KCS Group Europe

‘Silent Partners’ – organised crime’s profitable collaboration with sanctioned regimes

October 2023

Three decades after the conclusion of Cold War 1.0, the global stage is witnessing an unsettling revival of Cold War dynamics and tensions. The fall of the Soviet Union in 1991 was supposed to mark the start of a new era. However, relations between the United States of America, Russia, China, Ukraine, Iran, North Korea, Venezuela, Cuba and Syria are increasingly tense.

The new Cold War landscape

The three key players in this geopolitical theatre are the USA, China and Russia. Ukraine, Iran, North Korea, Venezuela, Cuba and Syria are either aligned with one of the major three or engaged in proxy wars with one another.

Cold War 2.0 is a complicated and fluid engagement with no indication as to how long it could last. Unlike the first Cold War, where conflict was essentially between the USA and Russia, this one is indirect. The three superpowers are covertly supporting various movements and opposing sides in proxy physical and cyber conflict across the globe – and it is on a biblical scale. What is certain is that the USA, Russia and China are all focused on competing with one another for global influence and control.

The negative effects on global stability and security are clear, including the increased chance of military conflict destabilising entire regions. However, it is the nuclear capability of the key players, along with the fear of what their potential could bring to a major conflict, which is far more concerning.

The tension has led to US-led Western sanctions on a massive scale. These have been implemented to apply pressure on target countries in a bid to achieve foreign policy outcomes. Efforts by Russia and China to circumvent the restrictions have caused profound destabilisation, impacting not only the citizens of the target country but also the global monitoring and control of organised crime groups (OCGs). Attempts to avoid the sanctions are affecting the global environment – take, for example, the impact of Russia's illegal dilapidated, shadow oil distribution fleet worth US$1.5 billion.

It is acknowledged that, in times of war, OCGs will silently partner with sanctioned regimes to take advantage of diverted attentions and lack of adequate security measures in a temporary, mutually beneficial, backscratching exercise. Both parties use each other's abilities, skills and influence, and this permits the bad actor criminals to feather their own nests with ill-gotten gains.

Organised crime in the digital age

OCGs have been quick to take advantage of unprecedented advances in technology. In addition to profiting from ransomware attacks, this new Cold War now involves the sale of stolen critical business intelligence and intellectual property (IP) to the highest bidder. IP is usually obtained via state-sponsored organisations.

The moans and groans from hammered Western corporations and institutions have been heard for some years now. However, more recently, the US and UK intelligence services appear to be back to the drawing board as they try to combat the level of sophistication and sheer volume of cyberattacks. Although China is now believed to have the most powerful state-sponsored hacking operation in the world, it is said (even within US and UK cyber intelligence defence circles) that Russia's Turla is the most revered and admired for its level of sophistication and ingenuity. OCG scamming offices can be found in the restricted zones of sanctioned Myanmar. US-sanctioned Vietnam's thriving cybercrime market came to prominence during the pandemic.

Black market trade and corruption

The abuse of sanctions, weak governance, conflict and instability, along with high demand for illegal (sanctioned) goods, has given rise to an increase in OCG international smuggling network and black market trading activity.

Items being trafficked at present include wildlife (valued at approximately US$27 billion), weapons (destined for Ukraine but diverted), opioids including fentanyl, oil, and even people – especially young men who are fit for military work.

Corrupt law enforcement, officials and politicians have facilitated the activities of OCG operations – in particular in Mexico, Ukraine and Bali. In central America, the 2015 Panama Papers incident caused international outcry and initiated investigations into several countries involved in tax evasion and money laundering. The breathtaking scale and impact of this scandal highlighted the extreme lengths to which the international banking system was facilitated and abused in order to evade sanctions.

There are reports of the Western Balkans being a major gateway for sanctioned Russian money to cross borders covertly as well as a hot bed for OCG trade. Latin America is seeing a huge rise in illegal gold mining following the US ‘War on Drugs’ campaign. Myanmar has also seen a rise in illegal gambling, vast online scamming operations and trafficked organs of victims who refused to work in Myanmar’s OCG scamming offices. US-sanctioned Vietnam is a prolific cybercrime hotspot.

Conclusion

A new dawn over the current geopolitical landscape has cast a dark shadow on this Cold War 2.0. It is having a significant impact on the world’s security, especially given the relentless battling for power between the US, China and Russia. These times, defined by both overt and covert confrontations, have seen an exponential rise in organised crime/cybercrime groups and the unsettling collusion of underworld syndicates with state actors. As a consequence, imposed sanctions have given rise to a complicated network of illegal smuggling routes and illicit trade, often facilitated by the very same sanctions meant to deter them.

History is repeating itself. Yet again, the world stands at a crossroads. Carefully considered efforts to mitigate existing threats are required more than ever to preserve global peace and security.

Next week: Part 2 – a detailed look at how organised crime groups are evading US-led sanctions against Russia.