IT ARMY OF UKRAINE
https://t.me/itarmyofukraine2022
itarmyua@gmail.com

Your legal status as a participant in the cyber war with Russia.

Copyright 2022 IT Army of Ukraine

Version	Author	Release date	Changes/comments
1.1	Hactic	18.03.2022	First release

DISCLAIMER : This document is written to the best of our knowledge and understanding of the international agreed conventions and laws. If you are a legal council and you feel that the information distributed in this document is false or needs clarification, please contact @hactic.

So .. after reading a few articles about some hackers and DDoS'ers in the Ukraine, you decided to take a look in the channels and groups that were mentioned in the articles. Maybe you're just curious what all the hubbub is all about or you're actually thinking about participating in the IT Army of Ukraine. So you create an account, log in, start reading the manuals and ask a few questions in the chat groups, such as "I don't have a lot of IT knowledge but how can I help?" After you read all the pinned messages and the manuals, you feel pretty confident about the whole thing.

"Wow, participating is super easy", you may think to yourself. "I've got a computer and an internet connection, a lot of helpful people and a few scripts and programs. Let's do this, what can possibly go wrong."

A lot.

First of all, what you're doing is illegal. Many, if not all, countries have very strict laws regarding computer crimes. In fact, they are similar to actual physical violations. For example, a digital port scan on a computer is legally the same as physically checking if someone's front door is open in the middle of the night. Both cases are trialed and punished equally. Yes, you can go to jail for a simple port scan.

Second, and this applies to the current situation in Ukraine, very few people realize that by actively participating in the cyber war you immediately become what is known as a combatant of war. Let's dig into this a little bit deeper.

Combatant.

Combatant is the legal status of an individual who has the right to engage in hostilities during an armed conflict. The legal definition of "combatant" is found at article 43(2) of Additional Protocol I (AP1) to the Geneva Conventions of 1949.

https://en.wikipedia.org/wiki/Combatant

Of course, in 1949 the computers and network as we know them today did not exist yet and although the above article of the Geneva Convention of 1949 does not describe digital warfare as such, you as active participant are classed as a combatant. This is very well explained in this article:

https://link.springer.com/article/10.1007/s13347-015-0196-9

Am I participating in hostile activities?

That is really hard to judge because it depends on several variables:

- Your country of presence. Different laws may apply in different countries.
- They type of activity you're conducting. Leaving a review is judged differently than breaking into a computer system.
- Your intentions. If you are a professional IT pen tester you'll be more likely to perform security related testing in large networks where the internet is made of then a non IT civilian.

Please check the local laws in your country. Please keep in mind that the cyber laws apply to the country that you are conducting your activities from. If you are a Brazilian national and you're on a business trip to Sweden and decide to perform a few port scans whilst staying at a hotel in Stockholm, then the Swedish cyber security laws apply to you as in individual, not the Brazilian laws. Please read the article below:

https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities/

Another article worth reading:

https://restofworld.org/2022/in-ukraines-cyber-war-with-russia-who-is-a-civilian-and-what-is-a-war-crime/

Shall I participate in interviews?

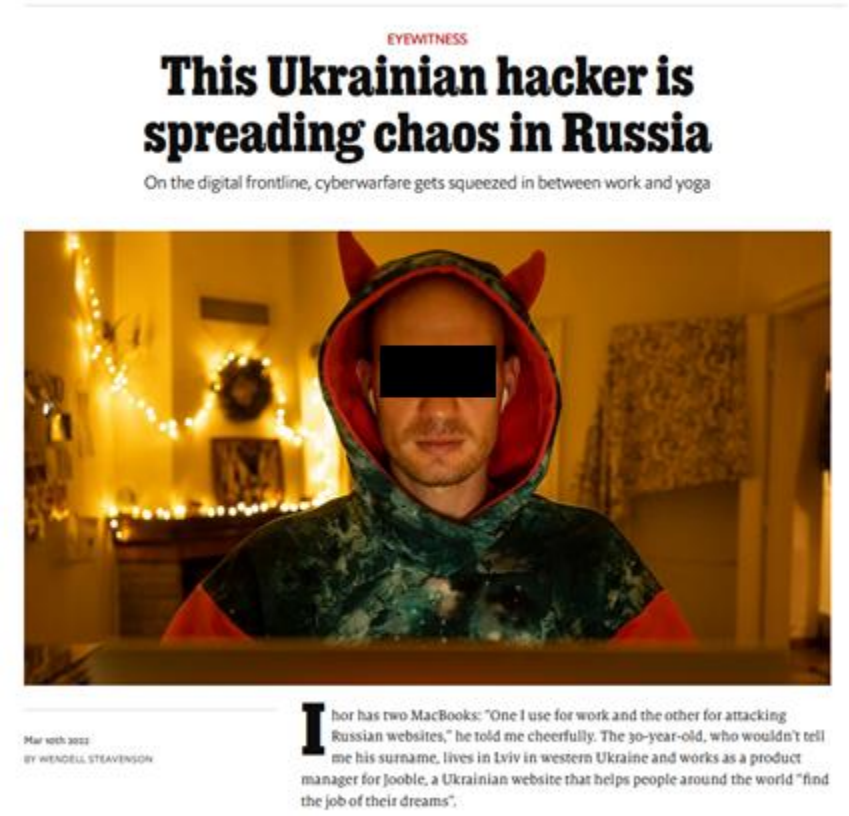
Short answer? No!

You're a potential combatant in a cyber-war and unless you are absolutely convinced that you're not doing anything illegal, you should never, ever openly confess to anyone (not even at a birthday party) that you're involved in such activities.

IT Army of Ukraine has a dedicated administrator who handles news and media. If a journalist starts talking to you, please redirect him or her to an administrator. Like the DDoS activities that you're involved in, news and media are only effective if it's handled in a controlled manner.

Copyright 2022 IT Army of Ukraine

Recently a person by the name of Ihon gave an interview in a magazine, naming his company, age, city and whole lot more. A few database searches on the internet revealed everything else he didn't want to share, which of course we won't either.



EYEWITNESS

This Ukrainian hacker is spreading chaos in Russia

On the digital frontline, cyberwarfare gets squeezed in between work and yoga

Mar 10th 2022
BY WENDELL STEAVENSON

Ihor has two MacBooks: "One I use for work and the other for attacking Russian websites," he told me cheerfully. The 30-year-old, who wouldn't tell me his surname, lives in Lviv in western Ukraine and works as a product manager for Jooble, a Ukrainian website that helps people around the world "find the job of their dreams".

Although to many people this may look 'cool' (and it probably gave him a few fans), it is incredibly stupid. The first law that a hacker, cracker, DDoSer or any other person involved in cybercrime should adhere to, is anonymity. Any person that is serious about cyber security does not reveal himself to the outside world. Ever.

Openly boasting about your achievements is just plain dangerous. You're a combatant in a cyber-war and you never know who you're going to run into in the street. It might be a pro-Russian sympathizer who recognizes you in a supermarket who happens to carry a 10 inch blade in his back pocket. No more keyboard strokes for you. Also you might (and probably will) be actively pursued and sentenced by your own government. Use your brain. You got it for a reason.

Also, by giving an interview like this, you're admitting you're performing actions in a cyber-war which makes you an active and legal target for the opponent.

Summary

Before participating in a cyber-war, please be aware of your status and the potential legal consequences your actions may cause, not just for yourself but also for your family. Also think of the personal danger that you may put yourself into by consenting to interviews or boasting about it on parties. Like corona, this war also divides people. Some are pro-Russian, others are pro-Ukrainian. Be aware of the potential risk. Use your common sense.

Links

A few more interesting articles to read about the subject:

https://link.springer.com/article/10.1007/s13347-015-0196-9

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjftd228c_2AhWE-qQKHTdrB0E4ChAWegQIBRAB&url=https%3A%2F%2Fndupress.ndu.edu%2Fportals%2F68%2Fdocuments%2Fjfq%2Fjfq-70%2Fjfq-70_70-75_phillips.pdf&usg=AOvVaw1xjdOgZ7P-8baAHdyes4hM

https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780198717492.001.0001/acprof-9780198717492