War in Ukraine

—

Situational Awareness Briefing

7 November 2023

Situational Awareness – Briefing as of 7 November 2023 (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/Topic/Country Special
- Forecast
- People
- Operations
- Finance

Overall Geopolitical Assessment

The world is focusing on the Israel-Hamas War and monitoring the progress of Israeli ground operations. Russia relaunched its large-scale attacks on the Avdiivka salient, as the Ukrainian summer offensive has ended in failure. For three weeks Russia has only achieved limited success while significant losses were incurred. Debates sparked in Western capitals whether to engage in negotiations with Russia.

Inside-out view on reconstruction efforts in Ukraine

The UK and EBRD collaborate on war risk insurance project for Ukraine, while Germany and Bpifrance provide additional support to Ukrainian exporters and investors // Poland plans to launch an investment fund with insurance for Polish and Ukrainian entrepreneurs in Ukraine // The EU approves the transfer of profits from frozen Russian assets to Ukraine, with legal proposals to be presented in December 2023, including funds held at Euroclear.

Forecast

Ukraine's Naftogaz decides not to resume Russian gas transit to Europe after 2024 due to alleged contract non-compliance, impacting European gas markets // Chinese President Xi Jinping calls on Germany to mediate and prevent a potential trade war between the EU and China, highlighting concerns about EU-China relations amidst global shifts.

People

Raiffeisen Bank earns nearly half of its profits from Russia despite reducing operations // Several Western companies exit the Russian market, Carlsberg faces complications in selling its Russian subsidiary // Ukrainian businesses gradually resume operations, with 77% of European Business Association members fully operational in November 2023.

Operations (Focus: Cyber)

Hackers targeted the website of Russia's National Payment System and Mir payment system, claiming to have stolen user data, but the operator states the site contained no confidential information // Ukrainian hackers, known as the IT Army, disrupted internet providers in Russia-occupied territories, aiming to disrupt enemy military communication and counter Russian propaganda efforts through information control. This is part of a series of cyberattacks on Russian operators, including surveillance cameras and satellite communications providers.

Finance (Focus: Sanctions)

Over 100 UK-based companies admit to breaching British sanctions on Russia // The US imposes new anti-Russian sanctions targeting 130 individuals and entities related to the Russian military machine // The US blocks a channel for Russians to circumvent sanctions by imposing sanctions on Ekaterina Zhdanova and her cryptocurrency accounts, which were used to help Russian oligarchs and fraudsters move money abroad.

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

Overall Geopolitical Assessment (1 of 3)

Key takeaways

- Russia's catastrophic attacks at Avdiivka continue. It currently focuses its war effort there.
- Russia initiated another offensive in the vicinity of Vuhledar.
- In Kiev, fears increase that the US and Western supporters will recommend to initiate peace talks with Russia.

Current topics

Current situation in the Russo-Ukrainian War

The Ukrainian strategic counteroffensive has reached its culmination point and only local attacks were conducted along the Zaporizhzhia front. After four months the offensive has stalled, creating a small salient in the area of Robotyne, but ultimately failing to achieve a decisive breakthrough. Ukraine continues with small scale attacks further east and occupied Sahirne this week. However, it is evident that the summer offensive has failed and that it will be highly unlikely to reach any of the Mariupol, Tokmak or the Crimea in the coming months. Despite this setback, Ukraine has used its newly arrived cruise missiles for multiple successful strategic attacks on the Crimea and the Russian hinterland to effectively hamper Russian logistics, ammo depots and force concentrations. On the Kherson front, Ukrainian forces continued their operations on the southern bank of the Dnieper. Ukraine achieved minor territorial gains south of Cherson extending the bridgehead along the line of Oleschky, Pishchanivka to Krynky. With these operations the river swamp lands have now been crossed, and Ukraine can use the foothold around Dachy for potential future operations. Russia had launched an extensive counteroffensive three weeks ago in the vicinity of Avdiivka in an attempt to encircle the city from north and south but suffered high losses in materiel and personnel with limited to no gains. This week Russia reinitiated its attacks to encircle the town. It also launched secondary offensives in the areas of Vulhedar of Kupiansk. The Russian attacks can be considered as an attempt by Moscow to shift the strategic initiative in their favor as the Ukrainian offensive along the Zaporizhzhia front has come to a halt. Russian losses in all those engagements have been catastrophic so far as they repeat the same pattern of advance. Hundreds of soldiers and several armored vehicles are lost in seemingly uncoordinated attacks along mined gateways and Ukrainian artillery kill zones. Politically Moscow seems to attempt to exploit the concentration of the West on the Israel-Hamas War. In addition, it seeks to capitalize on signals from some US and EU politicians to limit their support to Ukraine as rumors of US lawmakers pushing Ukraine towards the negotiation table emerged. Within the EU Slovakia and Hungary have openly refused to continue to support Ukraine.

Hybrid disinformation warfare: Social Media as potential weapon

Social media has established itself as a modern means of information and communication. Disinformation has accompanied its rise from the very beginning. State regulatory measures and rules introduced by the operating companies - depending on the respective national context - attempt to curb content that glorifies violence, racist or sexist content and obvious misinformation through censorship, filters, community feedback, warnings or account blockings. To circumvent these measures, users turn to less regulated messenger services such as Telegram. US platforms such as Google (YouTube), Meta (Facebook, Instagram, WhatsApp) and X primarily pursue economic interests and collect user data for advertising purposes. Newer services such as TikTok from Chinese operator ByteDance present an evolution of hybrid threats in the information sector. Unlike in the past, they are not just an information battlefield; the platforms themselves are the hybrid means of exerting influence. TikTok's operating company is not a purely private-sector provider, but can be considered a semi-state actor due to its proximity to the Chinese government. The app collects more data about users than comparable applications. The app also reportedly conceals which data is collected and where it is sent. TikTok's content is usually created by the users themselves. However, the algorithm is allegedly optimized in such a way that it can captivate users for hours every day with short-lived videos. Controversial political topics, such as videos about demonstrations in Hong Kong, are deliberately censored. Allegedly the algorithm creates a profile of the user and slowly learns how it can distract the user or lead them in a certain direction of thought through the presentation of content. This potentially makes TikTok a kind of Trojan horse, which not only acts as a data octopus but is also can used as a means of influence.

Overall Geopolitical Assessment (2 of 3)

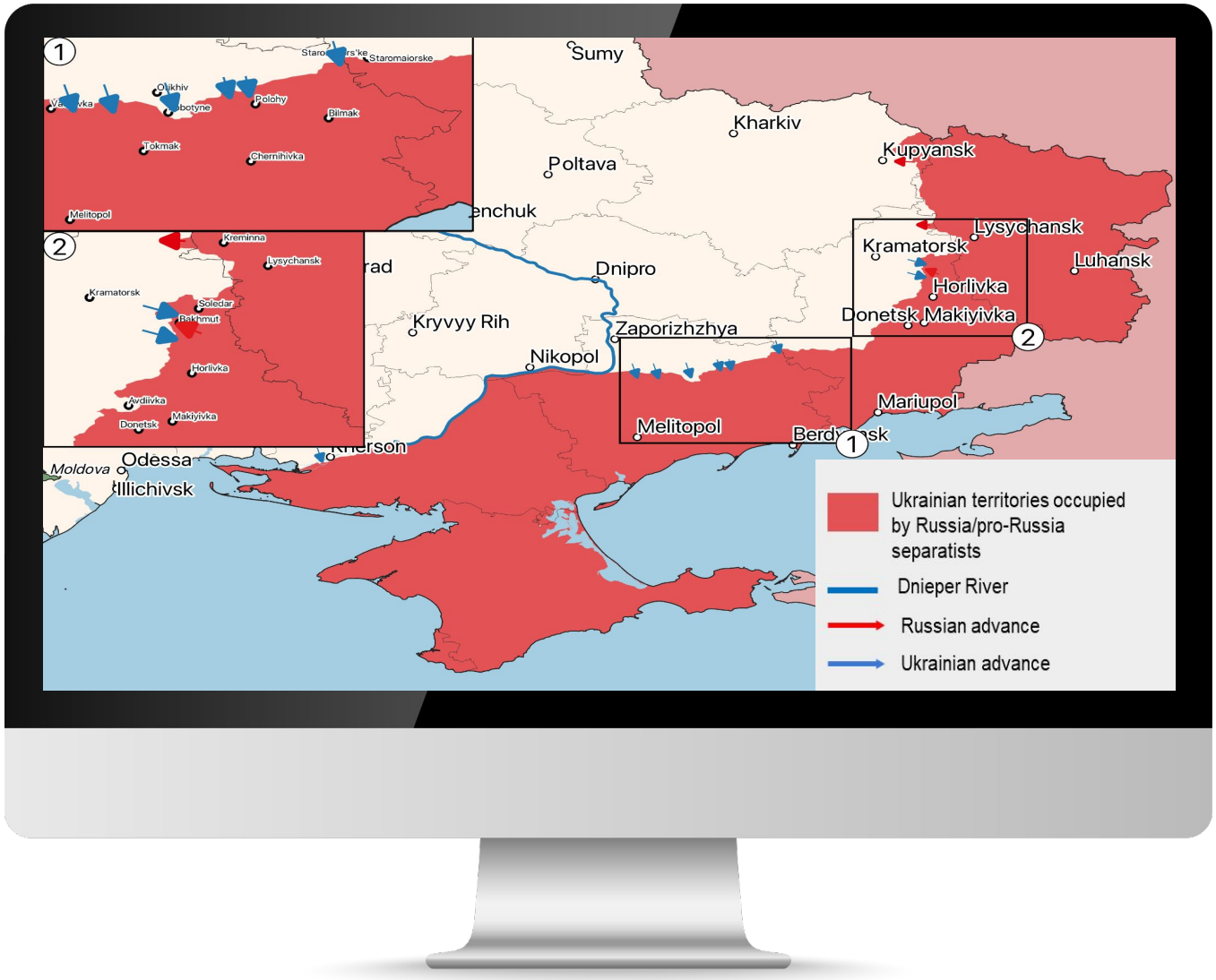
Key takeaways

- The Ukrainian offensive has stalled in the central sector of the Zaporizhzhia front.
- A large-scale Russian counteroffensive at Avdiivka and two secondary offensives at Vulhedar and Kupiasnk led to significant losses to the Russian Army while achieving only minimal gains.

Selected upcoming events

- 26 November 2023: OPEC and non-OPEC ministerial meeting, Vienna/Austria

Current military situation in Ukraine (blue arrows indicate current Ukrainian counterattack, red arrows indicate potential future Russian operations in the coming weeks)



Key takeaways

- Iran operates a network of proxies in the Middle East which it employs to support as well as to challenge local governments and further its political influence.
- Iran's regional hegemonic ambitions put it at odds with other Gulf countries, in particular Saudi Arabia, the United Arab Emirates and Bahrain.
- While some rapprochement between Saudi Arabia and Iran has occurred in 2023, a latent conflict escalation risk persists. While the risk is low overall, such an escalation could have far-reaching consequences in the worst case scenario, and, for example, involve the prolonged closure of important maritime routes in the Persian Gulf.

Special topic

Iran's network of proxies in the Middle East and its implications for regional stability

Iran has established a network of proxies in the Middle East to expand its regional influence and for power projection. The country maintains ties to over a dozen (mostly Shiite) militias in the region that it provides with arms, training or financial support. It employs such militias both to support and challenge local as well as neighboring governments.

In Syria, four Iranian-supported militias (Fatemiyoun Brigade, Zainabiyoun Brigade, Quwat al-Ridha, Baqir Brigade) estimated to number around 20,000 members support the Assad regime during the ongoing civil war. In Iraq, various Shiite militias (Kata'ib Hezbollah, Badr Organization, Asa'ib Ahl al-Haq) estimated to number up to 75.000 members likewise support the government and meddle in domestic politics. In Lebanon, Iran supports Hezbollah, an important faction in domestic politics and antagonist of Israel. In the Palestinian territories, Iran is a major backer of Hamas as well as the Palestinian Islamic Jihad. It is likely that Hamas' recent attack on Israel had Iranian backing and support. In Yemen, Iran supports the Houthi movement in the ongoing civil war against the internationally recognized government. Finally, Iran supports the Al-Ashtar Brigades in Bahrain against the local government, which does not maintain political relations with Iran.

US and Western efforts to sanction militias and curb financial transfers had limited success so far and Iranian militias continue to present a significant threat to US military personnel and Western assets in the region.

Iran's regional hegemonic ambitions put it at odds with Western-allied countries in the region, in particular Saudi Arabia, the United Arab Emirates (UAE), Bahrain and Jordan. Iran has employed its proxies to conduct attacks on assets in the UAE and Saudi Arabia. Even though some rapprochement has taken place this year between Saudi Arabia and Iran and diplomatic relations were reestablished, their status as strategic antagonists is unlikely to change.

In consequence, a latent conflict escalation risk exists in the Middle East between Iran, Saudi Arabia and its allies as well as Israel. While this risk appears relatively low, it could have major consequences. A direct conflict between Iran and one of the Gulf monarchies could impair maritime traffic in the Persian Gulf and through the Strait of Hormuz, affecting a substantial part of global fossil fuel trade. It could also lead to airspace closures, further disrupting air traffic between Europe and Asia. Finally, it could also spark direct Western military involvement and further aggravate conflict between the West and Russia and China, both of which maintain close relations with Iran.

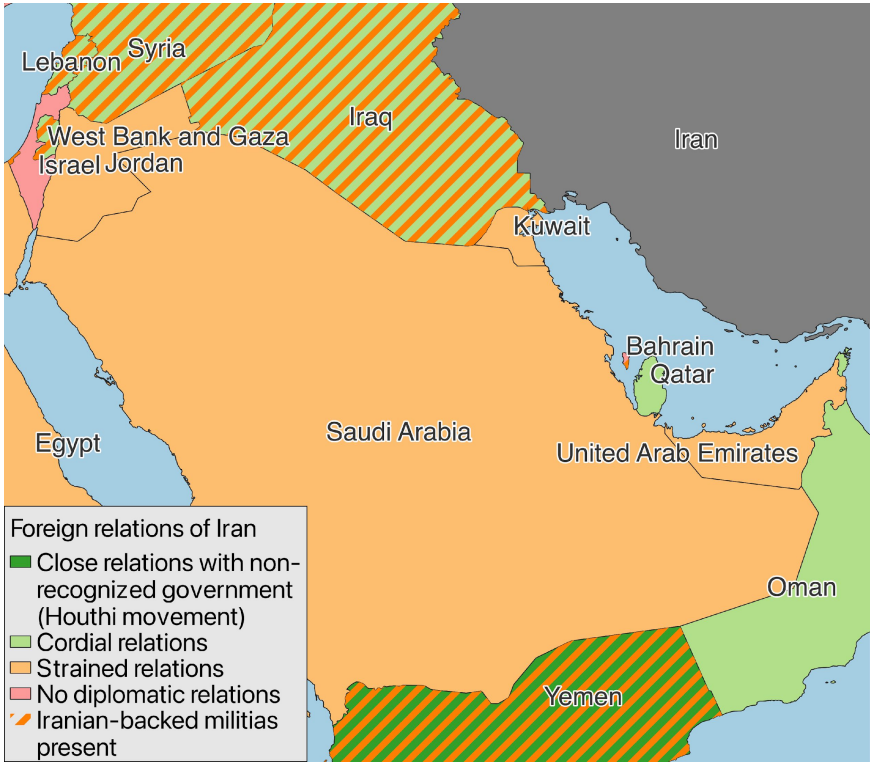


Figure 1: Foreign relations of Iran (illustration based upon own research)

Inside-out view on Ukraine reconstruction efforts

Donor activity - update

- In October 2023, the state budget of Ukraine received approximately USD 2.8 bln in external financing. Grant funds, provided on a non-repayable basis, accounted for over 40% of the total volume of financial aid. Among the donors in October 2023 were the European Union – USD 1.6 bln (concessional financing, the ninth installment within the framework of large-scale macro-financial assistance for 2023); and the United States of America – USD 1.15 bln (grant).
- The European Investment Bank will allocate the first two tranches of EUR 100 mln each to Ukraine by the end of 2023, out of the planned total of EUR 450 mln for two projects: Ukraine Recovery III Framework Loan for financing critically important social and urban infrastructure, and Ukraine Water Recovery Framework Loan for financing investments in critically important water infrastructure.
- The Government of Ukraine has agreed to sign an Agreement with the European Commission on funding the EU Support for Recovery and Reforms program. The total funding under the agreement will amount to EUR 335 mln. The funding is aimed at repairing or reconstructing residential and vital economic assets; enhancing resilience and strengthening the institutional and administrative capacity of Ukrainian state bodies; bolstering the capability of civil society organizations to participate in responding to the consequences of the war; intensifying the implementation of the EU-Ukraine Solidarity Lanes initiative; strengthening food security, among other objectives.
- The German Federal Ministry for Economic Affairs and Climate Action will contribute EUR 54.3 mln to the Ukraine Energy Support Fund to procure energy equipment necessary for the restoration and repair of Ukrainian energy facilities.

Current topics

War Risk Insurance Project

The United Kingdom is going to collaborate with the European Bank for Reconstruction and Development (EBRD) on the development and implementation of a pilot project for war risk insurance in Ukraine. An intention statement was signed between the Government of the United Kingdom and the EBRD on October 31, 2023. The EBRD's project entails the establishment of a new fund aimed at fostering the growth of the international reinsurance market, as well as property and trade risk insurance, which includes coverage for goods in transit or stored in warehouses. Recently, the Federal Government of Germany has decided to provide Ukraine with export credit guarantees, also known as Hermes Cover. It expands the coverage options and supports exporters engaging with Ukraine. Additionally, the French state-owned insurance company Bpifrance Assurance Export announced it will insure French companies willing to invest in Ukraine and actively participate in the country's reconstruction efforts without waiting for the end of the conflict.

Polish investment fund

Poland is planning to launch an investment fund designed to support the development of Polish and Ukrainian entrepreneurs in Ukraine, offering the possibility of investment insurance. In support of this initiative, the Polish Ministry of Finance has agreed to increase state funding from 2024 for cooperation programs with Ukraine. The investment insurance will be provided by the Polish State Corporation for export credit insurance (KUKE), which, following legislative changes, has expanded its scope of operations. As of September 2023, KUKE insures and reinsures investment and export contracts not only for Polish but also for international companies, including Ukrainian ones. Furthermore, to attract investments for Ukraine's reconstruction, an agreement was signed with the United Nations in September 2023, which includes the establishment of a United Nations Office for Project Services (UNOPS) in Poland to facilitate such projects.

Transfer of Russian profits

The European Union has approved plans to transfer the profits from frozen Russian assets to Ukraine. The European Commission is expected to present legal proposals in December 2023. Western sanctions have frozen USD 300 bln belonging to the Russian central bank. Most of these funds – EUR 180 bln – are held at Euroclear, the world's largest securities depository headquartered in Brussels. Euroclear recently reported earning approximately EUR 3 bln on frozen Russian assets in the first nine months of 2023, compared to EUR 347 bln in 2022, attributing this increase to rising interest rates.

- The United States International Development Finance Corporation (DFC) has approved five new projects in Ukraine, with a combined value of over USD 380 mln. These initiatives aim to bolster food security, support small businesses, strengthen the healthcare system, and enhance international trade.
- The United States International Development Finance Corporation (DFC) has approved five new projects in Ukraine, with a combined value of over USD 380 mln. These initiatives aim to bolster food security, support small businesses, strengthen the healthcare system, and enhance international trade.
- On November 3, 2023 the Ukrainian Government approved regulatory changes for managing territories contaminated by radioactive pollution following the Chornobyl disaster. These changes are part of a strategic initiative to transform the Exclusion Zone into an area of industrial potential development and to encourage investment. The modifications introduce transparent regulations for conducting economic activities within the Exclusion Zone, including constructing alternative energy projects and high- tech manufacturing facilities.
- On November 2, 2023, the Ukrainian electricity transmission system operator Ukrenergo conducted its inaugural auction to sell cross-border transmission capacity on the Ukraine-Romania and Romania-Ukraine interconnection lines following European regulations. Ukrenergo also anticipates that joint auctions with Poland, Hungary, and Slovakia will become operational on the pan-European platform JAO in the first quarter of 2024.

Forecast

General context

Considerations on implications for businesses along the PESTEL framework

P Political	De-risking EU relationship with China
E Economic	China calls on Germany to mediate China-EU trade war
S Social	Challenges for Hungary, Slovakia, the Czech Republic, and Austria gas markets
T Techno-logical	Technology related implications: e.g. cyber threats and disinformation, IT infrastructure disruptions
E Environ-mental	Environment related implications: e.g. Resource scarcity, energy embargo
L Legal	Legal implications: Compliance with changing regulations, contractual obligations, etc.

Current topics

End of the agreement on Russian gas transit to the EU

Ukraine's state gas company, Naftogaz, has announced that it does not plan to resume the transit of Russian gas to Europe once its contract expires in 2024. The decision is primarily due to Russia's alleged non-compliance with the terms of the contract, particularly regarding payment for gas transit through the Russian-occupied territory of Sohranivka (Luhansk Oblast).
Despite the financial challenges, Naftogaz is still currently ensuring gas supplies to European countries. The European Union, however, plans to cease using Russian gas by 2027 and is not insisting on the continuation of Ukrainian transit. This decision has created challenges for markets in Hungary, Slovakia, the Czech Republic, and Austria, as they currently rely on Ukrainian routes for approximately 42 million cubic meters of gas per day.

Xi Jinping calls on Germany to prevent EU-China Trade War

Chinese President Xi Jinping has called on Germany to mediate and help prevent a potential trade war between the EU and China. Xi's comments were made during a virtual meeting with German Chancellor Olaf Scholz. Xi urged Germany to uphold principles of market and fairness, emphasizing the importance of maintaining fair market competition and trade as well as stable industrial and value chains.
The EU has initiated a probe into state subsidies for made-in-China electric vehicles, which has raised tensions. Xi's appeal to Germany reflects China's concerns about the EU aligning with the United States in its approach to China. Beijing's increasing focus on ideology, coercion against US allies such as Japan, Canada and Lithuania, and assertive posture against Taiwan have forced EU governments to focus on so-called "de-risking" the bloc's relationships with China. Earlier, the prime ministers of the Netherlands and Ireland — which have massive trade ties with China — are touring countries from Malaysia and Vietnam to South Korea, looking for alternative markets in Asia.

Preliminary Assessment

- In early October, the European Commission reported a significant reduction in the impact of Russian energy supplies on Europe.
- It was previously announced that four European countries would receive gas from Qatar. These countries are Italy, the Netherlands, Germany, and France.

- Xi is expected to meet Ursula von der Leyen and Charles Michel, heads of the European Commission and European Council, by the end of the year.
- According to Xinhua, Scholz expressed interest in "deepening German-Chinese relations" and in the "biggest successes for German companies in China," without any mention of his stance on EU-China relations specifically.

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	Preliminary Assessment
Half of Raiffeisen’s profits this year came from Russia Raiffeisen Bank has generated nearly half of its profits from its Russian operations this year, despite efforts to reduce its presence in the country. The bank has reduced its lending in Russia by 30% in response to criticism of its operations under Vladimir Putin's regime. While exploring options for a strategic exit, the bank's talks with Russian institutions have stalled, and it faces challenges due to increased restrictions on Western businesses in Russia. As well as reducing its Russian loan book — now EUR 6.3bn in size — Raiffeisen has scaled back its payments business and terminated relationships with local banks. Profits from Western companies in "unfriendly" countries are also trapped in Russia. Raiffeisen's strong profits have been driven by other Western businesses flocking to the bank.	• According to the Kyiv School of Economics, approximately USD 20 mn of the profits of companies headquartered in “unfriendly” countries — which face restrictions from the Kremlin — are stuck in Russia • In February, the US Treasury announced it was probing Raiffeisen over its Russian business.
More Western companies existing Russia In October 2023, 12 new exits of foreign companies from the Russian market were recorded as evidenced by the results of the KSE Institute's monitoring. For instance, Russian subsidiary of “Google” was declared bankrupt end of October. Carlsberg since last year has been trying to sell its “Baltika” subsidiary in Russia. However, after Carlsberg announced in June that it had found a buyer for the business, the following month Russian President Vladimir Putin ordered the temporary seizure of Carlsberg's stake in the local brewery. The Danish group refused to enter into an agreement with the Russian government that would make Moscow's seizure of assets legitimate.	• In total, the number of international firms and corporations that have completely withdrawn from Russia reached 296 in October. • Earlier this month, Carlsberg responded by terminating licensing agreements for its brands in Russia that allowed Baltika to manufacture, market and sell all Carlsberg products in the country.
Businesses in Ukraine that have restrictions on their operations due to the war has halved As of November 2023, three quarters of Ukrainian companies that are members of the European Business Association have resumed full operations, ar reported on the EBA website. Thus, in October 2023, 77% of EBA member companies stated that they were fully operational. For comparison, in August of this year, 69% were fully operational, and a year ago - 44% of EBA member companies. The number of businesses that say they have restrictions on their operations due to the war has decreased from 53% in October 2022 to the current 23%. The most common restriction is still the reduction in the geography of companies' operations. 46% of companies report direct losses from the hostilities. In addition, 22% of companies still have assets in the occupied territories.	• 53% of the companies have up to 10% of their employees in the Armed Forces of Ukraine. In 25%, the number of mobilised employees reaches 10-20%, and in 5% - 20-30%. • 45% of the companies have mobilised or volunteered specialists critical to the company's operations, including engineers, IT specialists, logistics specialists, electricians, mechanics, operators, and managers.

Operations (Focus: Cyber Threats)

Attack vectors to focus on in the wake of the Israel-Hamas war

In the recent conflict between Israel and Hamas, hacktivist groups attempt many of the same techniques that were applied in the Russia-Ukraine war. Security experts list the following biggest threats that companies should look out for:

- Denial of service attacks

Relatively low-tech, but effective at disrupting networks, services, or websites by overwhelming them with a massive flood of traffic requests

- Propaganda and misinformation

This has become the easiest of all cyberwarfare tactics for the average person because it requires almost no technical knowledge and only an internet connection. Additionally, sophisticated bot networks are more prevalent than ever on social media, making it even easier to use this tactic.

- Cyber espionage

State actors or cyber criminals can monitor communications, infiltrating networks, and gain valuable trade or secret information that they can use for a wide range of future attacks. Social engineering campaigns are also often a first step to deploy backdoors that bypass traditional security methods and then gather information through social engineering instead of relying only on bruteforce hacking attempts.

- Hacking and defacement

Hacked records may reveal sensitive personal information which can be exploited for harassment or additional cyberattacks. Access to private data can put employees or customers at risk for targeted phishing attempts and malware distribution.

- Defacing

Attackers often look to deface websites, social media accounts, and digital platforms. They aim to hack the website and convey political messages and ideologies.

Current topics

Hackers attacked the website of the Mir payment system operator

On Monday, 30 October 2023, attackers hacked the website of Russia's National Payment System and the Mir payment system. They left a message with a link to the website of the pro-Ukrainian hacker group DumpForums, which hints at the theft of users' personal data. The hackers also posted a screenshot showing that they have a database called privetmir weighing 31 gigabytes.

However, the press service of the National Payment Card System reported that the site is only a "business card with information about the company's activities" and does not contain any confidential data, and is not related to the payment infrastructure. It is impossible to gain access to any of the company's systems from the site, the company assured, clarifying that their servers and data centers do not have access to the Internet.

Ukrainian hackers disrupt internet providers in Russia-occupied territories

Ukrainian hackers have temporarily disabled internet services in parts of the country's territories that have been occupied by Russia.

The group of cyber activists known as the IT Army said on Telegram that their distributed denial-of-service (DDoS) attack took down three Russian internet providers — Miranda-media, Krimtelekom, and MirTelekom — operating in the territories.

"This is yet another blow by our cyber army disrupting enemy military communication at the frontlines," the hackers said.

After occupying parts of eastern Ukraine and the Crimea peninsula, Russia disconnected Ukrainian telecommunications infrastructure there and rerouted internet traffic through Russia's network instead. Ukraine strongly criticized this move, saying that Russia wants to make its propaganda "an uncontested source of information."

The attacks on Russian internet operators, including those operating in occupied territories, have happened before. Earlier in October, Ukraine's IT Army targeted Crimean internet operators and one of the attacks reportedly disabled surveillance cameras in a city in western Crimea. In July, a previously unknown group of hackers targeted a Russian satellite communications provider, which is used by energy companies, as well as the country's defense and security services.

Preliminary Assessment

- Previously, DumpForums reported on the hacking of the websites of the tour operator Intourist, the insurance company SOGAZ Life, as well as the database of the State Services service.

- In Ukraine, telecommunication service providers are also frequently targeted by Russian hackers, according to Illia Vitiuk, the head of the cyber department at the Security Service of Ukraine. Thus, on October 20th, Vitiuk told Recorded Future News that Russia recently made a "serious attempt" to breach one of Ukraine's three telecom operators. The Ukrainian cybersecurity services thwarted this attack, but a successful penetration could lead to eavesdropping, and interception of phone calls and messages.

Finance (Focus: Sanctions)

Key Considerations

Sanctions Screening Activities

- Screening solutions generate increasing number of alerts (especially banks must deal with the 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	Preliminary Assessment
British companies admit breaching sanctions on Russia According to data unearthed through a freedom of information request submitted to the HM Treasury, more than 100 UK-based companies confessed to violating British sanctions against Russia. In a bid to lessen their penalties, these companies voluntarily stepped forward and cooperated with investigations. The challenge arises from Russia's deep integration into the global economy, making it difficult for UK businesses to comply with the sanctions.	
The US imposed new anti-Russian sanctions The US has imposed another package of anti-Russian sanctions, which includes 130 individuals and entities from Russia. The sanctions are focused on individuals and entities that contribute to war by providing Russia with technology and equipment from third countries, the US Treasury Department reports. In addition, the latest restrictive measures are aimed at Russia's domestic industrial base, which is seeking to redefine itself as a supporter of the Russian military machine. The report specifies that on 2 November, the US State Department also imposed another package of sanctions. More than 100 State Department sanctions target Russia's future production and revenues from energy, metals and mining, defence procurement, and those involved in supporting the Russian government's war effort and other malicious activities. In particular, Russia continues to use legitimate economic relations with the China,Turkey and the United Arab Emirates, which have become hubs for exporting, re-exporting and transshipment of foreign-made technology and equipment to Russia.	• In particular, the blacklisted entities include a diversified holding company Arctic LNG-2, SPB Exchange, which specialises in trading in foreign shares, Russian Standard Bank, Home Credit Bank, Pochta Bank, Absolute Bank, VBRD bank, East West United bank. • The sanctions were also imposed on Bauman Moscow State Technical University.
The US blocks a channel for Russians to circumvent sanctions in cryptocurrencies The US has announced sanctions against Russian citizen Ekaterina Zhdanova and her accounts on cryptocurrency exchanges, which she used to help Russian oligarchs and fraudsters move hundreds of millions of dollars abroad amid sanctions. "Through key intermediaries such as Zhdanova, the Russian elite, online extortion groups, and other illicit actors have sought to evade US and international sanctions, including through the abuse of virtual currency," said US. Deputy Treasury Secretary Brian Nelson in this regard. In particular, it is reported that in March 2022, Zhdanova transferred more than USD 2.3 mn of funds from a Russian representative to Western Europe through a fraudulent investment account and a real estate purchase. In another case, she helped a Russian oligarch transfer more than USD 100 mn to the United Arab Emirates.	• Zhdanova reportedly used the services of organisations that do not have anti-money laundering controls and safeguards. Among such institutions is, in particular, the Russian cryptocurrency exchange Garantex Europe OU, against which the United States has already imposed sanctions. • In addition, Zhdanova allegedly provided services to the Russian online extortionist group Ryuk, laundering more than USD 2.3 mn of their illicit funds.

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.