Legal Safeguards for the Volunteers of Ukraine's Cyber Militia

Svantesson, Dan Jerker B

Published in:
Verfassungsblog

DOI:
10.17176/20220323-121142-0

Legal Safeguards for the Volunteers of Ukraine's Cyber Militia

Dan Jerker B. Svantesson 2022-03-23T12:09:46

What is the legal status of foreigners who enlist in Ukraine's volunteer cyber militia? The Putin regime's brutal invasion of Ukraine means that getting clarity on this question is a matter of urgency. However, more broadly, this is a question that will remain important for future conflicts if we do not properly engage with it now.

A cyber militia, including one with foreign participants, can be a powerful tool for national defence. Countries do well to consider both their position on what they allow their citizens to do, and to consider how they can lawfully integrate a cyber militia into their own defence structures.

A willingness to help

The way in which countries around the world have reacted to the Russian invasion of Ukraine is well documented. Severe sanctions have been imposed, and many countries have already provided weapons to Ukraine. There is a widespread willingness to help Ukraine.

The question is just how far countries are willing to go. No country has pledged to deploy its military to support Ukraine. And while some countries have opened the door for their citizens to enlist in Ukraine's 'international territorial defence legion', other countries have so far advised against their citizens doing so.

As correctly pointed out by Ciaran Martin, the Russian attack has, so far, led to a traditional war rather that a war fought in Cyberspace. Nevertheless, cyberattacks have formed part of the Russian aggression, and in response, the Ukraine is recruiting for an 'IT army' – or perhaps more accurately, a cyber militia – of volunteers.

The legality of enlisting in the cyber militia

Enlisting in the Ukrainian cyber militia may be an attractive option for many people around the world who want to help Ukraine's fight for humanitarian and/or geopolitical reasons. The question that arises is whether they may lawfully do so. After all, the cybercrime laws of many countries make some activities that a cyber militia may get involved in – we can use the umbrella label 'hacking' – illegal.

To help facilitate foreigners joining the Ukrainian cyber militia, I have drafted a law reform proposal – a *Designated Cyber Militia Bill* – with the aim of creating legal safeguards for genuine members of a foreign state-run 'Designated Cyber Militia' in a narrowly defined set of circumstances.

A proposal for a *Designated Cyber Militia Bill*

The proposed Bill will no doubt need to be amended for each country that considers it. However, as it stands, the proposal may be expressed in five Articles. To make the proposal as accessible as possible, I will here go through it, Article-by-Article, and briefly discuss its position under international law. I will also say a few words about the risks associated with the proposal.

Article 1

The government of [INSERT STATE ADOPTING THIS LAW] can proclaim a foreign Cyber Militia as a *Designated Cyber Militia* under the following circumstances:

1. **A foreign state has established the Cyber Militia;**
2. **That foreign state has invited foreigners to join its Cyber Militia; and**
3. **The foreign state is under armed attack [by another state].**

It is crucial that any proposed protection for the members of a cyber militia is conditioned on state oversight and control; after all, as is implied in the term 'militia' properly applied, we are here talking about volunteers carrying out activities in an organised manner based on orders issues by a state. In my proposal, Article 1 is the first mechanism to ensure such state control and oversight.

Article 1 gives a government the power to, in a sense, recognise as legitimate a foreign cyber militia. There is no duty to do so. Thus, a state adopting my proposal has full discretion as to when they activate the anticipated legal safeguards (Articles 3-5) for their citizens who join the foreign cyber militia. Under this approach, the starting point is that persons are prevented from joining a foreign cyber militia to the extent that their activities fall foul of cybercrime laws, and only where their government has recognised as valuable the activities of the foreign cyber militia could they enjoy the relevant legal safeguards.

The alternative to this 'institutionalisation approach' would be to focus solely on the activities themselves – prosecutorial discretion could allow "good" activities to go unpunished. However, I fear that such a structure would be unworkable due to its inherent lack of predictability.

Article 2

Unless the activities constitute a violation of international law, a genuine member of a *Designated Cyber Militia* enjoys the protection of the legal safeguards outlined in Articles 3-5 in relation to activities that are:

1. **Undertaken in the capacity as a member of a *Designated Cyber Militia*;**
2. **Undertaken based on an order issued by the foreign state in command of the *Designated Cyber Militia*; and**
3. **Defensive in nature.**

Article 2 seeks to set criteria for when a member of a *Designated Cyber Militia* is entitled to the legal safeguards this Bill aims to provide. It is the most complex, and likely the most controversial, provision of the proposed Bill.

First, and most obviously, the phrase “Unless the activities constitute a violation of international law” can be attacked for its vagueness, or perhaps more specifically, for its reliance on international law that is too vague currently. This is a genuine concern. However, on balance I opted for this structure to emphasise that international law must play a role here and to acknowledge that violations of international law – where they can be established – must invalidate the legal safeguards in question.

Second, the fact that only activities undertaken based on an order issued by the foreign state in command of the *Designated Cyber Militia* adds further legal safeguards and constitutes the second mechanism to ensure adequate state control and oversight.

Finally, some observations must be made as to the limitation to activities that are “Defensive in nature”. Some cyber activities are inherently defensive. Others are inherently offensive. However, drawing a distinction between cyber activities that are defensive and those that are offensive is not always going to be easy. Against that background, states considering adopting a version of my proposed Bill may wish to include a definition of what amounts to activities that are ‘defensive in nature’.

Article 3

A person classed as a genuine member of a *Designated Cyber Militia* under Article 2 is exempt from criminal liability under the following provisions:

[INSERT LIST OF RELEVANT LEGAL PROVISIONS FROM DOMESTIC LAW]

The delineation of criminal liability for computer-related offenses varies from state to state. However, a common feature is that activities such as (a) the access to the whole or any part of a computer system without right, (b) the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, (c) data interference and (d) system interference, are illegal. Each state considering this Bill will need to map out what provisions of its criminal law needs to be listed in Article 3.

Article 4

[INSERT STATE ADOPTING THIS LAW] will refuse any extradition request received where it relates to the activities of a person classed as a genuine member of a *Designated Cyber Militia* under Article 2

This does not prevent [INSERT STATE ADOPTING THIS LAW] cooperating in the case of allegations of war crime being brought against the person before a recognised international war crimes tribunal.

The combination of Article 3 and the need for ‘dual criminality’ (that is, the activity must be a crime punishable in both the country where a suspect is being held, and in the country asking for the suspect to be extradited) may dispose of the risk of extradition in many states. Article 4 is included to specifically and expressly exclude the possibility of a person enjoying the protection of this Bill being extradited.

In addition, the second paragraph of Article 4 clarifies that the legal safeguards in question do not extend to allegations of war crime before a war crimes tribunal recognised by the state adopting the Bill.

Article 5

A person classed as a genuine member of a *Designated Cyber Militia* under Article 2 is exempt from civil liability in relation to activities carried out in that capacity.

While excluding criminal liability (Article 3) and the risk of extradition (Article 4) may be the most important legal safeguards for someone joining a foreign Designated Cyber Militia, the protection would clearly be incomplete if it did not extend to civil liability that may arise from the activities. This makes a provision such as that of Article 5 a necessary addition.

The risks and their mitigation

So, what are the risks? Do we, for example need to be concerned if other states (e.g., Russia) also adopt a structure such as this? One need only consider the cyber incidents over the past couple of years to realise that the states we may worry about already make effective use of non-state actors going far beyond what is being discussed here. My proposal emphasises state control, while those countries happily facilitate, and utilise, criminal gangs of non-state actors.

A more serious concern relates to the risk of escalation which is one of the main concerns associated with cyber operations. The risk that a cyber militia may, intentionally or unintentionally, cause harm that leads to escalation cannot be eliminated. It can, however, be minimised. Primarily, this is a task for the state in direct command of the cyber militia both in the context of recruitment, and in the context of oversight and how orders are issued. The state adopting the proposed Bill will obviously also need to take care in what foreign cyber militia it decides to recognise as a Designated Cyber Militia. Indeed, states considering adopting the structure advocated here could impose further requirements, such as vetting or training requirements, on a foreign cyber militia for it to be recognised as a Designated Cyber Militia.

Another aspect of the escalation risk is that of states being dragged into conflicts based on their citizens being authorised to enlist in a foreign cyber militia. Under the obligation of due diligence articulated by the International Court of Justice’s *Corfu Channel* judgment, “it is every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States” (*Corfu Channel* judgment, at

22). Clearly a cyber militia could undertake hostile acts contrary to the rights of other States and where a State has adopted the proposed Bill and proclaimed a foreign cyber militia as a Designated Cyber Militia, there can be no doubt that it knowingly allows its territory to be used for acts that may be contrary to the rights of other States.

To address this potential concern, I have limited my proposal to cover only activities that are defensive in nature (Article 2) since they potentially can be limited to activities that are not contrary to the rights of other States. However, as highlighted in the discussion of Article 2, States may wish to define what they accept as 'defensive' activities.

Concluding remarks

One of the many reasons to stand up for Ukraine is that in doing so one is also standing up for the rule of law against the geopolitical 'might is right' approach pursued by Putin. Thus, it is not my aim to advocate anything going beyond what is permitted under international law. For example, it is precisely out of concern for ensuring compliance with international law that the proposal is limited to defensive activities.

At the same time, we must recognise that the democratic world is in a fight for survival. And in such a fight we cannot afford to unnecessarily tie one hand behind our back. International law must be respected but as noted above, it is partly a grey zone. We need to ensure that our domestic law – while complying with international law – facilitates our aims.
