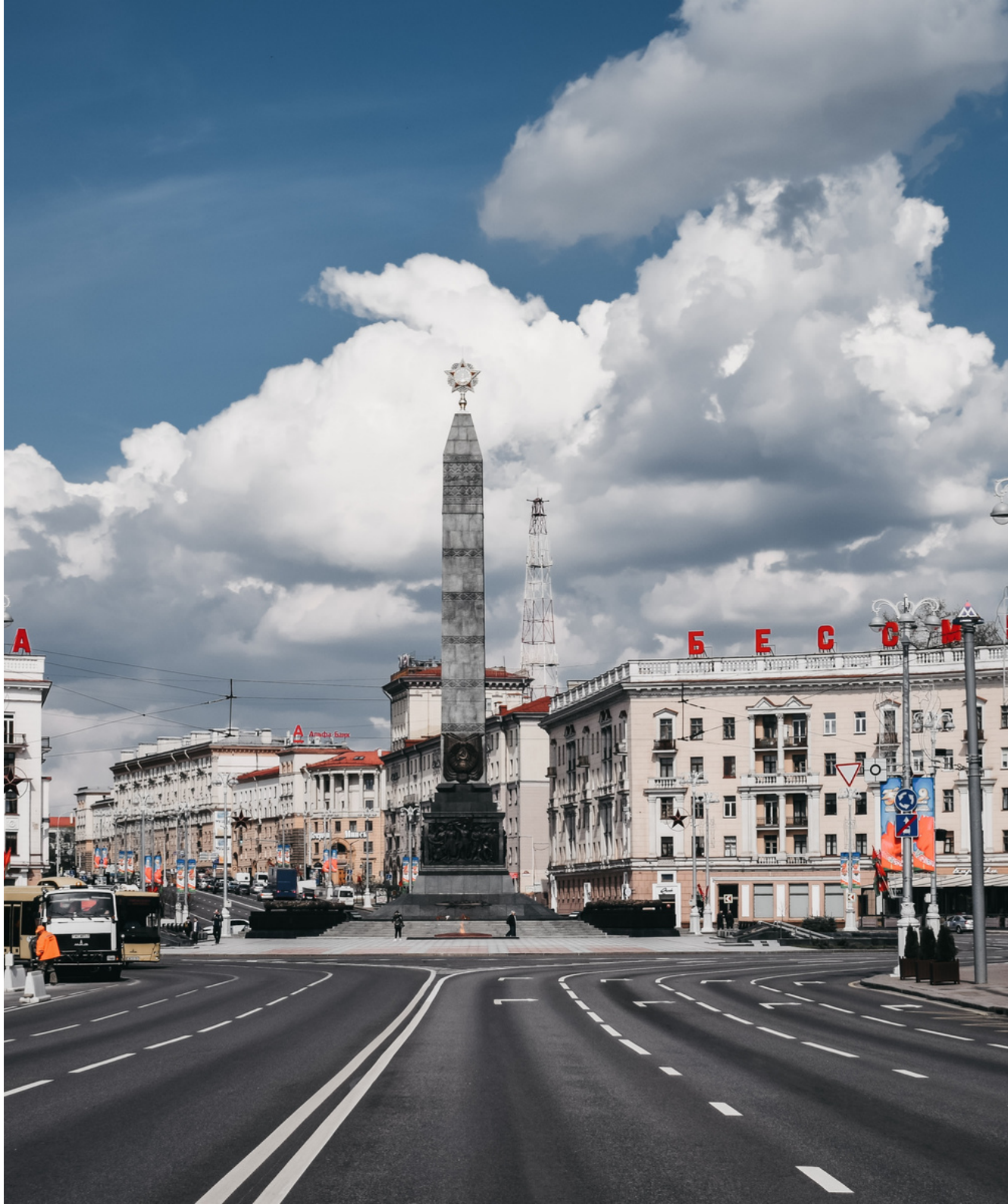
HYBRID WARFARE BETWEEN POLAND AND BELARUS

A "hybrid war" on the border between Poland and Belarus is becoming more complex each day. Belarussian political leadership is accused of transporting civilians from primarily Middle Eastern countries based on false promises they would reach wealthy European Union countries soon after they land in Minsk. Instead, migrants, including women and children, are stuck at the Polish border. And Warsaw has already deployed the army to monitor the situation. Thus, EU officials believe that Belarus is using migrants and propaganda as pawns in a game of hybrid warfare against the EU, as a sign of retribution after this close Russian ally was sanctioned on 1 October 2020.

While the European Union discusses a new set of sanctions against Belarus, no solution is in sight. In a hybrid war, any activity or resource can be weaponized, and many experts believe that Russia has perfected its methods. As they claim, Russia is using Belarus as a proxy in this hybrid warfare, mounting pressure on the Baltic countries and Poland as migrants grow restless. Western intelligence notes that this is one more example of Russian pressure, with an aim to win certain political concessions for Belarus and itself. For other experts, this might be just a diversion needed for the renewal of the Ukraine crisis.

Whatever it may be, the role of technology in hybrid warfare is undeniable. Most hybrid war models rely on cyber-weapons and information campaigns, and the situation on the Polish-Belarus border certainly cannot be the exception. To better understand why technology plays such an important role in hybrid warfare, it is important to note that the human psyche is the weakest link in tech adoption. This was illustrated during the 2019 controversy when NATO soldiers, during military training, used various purposely created social media apps that extract the geolocation of their users. The soldiers also conversed with fake profiles on Tinder, sharing sensitive and confidential information without being aware that the Latvian military created those portals and profiles to diagnose cyber vulnerabilities in the NATO ranks. If the similar behavior of NATO soldiers is displayed in the migrant crisis on Polish borders, the damage could be severe.

Even without such safety risks, sophisticated spyware has been on the rise, especially after Pegasus, a spyware used to infect any smartphone and remain undetectable, became widely known. Despite Russia not being on the list of countries using Pegasus, it is no secret that the country has developed similar tracking algorithms that could reveal sensitive information. Thus, Belarus or the Russian military could know the most critical elements of NATO strategy and successfully anticipate its moves. The outcome of this crisis is yet to be witnessed, but it is undeniable that sophisticated technology is at the forefront of any hybrid warfare.



RUSSIAN MOBILIZATION ALONG THE UKRAINIAN BORDER

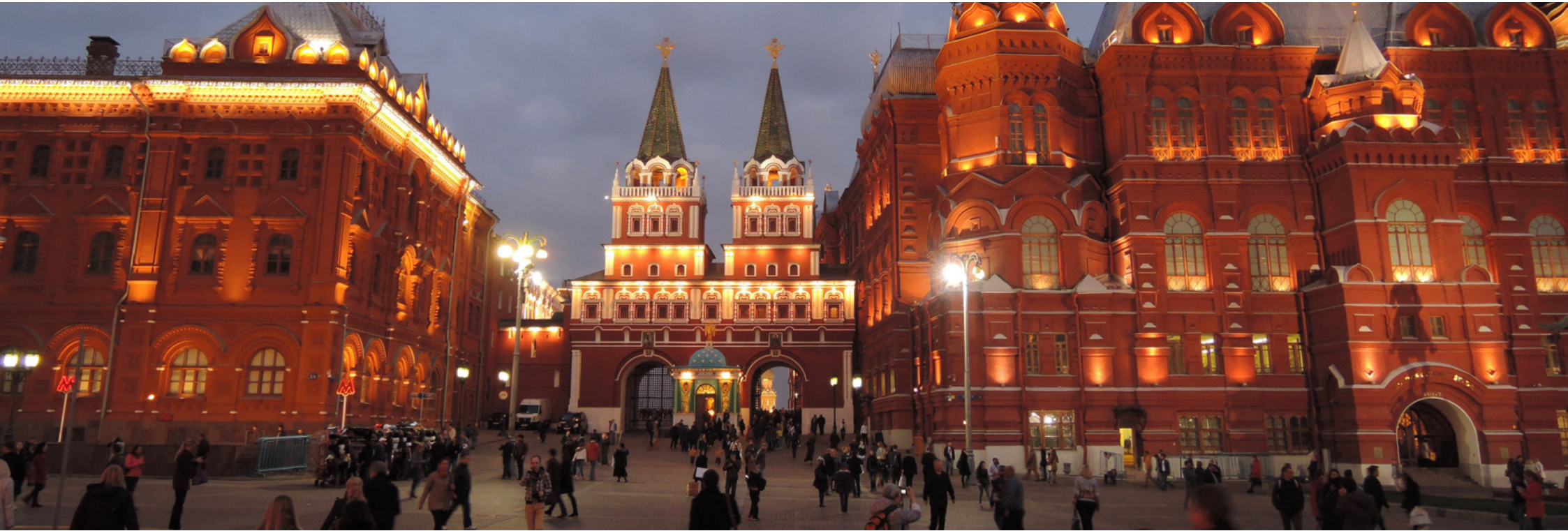
As of the time of writing over 90'000 Russian troops have begun amassing along the Ukrainian border. The recently appointed Ukrainian Defense Minister Oleksii Reznikov has announced that their intelligence estimates assessed that a large-scale Russian offensive could be launched as early as January 2021. The situation along the Ukrainian border has deteriorated rapidly in the last few weeks, and observers are wondering if this is just saber-rattling or a harbinger of a coming conflict. US Intelligence estimates have predicted that the Russian force could grow upwards of 170,000 by the end of January 2022.

Earlier in September of this year the Russian Federation alongside its partner Belarus, staged its large-scale military exercise Zapad (West) 21. The Armed Forces of Russia stage a similar event annually rotating through each of Russia's designated military districts: Zapad (West), Vostok (East), Tsentr (Central), and Kavkaz (Caucuses) where the Southern Military District is based. As of January 2021, a Northern military district was created which has yet to see one of these exercises, but can be expected in the years to come, as Russian influence in the Arctic grows. The exercise concluded on 16 September and featured the same theme it had in its prior iteration in 2017, an incursion by a fictional NATO expeditionary force hellbent on regime change in Belarus. Not only are these exercises a chance for Russia and its partners to enhance military readiness, but are intended to send a clear signal to Brussels not to intervene in Moscow or her partners' affairs.

However, as Ukrainian military officials have warned, while most of the military personnel initially returned to their permanent bases following the exercise, much of the material, units, and subunits have remained near the Ukrainian borders. Alarmingly for Kiev, tanks, armored vehicles, and nuclear-capable Iskander short-range ballistic missiles have remained in the area, in a buildup that is being characterized as preparations for an invasion in the West. Ukraine has warned that Moscow is nearing a "strategic encirclement" of Ukraine, and is growing concerned that an invasion is possible. Washington and NATO have both issued warnings to Russia to de-escalate tensions, but Moscow shows no signs of backing down. In late October of 2021, the Ukrainian Defense Ministry posted a video of a drone strike on a Russian-made artillery piece in a separatist-controlled area in Eastern Ukraine. The drone was a Turkish-made Bayraktar TB2 and marked an evolution in Kiev's strategy to deal with Russian-backed separatists that have plagued the country since 2014. The Kremlin, on the other hand, viewed the drone strike as a violation of the internationally negotiated Minsk agreements.

Putin and Biden held a secure video call, where according to National Security Advisor Sullivan, President Biden reiterated the US commitment to robust economic measures to deter any Russian incursion into Ukraine. But the Kremlin has made its position clear, any further attempts to bring Kiev into the fold of the EU or NATO will catalyze a Russian response.

Moscow could just be displaying its resolve to dictate the terms of Ukraine's future EU or NATO hopes. But with the colder months arriving in Western Europe, and the Omicron variant ripping through the EU, it remains to be seen how committed the Member States will be to Ukrainian territorial sovereignty. That's not to say that Nord Stream 2 will not prove a valuable bargaining chip for EU member states. However, for a country that has remained under sanctions since 2014 following the annexation of Crimea, the prospect of a "robust economic package of responses" is not a lot for Ukrainians to pin their hopes on.



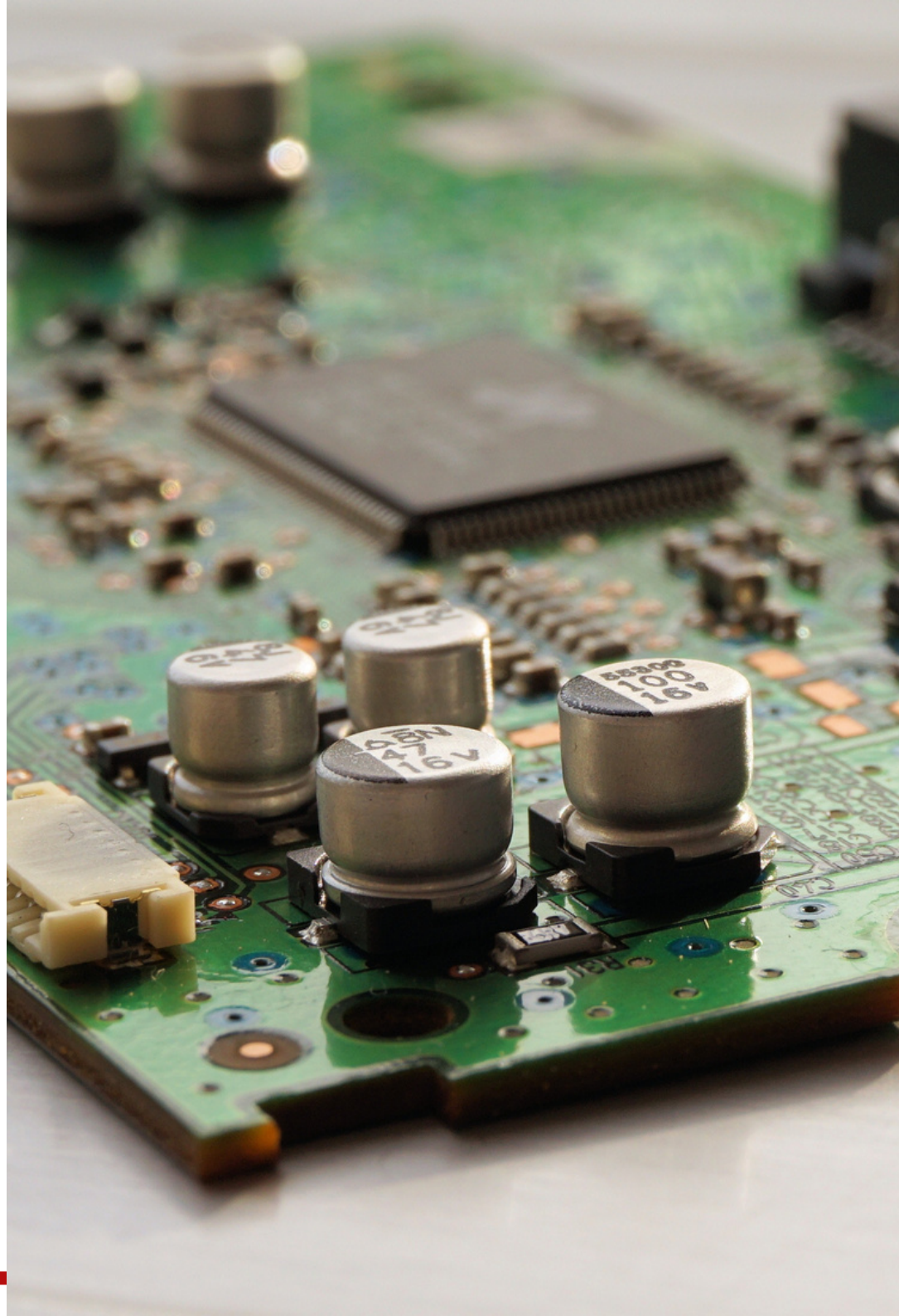
CYBERSECURITY IN THE POST-COVID ERA: KEY INDUSTRIES UNDER THREAT

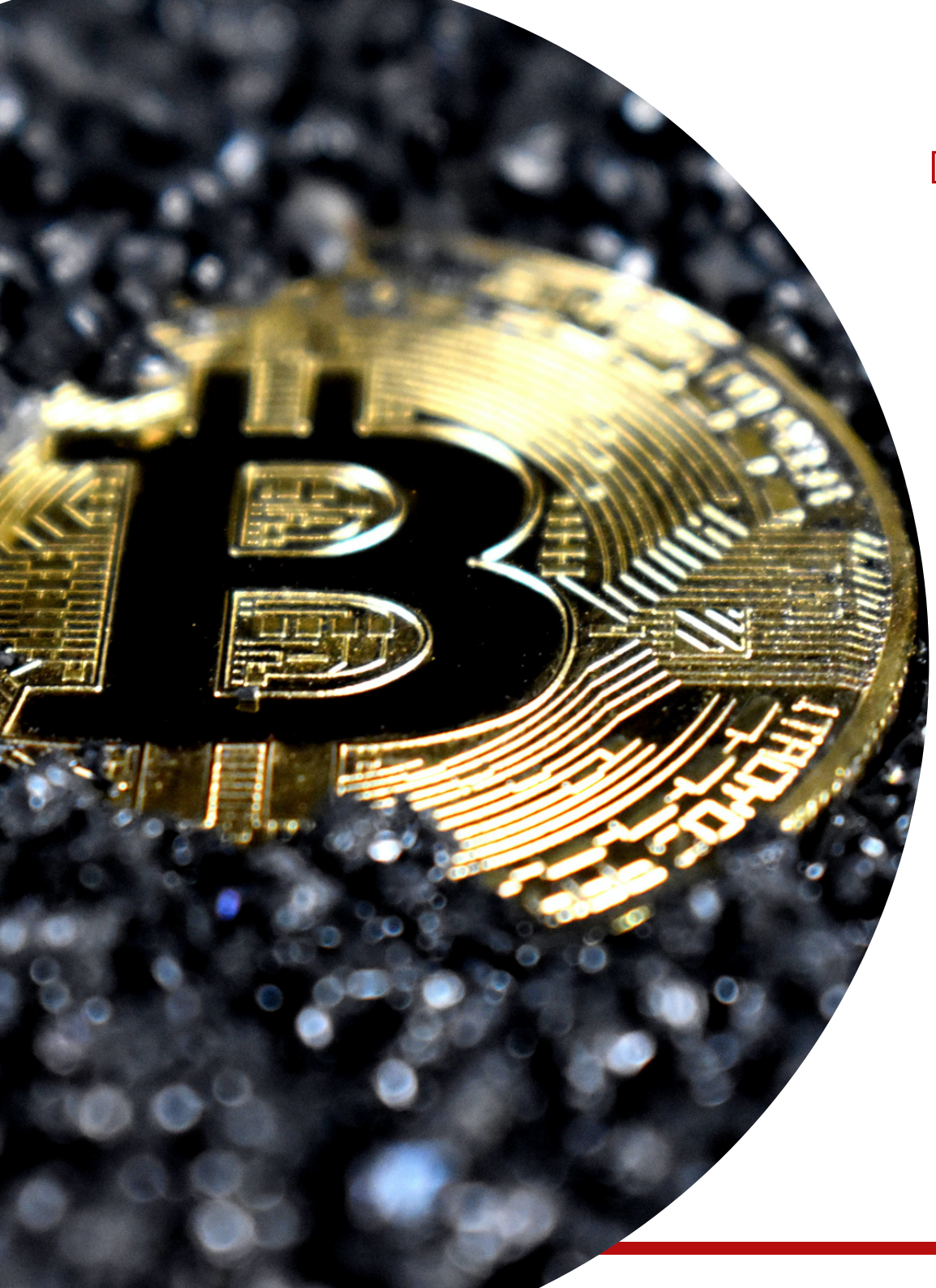
In the wake of the coronavirus pandemic, the global economy is facing increased cybersecurity threats across a number of different industries. Since the health crisis began to take hold in early 2020, multiple industries have been forced to adapt to the new social and working environments by introducing changes like remote work. In the US alone, remote work increased by circa 30 percent during the pandemic. These new working circumstances came as a result of the numerous restrictions introduced by governments across the globe to tackle the pandemic, like social distancing and mask-wearing. But apart from the pandemic's impact on the work environment, Covid-19 brought with it new security challenges as well.

Some of the industries that have been most exposed to increased cybersecurity threats amid remote work and online communication are financial services, IT, energy, and manufacturing. According to a telling report published by the FBI last year, the number of cyberattack complaints surged to 4 000 per day during the pandemic, representing an increase of roughly 400% compared to pre-Covid levels. At the same time, the growing number of complaints is responsible for an increase in security costs from USD 3.86 million to USD 4.24 million on average across industries worldwide.

Both developed and emerging markets are being increasingly targeted by cybercriminal groups and hackers. The frequency of these attacks, directed across a range of sectors, are expected to decrease once the pandemic is declared over, however, companies are encouraged to implement certain measures until then in order to deal with the influx of cyber threats. Namely, measures like heavier investments in cybersecurity, personal data protection, and employing full-time cybersecurity experts could help companies mitigate these costly risks as much as possible.

Several measures companies already started implementing to address the new cybersecurity challenges include educating their staff and developing increased cybersecurity awareness, as well as constant updates to operating systems and security software. In addition, cybersecurity experts recommend enabling multi-factor authentication (MFA) with a one-time code sent to smartphones or an authentication app as an important measure for strengthening company security. Keeping in mind the increased role remote work will play and businesses' dependence on digital technology which is set to continue after the Covid-19 pandemic, the Chief Information Security Officer (CISO) role will become of greater importance for companies strategic planning and a safer business development.





DOES THE COLONIAL PIPELINE ATTACK UNRAVEL THE MYTH OF BITCOIN'S UNTRACEABILITY?

Few assets in history have been as polarizing as bitcoin. Notorious for its volatility, the world's most popular cryptocurrency has many detractors, including some of the most prominent economists and financial experts. Despite its critics and abundant predictions of failure, 2021 has undoubtedly been bitcoin's breakout year.

Many developments this past year point to the growing mainstream acceptance of bitcoin. More notable examples include investment banking giants Goldman Sachs and Morgan Stanley announcing they will start offering bitcoin and other cryptocurrency assets to their private wealth management clients, while the Central American nation of El Salvador became the first country in the world to adopt bitcoin as legal tender. With a combined market cap of nearly USD 2 trillion, it appears bitcoin and other cryptocurrencies are here to stay, carrying with them enormous challenges to anti-money laundering (AML) and counterterrorist financing (CTF) regulation.

The inability to trace the flow of these virtual assets has been posed great risks to AML/CTF regulations, but the Colonial Pipeline ransomware attack appears to upend the notion cryptocurrency tracing is impossible. Back in May, a cybercriminal hacking group, DarkSide, targeted the Colonial Pipeline system, a critically important piece of infrastructure that supplies fuel to much of the eastern United States. The attack on Colonial's computer network forced the pipeline into closure, which led to panic buying and fuel shortages that lasted several days. The six-day-long shutdown finally ended when Colonial Pipeline's management decided to pay the cybercriminals USD 4.4 million worth of bitcoin in ransom.

The company's decision to pay off the hackers was met with criticism as journalists and the public believed this would only encourage other criminals in similar endeavors. However, in a surprising turn of events, FBI agents managed to recover more than half of the ransom amount in the course of several weeks. Despite not disclosing the details of this recovery, it demonstrated the growing technical capabilities that might be able to counter cryptocurrencies' lack of transparency in the near future. Experts have warned this success in recovering the funds was likely a potent warning sign to criminals, who are now expected to resort to new, more complex money laundering techniques as a result. But for now, at least, the Colonial Pipeline ransomware attack appears to suggest AML regulators and financial crime watchdogs may be closer to tackling cryptocurrency risks than was earlier thought.

THE EU RAMPS UP ANTI-MONEY LAUNDERING MEASURES

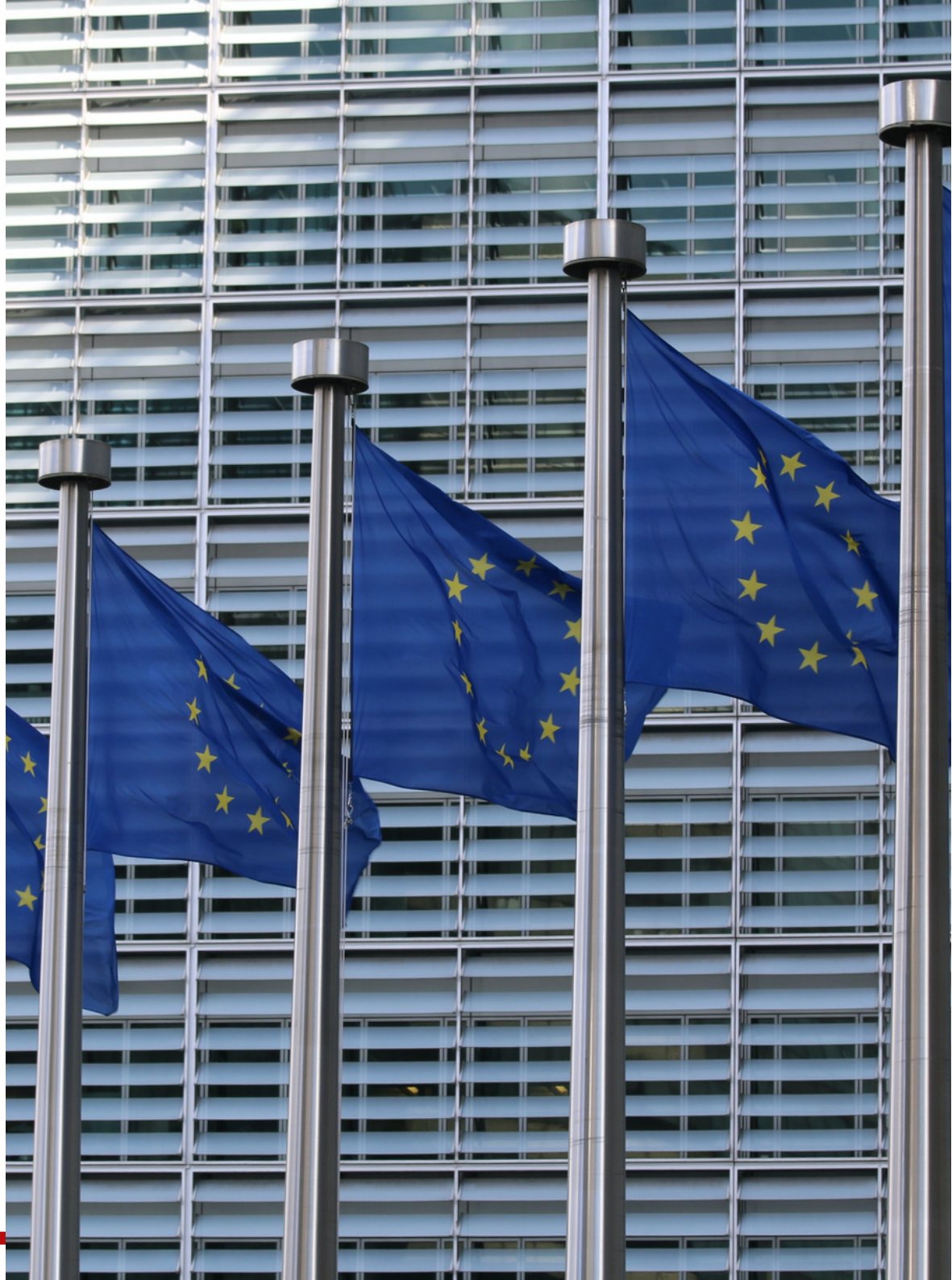
In 2018, Rob Wainwright, the outgoing head of EU's law enforcement agency Europol, estimated that 99 percent of money laundering in the EU goes unpunished. According to Euractiv, 90 percent of banks on the continent have faced fines for money-laundering-related offenses in spite of the fact that EU financial institutions spend about 60 billion US dollars on compliance annually. In order to bolster its anti-money laundering (AML) efforts, in July 2021, the European Commission announced plans to adopt an EU-wide AML ruleset and establish EU Anti-Money Laundering Authority (AMLA).

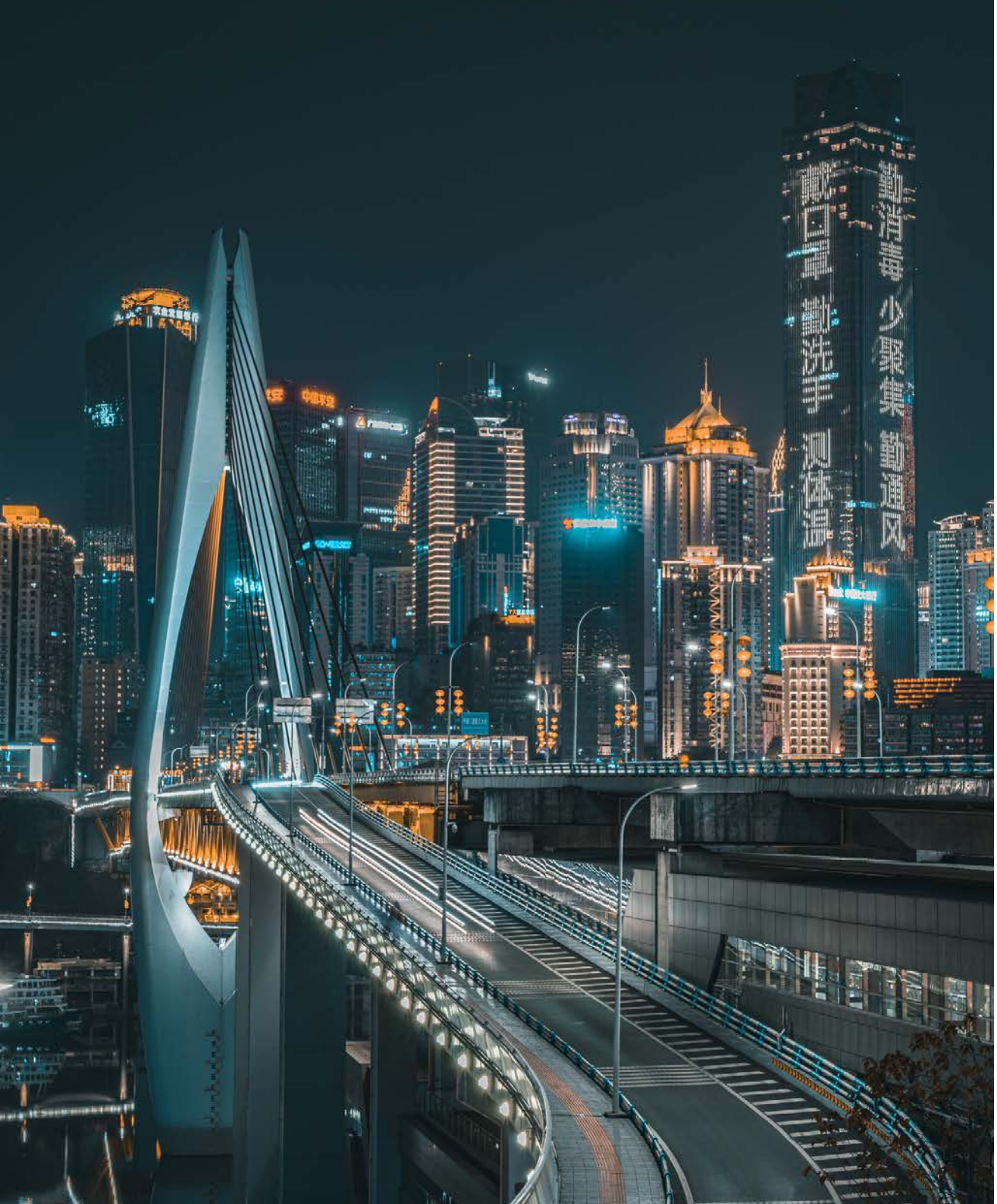
AML rules have been formalized in the Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The regulation aims to iron out AML-related inter-jurisdictional inconsistencies and unify AML standards. A notable change is the expansion of the scope of organizations covered by AML rules. These will now also include unregulated crowdfunding service providers, creditors for mortgage and consumer loans, and associated intermediaries, as well as investment migration operators. It is important to note that EU Regulations are directly applicable to member states. Unlike EU Directives, they do not need to be transposed by national legislative assemblies, which speeds up their implementation.

The second proposed innovation, the founding of the AMLA, comes in response to the noted shortcomings of AML in the EU in terms of poor cooperation and coordination between the national Financial Intelligence Units (FIUs). The AMLA aims to improve on the current situation by serving as the focal point of coordination among FIU's. Additionally, it will be responsible for directly supervising high-risk financial institutions that are present throughout EU member states. It will also serve to draft and suggest policy changes on the EU level in order to improve the way the Union goes about preventing money laundering.

Overall, the EU is currently going into overdrive in order to improve its AML track record. The 6th Anti-Money Laundering Directive that has recently come into force prescribes penalties for accomplices and enablers of money laundering, which now also include legal entities. Although it will take some time before all proposals come to fruition—for example, the AMLA is not expected to be fully implemented before 2024—the trend of intensifying regulatory and institutional activity is clear.

What does this mean for financial institutions? They can expect the future to bring rising AML compliance costs as well as heightened scrutiny of their operations. It is crucial to identify weaknesses in their systems and devote attention to expanding internal and third-party engagement in order to minimize risks.





ALL WORK AND NO PLAY MAKES CHINESE GAMING COMPANIES A BAD INVESTMENT?

Since August 2021, facial recognition devices have been restricting minors in China from playing online games for no more than three hours per week. In addition to this hit on their revenue stream, gaming companies in China are facing all the policymaking hurdles encountered by Chinese tech companies in general, such as restrictions on personal data processing imposed by the new data protection law and stricter application of antitrust policies leading to hefty fines for practices now deemed monopolistic.

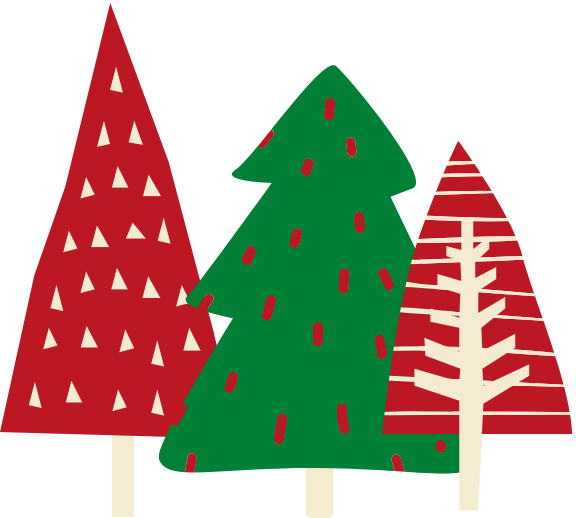
China is putting the screws on the gaming industry due to concern for the development of its youth and fear of minors getting addicted to games. However, these regulations are also seemingly part of the new "common prosperity concept" of wealth distribution in China, which aims to narrow the vast income gap in the country. Introducing new regulations and tightening existing rules can be seen as China's attempt to moderate huge earnings of its tech industry, estimated to be worth almost USD 600 billion in 2020. These regulatory crackdowns also prompted Chinese tech companies to make significant donations to remain on the government's good side. Tencent Holdings Ltd. (Tencent), one of the largest Chinese gaming companies, made a USD 7.7 billion donation to pledge its allegiance to the common prosperity cause.

Nonetheless, due to investors' fears surrounding the mentioned crackdown, Tencent and NetEase Inc., another large Chinese gaming company, jointly suffered a decrease in value of more than USD 60 billion in September 2021. Even important figures such as Masayoshi Son (the Japanese billionaire investor) are hitting pause on Chinese tech investments. These fears are not unfounded, as Chinese regulators' tightening grip on tech companies could have grave consequences. Overly strict regulation would leave no room for growth and would result in a probably irreparable decline in value. In a worst-case scenario, the common prosperity concept could ultimately lead to the Chinese government's control over tech companies' corporate decision-making, and the complete exclusion of foreign investments and interests. It remains to be seen if there is room for gaming mega-corporations (and tech billionaires) in China's new, common prosperity society. The outlook is, however, grim.

2022

HAPPY NEW YEAR

from the Brasidas Group AG



BRASIDAS
GROUP