War in Ukraine

—

Situational awareness briefing

26 April 2022

Situational Awareness – Briefing as of 26 April 2022 (Summary)

Ukraine Crisis

The current geopolitical developments in Eastern Europe and the unprecedented attack on Ukraine are also an attack on our way of living and doing business together.

At the moment, no one can foresee all the consequences of this aggression. This is why urgent questions are now being asked in all areas of our social life. Also for companies this means far-reaching cuts and changes.

This Situation Awareness Briefing is provided for information purposes only by PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft and will be updated regularly.

The overview to the right represents a summary of points along the following five dimensions:

- Overall Geopolitical Assessment
- Industry Special
- Forecast
- People
- Operations
- Finance

Overall Geopolitical Assessment

The northern wing of the Russian offensive has commenced its operations. The siege of Mariupol is in its final stage with the last defenders holding on to the Azovstal factory. The fall of the city would herald the initiation of a renewed Russian offensive in the south and southeast.

Industry Special: Information Technology

The IT sector in Ukraine is fairing well with 80% capacity compared to pre-war levels, thanks to the sectors preparation and the flexibility of the workforce. In Russia the IT sector has taken a big hit with a large exodus of IT professionals from the country, escaping sanctions and their economic consequences.

Forecast

As a reaction to the increased geopolitical tensions, Volkswagen decided to strengthen its expansion strategy into the US to mitigate its sales and supply chain dependency on China. The decision follows China's unclear positioning concerning Russia's invasion of Ukraine and its decision against imposing sanctions as an instrument to put economic pressure on Russia.

People

Ukraine's humanitarian committee claims that 500,000 people have been deported from Ukraine to Russia. The Organization for Security and Cooperation in Europe (OSCE) announced on 24 April that they are seeking possibilities to facilitate the release of several of its staff members who have been "deprived of their liberty in Donetsk and Luhansk".

Operations

On 20 April, the US Cybersecurity and Infrastructure Security Agency warned that organizations could see "increased malicious cyber activity" from Russian actors. The warning cited "evolving intelligence" that indicated Russia's government could be weighing options for potential cyberattacks. The warning comes as Russian President Vladimir Putin initiated a new phase of the war by pushing into Eastern Ukraine's Donbas region.

Finance

Attempts to avoid US sanctions have been met with expanded sanctions against 30 individuals and 40 companies and further visa restrictions. Meanwhile, the UK banned imports of caviar and high-end products from Russia. The import ban also covers silver and wood products, combined with a 35% increase of the tariffs on imports of diamonds and rubber from Russia and Belarus.

For questions, comments or details, please contact Joint Crisis Center team: **de_ukraine-crisis@pwc.com**

Overall Geopolitical Assessment (1 of 2)

Key takeaways

Russian forces are massing at Izium and south of Donetsk for an alleged large-scale operation to occupy Donetsk and Luhansk Oblasts and destroy a large section of the Ukrainian army.

Current topics

Current Situation in the Russo-Ukrainian War

Russian offensive operations commenced along the entire Donbas contact line with multiple minor incursions at Zelene Pole, Novobakhumtivka, Poposna, Torske and Dibrovne. Of all those breakthroughs the Dibrovne spearhead coming out of the Izium salient poses the biggest threat to the Ukrainian positions in the Donbas. The Russian intentions seem to aim at outflanking Sloviansk and Kramatorsk from the west and pin Ukrainian forces in the Sloviansk-Kramatorsk and Sievierodonetsk-Lysychank area along the Donbas contact line. The Russian operations have become more methodical and concentrate on gradual gains over speed. The terrain also suits maneuver warfare making it more difficult for static defenders to gain the upper hand. Ukrainian losses have increased as a result of artillery and aerial bombardment. A major offensive in the south has yet to materialize and is unlikely to do so before the fall of Mariupol. In Mariupol, Russian forces have further reduced the defensive pockets and only a single one remains now at the Azovstal metallurgical plant. Kiev has offered negotiations to take place for the evacuation of the entrapped defenders and civilians. Such requests were ignored by Moscow so far. At Kherson and in the vicinity of Kharkov Ukrainian forces have conducted several counterattacks and liberated settlements. Such attacks seek to ease the pressure on Ukrainian forces in the Donbas, as Russia will be forced to redirect some of its forces, reinforcements and supplies to stabilize their defenses there.

German national security strategy

As a response to the political, economic and security challenges for Europe and Germany in light of the Russo-Ukrainian War, Germany has announced it is working a German National Security Strategy (GNSS). The GNSS will focus on three central pillars:

1. The security of the inviolability of life of its citizens, first and foremost from violence and war.
2. The security of freedom as a core resilience of German democracy.
3. The security of livelihoods, the protection of the environment and resources.

The GNSS is being developed in a joint process involving various departments of the Federal Government, the German Bundestag, and many national and international partners. Its development will be based on intragovernmental cooperation between various ministries, national and international experts and key industrial and economic players. Its goal is to frame the necessary security coordination, develop sound mechanisms to enhance national resilience. Elements of the GNSS will also address the readiness, protection and safeguarding of critical infrastructure, supply chains and energy security on the basis of comprehensive approach and understanding of national security.

Moldova and Transnistria

Russian aspirations in Moldova reach back to the 19th century, when the Russian Empire acquired Bessarabia from the Ottoman Empire. From 1918 to 1940 Moldova was part of the Kingdom of Romania until it was annexed again by the Soviet Union. During the collapse of the Soviet Union Moldova declared its independence, while Transnistria broke away with the help of the Russian Federation. Since then an “Operational Group of Russian Forces” is based in Transnistria, which is internationally still recognized as a part Moldova. Its exact current capacity is reportedly unknown but is estimated between 1,200 and 1,700 in different sources; one of its missions is guarding the largest ammunition depot in Eastern Europe (around 22,000 tons of ammunition and military equipment) located in Cobasna, which is only 2 km away from the Ukrainian border. Recent statements by Moscow officials referring to a land bridge to protect the Russian minority in Moldova and the Russians of Transnistria have given rise to fears that Russia will also target Moldova as the war in Ukraine progresses. Paired with the Russian focus on southern Ukraine, the renewed likelihood of a Russian dash towards Odessa and the prospect of incorporating all of the Ukrainian coast into a pro-Russian Ukrainian republic, such a scenario remains plausible. As currently less than 2,000 Russian forces are stationed in Transnistria and the Transnistrian army can only mobilize a few brigades, it is unlikely that an attack will commence unless the military situation in Ukraine takes a more favorable Russian turn. Moscow, despite public statements to the contrary, can currently ill-afford opening another isolated front in Ukraine, Moldova or Transnistria. In the future, however, the political situation of Transnistria, Moldovan EU and NATO membership aspirations as well as Russian expansionism will redirect Western and Russian attention to this existing frozen conflict.

Overall Geopolitical Assessment (2 of 2)

Key takeaways

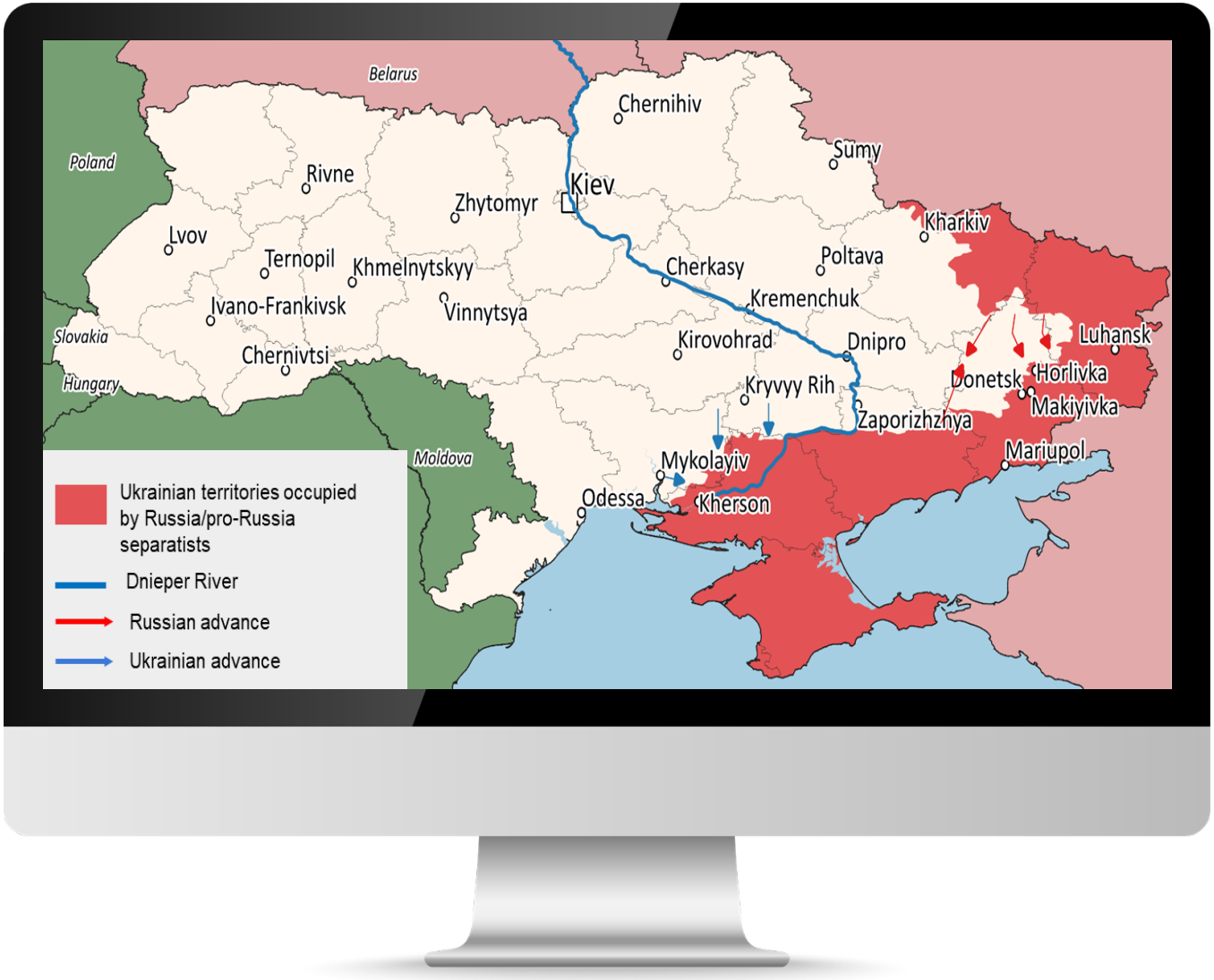
The current fighting is characterized by artillery exchanges along the front and tactical attacks to improve local positions. A larger Russian operation is likely to occur once reorganization is complete.

Four Week Horizon Selected events 26 April – 20 May 2022

Recent debates have centered on the likely start and duration of the anticipated Russian offensive, with the Russian Victory Day on 9 May being at the forefront of speculations as a potential end date.

Date	Country/ Region	Event
26 April	40 countries invited by the US Defense Minister	Meeting of Defense Ministers at the US Ramstein Airbase
26-27 April	UN	UN Secretary-General to meet with President Putin (26.04) and President Zelenskyy (27.04)
27-29 April	EU (Council of the EU and European Council)	Meetings of the Permanent Representatives Committee
02 May	EU (European Parliament)	Plenary session
16-17 May	EU (Council of the EU and European Council)	Foreign Affairs Council

Current Military Situation in Ukraine (arrows indicate potential future Russian operations in the coming weeks)



Industry Special: Information Technology

General context

Before the war, the Ukrainian information technology sector has been booming. The IT exports volume had increased by 36% from USD 5bn in 2020 to USD 6.8bn in 2021.

Since the Russian invasion of Ukraine, the IT services sector has been exposed to the consequences as all other industries. While in Ukraine the IT industry has survived fairly well and is even considered to be a beacon of light in the otherwise war torn economy – its Russian counterpart has fallen apart. Crushing sanctions and a increasingly hostile environment makes Russian IT workers leave the country in search of more favorable conditions abroad.

Current topics

The IT sector in Ukraine

According to the Ukrainian IT Association, in 2022, the sector employs 285,000 IT professionals in the country and accounts for 4% of the national economic output. Technology companies such as SAP SE, Revolut Ltd, and Fiverr International Ltd. employ workers in the region.
In face of the Russian invasion, the sector has performed comparatively well, operating at 80% capacity compared to the pre-war levels. Businesses were reportedly preparing for a war to break out since the 2014 annexation of Crimea and conflicts in Eastern regions of the country. Further, the flexibility of the workforce and industry has allowed businesses to easily relocate and work remotely.
An example of what the sector has done for the country is SoftServe. It is one of Ukraine's largest tech corporations, which prepaid its taxes, UAH 24m (approx. USD 812,000), giving much needed financial support to the Ukrainian treasury. Thanks to the current high liquidity of the sector, Ukrainian IT companies have been able to donate around EUR 25m in humanitarian aid and to the Ukrainian military.

The IT sector in Russia

Since the beginning of the war, Russia experienced a large exodus of tech workers. Multinational technology companies supported their employees to evacuate from the country, chartering planes and procuring visas for them. In the first four weeks of the war, between 50,000 and 70,000 workers from the sector left the country and another 70,000 to 100,000 are estimated to have left from then until now. In 2020, before the war, Russia had about 1.8 million IT professionals according to the Moscow-based Association of Computer and Technology Companies (ACITC), meaning that up to 10% of the IT workforce could have emigrated by now.
In an effort to curve this development, the Russian government exempted young workers in the technology sector from compulsory military service. Furthermore, the government is offering them advantageous mortgage rates and freeing IT companies from income tax and inspections, as well as granting them access to cheap loans.
Nonetheless, there are many businesses like DataArt which had 4 offices in Russia before the invasion. Now the company took off all four locations from their website stating it would “stop all investments, hiring and business development activities”.

Preliminary Assessment

- How long and whether the IT sector can continue to operate in Ukraine remains uncertain. Should the conflict continue for a long time, clients could be pushed to find alternative delivery locations such as, for example, India – which would be eager to accept the business
- In Russia the war will have consequences for years to come. The brain drain of a much needed young and educated workforce will worsen the already problematic situation with regards to the country's birth rate and the sector will feel the fallout for many years

Forecast

General context

Considerations on implications for businesses along the PESTEL framework

P Political	Sanctions Exit from Russia
E Economic	Business Relationships Supply chain
S Social	Brain Drain Refugees Disinformation
T Technological	Cyber threats Disrupted IT operations
E Environmental	Resource scarcity Energy embargo
L Legal	Compliance with changing regulations Contractual obligations

Current topics

Foreign companies' exit out of Russia - update

SAP has stopped the distribution and support of their software and cloud products in Russia and Belarus. Non-sanctioned customers are offered the migration of their server data to servers operated by SAP abroad.
Additionally, despite its earlier decision to continue business operations in Russia, consumer goods company Henkel also decided to exit the Russian market.
Further, two India-based companies, multinational tech company Infosys and global steelmaker Tata Steel, are moving out of Russia, despite India's "soft position" vis-à-vis Russia regarding its invasion of Ukraine.
Meanwhile, automotive parts manufacturer Continental claimed that it had to resume production at its tire factory in Kaluga, Russia to protect its workers from possible criminal prosecution should the company upkeep its decision to halt operations in Russia. Continental further stated that the production resumption was not motivated by profit considerations.

Volkswagen increase of US business

As a reaction to the increased geopolitical tensions, Volkswagen decided to strengthen its expansion strategy into the US to mitigate its sales and supply chain dependency on China. The decision follows China's unclear positioning concerning Russia's invasion of Ukraine and its decision against imposing sanctions as an instrument to put economic pressure on Russia.

Russian response to foreign companies' exit out of Russia

Following French carmaker Renault's announcement of its exit from Russia, the Russian car producer Avtovaz (which was partially owned by Renault) revealed that it would be redesigning several Lada models to make them less dependent on imported components.
Further, Vkontakte, Russia's equivalent of Facebook, is reportedly profiting from Russia's communications regulator cutting off access to Facebook and Instagram, with the number of its users hitting a record number in March. Nevertheless, some Russia-based users manage to use Facebook and Instagram via VPN connections.
Additionally, since the 2014 sanctions following the Crimea annexation, Russia developed its National Payment Card System and the bank card system built on it, named "Mir,", which has grown considerably since Visa and Mastercard announced in March the suspension of transactions and operations in Russia. However, it can only be used within Russia and few other countries, mostly ex-Soviet states.

Preliminary Assessment

- More globally active companies consider increasingly severe reputational consequences associated with continued business operations in Russia, leading to an increasing number of foreign companies leaving the Russian market
- As China's position in the Ukrainian crisis is unclear, companies tend to shift business activities from China into the US

People

Key Considerations

Response measures may include the following:

- Scenario planning sessions to explore how the escalating situation could impact the organization and identify the risks and mitigating actions.
- “Table-top exercising” can be used to validate response structures if they are not already in operation.
- Ensuring that playbooks are in place for extreme but plausible scenarios such as loss of IT for an extended period and disruption to critical suppliers.
- Ensuring the ability to locate all personnel based in, or travelling to, regions of conflict and ensure appropriate steps are taken for their protection.

Current topics

Ukrainian refugees - update

As of 24 April, according to United Nations High Commissioner for Refugees (UNHCR) data, over 5.2 million refugees fled from the war in Ukraine. The UNHCR also counts nearly 1.2 million Ukrainians entering Ukraine, which may include returnees as well as aid worker moving back-and-forth across the borders. Meanwhile, Ukraine's humanitarian committee claims that 500,000 people have been deported from Ukraine to Russia. Ukrainian authorities are working with the Red Cross in attempts to contact and locate the missing people, including women and children.

OSCE staff detained in eastern Ukraine

The Organization for Security and Cooperation in Europe (OSCE) announced on 24 April that they are seeking possibilities to facilitate the release of several of its Special Monitoring Mission (SMM) members who have been "deprived of their liberty in Donetsk and Luhansk".
The SMM is a civilian division of the OSCE, tasked with observing and reporting on conflict zones. The mission in Ukraine was present in the country since the annexation of Crimea in 2014. Its mandate expired on 31 March as Russia, one of the participating states of the OSCE, blocked its extension. Since then, the SMM has been operating in an administrative role to ensure the safety of its members, while still reporting on violations of international law by the Russian military.

Russian demonstrations in Europe against the war in Ukraine

Over the weekend, hundreds of Russian people joined a demonstration in Düsseldorf, Germany in support of Ukraine, under the slogan “We are Russians, and we are against war”. Many of them were carrying white-blue-white flags, symbolizing “free Russia”. Similar demonstration had previously taken place in Spain and other European countries.
Meanwhile, protesters in Russia are facing criminal prosecution since the implementation of a law prohibiting the "discrediting the Russian Armed Forces" in March. According to OVD-Info, a Russian non-profit human rights media project, as of 25 April, nearly 15,500 people have been detained in Russia in connection with anti-war protests.

Workforce shortages at construction sites

Since the Russian invasion of Ukraine, construction companies have suffered workforce shortages due to Ukrainian workers going back to their country following military mobilization requirements. In particular, construction companies in Poland are experiencing difficulties to continue activities at some sites as well as to start new projects due to lack of workers.

Preliminary Assessment

- Considering the reported deportations, detainment and persecution in Ukraine and Russia, companies in the region are advised to continue their efforts to ensure the safety of their staff
- Companies may turn to other countries in Eastern Europe to compensate for staff shortages. For construction companies, Moldovan workers could become an alternative

Operations (Focus: Cyber Threats)

Hacking groups take sides

One of the most troubling aspects of the Russo-Ukrainian conflict is the presence of numerous non-state actors on the cyber front. But why does a criminal group have to side with a government that should in fact prosecute its operations? There are two hypotheses:

- Criminal groups offer support to a government in exchange for an amnesty on past crimes.
- The line that divides nation-state actors from cyber criminal groups is thinner than we imagine, revealing dangerous overlaps between the two worlds.

Some experts believe that while hackers on the Ukrainian side are frequently motivated by ideology, most hackers supporting Russia might be doing so as they feel pressured by the Kremlin to operate on their behalf. Others assume a direct connection to the Russian government and state sponsorship.

However, when moving away from their usual financial motives for attacks and engaging in politics, hacking groups may turn themselves into targets. Thus, after Conti sided with Moscow, their systems were penetrated and a trove of internal chat messages and other files was leaked, significantly damaging the group.

The war in Ukraine could be a pivotal moment for hacktivism. It may go down in history as the conflict that allowed this form of activism to become known worldwide as an effective fighting method. But it could also be the factor that would lead to further escalation of the conflict.

Current topics

Stormous group support for Russia

The Stormous “ransomware gang”, known for website defacement and information theft, represents itself as a group of Arabic-speaking hackers. The group has been active since 2021, and recently it officially announced its support for the Russian government and its intention to target Ukrainian government institutions such as the Ukrainian foreign ministry. Recently, the group also issued a warning against “western unions” and more specifically companies in the US, after being attacked by unspecified US companies causing their site to be shut down.

Possible increase of Russian cyberattacks

On 20 April, the US Cybersecurity and Infrastructure Security Agency (CISA) warned that organizations could see "increased malicious cyber activity" either from state-sponsored actors in Russia or cybercrime groups aligned with Russia. The warning cited "evolving intelligence" that indicated Russia's government could be weighing options for potential cyberattacks. The possible targets are organizations within Ukraine as well as outside the region, including the US.
The warning comes as Russian President Vladimir Putin initiated a new phase of the Russo-Ukrainian war by pushing into Eastern Ukraine's Donbas region this week.

NATO’s cyberwar training in preparation for a real Russian attack

Last week, cybersecurity experts representing 30 NATO members gathered to fight a digital war to defend a fictional island country in the northern Atlantic Ocean. Though “Berylia” is fake, experts involved hope the lessons learned from the staged attack will better prepare them for the possibility of a Russian attack as the war in Ukraine continues.
The war games, dubbed the “Locked Shields’’ exercises by The North Atlantic Treaty Organization’s Cooperative Cyber Defense Centre of Excellence (NATO’s CCDCOE) are heralded by the organization as the “World’s Largest International Live-Fire Cyber Exercise”. CCDCOE conducts Locked Shields annually, though the stakes of the exercise are much higher in 2022 with a real-world war underway. The cybersecurity experts are looking to find cracks in their defenses and patch them, something particularly important as fears of a cyberattack against Ukraine and bordering NATO countries become larger.

Preliminary Assessment

- “Ransomware gangs” and other hacking groups have taken to social media to announce where their allegiances lie
- The US advisory for the first time addressed the dangers posed by private cybercriminal hacking groups acting on Russia’s side
- Administrators were advised to adopt some best practices to secure their networks from attacks. In addition to basic measures such as patching systems and providing end users with security awareness training, they are being encouraged to enforce multifactor authentication and either block or closely monitor the use of remote access protocols such as RDP
- The results of previous “war games” spotlighted the need for increased communication between the civilian and military sides of the IT industry during attacks. Those issues of cross sector communication appear as equally important worries in this year’s games

Finance (Focus: Sanctions)

Key Considerations

Sanctions Screening Activities

- Screening solutions generate increasing number of alerts (especially banks must deal with increased workload)
- Appropriateness and effectiveness of sanctions screening measures in identifying sanctioned parties and activities must be ensured. Complex ownership structures complicate the proper identification of involved parties (OFAC 50% rule)
- Trade transactions with Russia and Belarus must be reviewed

Sanctions Compliance Governance

- Sanctions Compliance Governance as a key requirement increasingly in the focus of regulatory authorities
- Robustness of Sanctions Compliance Management System and sanctions controls to counter the current and new sanctions regulations
- Adequateness of internal safeguards to prevent sanctions circumvention activities

Current topics

6th EU sanctions package to be presented to EU countries

As mentioned in last week's briefing, the EU is discussing the next round of sanctions against Russia, targeting further Russian banks as well as a form of oil ban. Reportedly, the new measures will be presented to EU member states this week. Meanwhile, on 21 April, the EU imposed an asset freeze and travel ban on two individuals allegedly involved in Russia's annexation of Crimea and destabilization of eastern Ukraine. Reportedly, EU restrictive measures imposed for "undermining of territorial integrity of Ukraine" currently apply to a total of 1093 individuals and 80 entities.

Extended US sanctions to prevent SWIFT circumvention

Attempts to avoid US sanctions have been met with expanded sanctions against 30 individuals and 40 companies and further visa restrictions. TransCapitalBank and the network of Russian oligarch Malofeev have been accused of setting up global networks to circumvent the SWIFT system and to continue processing business in US dollar. Further, for the first time companies in the crypto mining sector have been added to the US sanctions list. The US Treasury Department hereby reacts to the potential contribution of large crypto currency mining farms to the Russian economy. The country's climatological conditions strongly favor the mining process and further support the monetization of Russia's natural resources.
The US also announced a ban on Russian ships in all US ports.

New UK and Australia sanctions

The UK banned imports of caviar and high-end products from Russia. The import ban also covers silver and wood products, combined with a 35% increase of the tariffs on imports of diamonds and rubber from Russia and Belarus. Additionally, the UK announced further sanctions targeting Russian generals "committing atrocities on the front line", and individuals and businesses supporting the Russian military. Meanwhile, on 22 April, the Australian government imposed targeted financial sanctions in connection with the Russian invasion of Ukraine on a further 147 individuals, including Russian senators and family members of Russian President Vladimir Putin and Foreign Minister Sergey Lavrov, bringing the total number of sanctioned individuals and entities to nearly 750.

Further Russian countermeasures

On 21 April, Russia banned entry into the country for an additional 29 American officials and public figures, including US Vice President Kamala Harris and Meta CEO Mark Zuckerberg. Further, Russia stopped publishing data on banks, oil production, state debt and trade statistics, without which it is more difficult to estimate the impact of Western sanctions on the country's economy.

Preliminary Assessment

- The new and refined US sanctions further distance Russia from the world's financial system and intend to decrease the revenues derived from important business sectors
- With a total of over 5,500 sanctions imposed pre- and post-invasion of Ukraine, Russia is currently the most sanctioned country in the world. Nevertheless, it has so far managed to keep its financial system from collapsing under the weight of Western sanctions, which is largely due to the Russian central bank's measures, including raising interest rates and imposing strict capital controls. However, IMF estimates that Russian economy could shrink by 8.5% this year; and the Russian opposition party "Jabloko" ("Apple") foresees an overall economic decrease of 10%-11% with a particular impact on the following industries: mechanical engineering, pharmaceuticals, food industry, airfreight, telecommunications, electronics production, financial services, metal mining, high-tech industries, logistics. The inflation is already at 17.5%, which takes its toll on Russian citizens. An even larger economic impact could be achieved by an EU ban on Russian oil imports. Additionally, Russia's reliance on imported products, a number of which are now under sanctions, could be more difficult to counterbalance than addressing adverse macroeconomic measures

General remarks

- The information contained in this briefing is prepared by PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Frankfurt am Main. It is for general guidance on matters of interest, and intended for the personal use of the reader only and in connection to the PwC Webcast series “War in Ukraine” or based on individual consent in the context of an existing client relationship. This informational material shall not be deemed to establish a contractual relationship between PwC and the reader. Further distribution requires the explicit consent of PwC.

- The information contained in the briefing is selected with due care. We have made every attempt to ensure that the information contained in this briefing has been obtained and arranged with due care. No representation or warranty of any kind (whether expressed or implied) is given by PwC as to the accuracy or completeness of the information contained within this briefing.

- PwC accepts no liability for any actions taken as response hereto. The information is provided on the understanding that the authors are not herein engaged in rendering legal, accounting, tax or other professional advice or services. As such, it should not be used as a substitute for consultation.

- PwC reserves the right to change or update at any time the briefing without prior notice.

- This briefing may contain references to public sources (e.g. media outlets) maintained by third parties. PwC has no control or influence over the content of such sources. The information from such sources have neither been checked nor approved by PwC in any way. References do not mean that PwC adopts the content behind the reference or link as its own. Therefore, PwC does not assume, for whatever legal reason, any responsibility for the content of the websites of third parties.