Opinion Piece
February 2023

European Repository of Cyber Incidents

With a little help from my friends? Cyber assistance and Ukraine's successful cyber defence

Martin Müller, Innsbruck University
Sebastian Harnisch, Heidelberg University

As we reach one year into military hostilities in Ukraine, the utility of sharing intelligence and the limited impact of cyber actions for the success of conventional military operations has become somewhat apparent. Examples are plenty: In the early phases of the war, CERT-UA was able to mitigate the impact of the "Caddy Wiper/Industroyer2" malware and others through cooperation with the intelligence services of other states (e.g. UK, US and Poland) and cybersecurity companies such as ESET and Microsoft. More recently, reports of "offensive cyber operations" by US authorities have appeared publicly, though details (time, location, and means) of these are not available yet.

Providing (cyber) assistance to Ukraine has raised immediate concerns in many countries about supporting governments becoming direct parties to hostilities (DPH), e.g. in Germany (here, here and here). While sharing some of these concerns about escalatory dynamics of cyber assistance to Ukraine, we beg to differ about the escalatory effects of cyber assistance. Politically, cyber operations tend to manipulate the access to or content of information, with very few operations involving kinetic effects. As such, cyber assistance may even constitute an "off-ramp" before, during, or towards the end of hostilities. Legally, we argue here that Russia's attack on Ukraine is an unlawful use of force, an armed attack in direct and clear contravention of the UN Charter.

The attack, in our view, allows for two lawful responses in cyberspace: first, the party attacked, Ukraine, may defend itself individually or collectively under Art. 51 of the UN Charter; second, for third parties, the (unprovoked) armed attack gives rise to either a status of non-belligerency, in which third parties may support the right to individual self-defence under Art. 51 (2) of the UN Charter or a status of co-belligerency, in which a third party directly participates in hostilities (here and here).

While the discussion about cyber assistance to Ukraine has been going on for a while now (see here and in more detail here), the debate, in our view, has not tackled the question squarely as to whether the evolving state practice during the first year of hostilities has already shifted the line between cyber non-belligerency and co-belligerency.

In this brief spotlight article, we address this question. We first discuss the international legal obligations of state and non-state actors assisting Ukraine in cyberspace and reflect upon their respective practices. We conclude that, even though offensive cyber operations appear to have been conducted by Ukraine and US authorities, these have not amounted to a "use of force" thus involving an assisting third party to become a party to an international armed conflict. In the policy recommendations, we will delineate the lines states should consider when supporting Ukraine's cyber defence.

Cyber operations supporting Ukraine: between non-belligerency and co-belligerency

The conditions under which states become direct parties to hostilities are crucial to the applicability of international humanitarian law (IHL), commonly known as the Geneva Conventions. The circumstances, however, that make a state a party to an international armed conflict (IAC) have changed considerably over time. A contemporary understanding, explained in more detail here (pp. 7-15), purports that participation in an ongoing armed conflict requires a "direct operational link to harm the adversary" combined with a "form of coordination" between the supporting and supported state.

Based on these two criteria, we argue that providing operational assistance or intelligence information for purely defensive operations against cyberattacks cannot make a state a party to an IAC. First, these operations regularly lack "the operational link of harming the adversary" because they either do not harm the attacker directly, i.e., they merely assist efforts of the party in hostilities, and/or they deny the attacker gains from wrongful actions. As such, these activities constitute a status of non-belligerency because the assisting state is neither using measures that rise to the level of "armed force" nor are the measures taken intentionally, autonomously, and with the direct intent of harming the adversary.

During the hostilities in Ukraine, thus far, no assisting state has reported its supportive measures to the UN Security Council as required by Art. 51(2) of the UN Charter, so, in our view, cyber assistance state practice has created a grey area of "undeclared cyber non-belligerency." Russian authorities have signalled that certain cyber operations, e.g., those resulting in the disconnection of a reconnaissance satellite, would amount to an act of war. But for now, we may tentatively conclude that the state practice of "undeclared cyber non-belligerency" during hostilities is undisputed. It follows that measures taken by various assisting states to prevent cyberattacks in Ukraine - sending their own IT-security personnel, training foreign IT-security personnel, or providing "customized" security software solutions to protect IT systems or, once hostilities started, to detect attackers in the penetrated systems and prevent them from further actions - are legitimate state practice under this "undeclared status."

And yet, assisting states may become co-belligerents in an IAC, thus crossing the threshold between assisting in individual self-defence by Ukraine and collective self-defence of Ukraine by a (declared) coalition of states under Art. 51. The latter status would still be a legitimate response to the act of aggression by Russia, Art. 21 Articles on State Responsibility (ASR), especially if declared to the UN Security Council. But co-belligerency would trigger the rules of jus in bello (IHL), thereby allowing for Russian (albeit unjustified) countermeasures against the members of the coalition of collective defenders (these countermeasures would of course still be bound by IHL, i.a., the proportionality principle). Arguably, the type of offensive cyber operations involved, e.g., stopping an attack by way of (temporarily) disabling a (Russian) server, providing actionable intelligence, or otherwise manipulating the direct operational means of the attacker may or may not clearly tackle the threshold of becoming a direct party to hostilities, also depending on the interpretation of whether the measures taken to the use of force (a list of state positions can be found here).

Today, neither a state government assisting Ukraine has become a co-belligerent by declaring its participation in collective self-defence to the UN Security Council, nor have alleged offensive operations (allegedly) taken by the US been interpreted and declared by Russian authorities to amount to "the use of armed force." However, reports on US intelligence-sharing about the exact geolocation of military assets (e.g., the destroyer Moskva) and personnel (e.g., senior Russian officers) has triggered a detailed politico-legal debate about the criteria that bring a supporting state into an ongoing international armed conflict (cf. here, here and here). In addition, on various occasions, Russian officials have threatened to consider commercial satellite systems as legitimate targets if they are used for "military purposes."

Under the legal framework of non- or co-belligerency, we suggest that at least two dimensions must be considered when the sharing of intelligence information. First, the sharing of intelligence may be unlawful because the state sharing the information may have acquired it unlawfully, for example, through the use of torture, which is prohibited by *jus cogens*, or it may be acquired in violation of the sovereignty of another state, for example through their own unjustified cyber-attacks. Second, the sharing of intelligence may support an unlawful act by the receiving state. In both cases, complicity as defined in Art. 16 ASR and related provisions may become relevant (cf. in detail pp. 1385ff).

Considering the absence of Russian legal or direct kinetic action against the US as an intelligence-sharing state and being mindful of the relative functionality of intelligence-sharing operations versus cyber-assisted conventional force operations, we conclude that (signal) intelligence sharing bears a significantly higher risk of pulling a third party into an IAC than any "offensive cyber operations." This is because the costs to integrate offensive cyber operations effectively into conventional military action or to pursue offensive cyber operations effectively that amount to the "use of force" remain (very) high, and the gains from using unlawful, offensive cyber activities, e.g., manipulating a nuclear power plant or attacking a hospital, remain low.

Non-state actors and cyber operations during hostilities in Ukraine

Non-state actors have shared intelligence and conducted cyber operations since February 24, 2022. Thus far, however, these acts have not amounted to the level of "use of force" or "armed attack." Instead, the overwhelming majority of operations have been "loud and short," focusing on DDoS, defacement, and data leakage. Focusing on cyber assistance to Ukraine, three different groups can be identified: individuals and groups that act independently from Ukrainian authorities; groups and individuals which have organized in the "IT Army of Ukraine;" and private corporate actors, which in most cases have (and had before the beginning of the war) contractual relationships with the Ukrainian or other governments in support of Ukrainian interests. These non-state actors can be distinguished from state authorities, such as CERT-UA, which is part of the "State Service of Special Communication and Information Protection." Actions by these actors can be assigned to Ukraine under international law as organs of a state according to Article 4 of the Articles of State Responsibility (ASR).

As to the first group of independent actors, various groups of hacktivists, such as Anonymous, GNG, NB65, Ghostsec, and Cyber Partisans, have declared "cyber war against Russia" or engaged in cyber operations against Russian interests.

While some of these operations bear the hallmarks of indirect participation in hostilities, i.e., lacking military harm and coordination to an extent amounting to direct participation, they have not triggered identifiable responses from Russian authorities thus far. Nor has Russia taken action to hold respective countries of residence, if known, responsible for violating the due diligence principle (here for a cyberspace-related interpretation, p. 30ff.). Furthermore, to our knowledge, Russian authorities have not attempted to cooperate with other states or international organisations (e.g., Interpol) to hold these individuals accountable for cyber-criminal offences under the Russian Penal Code. Hence, encountering numerous (irregular) cyber operations by independent non-state actors during hostilities in Ukraine, Russia's government has preferred to stay silent, legally speaking.

The second group of actors, in particular the "IT Army of Ukraine," may be called a "cyber proxy" of some sort, as its establishment, functionality, and coordination go back to the Ukrainian government, i.e., the Ministry of Digital Transformation, calling for international societal support to defend Ukraine. Participating individuals and groups (reports counted as many as 300,000 individuals at some point in time) engage in various defensive and offensive cyber operations. They may thus, legally speaking, be categorised as civilians either directly or indirectly supporting hostilities. The former category would apply to individuals that engage intentionally in cyber operations to adversely affect the military operations or capacity of Russian military forces, resulting in direct causal links between activities and harmful effects to the benefit of Ukraine. As to our knowledge, Russian authorities also have not openly addressed, neither legally nor politically, the members of these groups individually, or collectively as components of the IT Army of Ukraine. In contrast, Russian authorities have claimed that "none of the mercenaries the West is sending to Ukraine to fight for the nationalist regime in Kiev can be considered as combatants in accordance with international humanitarian law or enjoy the status of prisoners of war."

A third group of actors involves a broad variety of private corporate actors: big, mostly US-based IT-platforms, such as Microsoft and Google, as well as small, more specialised IT security companies. Reportedly, these companies have been instrumental in "evacuating" vital Ukrainian government data to cloud services in February/March 2022 and protecting them while providing network security for Ukrainian government and public networks through threat intelligence, detection, and defence activities ever since then.

Reportedly, some of these companies have worked in close coordination with the US and Ukrainian governments, even though there may not be contractual relationships for most of the services involved (here and here). Considering state responsibility in international law, an attribution to either Ukraine or the US under Article 8 of the ASR (conduct directed or controlled by a State) could be considered but must be denied at the moment, as there is no evidence that the influence by the US or Ukrainian governments was major enough to reach that high of a threshold. Moreover, with the "Cybersecurity Tech Accord" more than 100 leading IT-security companies have pledged not to support cyberattacks by governments. As well as to "cyber proxies", we have not observed any Russian activities against IT security companies at that point in time. However, as attacks on Poland's vital logistics infrastructure with the "Prestige" ransomware show, support of Ukrainian infrastructure from third countries can be endangered as well.

Conclusion

Some western cyber experts expected Russia to deploy massive cyber operations in combination with conventional warfare in Ukraine, which arguably did not occur. Instead, Russian regular and irregular cyber actors engaged in the cyber operations they were capable of, focusing on disinformation and espionage to assist conventional warfare and occupational forces. As Russian operations have ebbed and flowed, Ukraine, with substantial help from its friends, has put up a fight in the cyber space, disarming many Russian offensive operations and exploiting Russia's weak cyber defences.

Cyber assistance by various actors to Ukraine's self-defence has established a (preliminary) state practice of undeclared non-belligerency, resulting in various forms of operational collaboration below the legal threshold of direct participation in hostilities. Arguably, the assistance has been non-escalatory, as illegitimate aggression against Ukraine has been thwarted, and the aggressor has been mute as to the (il-)legality of the cyber support. But make no mistake about the generalisability of this finding: first, few state aggressors will start hostilities as unprepared after the Russian experience in Ukraine, and few will have the wherewithal to employ offensive cyber capacities Russia brought to bear in the first month of the hostilities. Second, while democratic states have rushed to cyber assistance to bolster Ukraine's defence in an uncoordinated manner, they are unlikely to do in the future. As operational cyber collaboration becomes more prevalent and efficient, Russia and other actors are more likely to address it legally, politically, or militarily. To preserve the non-escalatory effects of enhanced operational collaboration, democratic states should be transparent about legal concepts and practices, so that norms about cyber non-belligerency below the threshold of the use of force may evolve.

Cyber assistance by various non-state actors on behalf of Ukraine has been strong and arguably effective in exposing weaknesses in Russia's cyber offence and defence. So far, Russian authorities appear to treat these as nuisances, regarding its own conventional proxies, e.g., the Wagner Group, as more important. But as hostilities move to the next stage, with recruiting and ammunition shortages being exposed, operational discipline by non-state actors, especially the IT Army, should not be taken for granted. As the conventional war deepens in 2023, cyber vigilantism may become more unpredictable and less restrained, and thus a force to reckon with for Russia. As Russia has used political murder beyond its borders for various purposes, it is conceivable that cyber operations may spill back into the conventional realm.

Moreover, as Erica Lonergan has pointed out, Ukraine's recruitment of transnational cyber assistance may become a caveat for efforts to establish responsible state behavior for attacks that emanate from their territory. If some independent groups target critical civilian infrastructure in Russia, claiming publicly to respond in kind to Russian attacks in Ukraine, it is conceivable that Russia may hold the governments hosting these groups accountable. Moreover, as various states have sought to promote norms against targeting critical civilian infrastructure with offensive cyber capabilities, in contrast to cyber operations to gain access for (legitimate) intelligence collection purposes, the sustained reliance on "irregular forces" in the cyber realm by Ukraine draws the states providing cyber assistance closer to groups which may change their objectives suddenly and without regard to consequences in interstate relations. Therefore, the friends of Ukraine should establish firmer rules for their cyber solidarity as the hostilities become more persistent.

Third, IT companies have been instrumental in defending Ukraine through providing "cyber shelter" and operational support. In doing so, they acquire tacit knowledge in the cyber defence of nations and thus (very) powerful positions vis-à-vis elected governments. Such close public-private partnership in operational cyber defence may be necessary. But as it turns transnational, its legal and political implications must be seriously considered and regulated. As the crucial support by Starlink for Ukraine's conventional warfare shows, private corporate actors' behaviour can be consequential for interstate relations. It follows that their behaviour must be taken into consideration when devising the threshold between non-belligerency and co-belligerency for non-state actors.

Policy Implications

- In this brief, we find that cyber operations in support of Ukraine's right to individual self-defence under Art. 51 are legal if they lack direct operational control, if they are proportionate, and if they do not originate from unlawful acts themselves.

- Supportive cyber action to bolster individual self-defence under Art. 51 may, however, turn out to be rare, as inter-state wars are still not common. Yet, as more and more states integrate cyber operations into their security and defence policies, state practice is clearly evolving.

- Since cyber operations by non-state actors and cyber proxies have become prevalent in the Russo-Ukraine war, we stress that the due diligence principle will have to facilitate restraint by non-state actors in order to limit the escalatory effects of "crowd-based cyber defence."

- Crowd-based cyber defence poses a considerable risk of blurring the lines between permissible defensive actions and direct operational harm as non-state actors may deem the chances for legal liability as limited.

- Support for offensive cyber activities is bound to redraw the fine line to "direct operational harm" and has thus serious consequences to party status and collective self-defence.

- To further develop and sustain international law and the UN Charter in particular, states supporting Ukraine should report their status as non-belligerent supporters to the UN Security Council, outlining the legal thresholds constituting the status of non-belligerency more transparently.

- To strengthen the non-escalatory character of collaborative cyber defence measures, governments supporting Ukraine should share, confidentially, the legal concepts that underpin their assistance to the party attacked with members of the UN Security Council, including Russia.

- To alleviate escalatory pressures by actions of non-state actors, both cyber and conventional proxies, states knowingly hosting members of the IT Army of Ukraine should engage with the Ukrainian government. The goal of this engagement should be that the Ukrainian government, in potential future talks with Russian authorities, stresses the necessity to build confidence between the parties in hostilities by limiting the actions of non-state actors, i.e., both conventional and cyber proxies.

- G-7 countries should address the role of IT platforms and companies assisting state governments in cyber defence through a working group. The goal of that working group should be a catalogue of rules and procedures that govern transnational cyber assistance by corporate actors. Protecting the integrity and sovereignty of elected governments at all times while still enabling temporary assistance by capable IT companies should be the working consensus so as to safeguard existing norms and state responsibility, i.e. due diligence, in particular.