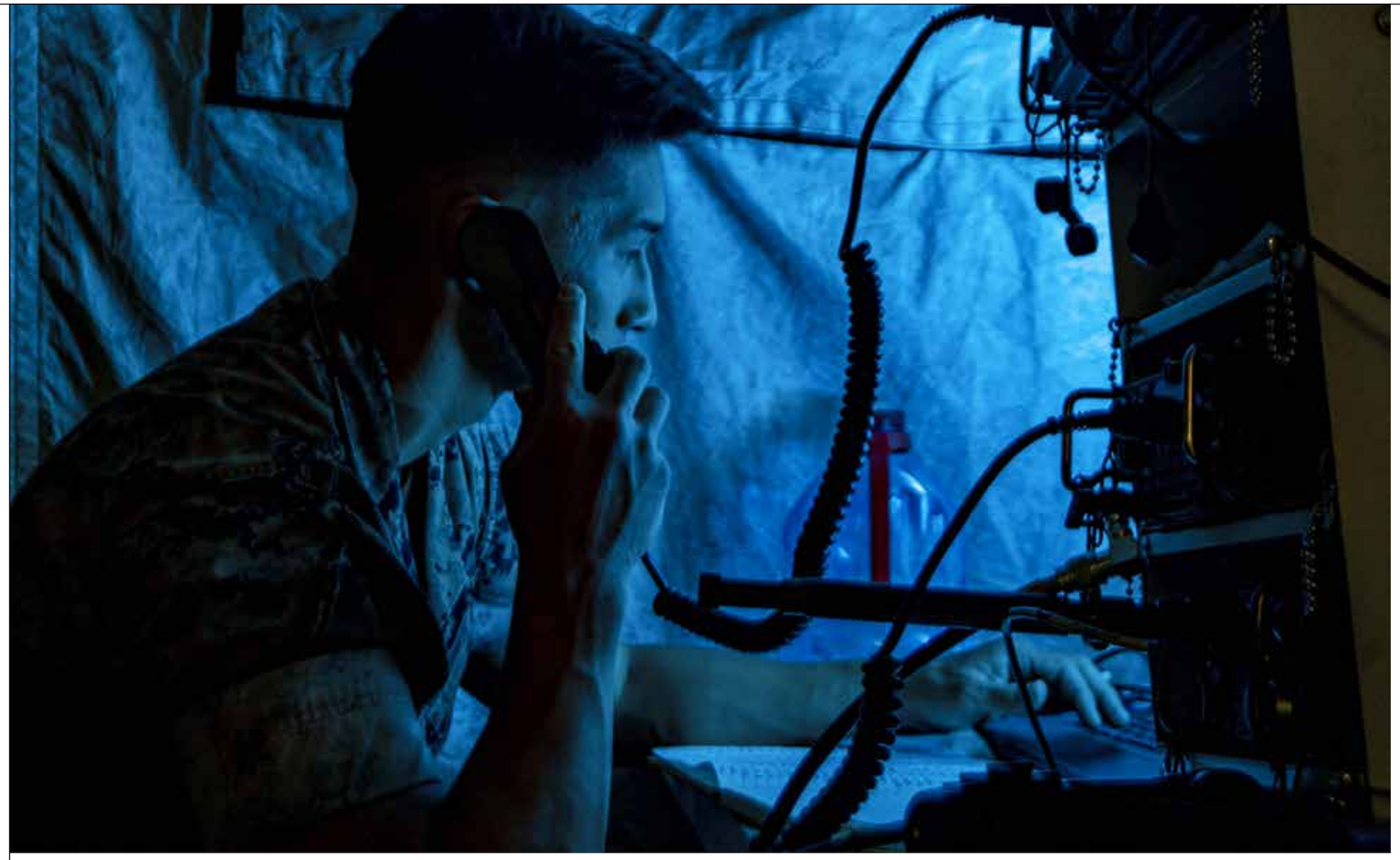

Picture credit: US Dept Defense

CROWD-SOURCED CYBER ARMY

Ziv Mador *reveals the significance of the Ukrainian cyber counter-offensive*

Over the last year, the ongoing Russia-Ukraine war has brought geopolitical unrest and associated nuclear threats. This has been one of the most intense European conflicts of recent times with the crippling economic impact of this war being felt by nearly every country across the globe. However, the conflict hasn't panned out according to the traditional trajectory of military warfare. While the mainstream media is significantly focused on the ground proceedings, the war is also being fought in the cyber field. This has very much been an active, hybrid war being fought in both cyber and physical domains.

Cyberwarfare isn't new. We have seen a wide range of state-sponsored and hacktivist attacks amidst global conflicts. However, the scale of the Ukraine war has provided a window into how war and cyberwarfare will look in the future. During the initial phases, Ukraine was mostly on its back foot in the cyber domain, as Russia came into this war with a strategically planned cyber offensive. As earlier reports from Trustwave and other security researchers show, Russia has been using a wide range of targeted attacks to either destroy or gain control over critical information and communication systems in Ukraine.

It is unsurprising that Russia gained the initial upper hand in cyberwarfare due to its existing networks of highly skilled state-backed groups such as APT28, SANDWORM, SVR, DRAGONFLY and more. These groups have been active for several years and have contributed to some of the most infamous cyberattacks in recent history.

Ukraine's counter-offensive strategy was based on several loose collective efforts. Unlike Russia, the country was less known for its state-sponsored cybercriminal activity, rather Ukraine's counter-offensive tactics included the efforts of its individual hackers and security professionals. Surprisingly, however, these isolated and scattered groups of digital talents and hackers have now grown into a fully-fledged IT army – an army which is continuously foiling Russia's cyber warfare tactics through strategically coordinated defensive and offensive tactics.

Ukraine's counter-offensive efforts started with a cry for help from Yegor Aushev, one of the leading Ukrainian entrepreneurs in the cybersecurity industry. On 24 February, when Russia began its invasion, Aushev and other security professionals across the world knew that it was going to be a hybrid war. He went onto several hacker forums, calling for the help of all security professionals and individuals with any offensive cyber skills.

This initiative was also followed up by Mykhailo Fedorov, the country's Minister of Digital Transformation, as he called for digital talents on social media to join Ukraine's IT army. What followed was a large number of volunteers and hacktivists coming together to serve Ukraine's cyber front.

Aushev, along with other defence ministry officials, has been coordinating the groups, assigning specific roles to everyone and dividing the team into specific defensive and offensive units to conduct cyber espionage campaigns against Russian forces, according to Stefan Soesanto's CSS Cyberdefense Report. This translated into the development of a well-organised group that has been critical in Ukraine's advancements and achievements so far in this war.

Currently, Ukraine's state-backed cyber operations are divided into two groups: an open collective of remote hacktivists, responsible for carrying out DDoS attacks against Russian infrastructure and an in-house team of operatives which plots and carries out more complex cyber operations.

Ukraine's counter-offensive operations have been largely based on DDoS attacks against critical infrastructure like airports, government facilities, public transport and private enterprises in Russia. Some of their biggest achievements so far include disrupting Moscow's Stock Exchange site, federal tax services and breaching the Central Bank's database. Ukrainian cyber operatives exfiltrated thousands of internal documents from the Central Bank of Russia and publicly leaked 2.6GB of sensitive data. Most attacks did not last long and had a short-term impact.

The Ukrainian IT army also targeted Sberbank, one of the largest state-owned banks in Russia. Although the attack didn't have any major impact, it significantly disrupted the bank's payment system services for 24 hours and triggered a small loss of funds.

Most notably, Ukrainian cyber operatives were able to successfully launch a continuous succession of DDoS attacks against Mir, Russia's national online payment system. This attack resulted in the suspension of major payment services in the country, including Mastercard, Amex, Visa and PayPal.

Ukraine's cyber operations are carried out by an open collective of remote hacktivists and more specialist professional operatives

The continuous success of these attacks was largely a result of Ukraine's efficient information and resource pipeline. From the outset, Ukraine wasn't just recruiting the best hackers and security professionals, rather the leaders that have been transforming digital talents into highly skilled cyber operatives through a continuous supply of resources, information and guidance. They have been launching social media campaigns to urge anyone with basic computer skills to join the IT Army of Ukraine and then equipping them with complete step-by-step tutorials, toolsets and guidelines on crafting targeted DDoS attacks.

WHILE THE FOCUS HAS BEEN ON THE GROUND, THE WAR IS ALSO BEING FOUGHT IN CYBER SPACE

Trustwave's SpiderLabs researchers came across several Ukrainian Facebook, Telegram and Twitter advertisements that included extremely detailed guidelines and toolsets for launching DDoS attacks against specific Russian targets. This incredibly extensive resource pipeline allowed even the most novice computer operative to join Ukraine's cause and contribute to its counter-offensive cyber measures.

Beyond the discussion of warfare, there is an important lesson in Ukraine's offensive cyber strategy. Its tactics have demonstrated that an effective flow of information and resources is critical for the field of cybersecurity. This is very relevant from a business or industry perspective as well. No matter what technology and solutions we implement, without an effective allocation of information and resources, even the most advanced cyber strategy will fail. Of course, crowd-sourced cyberwarfare isn't new. In the last decade there have been many instances of global conflicts, when a country's cyber offensive and defensive operations were reliant on collective cybersecurity talents. For instance, during the Rohingya conflict between Bangladesh and Myanmar, several cyber collectives from both sides targeted critical infrastructures and disrupted government networks and services.

However, Ukraine's IT army is the most prominent example of crowd-sourced cyberwarfare to date. Never has crowdsourcing been used at such a scale in an active war. What's more exemplary is how this crowd-sourced IT army of Ukraine's operations has matured during the past year.

Initially when the call was made by Aushev in February, Ukraine's cyber operations were managed through Telegram. The platform's end-to-end encryption and high media compression features made it the perfect central communication point for thousands of cyber collectives that wanted to be a part of Ukraine's cyber frontier.

In addition to tasking the IT Army of Ukraine with launching DDoS attacks against specified Russian targets, other attack types encouraged on Telegram's 'itarmyofukraine2022' channel include reporting Russian Youtube propaganda channels and signing petitions to block PayPal, GitHub and similar services in Russia. New targets and operational methods continue to be posted in the 'itarmyofukraine2022' channel.

The growth in size and mission scope created a need to support the IT army of Ukraine's members by furnishing them with scripts to run and highlighted an opportunity to develop and introduce educational materials and hacking guidelines, which could be accessed and shared via an educational portal. This led to the development of HackYourMom – a community-driven portal, lab and academy to equip the cyber army of hackers with sufficient guidelines, scripts and other resources.

The HackYourMom team introduced multiple educational articles, from OSINT basics to reverse engineering articles and important lessons on Youtube. The wide range of materials on the platform included everything someone needed to go from a novice programmer to an experienced hacker and security operative. This is how Ukraine systematically used its crowd-sourced group of volunteers and hacktivists to form a well-organised and fully operational nation-state actor.

THIS WAR HAS PROVIDED A WINDOW INTO HOW CYBERWARFARE WILL LOOK IN THE FUTURE

In order to stay competitive, a key goal for Ukraine was efficiency, and this is where building a robust educational process became a key part of the country's counter-offensive strategy. On 1 April, 2022, the IT army of Ukraine launched an automated chatbot on Telegram that responds to questions and provides an instruction guide detailing how to execute DDoS attacks. Not long after the chatbot became active, the IT army of Ukraine created a website sharing its target list and details on how to launch a DDoS attack. The aim was to significantly reduce the time it takes to develop, script and deploy a DDoS attack.

In May, an attack automation function was introduced to the Telegram chatbot, which allowed volunteers to grant bot access to their cloud resources. This action could allow a coordinated attack from all available servers, maximising the scale of a DDoS attack. To prevent proactive fixes on the attacked resources, the IT army of Ukraine closed sourced its mhddos_proxy tool to gain better operational security against abuse from hostile threat actors. The cyber collective also stopped publicly sharing their target list to make it more difficult for Russian organisations to know who the next target would be.

Overall, Ukraine's efforts and strategies to date in this hybrid war have demonstrated the power and potential of the 'crowd-sourced' methodology in the cybersecurity domain. It is indeed a reminder that effective distribution of resources and the proficient coordination of skills can create significant traction in the cyber space. Ukraine's strategies will indeed become a case study and a guideline in future cyberwarfare, but it will also inspire governments to develop a resilient cyber community ●

Ziv Mador is Vice President of Security Research at Trustwave SpiderLabs.

Hacktivists and volunteers are provided with guidelines, which are accessed and shared via an educational portal