

UKRAINE CONFLICT OVERVIEW AND IMPACT TO SECURITY IN THE UK

A G4S ACADEMY BRIEFING



Abstract

This document assesses and explores key elements of the conflict in Ukraine. The paper puts forward a short tactical breakdown and highlights how the conflict will influence business continuity and security at sites in the UK

Contents

1	<u>Overview</u>	<u>3</u>
2	<u>Tactical Update</u>	<u>5</u>
3	<u>Impact To Security And Business Continuity In The UK</u>	<u>7</u>

I Overview

As of 24 February 2022, Russia launched an invasion of Ukraine. This section of the report will seek to provide some general assessment around the status of the conflict. Please take into account that this is a dynamic conflict that is subject to regular change.

Please also take note that some content in this section may be upsetting for some readers for whom it may be of interest to skip forwards to the later section on business continuity and security implications of the conflict to sites in the UK.

- As of the morning of the 24 February 2022, Russian President Vladimir Putin initiated the movement of Russian troops into Ukraine stating that the purpose of the attack was to free Ukraine from oppression and to ensure the country be 'cleansed of Nazis'. It is highly likely that this was an excuse for the invasion rather than the true motive behind the conflict.
- Whilst the true reason for the invasion is still unknown, it is highly likely that factors behind the conflict include: Putin's desire to re-write the Vladimir Lenin era 'wrongs' of allowing Ukrainian sovereignty; an ambition from Putin to return Russia to former greatness and security concerns around the eastward expansion of NATO and the European Union.
- It is currently unclear what Russia's goals are for the invasion of Ukraine, there appear to be several working theories including the most likely which would include full succession of Ukraine to Russia or creation of a cold war era style eastern and western Ukraine.
- It is highly likely that Russia had aimed to conclude the conflict quickly to avoid a protracted war with the potential for a higher number of casualties; it is unlikely that the Russian military had expected to encounter heavy resistance from Ukrainian military and civilians. Since 2008, Russia has funded the modernisation of its military into a small, dynamic force capable of lightning-fast cross border attacks, as such it is unlikely that its forces would be able to engage in direct conflict with the North Atlantic Treaty Organisation (NATO), making it highly unlikely that this conflict will escalate beyond Ukraine.
- Due to the increasingly protracted nature of the conflict, it is highly likely that Russia will have to move towards a heavier type of warfare, with aerial and land-based bombardment of key targets to achieve its objectives. The Ukrainian Government has requested NATO forces to close Ukrainian airspace as one way of countering this form of Russian military superiority, there is a remote chance that NATO would agree to this due to fears around direct engagement with Russian forces leading to escalation. It is almost certain that there would be a much higher number of Ukrainian casualties if Russia has to use heavy artillery to successfully achieve its outcomes.
- In response to the Russian invasion of Ukraine all of 'the West' (roughly UK, US, Canada, Europe, Australia and New Zealand) and many other countries across the world have condemned Russian actions, introducing unprecedented tough sanctions against the Russian Government and Russian business owners.

Sanctions include:

- Freezing overseas assets
- Restriction of air and sea travel
- Sanctions on imports and exports including some oil and gas
- Considering removal from United Nations groups e.g. Council for Human Rights and the Security Council
- Removal of investment and sponsorship deals
- Removal from international sports
- Direct sanctions on Russian banks and businesses
- Potential removal from the Swift international banking system

- Due to the unprecedented nature and scale of the sanctions introduced, it is unclear what impact the sanctions will have on the Russian Government and its military campaign in Ukraine. It is almost certain that sanctions have already started to hit the Russian economy hard with the Russian ministry of finance increasing interest rates to 20%. However, it is unclear if the burden of the sanctions will be felt by the political and elite classes and indirectly effect military capability, or if the bulk of the hardship from sanctions will be felt by people with lower economic status across the country. Pressure on communities with lower economic status would likely increase the internal scrutiny and instability of Putin's Russian Government through unrest.
- As with most major conflict zones, there has been a significant impact on the civilian population of the Ukraine, with individuals signing up to fight, seeking safety in cities under Russian fire, or claiming refugee status in the surrounding countries. Stunted peace talks between Ukraine and Russia have reportedly found the most common ground on protecting the civilian population from further harm. These negotiations are happening sporadically but may lead to some breakthrough results in the coming days. Peace talks are yet to include both Putin and Ukrainian president Zelensky which would likely be a strong step toward reducing the current heat in the conflict.
- Reports have suggested that approximately two million Ukrainian people have sought refugee status in bordering countries such as Poland, Hungary, Slovakia, Romania, Russia (likely Russian speaking) and Belarus. It is almost certain that this influx of refugees will have a significant impact on the geo-political situation in Europe for many years to come. In all probability, it will stretch resources and worsen conditions for refugees seeking access from the Middle East and Africa to south-eastern Europe.
- Reports have suggested that Russia has placed its Nuclear arsenal on special alert following 'aggressive rhetoric' from Western leaders. Russia is in the middle of a nuclear capability regeneration project, as such it is unlikely to pose the same level of nuclear threat as at the height of the Soviet Union. Despite this reduced capability, it almost certainly maintains enough nuclear capability to threaten every major city in the West. There is currently a remote chance of an escalation to nuclear warfare with the West, however, in recognition that tensions could rapidly escalate, the United States and Russia have established an incident hotline for de-escalation.



2 Tactical Update

- Russia launched its invasion with a three-pronged attack that demonstrated a clear intent to bring the conflict to a swift conclusion. This did not come to fruition for a number of reasons, including but not limited to:
 - Setbacks in taking key targets
 - Unexpected resistance of the Ukrainian people
 - Strong Ukrainian anti-aircraft capability.

It is unclear why Russia has not deployed its full aerial superiority to this point in the conflict.

- The attack from the north saw the Russian military enter Ukraine through Belarus (Russian ally), and take the Chernobyl nuclear disaster area, before pressing further south to make a concerted effort, but reportedly failed attempt to take Hostomel airport to the north of Kiev. It is highly likely that the aim of taking the airport was to give Russia a launch pad for landing a force to invade Kiev. After meeting fierce resistance and failing to take Kiev quickly, Russia has sent a large 'convoy' of military support to surround Kiev. It is likely that if the conflict continues, this convoy will have the capability to strike key targets in Kiev and gradually move through the city to clear Ukrainian resistance block by block. This approach would highly likely mean a significant escalation in the risk to civilians and ensure a more protracted conflict between Russia and Ukraine. Kiev is highly likely to be the key objective for Russia to bring the conflict to a quick resolution.
- The attack from the south saw the Russian military enter Ukraine from the contested Crimean Peninsula. It is highly likely that the objective of the southern invasion force is to take the Black Sea port city of Odessa. Odessa sits as a hub of maritime trade, providing Ukraine with essential access to the Black Sea. Odessa is highly likely the key gas and oil terminus in the Ukraine. Despite fierce resistance from civilians and the Ukrainian military, cities and towns on the road to Odessa are reportedly beginning to succumb to Russian forces. It is highly likely that the battle for Odessa would become a key battle if the war in Ukraine continues. Another key tactical objective of the southern invasion force is the capture of the key Zaporizhzhya and South Ukraine nuclear power stations.
- The attack from the east saw Russian troops move into a larger swathe of territory to support pro-Russian rebels that have been conducting a war in eastern-Ukraine since 2014. With battle lines already drawn in eastern-Ukraine it is highly likely that Russian re-enforcements will lead to Russian success in the eastern region. It is likely that a key battle is being fought in the city of Kharkiv. It is highly likely that Russia has recently taken the south-eastern city of Mariupol as units of the southern prong of Russian forces seek to create a corridor between the Russian forces in southern and eastern Ukraine.
- It is highly likely that the intent of the Russian tactics was to use its military superiority, size and speed to split the Ukrainian forces between these three attack prongs and essentially cause confusion around how to deploy its forces.
- Reports have suggested that the main body of the Russian navy has sailed to the eastern Mediterranean to likely act as a deterrent for Western naval powers seeking access to Ukraine from the Black Sea. With Turkey effectively closing the Bosphorus Strait there is a realistic possibility that the Russian navy could become stranded and unable effectively support the coastal battle for Odessa.

- In more recent days, Russia has demonstrated a clear intent to target, control or disrupt the critical national infrastructure of Ukraine. An 04 March 2022 successful attack on Zaporizhzhya nuclear power plant has caused international outrage, standing as a sign that Russia is willing to conduct high risk operations to achieve its tactical objectives in Ukraine.
- It is highly likely that Russia has failed in its original intent to win a quick victory in war with Ukraine, however, that does not mean that its forces have been defeated. It is almost certain that Russia has a vast amount more military capability in the form of predominantly battleground fire power and air power which can be used to secure victory, however, the cost of using this capability would almost certainly present a far greater risk of worse humanitarian catastrophe for the people of Ukraine. It is almost certain that the Ukrainian military and civilians would be outgunned in the medium to long-term if the conflict cannot be resolved by other means e.g. Peace talks, sanctions, internal instability in Russia etc.

How far have Russian troops advanced?



Source: Institute for the Study of War (21:00 GMT, 7 March)

BBC

3 Impact to Security and Business Continuity in the UK

There are multiple potential risks to security and business continuity in the UK following the outbreak of war in Ukraine and subsequent global reaction to the conflict. It is unlikely that every commercial, residential or Government site would face all of the listed risks and threats, however it is important to be aware of how sites across the UK could be influenced and affected by the ongoing situation.

- It is almost certain that businesses with links to Russia will be facing considerable impact from sanctions as well as scrutiny from the UK Government and other businesses. As of 04 March 2022, the UK Government sanctioned Russian entities includes but is not limited to:

The Black Sea Bank	IS Bank	GenBank
Promsvyabank	Rossiya Bank	VTB Bank
Sberbank	Veb.RF	Bank Otkritie
Sovcombank	JSC Research	United Aircraft Corporation
Rostec	Tactical Missiles Corporation	Aeroflot
UralVagonZavod	United Shipbuilding Corporation	

The United States and European Union has also sanctioned many more Russian banks and businesses that will almost certainly have an impact in the UK. As a result of the unprecedented sanctions against Russian business entities there is a realistic possibility that security and business continuity could be affected at sites by issues such as:

- Non-payment of bills by Russian linked businesses; loss of business and trade for UK and Western businesses
- Reputational damage from association with Russian linked business entities; and
- Potential protests against Russian linked businesses.
- It is almost certain that high net-worth Russian individuals located in the UK, or with business interests in the UK will face significant sanctions in the UK. Whilst the number of sanctioned individuals has continued to grow, as of 04 March 2022 the list of sanctioned individuals included but was not limited to:

Denis Bortnikov	Petr Fradkov	Elena Georgieva
Sergie Lavrov	Vladimir Putin	Boris Rotenberg
Igor Rotenberg	Kirill Shamalov	Yuri Slyusar
Gennady Timchenko	Alisher Usmanov	Igor Shuvalov
Roman Abramovich	Igor Sechin	Oleg Deripaska
Andrey Kostin	Alexei Miller	Nikolai Tokarev
Dmitri Lebedev		

Reports have suggested that the UK Government is pushing for further sanctions of Russian individuals in the short term. The most high-profile of those that may be sanctioned is the owner of Chelsea Football Club Roman Abramovich who has opted to sell his assets very quickly, causing extensive levels of disruption to business continuity at the business/ club. The impact to business continuity and security from sanctions against Russian individuals is highly likely to include but not be limited to:

- Non-payment of rent and other financial agreements
- Lost business investment
- Termination of business funding
- Potential protests against individuals as more information about their identity and investments become publicly known.

- As one of the world's major oil exporters, the impact of sanctions on Russia has caused the already inflated oil and gas prices to rise. Whilst there has been some movement on blocking the import of gas and oil from Russia into the West, the sanctions on this area of Russian business are yet to be as rigorously applied as other areas. It is highly likely that sanctions will be far more effective if Russia is cut off from the funding from its key oil and gas exports, this is highly likely one of the key reasons that Russia is seeking to target the sea-port of Odessa in southern Ukraine to further capture oil and gas resource. It is highly likely the impact on security and business continuity from reducing imports of Russian oil and gas would be: large increase in already inflated energy costs; disruption to the supply chain e.g. fuel shortages, less frequent building deliveries; potential for power shortages etc. Russia is also one of the leading exporters of other materials such as:
 - Grain
 - Wheat
 - Iron
 - Coal
 - Nickel
 - Fertilisers.

It is almost certain that the cost of these items will also increase dramatically in the short to medium term.

- Whilst the physical conflict is located in Ukraine and being fought between Russian and Ukrainian forces, a wider view would suggest that this is a battle over Western influence in Eastern Europe, as such there is almost certainly a heightened threat of cyber warfare between Russia and the West that is associated with this conflict. The National Cyber Security Centre has issued multiple warnings over a heightened threat of Cyber attacks in the UK (<https://www.ncsc.gov.uk/news/uk-organisations-encouraged-to-take-action-around-ukraine-situation>) – it has encouraged that sites are vigilant and seek to bolster cyber defences as much as possible. It is highly likely that the security industry sits as a key strategic target for cyber attacks due to the nature of occupiers at sites for which their security is provided. The threat to security and business continuity from Cyber attacks could include:
 - Stealing of personal data
 - Stealing of intellectual property,
 - Stealing of classified information (both public and private sector),
 - Monitoring communications,
 - Remotely manipulating building services e.g. energy, heat, water etc,
 - Corrupting IT systems and more

It is worth noting that it is highly likely that cyber security attacks could come from both those considered as hostile foreign states, but also include attacks of Western origins against Russian businesses or individuals.

- There has been a demonstrable rise in anti-war protest activity since the Russian invasion of Ukraine. Groups such as the 'Stop The War' coalition and the Ukraine Solidarity Campaign amongst others have organised multiple protest events, including a protest event on 06 March 2022 that took place across over 40 major cities in the UK. It is highly likely that anti-war protests will predominantly target foreign and domestic Government entities e.g. Houses of Parliament, Downing Street, Russian Embassy, Ukrainian Embassy, United States Embassy, Ministry of Defence etc. It is highly likely that there is also a heightened threat of protest activity against businesses with links to Russia e.g. Gas and Oil companies, finance companies, security companies etc. Finally, it is highly likely that there is a heightened threat of protest to individuals with links to Russia, the public unrest around high profile Russian individuals such as Roman Abramovich at the 05 March 2022 football game between Chelsea and Burnley demonstrates the level of contentiousness that surrounds high-profile and high-net worth Russian individuals that currently remain in the UK.

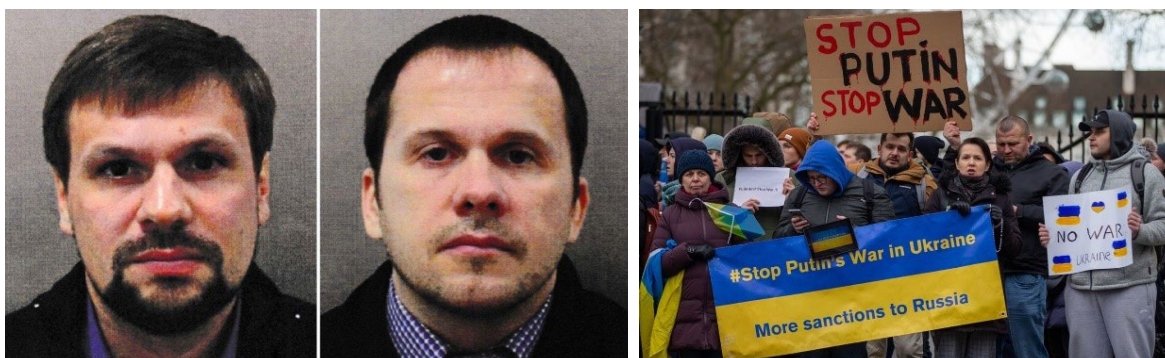
- It is highly likely that there is a current heightened threat from hostile foreign state espionage activity at sites across the UK. Espionage activity could include but is not limited to:
 - Planting of covert devices
 - Insider threat
 - Undercover operations
 - Theft of private or classified information
 - Bribing of staff members
 - Honey traps
 - Dead letter boxes and more

It is highly likely that Russia has conducted state sanctioned assassinations as part of its espionage capability, this includes the 2018 murder of former Russian agents using the chemical agent Novichok in Salisbury, and the 2006 murder of former FSB agent Alexander Litvinenko using chemical agent Polonium-210. It is highly unlikely that Russia would seek to assassinate targets in the UK, however, on 03 March 2022 police have opened an investigation into the potentially suspicious death of UK based former Ukrainian Oligarch Mikhail Watford that occurred on 28 February 2022. It is likely the threat to business continuity and security from espionage could include: theft of valuable information, reputational damage, impact on staff privacy, provision of sensitive information to hostile foreign states and more.

- It is likely that there will be some risks around the escalating refugee crisis in countries bordering Ukraine. As of 08 March 2022, approximately two million individuals have sought to claim refugee status in the area surrounding Ukraine, this number is almost certain to increase. The risk to business continuity and security from this issue are likely to revolve around protest actions against entities that are affiliated to the crisis such as foreign and domestic Government entities e.g. embassies and media entities. This could be from groups that are both pro and anti-refugees in outlook.
- Whilst there is a remote chance of the conflict escalating to nuclear war, it might be prescient to consider the impact of nuclear threat to sites. With emergency hot-lines established between the USA and Russia and the UK and Russia, it is highly likely that nuclear war would be avoided as tensions escalate, however, there is a realistic possibility that the threat of nuclear escalation could become a more common occurrence in the medium to long term. The Cold War period between 1947 and 1989 saw the frequent escalation of nuclear threat with Government, business, schools and more well drilled on how to manage and understand the threat. Whilst there is a remote chance of escalation to nuclear war, there is a realistic possibility that planning for a more turbulent nuclear threat environment could hold some merit. G4S will offer guidance if and when this becomes more necessary and proportionate.
- It is highly likely that there is an escalating threat to the mental health and wellbeing of individuals across all sites. The Covid-19 pandemic has almost certainly caused an endemic in mental health and wellbeing with large sections of the UK population becoming isolated through lockdown, losing friends and family members, losing employment, losing businesses and more. It is unlikely that all individuals have the mental resilience to process and rationalise the events in Ukraine, which mark an unprecedented return of conflict to Europe and the return of a cold-war era style of politics. As such, there is a heightened risk to security and business continuity from individuals succumbing to issues with mental health and wellbeing. Impaired mental health and wellbeing can lead to:
 - Compromised decision making,
 - Inability to concentrate
 - Lack of emotional control e.g. increased temper or frequently crying
 - Fatigue,
 - Absence from work
 - Extreme changes in weight and more.

It is almost certain that both Ukrainian and Russian individuals, or individuals with links to the conflict would be particularly impacted by mental health and wellbeing at this time. If you suspect any individual is suffering from mental health or wellbeing issues, please take the suitable action to support them by either following site specific guidelines or acting in a proportionate and considerate manner.

- There is a realistic possibility that UK based Ukrainian nationals could seek to travel to Ukraine to join the conflict, this could be mirrored by individuals from countries that border Ukraine e.g., Poland, Slovakia, Hungary, Romania, and Moldova. As such, sites should be aware that there could be some sudden employee absences and resignations.
- It is highly likely that the aviation sector has been negatively impacted by the tit-for-tat sanctions between Russia and the West. Much of the West has implemented a no-fly zone for Russian planes. In return, as of 08 March 2022 Russia has denied access to airlines from 36 countries including the UK, USA and the EU. There is a realistic possibility that this could impact security and business continuity at UK sites in the following ways:
 - Disruption of supply chain
 - Negative impact on flight availability and longer flights (to avoid Russian airspace)
 - Lack of access to Russia for individuals that need to travel
 - Potential future disruption and restrictions on airlines still operating flights to Russia e.g. Turkish Airlines, Emirates etc.
- In World War Two, a common tactic used by all sides of the conflict was to seek to influence military and civilian morale through the spread of information, or misinformation. This would commonly take the form of radio broadcasts, or airborne leaflet drops on enemy cities. The development of this type of warfare has almost certainly been escalated dramatically through the mass connectivity of the internet and in particular social media. It is almost certain that the Russia-Ukraine conflict is the first major war of the 'information age' with all parties claiming sets of objective facts around developments in the situation and seeking to disrupt and influence the will and morale of both military and civilians, domestically and in a foreign environment through a pipeline of information. It is likely that this would cause a risk to security and business continuity for the following reasons:
 - Contradictory information can cause friction in the workplace
 - Targeted misinformation can cause protest activity and encourage unrest e.g. destruction of 5g cell towers by individuals subjected to questionable information about causes of Covid-19
 - Misinformation can lead to the implementation of security decisions disproportionate to the level of threat
 - Misinformation can lead to a disruption of business continuity and reputational damage by making decisions on information that isn't based in truth



**If you would like to find out more
please contact us:**

UK: 08459 000 447 (option 1)
enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1 890 447 447
g4ssales@ie.g4s.com

