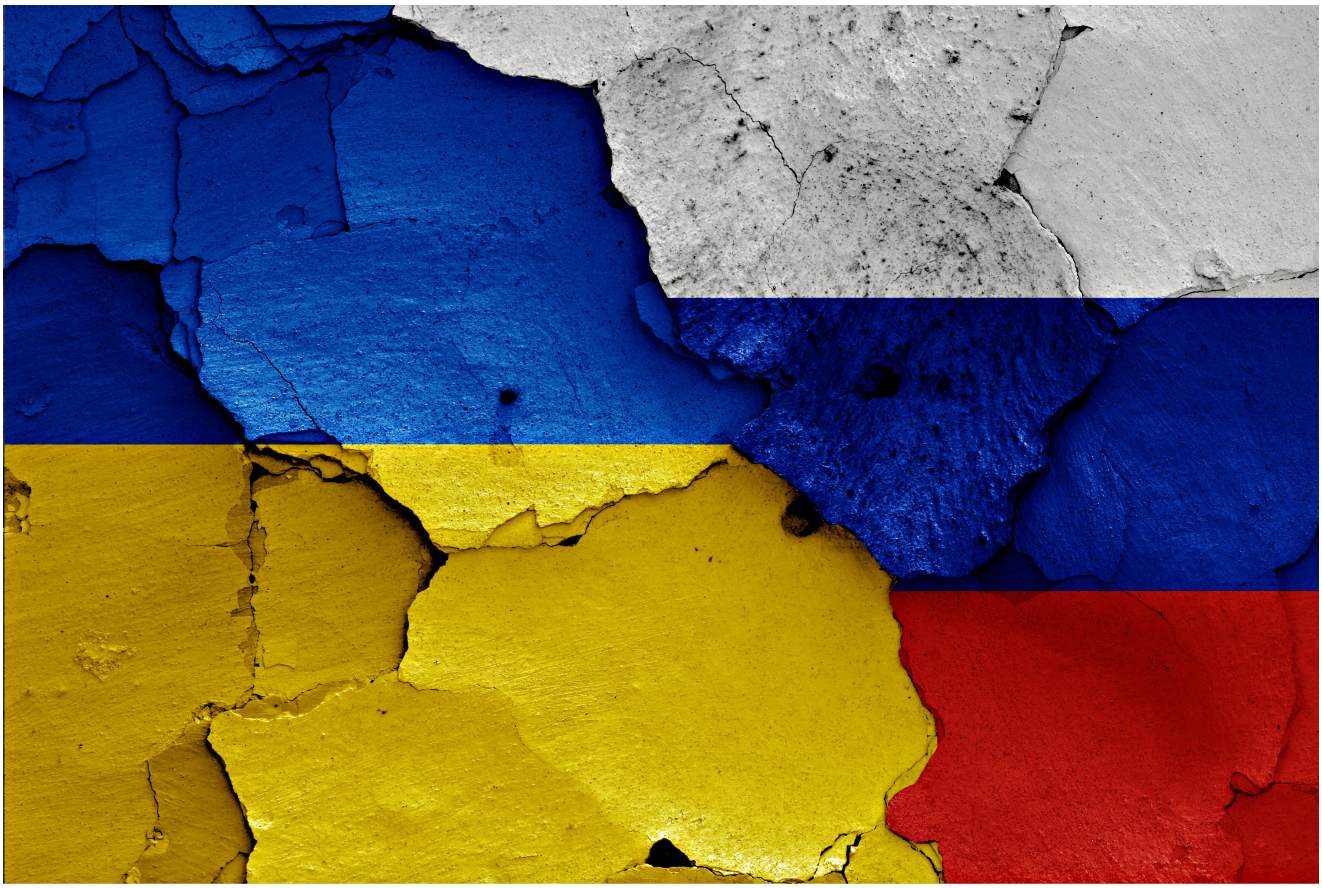
Is a coordinated cyberattack brewing in the escalating Russian-Ukrainian conflict?

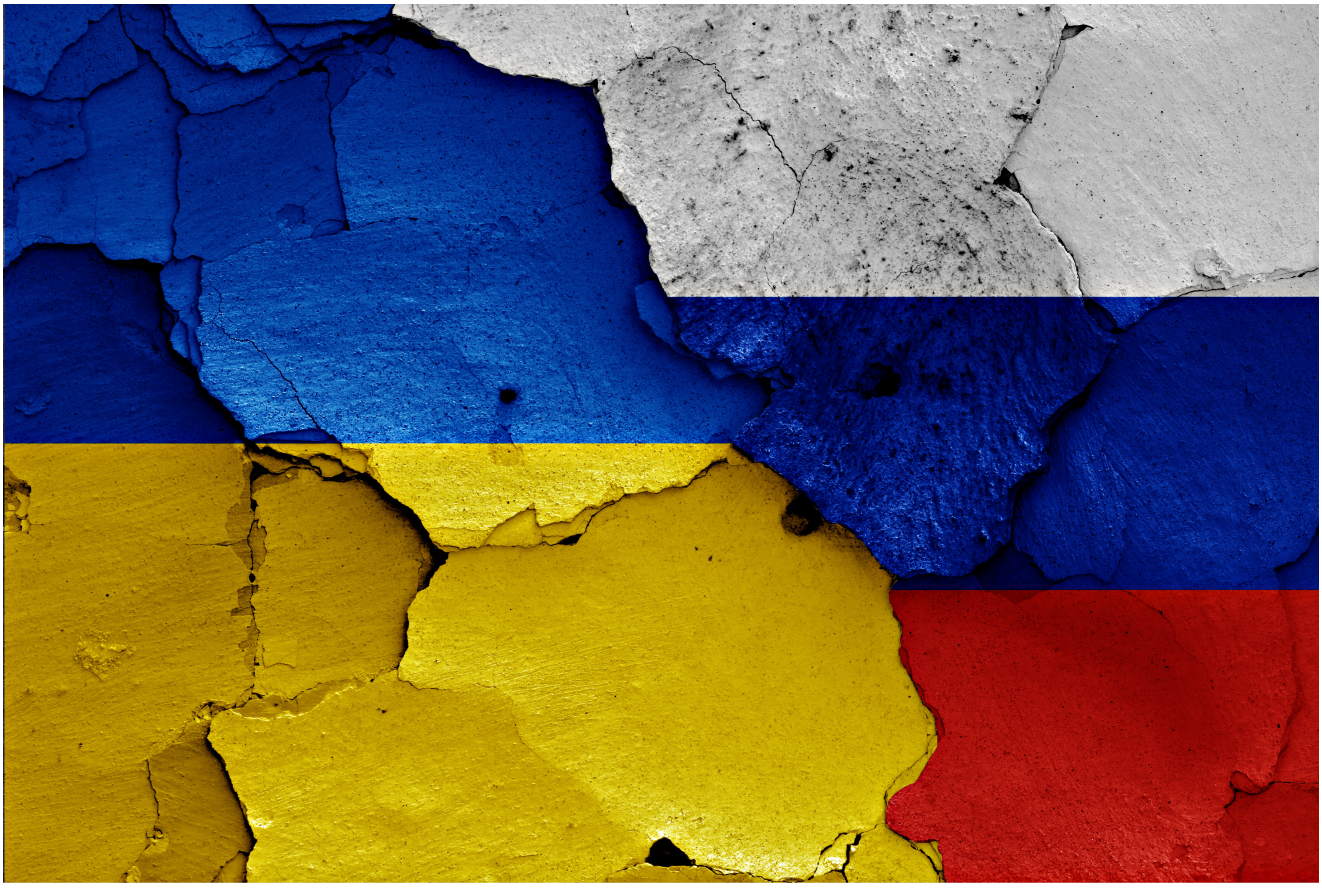
ironnet.com/blog/is-a-coordinated-cyberattack-brewing-in-the-escalating-russian-ukrainian-conflict



Back to IronNet Blog
Threat Research

Assessing the current threat based on the historical convergence of Russian military-cyber conflict

By Morgan Demboski



Nov 19, 2021

What's the Russian-Ukrainian situation?

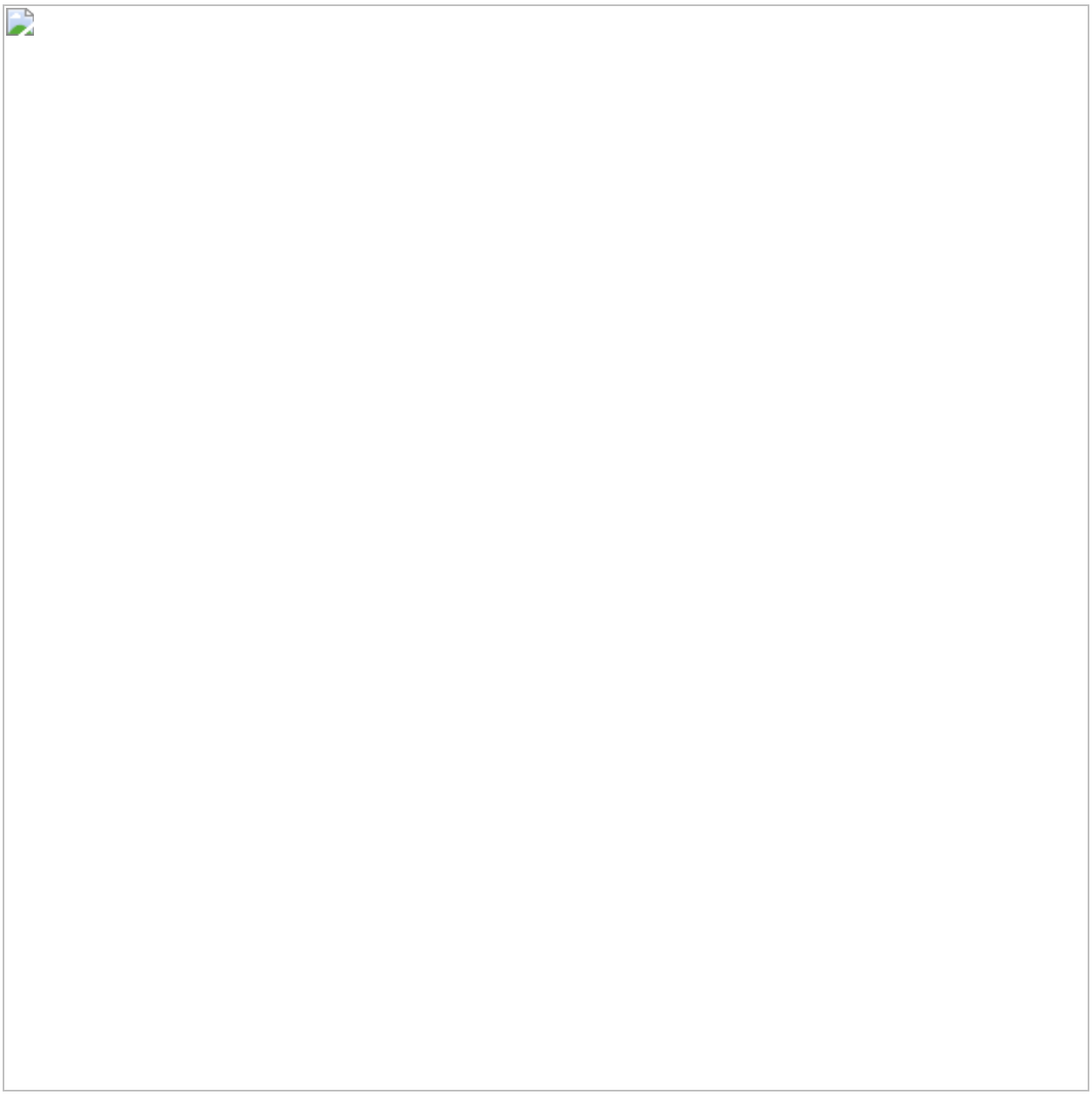
Currently, Ukraine – along with its allies in NATO – is highly concerned about the roughly 90,000 Russian troops that are massing close to the Donbas (aka Donbass) region of eastern Ukraine.

This unusual build-up of troops has prompted fears that Russia may be preparing to invade the region, thus escalating the already tense situation in Eastern Europe.

In many of Russia's modern military operations, it has employed cyberattacks to weaken its adversaries and support its strategic goals. If Russia mobilizes military action against Ukraine in the near future, there is a very high likelihood that there will be a cyberattack to go along with it.

Quick background on Russian-Ukrainian conflict

The current crisis in Ukraine first flared in 2014, when Russia invaded and annexed Crimea. Following this annexation, Russian-backed separatists in southeast Ukraine were motivated to seize the Donetsk and Luhansk regions, which are now collectively referred to as the Donbas region.



Despite multiple cease-fire agreements, sporadic fighting between the Donbas separatist rebels and Ukrainian forces continues. With renewed potential to escalate, this conflict in eastern Ukraine has led to the deaths of more than 14,000 people over the past seven years, as estimated by the International Crisis Group.

Over the past year, Russia has significantly increased its military presence along the Ukrainian border. In April 2021, roughly 100,000 to 150,000 Russian troops gathered along the border with Ukraine for about five weeks, representing the highest force mobilization since Crimea's annexation in 2014.

Mirroring the build-up in April, the most recent Russian troop movements have many countries concerned that the conflict might escalate or – in an extreme case – lead to an all-out war breaking out between the two countries.

Russian cyber-military coordination

In order to understand the probability of coordinated cyber-military activity in this potential conflict, it is important to review previous instances where Russia coordinated cyber operations and traditional military actions.

	Military Activity	Cyber Activity	Effect?
Georgia 2008	Russian invasion of South Ossetia, commencing the Russo-Georgian War	DDoS attacks	Georgia was cyber-locked, unable to communicate with the public and international partners during the conflict
Crimea 2014	Russian invasion and annexation of Crimea	DDoS attack; radio jamming; physical destruction of telecom facilities	Crimea was essentially cut-off from the rest of Ukraine, unable to communicate to outside parties
Ukraine 2021	Russian troop build-up near Ukrainian border	Spear-phishing attacks, attempts to infect government networks with malware	Ukraine had to juggle threats in both cyberspace and the real world, weakening its chance to effectively respond in the early stages of conflict.

Georgia 2008

Russia-affiliated threat actors committed a series of cyberattacks in the lead up to the Russo-Georgian War in August 2008, representing the first time cyber activity was coordinated with boots-on-the-ground operations.

The threat actors carried out two rounds of distributed-denial-of-service (DDoS) attacks against Georgian networks. Coinciding with Russian military intrusions into the separatist region of South Ossetia in Georgia (which marked the beginning of the five-day Russo-Georgian War), the second DDoS attack rendered most Georgian governmental websites inoperable by August 10th.

The attacks, which affected a total of 54 Georgian and Western websites [PDF], were designed to prevent the Georgian government from communicating with the public and international partners during the conflict – essentially cyber-locking the country.

In an effort to avoid direct responsibility for the cyber attacks, Russian intelligence agencies used a proxy cyber militia to carry out the cyber operations rather than conducting the operations themselves. Researchers from Recorded Future found that prior to the attacks, Russian government agencies created a hacking forum for “patriotic” cybercriminals, who could enable their own computers to join in on the DDoS attacks.

Crimea 2014

Russia also coordinated its military and cyber activity during its invasion of the Crimean Peninsula (located in southern Ukraine) in 2014. In February of that year, Russia stationed almost 150,000 troops along the Ukrainian border for what it referred to as a "military exercise."

It was on March 1st that the Russian Parliament unanimously approved the use of military force in Crimea, and Russia's "little green men" began to invade and seize buildings in the territory.

Around the same time, a DDoS attack – which was 32 times larger than the largest attack used during Russia's invasion of Georgia – temporarily disrupted the internet in Ukraine and degraded the peninsula's ability to communicate with the rest of the country. Additionally, Russian militias on the ground took control of numerous Crimean communications facilities and damaged the fiber optic trunk cables of a major telecommunications company (Ukrtelecom JSC).

The DDoS attack and compromise of the communications facilities, in conjunction with Russian naval vessels carrying jamming equipment to hinder radio communications, worked to effectively isolate the peninsula while Russian-armed rebels seized control of the territory.

Ukraine 2021

In April 2021, 100,000-150,000 Russian troops accumulated at the Ukrainian border. Though the Russian minister of defense stated the build-up was due to "training exercises" in response to threatening activities by NATO, the Russian troops were deployed for over five weeks — much longer than Russia's largest annual training exercises (which typically last for around a week).

Unsurprisingly, Russia also coordinated cyber activity with this military movement; however, this operation was different from the previous two instances discussed because the purpose of these cyberattacks was cyber-espionage instead of disruption or destruction.

From January to March 2021, Russian advanced persistent threat (APT) Gamaredon, which has been tied to Russia's Federal Security Service (FSB), targeted Ukrainian government officials with spearphishing attempts as tensions between the two nations rose. Like many of the other Russian spearphishing campaigns, these relatively short bursts of email spam were conducted in the hope of gaining initial access to Ukrainian organizations in order to collect intelligence.

In the midst of this in February 2021, Gamaredon also compromised a Ukrainian government file-sharing system and attempted to disseminate malicious documents to other government agencies with the goal to mass contaminate the information resources of public authorities.

At this time, it's unclear if these attempts were successful; however, coordinating these cyberattacks prior to building up troops represents a sustained effort to destabilize Ukraine and exploit weaknesses in its cyber defenses.

So what could we see in this potential conflict?

Similar to troop movements in April, this current build-up may just be another attempt by Russia to turn up the heat and abruptly lower it to keep Ukraine and NATO tense and off-balance. However, many officials, including Secretary of State Antony Blinken, are concerned that a Russian invasion of the Donbas region is imminent.

Given Russia's past coordination of military and cyber activity, I assess that if Russia does invade Donbas or mobilize its forces against Ukraine at any point, there almost certainly will be cyber operations carried out by Russian entities to support it.

Russian cyber-espionage attacks

In coordination with the build-up of troops on the Ukrainian border, Russian threat actors may be carrying out cyber-espionage attacks in an effort to gain access to Ukrainian government networks and collect information about strategies, plans, and troop positioning.

Cyber-espionage is frequently carried out as a prelude to military or diplomatic activity, and oftentimes the goal in espionage campaigns is to remain undetected in enemy networks for as long as possible. Given that it can be more difficult to detect these attacks and connect them to kinetic activity, they are often uncovered in retrospect to the offensive operation.

Disruptive/destructive Russian cyber attacks

Russia also could aim to weaken the Ukrainian government by compromising government networks or essential private companies that perform important services.

We have not yet seen Russia commit cyberattacks on critical infrastructure to directly support military operations. However, Russia has previously compromised Ukrainian electric grids on two occasions in 2015 and 2016 that led to temporary power outages for hundreds of thousands of civilians. In doing so, Russia exemplified its ability to compromise critical resources, and it is possible that Russia will try to inflict similar damage if it invades Donbas.

More advanced Russian TTPs and evasion techniques

I predict that if Russia tries to invade and annex Donbas, it will adopt relatively similar tactics to those used in Crimea in an effort to effectively cut off the region from the rest of the country. In this situation, however, the threat is even more severe.

Russia's past cyber operations in Crimea and around the world have allowed Russian APTs to gain insight into how to alter their TTPs to be more effective. Russian threat actors have been known to develop more sophisticated malware variants and alter their TTPs to better dodge defenders, meaning any future offensive cyber campaign will likely be more difficult to counter and detect.

Enlisting cybercriminals

As we saw in Georgia in 2008, it is also possible the Russian government will enlist the help of cybercriminals and hacktivists to carry out cyber attacks. Referred to as a "safe haven for cybercriminals," Russia has been reported to partner with cybercriminals living in the country for various operations. To avoid the consequences of direct attribution, Russian intelligence agencies may recruit these cybercriminals to carry out DDoS attacks, or even more sophisticated attacks, in order to weaken Ukrainian cyber infrastructure.

What is the significance of potential Russian military-cyber conflict?

Russia has become much more sophisticated in its cyber operations and has exemplified on multiple occasions its ability to cause major damage. The country's history of coordinating cyber and military activity supports the presumption that it will do the same if it engages in a future conflict with Ukraine.

The world is now entering a new conception of war-fighting, one in which "hybrid warfare" is becoming a key means by which countries carry out offensive operations. In the case of Russia, hybrid warfare has become an integral aspect of the country's geopolitical strategy as it leverages disinformation campaigns, cyber operations, and kinetic attacks to deliver an even larger blow to its adversaries.

Though influence campaigns and cyber operations can be carried out independent of other activities, it is highly unlikely that Russia will carry out military operations without coordinating it with other non-kinetic tactics. As a result, during high levels of geopolitical tension, an eye must be kept on Russia's activity in cyberspace as it tries to gain a competitive advantage over its adversaries.

To read more about historical Russian cyber attacks, see "Russian cyber attack campaigns and actors."

Back to IronNet Blog