Cyber-attacks: what is hybrid warfare and why is it such a threat?

21 July 2021, by Ethem Ilbiz, Christian Kaunert

Credit: Novikov Aleksey via Shutterstock

Washington and Moscow are engaged in a war of words over a spate of ransomware attacks against organizations and businesses in the US and other countries. These increasingly sophisticated cyber-attacks represent a new type of warfare aimed at disorganising and even destroying a nation's economy.

This has been called "hybrid warfare". It's a mixture of conventional and unconventional methods used against a much stronger adversary that aims to achieve political objectives that would not be possible with traditional warfare.

The problem is often identifying the culprits. In hybrid warfare the state responsible for the actions will often use non-state actors, which allows it to deny responsibility. But over the past two decades, many cyber-attacks targeting western state institutions and businesses have been far more sophisticated than a couple of tech-savvy individuals operating as "lone wolves" and bear the hallmarks of actions taken with the support or approval of a hostile government.

The scale of cyber-attacks conducted at a military level signals the involvement of state actors behind the scenes to organize or encourage these attacks. Russia has emerged as one of the international actors that has developed a sophisticated cyberwarfare strategy.

So what do we know about the way Russia pursues hybrid warfare via cyber-attacks? Russia's cyberwarfare doctrine, or "gibridnaya voyna" (hybrid war), was shaped by political scientists such as Alexandr Dugin—a Russian philosopher dubbed"Putin's Rasputin" or "Putin's brain". He is also a sociology professor at Moscow State University and was targeted by US sanctions following Russia's takeover of Crimea in 2014.

Another key thinker in this area is Igor Panarin, a senior adviser to Putin with a Ph.D. in psychology. Senior military figures include Valery Gerasimov, chief of Russia's general staff and the author of the "Gerasimov Doctrine," which, according to the Carnegie Foundation, is "a whole of government concept that fuses hard and soft power across many domains and transcends boundaries between peace- and wartime."

Thinkers such as these have long advocated that Russia pursue its political objectives via information warfare rather than by military force.

Sharing for security

Cyberspace is often shown as having a physical layer (hardware), a logical layer (how and where the data is distributed and processed) and a human layer (users). Mostly it is managed by private organizations rather than state actors. So cyber-attacks are in a grey area when it comes to who should be responsible for prevention. There is also the question of who is mounting the attacks and whether they are criminal enterprises or backed by a state agency.

This confusion for the responsibility to protect plays in the hands of the Russian government. It can hurt its adversaries, no matter how large or strong,

without having to wage a military campaign.

In recent years, cyber-attacks perpetrated by Russian crime groups have targeted hospitals, energy grids and industrial facilities. The Kremlin has described allegations of its involvement as "groundless". But even though there might not be a direct connection between the government and whoever is mounting the attacks, Russia knowingly allows these groups to operate from its territory.

Russia's state agencies have offered their services in tracking down these criminal groups. But this is a familiar pledge over the years and nothing has come of it—something that is thrown into sharp relief when compared with their enthusiasm to tackle activist groups operating domestically.

Many countries have intensified their efforts to develop strategies to counter cybercrime. These initiatives include hybrid warfare defense exercises in 24 EU member states, wargaming an orchestrated cyber-attack against EU military and cybersecurity infrastructure.

The EU has also established what it calls a "hybrid fusion cell" to provide strategic analysis to EU decision-makers in its bid to deter and respond to cyber-attacks. The group of analysts within the EU Intelligence and Situation Centre (EU Intcen) is analyzing intelligence coming from the EU and various national institutions such as the GCHQ, MI5 and police intelligence agencies in the UK and providing a risk assessment for policymakers to shape their domestic policy.

Both the EU and the US have imposed sanctions on Russian individuals and entities for their harmful activities targeting cyber infrastructure. But tackling such a threat from tightly disciplined and rigidly hierarchical state-sponsored groups is not easy.

As fast as western intelligence can develop new initiatives to tackle hybrid tactics, cybercriminals seem able to develop new means of attack. So an agile governance model is needed to efficiently use public and private resources to tackle the threat from hybrid warfare threat.

The EUCTER network, led by the International Centre for Policing and Security at the University of South Wales with 13 partners across Europe and Israel is developing a range of innovative models that you can read about in detail on our website.

Hybrid warfare is a vast, complex and fast-moving threat—which requires a proportionate response if nations are going to defend themselves against.

Provided by The Conversation

APA citation: Cyber-attacks: what is hybrid warfare and why is it such a threat? (2021, July 21) retrieved 31 July 2021 from https://techxplore.com/news/2021-07-cyber-attacks-hybrid-warfare-threat.html