groupsense

THE CYBER WARFARE REPORT

A look at the first eight months of cyber warfare waged against Ukraine.

groupsense

THE CYBER WARFARE REPORT

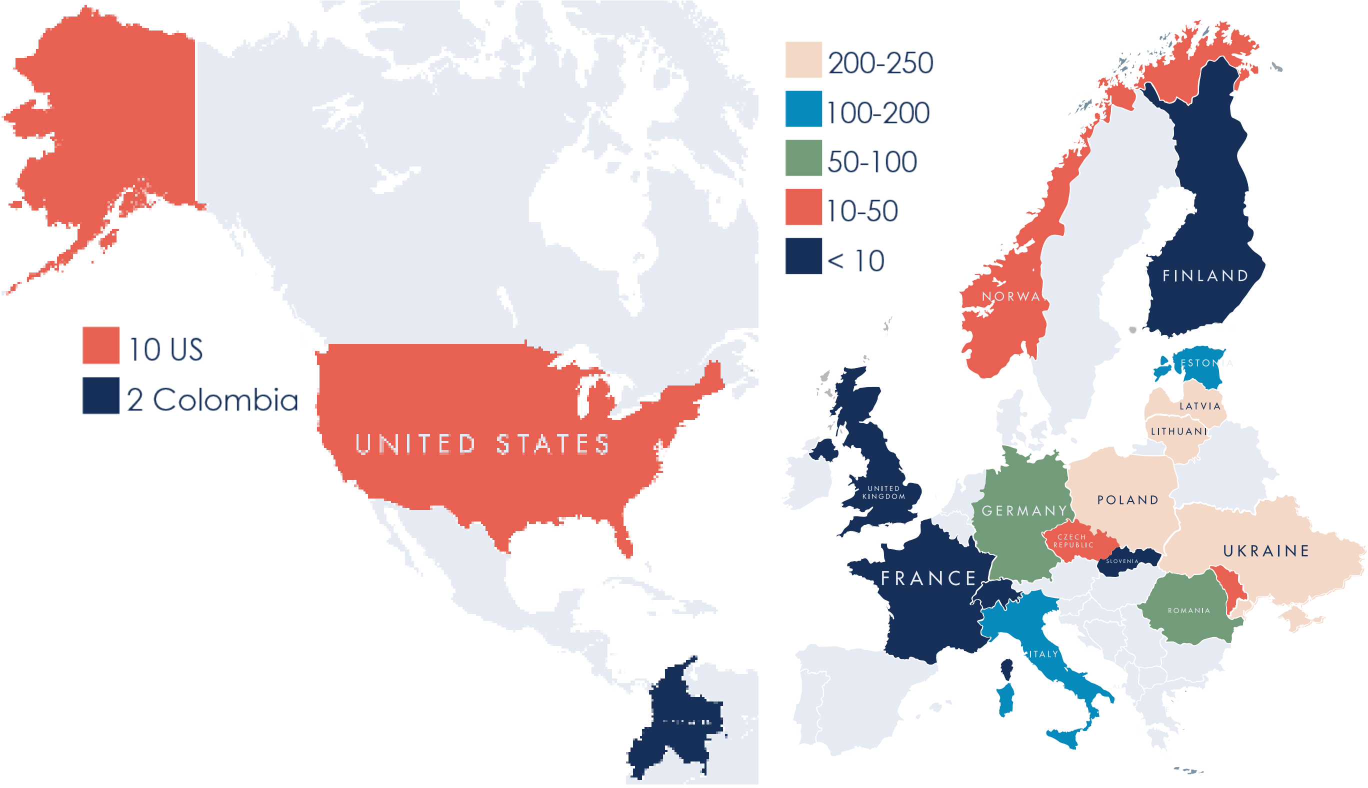
Reporting period: February-September 2022

Ever since Russia began a wholesale invasion of Ukraine in February 2022, there has been a wave of cyber attacks designed to make each side weaker. The following report is GroupSense's observations of the war and its impact on cyber operations. Please note that the following data represents cyber attacks designed specifically to advance war aims, and does not include all cyber attacks.

COUNTRIES ATTACKED MOST OFTEN

The most common countries to be attacked are, not surprisingly, former Warsaw Pact nations. These include the Baltic States, Poland, and of course, Ukraine. Germany and Romania have also seen significant cyber escalations during the war. Interestingly, Italy has also seen a large number of attacks since the outbreak of hostilities due to Italian state police claiming that they prevented a Russian cyber attack on the Eurovision song contest. Both sides in the war are getting attacked, but countries that voice or otherwise show support for Ukraine face the most attacks from pro-Russian threat actor groups.

TARGETED COUNTRIES



LITHUANIA

Aside from Ukraine, the country that suffered the biggest attack from hacktivist groups is Lithuania. Most of the active pro-Russian groups were involved in the attack. One such group, Killnet, targeted mainly governmental entities, airports, telecoms, and oil and gas companies such as Baltic Petroleum.

NORWAY

Norway was also targeted by Killnet due to Norwegian authorities rejecting Russia's application for the passage of cargo for Russian settlements on Spitsbergen (the largest and only permanently populated island in the Svalbard archipelago) through the only crossing point on the Russian-Norwegian border, Sturskug.

The waters around Svalbard are of strategic significance for Russia as the Northern Fleet must pass through the area to reach the Atlantic Ocean.

Killnet, together with Legion, attacked the online banking identification service of Norway - buypass.no, which, according to its website, is used by around 2 million people.

ITALY

Italy was among the first countries to experience an organized attack from Killnet, due to a statement from Italy that its government cyber-forces managed to block an attack attempt from Killnet on Eurovision. This, together with inner conflicts between Anonymous Italy and Killnet, made Killnet announce Italy as its "battlefield" on May 26, 2022.

Among the targets were Poste Italiane Sp A., an Italian postal service operator. Killnet attempted to attack the governmental site CSIRT - Computer Security Incident Response Team, but was unsuccessful.

ROMANIA

The Killnet attack on Romania started at the end of April and ended in the beginning of May. Killnet claimed that it successfully attacked airports, media resources, government websites, banks, payment systems, ROMPetrol, military intelligence and more. They also claimed that the media kept quiet and did not tell the public about the attacks.

LATVIA

Attacks on governmental entities such as Saeima, the website of the parliament of Latvia, were conducted.

USA

The most significant attack on the US was on Lockheed Martin, which started on August 1, 2022.

On August 8, 2022, in the channel "We are Killnet," a message was reshared from the KillMilk channel in which they claim to have attacked data.hrsa.gov, an Electronic Health Monitoring and tracking system for all American citizens. It also conducted a DDoS attack on PayUSATax.

ESTONIA

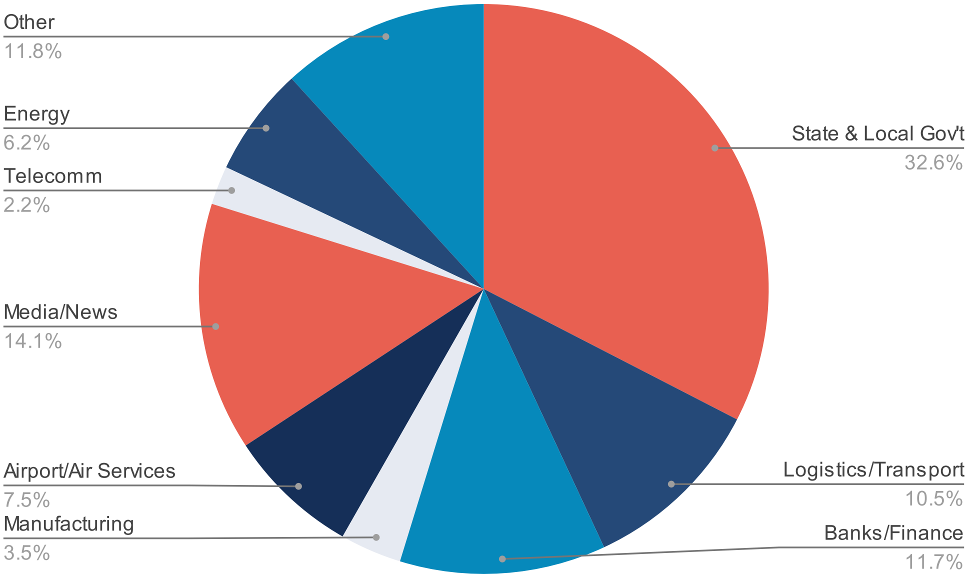
Attacks on Estonia resulted from the heavy anti-Russian sentiments from the Estonian government, including its decision to block entry to some 50,000 Russians who had been granted visas before the invasion began.

Other triggers for these attacks included the Twitter posts of Estonian Prime Minister Kaja Kallas, the removal of Soviet monuments from public spaces across Estonia and when Kallas advised to cease giving visas to Russians.

On August 17, 2022, a list of Estonian targets was shared in the hacktivist group channel "We are Killnet." Among them there are financial institutions, companies that provide "home" services such as gas and electricity companies, healthcare providers, educational platforms, Software-as-a-Service (SaaS), and governmental and commercial service companies.

TARGETED SECTORS

The highest percentage of attacks target government agencies, which is to be expected in large political conflicts. Attacks on media sites are second, with attacks on the financial sector landing third. Threat actor groups aim to disrupt the operations of these organizations to send political messages.



HACKTIVISTS LEVEL THE PLAYING FIELD

Interestingly, more hacktivist groups are openly pro-Ukraine than pro-Russia. Russia tends not to report on external cyber activities, so it is not known how effective these groups have been. However, we do know that there are more pro-Ukrainian groups than pro-Russian ones.

The hacktivist groups that are pro-Russian have doubled in size since the beginning of the war when pro-Ukrainian groups were larger than the Russian groups. There are a couple of other hacktivist groups which are quite active and have been an object of our sight for a while.

HACKTIVIST GROUPS

Almost all of the groups have been observed engaging in DDoS attacks, and many have been involved with other hacking operations and doxxing. Some carry out psychological operations (psyops) and open-source intelligence (OSINT). Among pro-Russia groups specifically, we have seen the delivery of wiper malware and support from ransomware groups.

42 | Pro-Ukraine

Notable groups include:
- IT Army of Ukraine
- AgainstTheWest/BlueHornet
- Network Battalion ‘65
- DoomSec
- GhostSec

36 | Pro-Russia

Notable groups include:
- Killnet
- Zarya
- NoName057(16)
- Beregini
- Nemezida

NOTABLE HACKING GROUPS

Throughout the eight months of the war, a few hacking groups have perpetrated a large number of attacks and become infamous in underground forums and the media. Many hackers come from Killnet, which has undergone organizational changes in recent months and may be seeing splinter groups. The most prolific attack groups include:

- **XakNet** – A pro-Russian group that is reported to be state-sponsored, but XakNet denies this linkage. XakNet emerged in February 2022 and has primarily attacked government and military targets, including the Ukrainian presidential website, the Cyber Police of Ukraine and military weapons guidance systems.
- **NoName 057(16)** – Similar to XakNet, NoName is a pro-Russian hacktivist group specializing in media intimidation. They appear to have participated in the Killnet collective's coordinated attacks on Lithuania in June 2022.
- **Beregini** – A group of Ukrainian hackers that are sympathetic to Russia. They specialize in mis- and disinformation. The group claims to consist entirely of women and to be actively hunted by Ukrainian police.
- **Nemezida** – A group of hacktivists who are known for doxxing Western military officials who have had involvement in Ukraine. Killnet channels have explicitly labeled them an ally, which suggests coordination between the two groups.
- **Zarya** – Originally an affiliate of Killnet, Zarya appears to have grown increasingly independent in its operations. While most pro-Russian hacktivists have focused on doxxing and DDoS attacks, Zarya has claimed to have penetrated Ukrainian government networks and to have stolen data.

A NEW KIND OF WAR

Cyber attacks are one of the ways in which this war is different from all wars that precede it. Cyber warfare gives independent entities and governments a way to accomplish objectives without using physical munitions, keeping motivations and attribution more muddled to outsiders. GroupSense analysts predict that many methods and attacks that occur during the conflict won't be discovered for years to come.