Ukraine: the Cyber frontier

The relentless headlines, and the bombing, and the suffering, as the destruction in the Ukraine cities intensifies, eyes are naturally turned away from another battle that's taking place – the one online. Ukraine, according to reports, has been facing a constant barrage of small-scale Cyber attacks in the last week. Local Cyber security operative, Vlad Styran, is one of those tasked with fending them off. He spoke to me from somewhere deep inside Ukraine.

"I see the government services off-line. Only essential government services are protected and we're still holding up where we really need to."

"And what are you doing? I mean, personally. Are you involved in those _____ to protect Ukrainian network?"

"Yes. We're seeing a lot of attempts to _____ _____ our voices abroad, right. So, English speaking media are attacked like crazy. So, the first thing we did is secure the _____ of journalists and editors to put information abroad and make it clear what's _____ _____."

"And last week there were reports that Ukraine was attacked by something like a wiper attack. I wasn't familiar with that term, something called hermetic wiper and attempt to prevent computers from rebooting. But is that something you saw?"

"Yeah, it was the second attempt to put essential government services off-line, but this is pretty much on the background now with everything going on the ground."

Well, whilst the destruction on the ground has been intense, it hasn't managed to take Ukrainian cities off the Internet. Elon Musk's Space X has _____ additional bandwidth from its Starlink _____ system. In fact, the hostile Cyber activity that is, perhaps, getting the most _____ and potentially _____ the most _____ is against Russia right now. Hacktivist group anonymous claims that they dephased the Russian news websites with Ukrainian messages of support recently. They may even have interrupted Russian TV channel, a Ukrainian website this week also published what were allegedly the names and addresses of thousands of Russian service personnel. Secret data hacked and claimed from the Russian military website. Dyma Budorin is the Ukrainian Cyber warrior _____ _____ a team of colleagues he moved to Spain before the invasion in order to continue what he calls "offensive operations".

"We've launched few initiatives in order to attack Russian Federation critical infrastructure, propaganda media and individual users. So, first was started with the easiest one – it's DDoS attacks to DdoS, some sites in order to stress testdom."

"Ddos is basically where you brought thousands of clicks which essentially overloaded the system"

"Yes, this is one of our product and this product we _____ it just like a few months ago. We made a call to Ukrainian IT industry and they started to _____ us and immediately they started even to build this product, _____ this product and right now

it's one of the most powerful tools that are basically DdoSing the whole government infrastructure of the Russian Federation. The Kremlin websites, the propaganda websites, the banks – all of them are not working _____ right now."

"We're seeing, I mean, you know, even on Russia Today, for instance, the TV network there in Russia, there've been attacks where the network's come down and there's the Ukrainian patriotic music or a picture of a flag or something. It's not really a complicated _____ though, is it?"

"I think that this definitely _____ the attention because if there's a Ukrainian music on the website, then people do _____ _____ to it. If they see that the website shows some Ukrainian grandpa died _____ ___ the bomb in her house, they'll ignore it, probably. The thing is right now is to make it loud so that people start to pay attention: that the attack is massive, the problem is _____, 'cause right now they don't think that the problem is huge. Right now they think it's a small army operation, cities are not bombed, they don't know that this terrible things are happening. So, third one is the attack on critical infrastructure."

"How does that work?"

"You need exploits," - "these are vulnerabilities within the software?"

"Yes, so, there's a call for exploit for all of the world to help to get into the infrastructure of energy companies, of transport companies, of iron space and defense comserssions(?)."

"So, it's kind a crowdsourced hack this, I mean, are you getting support from around the world?"

"It's decrowdsource gathering of exploit, then it's professional execution of exploits and it's a professional coordination of what needs to be focused on."

"Are you getting support from _____ the world?"

"Of course."

"Russia is attacking you, too, isn't it?"

"Not really. No, we don't see it. There was some DdoS attacks like 7 days ago on a lot of websites, but there are not even _____ to what's been done by the whole hackers' community right now on the Russian Federation critical infrastructure. No comparison."

"So, you're winning?"

"In Cyber space you'll see the results very soon. Right now Ukrainian music on the websites is just spinets. The big things are coming."

"What are you hoping to _____?"

"Complete _____ _____ of the Internet in Russian Federation. This is the _____."

"Do you think you'll _____ that?"

"Absolutely."

"How long is that gonna _____?"

"We'll see. One week"