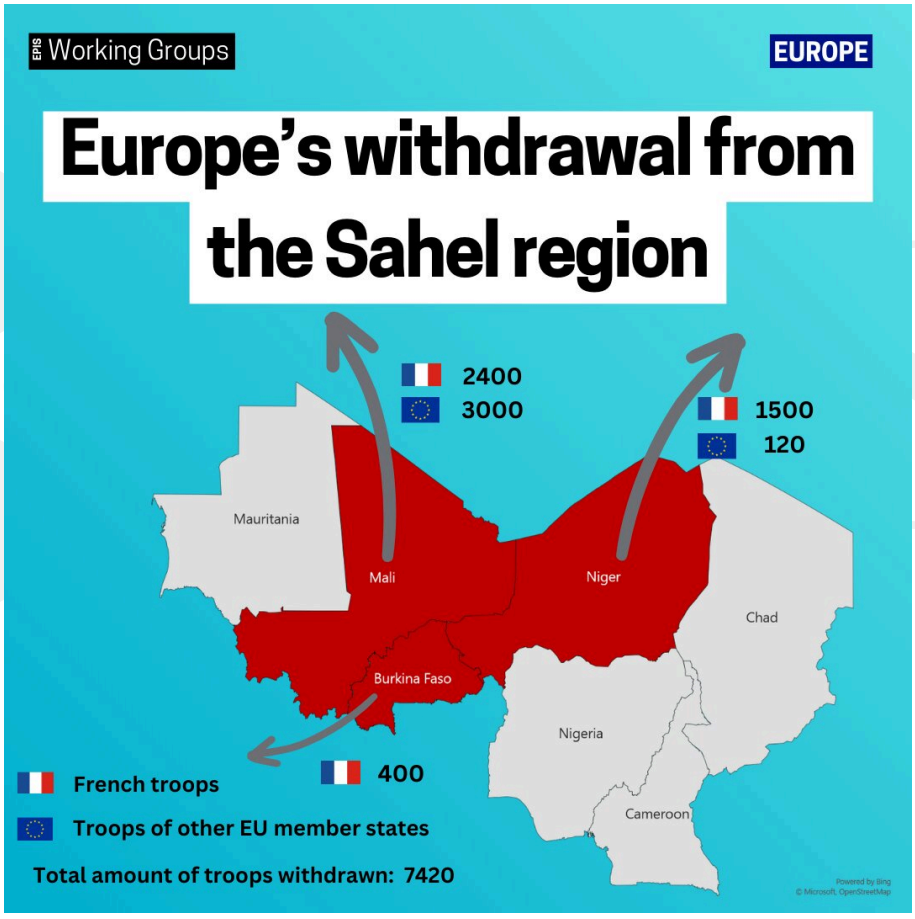
The Impact of Private Tech Companies on Cyberwar

4 MARCH 2024

Felix Heuner



Cyber warfare has developed into an essential aspect of armed conflict. Today, the control over information, the ability to quickly communicate with your troops, and the ability to disrupt the operations of your adversary are often decided in cyberspace.

The Russia-Ukraine war is the first large-scale conflict, in which the direct effects of cyberwar can be observed. Russia had and still has the reputation of having formidable cyber capabilities, which are organized through its intelligence services FSB and GRU. From the onset of the conflict, Russia has started to aggressively attack the Ukrainian government and civilian

digital infrastructure with cyber-attacks. However, these cyber-attacks by the Russian military and its controlled hacking groups have not generated any lasting strategic success for Russia. This lack of strategic impact has led some analysts to conclude that cyberspace does not have the strategic importance in warfare that was attributed to it before the start of the war.

However, I would argue that the lack of decisive strategic successes of Russian cyber attacks is not rooted in the inefficiency of cyber war itself but rather caused by an unexpected balance of forces in cyberspace between Russia and Ukraine. While Ukraine has capable cyber units, such as the 72nd Centre for Informational and Psychological Operations, a major boost to Ukraine's cyber capabilities was caused by the active involvement of private tech companies.

Defensive and Offensive Cyber-support by Private Companies

While Russia prepared its cyber offence before the war, global tech companies, such as Google or Microsoft prepared the defence of Ukrainian government data. Only days before the initial attack of Russia on Ukraine, Microsoft transferred large amounts of vital government data to its servers in the US, which protected them from the following cyber-attacks. Google's Threat Analysis Group (TAG), and Microsoft's Threat Intelligence Center (MSTIC) play a crucial part in the cyber defence effort of Ukraine. These cyber security units of global tech companies are actively engaged in the detection and countering of Russian cyber attacks on Ukrainian government infrastructure, such as the Foxblade wiper attack. Microsoft reports that it spent 239 million USD in support of Ukraine until June 2022. In addition to these direct interventions in the Russia-Ukraine war, companies such as Google and Microsoft indirectly support Ukraine by disrupting Russian information warfare operations on their platforms. Google reports that it has disrupted over 1,950 instances of such operations in 2022. Next to these defensive operations, global tech companies are also involved in offensive operations of the Ukrainian military. The star link system, which is provided to Ukraine free of charge, is the backbone of Ukraine's military communication in the field and is a central piece of any offensive military operation. Through the increased interconnectedness of its forces, Ukraine managed to reduce the average strike time of an artillery attack from 20 minutes after detection of the target to around one minute.

The New Balance of Power in Cyberspace

While states still have the monopoly of power in traditional warfare, cyberspace is at least partly operated and owned by private companies. These companies have access to vast financial and data resources, which makes them digital superpowers. Microsoft plans to invest over 20 billion USD into cybersecurity in the next five years. For reference, Germany's foreign intelligence service BND currently has an annual budget of around 1 billion USD.

In addition to these vast financial resources, private tech companies have access to large amounts of data. Microsoft's Threat Intelligence Centre can use the data of 24 trillion signals that Microsoft receives daily through all the devices and operating systems running on Windows.

Only global superpowers, such as the USA or China might be able to rival these vast resources. For any smaller country, they are impossible to match. Governments will have to find a way to deal with this reality in cyberspace. Many civil society organizations and governments want to curb the market power of global tech companies. In the future, they might also have to address the cyberwar capabilities of these companies.

EPIS