Executive Overview of Russian Aggression Against Ukraine

FEBRUARY 18, 2022 • INSIKT GROUP

***Editor's Note**:This report provides an executive-level overview of Insikt Group's unified view on the conflict between Russia and Ukraine, incorporating notable cyber offensive actions, influence operations, and geopolitical and physical threats. Research was*

conducted using the Recorded Future® Platform and other open sources.

Executive Summary

- In the event of a renewed Russian invasion of Ukraine, we believe it is likely that cyber offensive actions targeting Ukraine will primarily consist of distributed denial-of-service attacks and website defacements against Ukrainian government and media organizations, internet infrastructure, and e-services used by Ukrainian citizens such as digital banking. These cyberattacks would likely aim to cause confusion, hinder communications, weaken a Ukrainian military response, and demoralize the Ukrainian population as part of a wider hybrid warfare operation.
- Russia is almost certainly using influence assets and techniques, both covertly and overtly, to shape domestic, Ukrainian, and international audience perceptions of its military buildup along Ukraine's northern, southern, and eastern borders. Key influence narratives include that Russia, not Ukraine, is a victim of aggression; that Russia is a defensive protector; and allegations of infighting among NATO partners.
- Insikt Group has not observed Russian troop or asset withdrawal from the border of Ukraine, and we have observed additional troops and specialized equipment moving towards Ukraine, in line with US, NATO, and Ukrainian assessments. We further concur with assessments that Russia is plotting a false-flag operation as a pretext for a Russian invasion of Ukraine, with an increased presence of Russian private military companies and recent examples of likely false-flag operations being conducted. In addition, the Russian State Duma has prepared legislation to formally recognize the independence of the self-proclaimed Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR).

Cyber Offensive Actions

Recent Cyber Offensive Actions Targeting Ukraine

Recent cyberattacks targeting Ukraine have aligned with Russia's strategic objectives. The cyberattacks have consisted of distributed denial-of-service (DDoS) attacks, website

defacements, fraudulent messaging, and malware attacks, predominantly targeting Ukrainian government organizations, media organizations, e-services used by citizens, and other private sector organizations. Notable attacks are listed below:

- DDoS — On February 15, 2022, powerful DDoS attacks targeted Ukraine's armed forces, defense ministry, public radio, and the 2 largest national banks, knocking some services offline for 2 hours. The DDoS attacks left Ukrainians unable to use some vital services and resulted in confusion and worry as Russian forces continue to gather on the Ukrainian border. There has been further DDoS activity since, including targeting of the Government Services Portal of Ukraine, though there was reportedly no effect on the website.
- Fraudulent Messaging — In coordination with the DDoS attacks against Ukrainian organizations including banks on February 15, 2022, some users of Privatbank received an SMS message alerting them that the bank's ATMs were not working. However, these messages were not sent by Privatbank, and Ukrainian cyber police stated that "it was an information attack".
- Website Defacements — On January 14, 2022, threat actors likely serving Russian strategic objectives defaced nearly 70 Ukrainian government websites, including websites belonging to the Ukrainian Ministry of Foreign Affairs, Ministry of Defense, the State Emergency Service, Cabinet of Ministers, and Ministry of Education and Science. The attacks were later suspected to have been conducted by Advanced Persistent Threat (APT) UNC1151, a group linked to the Belarusian government that used malware bearing similarities to tools previously used by Russian state-sponsored APT29. The defacements vaguely warned Ukrainians to "expect the worst", spurring fears that the defacement is the beginning of additional threat activity preceding a Russian conventional military campaign in eastern Ukraine.
- Malware — Data-wiping malware disguised as ransomware, dubbed WhisperGate, targeted multiple industries in Ukraine, including government, non-profit, and information technology organizations in January 2022. Ukraine's CERT indicated the attacks were a false-flag operation, mimicking WhiteBlackCrypt ransomware, likely in an attempt to make attribution more difficult. Insikt Group analyzed the WhisperGate malware and created detection rules for our clients. We support the false-flag assessment and note that such tactics have previously been employed by Russian threat actors when targeting Ukraine, for example the use of BadRabbit ransomware.

Dark Web and Cybercriminal Activity Involving Ukraine

Insikt Group has identified a significant uptick in dark web advertisements and sales of data and network access methods related to Ukraine in the last 3 months. We identified 7 Insikt Group Threat Leads related to Ukraine in the last 12 months, with 6 of those being identified in the last 3 months. Per Insikt Group's report "Dark Covenant: Connections Between the Russian State and Criminal Actors", we believe it is highly likely that Russian intelligence services and law enforcement have a longstanding, tacit understanding with

criminal threat actors; in some cases, it is almost certain that the intelligence services maintain an established and systematic relationship with criminal threat actors, either through association or recruitment. Recently identified events of interest include:

- On February 2, 2022, we identified that “an3key”, a member of the mid-tier Raid Forums, advertised a 904 GB data leak from the internal mail server of the Ministry of Communities and Territories Development (minregion[.]gov[.]ua) of Ukraine.
- On January 28, 2022, we identified that “Kristina”, a member of the mid-tier Raid Forums, advertised a free document leak related to the Ukrainian National Police (mvs[.]gov[.]ua). Based on sample images and threat actor indications, the compromised information includes scans of passports, identification cards, and other sensitive documents related to local and federal police officers throughout Ukraine and occupied territories.
- Insikt Group reported on February 10, 2022, that Raid Forums was offline for a week. Since its reopening the week of February 14, 2022, the forum is being viewed by users with speculation, as the forum’s administrator “Omnipotent” remains unresponsive, other administrative-level accounts are acting irregular, and prominent threat actors on the forum (who have operated on it for years) are abandoning their activities. We cannot confirm if the forum has been seized by law enforcement at this time, but the aforementioned activities are leading threat actors to abandon the forum and move their activities elsewhere. This is a current and evolving situation, with Recorded Future monitoring and providing relevant updates accordingly.

Assessment on Cyber Offensive Actions in the Event of a Russian Invasion

In the event of a renewed Russian invasion of Ukraine, we believe it is likely that cyber offensive actions targeting Ukraine will primarily consist of DDoS attacks and website defacements against Ukrainian government and media organizations, internet infrastructure, and e-services used by Ukrainian citizens such as digital banking. These cyberattacks would likely aim to cause confusion, hinder communications, weaken a Ukrainian military response, and demoralize the Ukrainian population as part of a wider hybrid warfare operation.

- It is also likely that a more significant cyberattack will target Ukrainian physical infrastructure in the event of an invasion, reminiscent of previous cyberattacks against Ukraine’s power supply and destructive pseudo-ransomware attacks. We believe it’s almost certain that Russian state-sponsored APT groups have the capability to launch such significant and destructive attacks.
- We expect Russian state-sponsored threat actors, pro-Russian hacktivist and criminal groups enabled by the Russian government, and APT groups linked to the Belarusian government likely supported by the Russian government to be involved in cyber offensive actions targeting Ukraine in the event of a renewed Russian invasion of the country.

•The above assessments are based on Insikt Group's analysis of Russian hybrid warfare tactics targeting Estonia in 2007, Georgia in 2008, and Ukraine from 2014 onwards.

Assessment on Cyber Offensive Actions Against Other Countries

There are concerns that Russian state-sponsored cyberattacks could also be launched against organizations outside of Ukraine in conjunction with a Russian military invasion of Ukraine. The US and the UK have issued warnings to this extent. We believe these concerns are justified based on previous undisciplined Russian APT cyberattacks that were likely intended to target only Ukraine but spread much wider. Furthermore, it's plausible that Russia would seek to conduct cyberattacks against NATO countries to distract efforts and attention away from the invasion of Ukraine.

•An example of an undisciplined cyberattack likely intended to target Ukraine specifically is Sandworm Team's NotPetya attack in June 2017, which was estimated to have cost victims more than $10 billion in total. The attack first targeted Ukrainian companies on June 27, 2017, the eve of the Ukrainian holiday Constitution Day, but spread to other countries, including the US, UK, France, Germany, Italy, Poland, Australia, and even Russia. Security company ESET claimed that 80% of victims were located in Ukraine. There was temporary disruption of public infrastructure and business, lasting destruction of data, and significant economic damage across 65 countries.
•Another example is the BadRabbit ransomware attack in October 2017, also attributed to Russia, which similarly appeared to spread in an uncontrolled manner, affecting organizations primarily in Ukraine and Russia, but which also spread to other countries, including Turkey, Germany, Poland, Japan, South Korea, and the US.

Influence Operations

Russia's Multi-faceted and Versatile Influence Ecosystem Shaping Perceptions of Military Build-up

Russia is almost certainly using influence assets and techniques, both covertly and overtly, to shape domestic, Ukrainian, and international audience perceptions of its military buildup along Ukraine's northern, southern, and eastern borders. We believe that current Russian information operations are employing a multi-faceted and versatile approach to manipulate the narrative of this crisis, using developed human intelligence assets on the ground in Ukraine, covert elements of Russia's disinformation ecosystem (such as intelligence-directed or otherwise affiliated news sources), social media influence operations, and official, overt propaganda through the Russian state media and political apparatus.

•It is likely that the overarching goal of these efforts is to promote the rise of a pro-Russian or Russian-friendly government at the local and national levels of Ukraine's government in the long term. In the short term, these tactics are more likely aimed at

creating a destabilizing environment before a possible Russian invasion, in an attempt at achieving victory more easily and with less cost (through loss of life, economic damages, or other disruptions).

- The Ukrainian SBU issued a statement on February 14, 2022, warning that the "domestic information space is under unprecedented influence", stating that "Ukraine is facing attempts to systemically sow panic, spread fake information and distort the real state of affairs" and that "all this combined is nothing more than another massive wave of hybrid warfare".
- On February 9, 2022, the SBU announced that it had identified and shut down a social media bot farm consisting of 18,000 social media accounts allegedly spreading panic on social media as well as allegations of bomb threats on civilian and critical infrastructure.

Key Themes of Russian Influence Operations Involving Ukraine

Insikt Group has observed ongoing Russian covert and overt influence operations promoting a false primary narrative that Russia, not Ukraine, is a victim of aggression. These sources, often collectively, promote allegations and statements claiming that Ukraine, with support from its Western partners, is preparing to launch an offensive in eastern Ukraine. Often, we have found that these claims originate from proxies in eastern Ukraine (that is, pro-Russian separatists and their leadership), and then are amplified in Russian state media and government sources.

- In support of this larger theme, anti-American and anti-Ukrainian disinformation narratives in Russian sources tend to portray Russia as a defensive protector, while broadly accusing the West and Ukraine of unlawful and unjust actions. Additionally, these sources present NATO, the US, and Ukraine as the aggressors, alleging human rights violations against Russian minorities in Ukraine, demonizing Ukrainians as "fascists" and "neo-Nazis" and claiming that Ukraine does not follow the internationally recognized Minsk Agreements.
- Other widespread themes more recently include allegations of infighting among NATO partners suggesting that the West cannot achieve a consensus on how to manage Russia, as well as negative portrayals of Western media, claiming that Western news outlets spread malicious information about Russia in an attempt to force it into a war with Ukraine.

Geopolitics and Physical Threats

Russian Military Activities

Insikt Group has not observed Russian troop or asset withdrawal from the border of Ukraine, despite official Russian government and media reports of troops withdrawal. We observed new videos and photos posted on social media continuing to show troops and specialized equipment moving towards Ukraine, in line with the US, NATO, and Ukrainian assessments that Russia has in fact added 7,000 troops to the border. The

latest US assessments indicate that Russia has massed between 169,000 and 190,000 personnel in and near Ukraine, and we believe that Russia is in fact increasing the capabilities of its military on the border with Ukraine.

- US intelligence assessments state that a Russian invasion of Ukraine will likely start with air and missile attacks on key Ukrainian military infrastructure, including airfields, air defense, and early warning systems, and that the Russian military is likely to invade from multiple points on the Ukrainian border in the east and the north, in an attempt to surround Kyiv within 1-2 days. Indeed, the Estonian Foreign Intelligence Service released a report showing "targets in Ukraine compiled by Russian intelligence that, if neutralized, can interfere with the command, recovery, and supply of the Ukrainian Armed Forces and Ukraine's energy supply".
- Russia's military exercises with Belarus will conclude on February 20, 2022, as will the Beijing Winter Olympics, which we believe will be a pivotal moment to observe whether Russia does indeed decide to withdraw troops and military assets from Belarus and the border with Ukraine.

Provocations and False-Flag Operations

Insikt Group concurs with the US, UK, NATO, and other assessments that Russia is plotting false-flag operations as a pretext for a Russian invasion of Ukraine. We have observed discourse from Russian politicians suggesting there's a high probability that Ukraine will launch a military offensive in Donbas, that Russia has a right to "counterattack" if it felt the need to protect Russian citizens living in eastern Ukraine, that Russia is concerned about reports of Ukrainian violence in Donbas and is closely monitoring the situation, and Putin comparing the actions of Ukraine in Donbas to genocide. Furthermore, Russian private military companies have reportedly increased their presence in Ukraine, presenting the Russian government with a further avenue to conduct a false-flag operation. We have observed recent instances of potential false-flag attempts, including the shelling of a kindergarten in Donbas.

- On February 16, Kremlin Press Secretary Dmitry Peskov told reporters that there is a high probability that Ukraine will launch a military offensive in Donbas. On February 15, 2022, Putin once again compared the situation in Donbas to genocide, saying that Ukrainian authorities are abusing the human rights of ethnic Russians in the region. On February 14, 2022, the Russian ambassador to the EU Vladimir Chizhov stated that Russia has a right to "counterattack" if it felt the need to protect Russian citizens living in eastern Ukraine.
- Russian state-affiliated media continue to report on alleged Ukrainian military violence in Luhansk and Donetsk, for example Sputnik reported on February 17, 2022, "Ukrainian Armed Forces Fire Mortar Shells, Grenades on 4 LPR Localities".
- 2 recent potential false-flag operations include the Investigative Committee of Russia's decision to open a criminal case on "the discovery of mass graves of victims of the

Armed Forces of Ukraine in the [Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR)]" and the shelling of a kindergarten in Ukraine, with pro-Russian and pro-Ukrainian social media accounts accusing the other side of conducting the attack.

- On February 17, 2022, the Organization for Security and Co-operation in Europe's Special Monitoring Mission to Ukraine recorded 189 ceasefire violations, including 128 explosions, in the Donetsk region. There were a further 402 ceasefire violations, including 188 explosions, in the Luhansk region. This represents a significant increase from the previous day, with 24 and 129 ceasefire violations, respectively.

Russian Government Prepares Legislation to Formally Recognize LPR and DPR

On February 15, 2022, the Russian State Duma adopted a draft resolution on an appeal to the President of the Russian Federation with a request to recognize the independence of the self-proclaimed DPR and LPR. The document has now been sent to Russian President Vladimir Putin for consideration.

- On February 16, 2022, Wendy Sherman, the US Deputy Secretary of State, in an interview with Ukrainian Pravda, stated that Russia recognizing the DPR and LPR would mean the rejection of Russian obligations under the Minsk Agreements. Earlier, NATO Secretary-General Jens Stoltenberg and Ukrainian Minister of Foreign Affairs Dmytro Kuleba expressed similar views regarding the recognition of self-proclaimed republics by the Russian government.
- The heads of DPR and LPR both announced on social media that they welcomed the position of the Russian State Duma, and are grateful to the Russian Federation amid alleged increased aggression, including "daily shelling" and troop build-up from Ukraine.