GRU military unit 29155

BigBoss ⋮

GRU's military unit 29155 (161st Specialist Training Center) has been historically engaged in kinetic active measures such as subversion, assassinations or sabotage.

Soviet or Russian active measures refer to covert operations aimed at influencing third countries' politics or public opinion. They include from cyberspace activities to "wet stuff" (or "bloody stuff", or simply "stuff that stain your hands"). Among other operations, this unit has been blamed for sabotage at a Czech arms dump (2014), for a coup in Montenegro (2016) or for the Salisbury poison attacks (2018).

Although unit 29155 was previously known among analysts, it came to the public arena when it was linked to the "Havana Syndrome". This syndrome was first found among American and Canadian diplomats and intelligence staff in Cuba, in 2016, and was later identified in other destinations around the world. Affected people experienced unusual clinical symptoms, including visual problems, vertigo and cognitive difficulties, after they encountered strange sounds. Since its discovery, the origin of the Havana Syndrome has been unclear. Different research has linked the Havana Syndrome to the Russian intelligence using new generation warfare: from acoustic weapons to directed microwave energy.

In 2023, five separate United States intelligence agencies announced the results of their investigation into the origin and nature of the syndrome, concluding that it was deemed "highly unlikely" that the symptoms were caused by a sonic or microwave device or that a threat actor was involved. Instead, they concluded that this syndrome was a mix of preexisting health conditions, environmental factors and stress reactions. However, one year after the US intelligence report was published, in April 2024, a journalistic investigation concluded that the syndrome was caused by hostile operations of GRU unit 29155 by using non-lethal acoustic weapons.

Neither the Intelligence Community nor the scientific community has reached a consensus on the Havana Syndrome. In this way, the potential role of unit 29155 in the syndrome is at least unclear, although its implication in other kinetic operations seems beyond doubt.

In addition to kinetic active measures, GRU military unit 29155 has been recently unveiled performing cyberspace operations, including espionage but particularly cyberspace attack targeting critical infrastructures of NATO members, European countries, Latin America, and Central Asia. Unit 29155 is probably the threat actor known as Ember Bear, and its cyberspace activities date from 2020. In 2022, unit 29155 deployed the destructive WhisperGate malware targeting Ukrainian victims. At this point, it is important to highlight that the disruptive cyberspace operations are aligned with the unit 29155 kinetic sabotage capabilities.

One month ago, a Department of Justice indictment identified unit 29155 as a threat actor linked to the GRU but separated from units 26165 and 74455. In addition, this indictment details the use of non GRU actors, such as known cybercriminals and enablers, to conduct cyberspace operations. Even the FBI has

published a “most wanted” poster for unit 29155 members, as shown in the imagen and as it did in the past with 26165 or 74455 staff.

In front of the analysis of military units 26165 and 74455, the case of unit 29155 is particularly relevant for three key elements. The first relevant issue is **the rise of a new GRU unit engaging in cyberspace operations**. Not the discovery, as surely more GRU units have cyberspace capabilities apart from 26165 and 74455. The rise: a historical physical unit joins cyberspace arena in 2020 with a small group of young officers recruited from CTF competitions partnering with cyber criminals. Why? Probably, this fact reflects the competitiveness of Russian intelligence, not only between different services but also inside each of them. Is unit 29155 in coordination with 74455 or 26165? Are they independent units? To date, it is not known.

Secondly, it must be highlighted that **unit 29155 performs both kinetic and cyberspace active measures, reflecting the Russian views on information confrontation**. Unit 29155 is a heavily physical operating unit engaged in “wet stuff”, and now it has been discovered expanding its capabilities to the cyber arena, in cyber exploitation operations but also on cyber sabotage ones. Since September 2024, it is possible to confirm that the GRU is bluring the line between physical and cyber tactics in its approach to hybrid warfare, as Russian military doctrine states in theoretical approach.

The last relevant finding is **the use of actors outside the GRU to cooperate with the service**. The indictment published by US DoJ identifies both GRU officials and a civilian, Amin Timovich STIGAL. STIGAL is a known Russian cybercriminal, already under indictment for conspiracy to commit computer intrusion. The indictment states that STIGAL supported the activities of unit 29155 by setting up infrastructure to use in cyberspace operations. The use of staff outside the GRU provides a new example

of the complexity of the Russian intelligence ecosystem and the collaboration between entities (a topic that was discussed years ago in this blog). Unit 29155 has cooperated with third parties for its kinetic “wet stuff”: one of the best-known examples is its alleged relationships with **Wagner group**. It has been confirmed that this cooperation extends to the cyber arena.

For sure, more GRU military units and capabilities on cyberspace will come to light. The cyber arena is an interesting battlefield.