KCS Group Europe

Strictly Private & Confidential

Threat Level Protection: Amber

Hybrid Warfare

Date: 15 July 2024

The growth of hybrid warfare

Courtesy of our Russian friends and their increased activities, we have monitored and witnessed a significant increase in 2024, with the range and variety of hybrid warfare attacks taking place against NATO, Russian border countries and Ukraine supporters.

Overview

Western intelligence services have uncovered Russia's plans to conduct sabotage operations throughout NATO countries, and cause chaos and harm to all supporters of Ukraine. Western special services revealed plans for murder, monitored acts of arson and other sabotage operations in Europe against the companies and people connected with support for Ukraine. These include professionals and companies like Armin Papperger, CEO of the Rheinmetall armament production concern headquartered in Düsseldorf, Germany.

European leaders are now discussing the fight and action required in light of this rise in deniable hybrid warfare attacks.

Summary

As KCSGE has been reporting for some ten months, the number of serious incidents of sabotage and arson, or both, occurring in the UK and Europe has increased exponentially, which gives serious cause for concern.

Serious incidents and arson attacks

- A fire in an Ikea store in Vilnius, Lithuania;
- Fires in London and in the Midlands;
- Sabotage attempts in Bavaria in Germany;
- A fire attack in Prague in Czech Republic;
- A fire in a metal factory in Berlin in Germany;
- Several railway sabotage attacks and derailments in Sweden and Poland;
- Numerous attempts to destroy the signalling systems on Czech Republic railways;
- An attack on the interior minister’s car in Estonia.

Cyber attacks

A massive increase in cyberattacks on NATO companies and firms supporting Ukraine has been reported with Polish companies, in particular receiving the lion's share of such efforts.

Cyber-attacks on Lithuanian and Polish companies have, for example, increased fivefold, with malware giving hackers remote access to employees' computers. Some of the data recovered shows that the number of cyberattacks on businesses is growing. The increase in detected threats is enormous - in excess 400% - in particular for the types of threats that give criminals remote access to a computer, as opposed to disabling denial of service attacks or search and destroy malware.

Russian-Linked Cyber-campaigns have been focusing on Germany for the Football, and France for the Olympics and the Elections.

Disinformation designed to destabilise

Many reports issued in the past year have pointed to Russia intensifying its efforts to undermine France, specifically leading up to the anticipated Olympic Games, and President Emmanuel Macron, who has been one of Ukraine's most vocal European supporters.

Russian disinformation campaigns were identified as early as last year when more than 1,000 bots linked to Russia relayed photos of graffitied Stars of David in Paris. All these hybrid war efforts are part of a campaign orchestrated by GRU Units taking orders from the Kremlin to target NATO members supporting Ukraine.

The reported tags and acts of vandalism have no established direct connection to Russia; naturally, they would not, given the necessity for plausible deniability. This is, after all, the essence of hybrid warfare which causes confusion and disruption where possible, utilising propaganda, misinformation, disinformation, cyber-attacks, fake news, physical and non-physical threats or acts of violence.

Recruiting

Russia's specialist Units, managed by the SVR and the GRU, controlled by the Kremlin, are reported to be actively recruiting individuals from extremist elements from within the EU and UK to take the fight to the NATO countries by any means possible.

Conclusion

This dramatic rise in hybrid warfare tactics from Russia, as reported throughout 2024, is indicative of the evolving global conflict landscape. This new type of warfare navigates beyond the battlefield materialising as acts of indirect arson and sabotage in domestic towns, cyber-attacks targeting critical commercial and healthcare systems, and disinformation campaigns with geopolitical agendas.

Evidence directly implicating Russia is lacking which allows it to maintain deniability, which is consistent with Putin's strategic objectives, as observed by Western intelligence. The subtle and sinister nature of hybrid warfare not only challenges Western security defences but tests the resilience of its institutions, and the general public and their ability to remain aligned, patriotic and strong.