PROFILE: GRU CYBER AND HYBRID THREAT OPERATIONS

GRU cyber operations have played a role in the cross-border targeting of Yulia Skripal with cyber capabilities ahead of 4 March 2018 and during Russia's military campaign against Ukraine. The future trajectory of this threat remains uncertain and international partners need to prepare for its redirection and a range of potential scenarios.

HEADLINES

The United Kingdom is:

- **Sanctioning** three Russian Military Intelligence (GRU) Units (29155, 26165, 74455) and 18 military intelligence officers, alongside Africa Initiative and three of its leaders.
- **Collaborating closely** with the **Federal Bureau of Investigation (FBI)** and condemning and calling out GRU malicious cyber activity with **NATO allies** and the **European Union (EU) its Member States**.
- Sanctioning Aleksey LUKASHEV, Ivan YERMAKOV and GRU Unit 26165 for historic cross-border targeting of email accounts belonging to Yulia Skripal with X-Agent malware in 2013.
- **Highlighting GRU Unit 26165's** role in conducting online reconnaissance on civilian shelters in Mariupol and Kharkiv on **March 15, 2022.** Russian Armed Forces conducted artillery strikes on Mariupol Theatre on **March 16, 2022**, killing non-combatants sheltering there, including children.
- **Sanctioning GRU Unit 29155** for the first time in its entirety for cyber operations targeting Ukraine.
- **Holding GRU leadership accountable** by sanctioning Dmitriy MIKHAYLOV, Aleksey MORENETS, Sergey MORGACHEV, Viktor NETYKSHO, Yevgeniy SEREBRIAKOV, Yuriy SHIKOLENKO.
- **Calling out the breadth of Russia's malicious cyber activity targeting Ukraine** prior to, during and since Russia's full-scale invasion on 24 February 2022 — including destructive cyber operations like **Viasat** (2022) and **Whispergate** (2022), as well as Unit 26165's cyber espionage campaign which targeted foreign assistance to Ukraine.
- **Sanctioning** the Russian interference agency **African Initiative**, along with three of its leaders. African Initiative uses Russian intelligence officers, and Russian funding, to deliver influence operations in Africa.

GRU's established structures conducting cyber operations

GRU Units 29155, 26165 and 74455 are three entities with known cyber capabilities. Units 26165 and 74455 represent an advanced, comprehensive cyber capability which Russia deploys for the achievement of military and foreign policy objectives. This has been a pattern for the GRU's playbook of cyber operations targeting Ukraine, European partners, NATO allies and Ukraine. Unit 29155 also carries out operations against these targets, but it is unclear if this is coordinated with the activities of the other Units.

These units have the following titles:

- Unit 29155, also known as the 161st Specialist Training Center (TsPS), which has a cyber wing known in open source as Cadet Blizzard.
- Unit 26165, also known as the 85th Main Special Service Center (GTsSS), or APT28.
- Unit 74455, also known as the Main Center for Special Technologies (GTsST), or APT44 and Sandworm.

UNIT 29155

Unit 29155's cyber wing is a recently developed part of the GRU's cyber capability. Comprised mainly of young recruits working under seasoned handlers, the Unit has a range of capabilities but is ill-disciplined and haphazard in how it conducts its operations.

Unit 29155's cyber wing is known for carrying out disruptive and destructive cyber operations, including deploying a wiper malware known as 'WhisperGate' on over 70 Ukrainian government systems in the build-up to Russia's invasion of Ukraine. Wider GRU Unit 29155 operations include the Vrbětice ammunition warehouse explosions in Czechia (2014) and attempted murder of Yulia and Sergei Skripal in Salisbury (2018).

Widespread credible evidence indicates that these incidents are linked to Unit 29155:

- ***Estonian Government Hack (2020), Estonia.*** *Estonia attributed cyber-attacks carried out against national government ministries to GRU Unit 29155, who exfiltrated data from two ministries and unsuccessfully targeted a third ministry.*
- ***Whispergate (2022), Ukraine.*** *Estonia, UK, Ukraine, US and five other international partners called out GRU Unit 29155 for cyber-attacks and digital sabotage targeting Ukraine with collateral damage to US and global infrastructure. UK attributed Whispergate to Unit 29155 in 2022.*

UNIT 26165

Unit 26165 is a highly sophisticated, well-established cyber actor which conducts both advanced intelligence gathering and hack and leak operations - against Ukraine, European partners, NATO allies and the UK - in support of Russia's foreign policy and military objectives.

Widespread credible evidence indicates that these additional incidents are linked to Unit 26165:

- ***TV5 Monde (2015), France.*** *GRU Unit 26165 conducted operations to sabotage French broadcaster TV5 Monde. France attributed this to Unit 26165 in 2025.*
- *G**erman Bundestag Hack (2015), Germany.** In April and May 2015, the German Federal Parliament (Deutscher Bundestag) was attacked and a significant amount of data was stolen. Email accounts of Chancellor Angela Merkel and other MPs were affected.*
- ***Locating D-30 Howitzers in Donbas (2014 – 2016), Ukraine.*** *Cyber security industry reporting indicates that X-Agent was deployed by Unit 26165 for geolocation purposes to locate Ukrainian military hardware in Donbas between 2014 and 2016.*
- ***United States DNC and DCCC Hack (2016), USA.*** *In 2016, the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC) were hacked, and documents were subsequently published online. The DNC and DCCC hack involved the use of X-Agent malware for data exfiltration. UK attributed this to the GRU in 2016.*
- ***French Presidential elections hack (2017), France.*** *GRU Unit 26165 hacked emails linked to Emmanuel Macron's Presidential Campaign and leaked over 21,000 emails two days before the French Presidential Election in 2017. France restated its attribution of this to Unit 26165 in 2025.*
- ***DSTL, FCDO, OPCW and Spiez Laboratory (Novichok poisonings investigation) (2018), The Netherlands, OPCW, Switzerland, United Kingdom.*** *The GRU conducted (or intended to conduct) a series of spear-phishing and computer intrusion attacks on organisations involved in the investigation into the use of a chemical weapon by GRU Unit 29155 in Salisbury, United Kingdom. US DOJ Indictments also links Unit 74455 to this incident.*
- ***German Social Democratic Party (SDP) and Czech government institutions (2022), Czechia, European Union, Germany, NATO.*** *Germany, Czechia, NATO and the EU all strongly condemn APT28 for its long-term cyber espionage campaign focused on national government institutions by*

exploiting zero-day vulnerabilities in Microsoft Outlook. The German Social Democratic Party (SDP) and Czechia's government institutions were targeted. UK attributed this to Unit 26165 in 2022.

- ***IP Camera Access to map foreign assistance to Ukraine (2022-2024), Bulgaria, Czechia, France, Germany, Greece, Italy, Moldova, The Netherlands, Poland, Romania, Slovakia, Ukraine, United States.*** *Unit 26165 conducted operations using various cyber capabilities to map and interfere with foreign assistance to Ukraine, targeting ports, transport hubs, technology companies, defence and government infrastructure and border crossings in Moldova, Ukraine and 11 NATO countries. The UK's current announcement attributes this activity to Unit 26165.*
- ***2024 Paris Olympic and Paralympic Games (2024), France.*** *In 2025, France attributed Unit 26165 for cyber- attacks on entities involved in the Olympic and Paralympic Games.*

UNIT 74455

Unit 74455 is a highly sophisticated, longstanding cyber actor, specialising in destructive cyber operations. Unit 74455 principally targets critical national infrastructure (CNI), industrial control systems (ICS), and entities of strategic interest to Russia including Ukrainian military and governmental targets.

Widespread credible evidence indicates that these incidents are linked to Unit 74455:

- ***BlackEnergy (2015), Ukraine.*** *Unit 74455 disabled part of Ukraine's electricity grid through destructive cyber operations, with 230,000 people losing power for between 1—6 hours. The UK attributed this attack to Unit 74455 in 2015.*
- ***Industroyer (2016), Ukraine.*** *Unit 74455 used malware designed to disrupt electricity grids, resulting in a fifth of Kyiv losing power for over an hour. The UK attributed this attack to Unit 74455 in 2016.*
- ***NotPetya (2017), Ukraine, United States, Global.*** *Destructive cyber attack targeting the Ukrainian financial, energy, and government sectors, with widespread collateral impact on the global economy. The UK attributed this attack to Unit 74455 in 2018.*
- ***BadRabbit (2017), Ukraine, Russia.*** *Unit 74455 deployed ransomware to encrypt computer hard drives, making IT systems inoperable, impacting Kyiv metro, Odesa airport, Russia's central bank, and Russian media outlets. UK attributed this attack to Unit 74455 in 2017.*
- ***French Presidential Elections (2017), France.*** *France attributed Unit 74455 (alongside Unit 26165) in a spear-phishing campaign targeting Emmanuel Macron's presidential campaign.*
- ***DSTL, FCDO, OPCW and Spiez Laboratory (Novichok poisonings investigation) (2017) The Netherlands, OPCW, Switzerland, United Kingdom.*** *US DOJ indictments indicate Unit 74455's role (alongside Unit 26165) in attempts to target DSTL and OPCW investigations into the Novichok poisonings in Salisbury. The UK attributed this to Unit 74455 in 2018.*
- ***Georgian Companies and Government Entities (2018) Georgia.*** *Unit 74455 carried out large-scale destructive cyber-attacks on Georgian government and non-governmental organizations, as well as national broadcasters, using wipers to deface websites. The UK attributed this to Unit 74455 in 2020.*
- ***Pyeongchang Winter Olympic and Paralympic Games (2018) Republic of Korea.*** *Also known as "Olympic Destroyer," Unit 74455 used data-deletion malware to sabotage computers and networks required to run the Olympic and Paralympic Games. They disguised themselves as DPRK and Chinese hackers when conducting operations. The UK attributed this to Unit 74455 in 2019.*
- ***Kyivstar (2023) Ukraine.*** *The Security Service of Ukraine (SBU) named Unit 74455 for conducting the Kyivstar operation in December 2023, which knocked out telecommunications channels from*

Ukraine's biggest provider serving 24 million customers, amid continuing Russian military operations across Ukraine.

SKRIPAL

Development of X-Agent malware for GRU Unit 26165 was led by Sergey MORGACHEV and involved Aleksey LUKASHEV, Ivan YERMAKOV, Sergey VASYUK and Artem MALYSHEV in various different capacities. Unit 26165 has extensive, longstanding malware development capabilities and has used X-Agent and X-Tunnel malware in cyber intrusion operations, including in support of warfighting activities. For example, according to credible open-source reporting, X-Agent has been deployed by Unit 26165 for geolocation purposes to identify Ukrainian military hardware in Donbas between 2014 and 2016, enabling Russia to conduct artillery strikes on Ukrainian positions. In the UK context, Aleksey LUKASHEV, Ivan YERMAKOV and GRU Unit 26165 conducted historic cross-border targeting of email accounts belonging to Yulia Skripal with X-Agent malware, which took place in 2013. In 2018 GRU Unit 29155 attempted to murder Yulia and Sergei Skripal with a Novichok nerve agent, a substance banned under the Chemical Weapons Convention (CWC), on UK sovereign territory.

On 10-13 April 2018, Aleksey MORENETS, Yevgeniy SEREBRIAKOV, Oleg SOTNIKOV and Aleksey MININ travelled to the Hague to conduct close access operations on the Organisation for the Prohibition of Chemical Weapons (OPCW). These individuals acted on behalf of Unit 26165 at this time. The same unit and individuals then intended to target the Spiez Swiss Chemical Laboratory, an OPCW-accredited facility. Additionally, Unit 26165 and Unit 74455 attempted cyber intrusion operations to gain access to the Foreign, Commonwealth and Development Office (FCDO) in March 2018 and UK's Defence, Science and Technology Laboratory (DSTL) in April 2018.

The UK is exposing the role of GRU Unit 26165 and GRU Unit 74455 for cyber operations throughout the lifecycle of the Skripal poisonings, from Unit 26165's initial targeting of Yulia Skripal's emails through to both Unit 26165 and Unit 74455' attempts to disrupt investigations into the Skripals' attempted murder at the hands of GRU Unit 29155. This case study underscores how GRU Units integrate cyber operations into hybrid activity with the aim of furthering the Kremlin's objectives.

UKRAINE

Since Russia's full-scale invasion of Ukraine on 24 February 2022, the GRU has used cyber operations in support of Russia's military campaign to achieve the following aims:

1 . **Information and battlefield advantage**. To inform intelligence gathering and Russia's information advantage during the military campaign against Ukraine.

2. **Dual operations to exacerbate impact.** Coordinating the impact of military operations with cyber operations e.g., targeting the electricity grid in advance of artillery strikes on cities.

3. **Psychological warfare.** Generating fear, uncertainty and attempting to break morale of Ukrainian authorities, military and civilians with cyber operations in advance of military activity on civilian centres and the battlefield e.g., creating communications blackouts and an information vacuum by targeting telecommunications providers.

The below incidents illustrate that <u>all three units have been active in Ukraine.</u>

- **On March 15,** Unit 26165 conducted reconnaissance on civilian bomb shelters in Mariupol Theatre and Kharkiv "Cold Mountain" metro. The following day, **on March 16**, Mariupol Theatre was hit with air strikes by Russian military forces whilst sheltering non-combatants, leading to large-scale civilian deaths and casualties, including a significant number of children. Ukrainian civilians had written "**дети** " (Russian: "Children") on the earth in front of the site large enough that it was visible from the air. Given the site's significance to Ukrainian cultural heritage, and the city of Mariupol, the destruction of Mariupol Theatre was also an attack on Ukrainian cultural heritage.
- As Russian forces failed to achieve their objectives, Unit 26165's espionage campaign centred on reconnaissance efforts to monitor and prevent the passage of foreign assistance into Ukraine from European partners and NATO allies. Unit 26165 accessed private IP cameras near military facilities, ports, train stations and border crossings in Ukraine, Moldova and 11 NATO countries to track the movement of foreign assistance.
- Unit 29155's Whispergate wiper attack targeted Ukrainian government agencies and intended to demoralise authorities and civilians in advance of the full-scale invasion.
- According to The Security Service of Ukraine (SBU), Unit 74455 conducted the Kyivstar operation in December 2023, which knocked out telecommunications channels from Ukraine's biggest provider serving 24 million customers, amid continuing Russian military operations across Ukraine.

INFORMATION OPERATIONS

The UK is sanctioning Victor LUKOVENKO, Artyom KUREYEV and Anna ZAMAREYEVA for their role in the interference agency African Initiative. These sanctions highlight the hybridity of Russian operations and their expansion beyond Europe.

African Initiative launched in September 2023. It maintains a growing presence online and, since its launch until 30 April 2025, its website has published over 18,000 articles in French, Arabic, Spanish, Russian and English. It also produces content on a number of social media channels. The African Initiative was established in coordination with Russia, employs Russian intelligence officers, and receives funding from Russia for influence operations in the region.

Artyom Sergeevich KUREYEV is the Editor-in-Chief of Africa Initiative; he has additionally been linked to a previous role in the Russian FSB. Other individuals involved in African Initiative include Anna Sergeevna ZAMARAYEVA, the Deputy Editor-in-Chief. ZAMARAYEVA is known to have been employed as a spokesperson for the now defunct PMC Wagner. GRU linked Victor Aleksandrovich LUKOVENKO, alias Viktor Vasilyev, was a liaison officer with African Initiative's local offices and produced a number of articles for the African Initiative website.

African Initiative develops and distributes content which undermines Ukraine's Armed Forces and has organised a press tour to Mariupol, illegally occupied by Russia, for a delegation of bloggers and journalists.

THREAT TRAJECTORIES AND FUTURE SCENARIOS

The UK is concerned that the GRU has used Ukraine as a testing ground for the development of a range of cyber capabilities, integrated into its military doctrine, since 2014 onwards.

Russia's destabilising activities are not commensurate with its role as a permanent member of the United Nations Security Council (UNSC). They also run contrary to the UN norms of responsible state behaviour in cyberspace, which Russia claims to uphold.

Geopolitical uncertainty, Russia's intent and capability to target NATO allies and operational experience in Ukraine, provide the conditions for these threats to be redirected. It is imperative that the UK and our allies continue to support Ukraine and prepare for the potential redirection of GRU cyber and hybrid threats towards European partners, NATO allies and the United Kingdom now and in the future.

Together, through our work with NATO allies and the European Union, the UK will continue to raise awareness of the potential future threat scenarios which the GRU poses to us and our allies.