Policy Perspectives
Vol. 10/1, May 2022

CSS
ETH Zürich

Cyberneutrality: Discouraging Collateral Damage

The "cyberwar" in Ukraine is internationalized and may persist for years. In an effort to urge operational restraint among belligerents, neutral countries should insist on financial compensation for collateral damage from cyberattacks.

By Kevin Kohler

The law of neutrality is a set of rules dating back more than 100 years that aims to mitigate the risk of an inadvertent horizontal escalation of a war that draws in additional states. Given the continually growing dependence on digital infrastructure, scholars and states have been pondering how to apply neutrality to computer networks. Switzerland, as a permanently neutral state, can help to shape this discussion that has gained new relevance in the context of the Russian invasion of Ukraine. This issue of Policy Perspectives introduces the concept of cyberneutrality and makes the argument that neutral states that are affected by belligerent cyberattacks should demand financial compensation. This would provide an incentive for belligerents to exert more control over cyberattacks, which in turn would reduce their speed, impact, and potential for inadvertent horizontal escalation.

Understanding Neutrality

Neutrality refers to a status held by states for the duration of an international armed conflict and to a corresponding set of rules regulating the relationship between the belligerents and neutrals. The law of neutrality was codified in the 1907 Hague Conventions on warfare on land and at sea. After 1907, there were no new neutrality-centered treaties as wars were outlawed as an instrument of

Key Points

- Neutrality in cyberspace is not yet well defined and is significantly shaped by state practice and court cases during international armed conflicts.
- The Russian invasion of Ukraine has undermined international norms for restraint in cyberspace. The likely result is a permissive environment for offensive cyber operations.
- Historically, in airspace, the norm that collateral damage from attacks on neutral territory requires financial compensation has encouraged some operational restraint.
- Neutral states should claim financial compensation for collateral damage caused by cyberattacks. This will provide an incentive for belligerents to exercise restraint and to ensure that cyber operations are carefully targeted.

national policy. The focus shifted towards the creation of a global rules-based order in which wars of aggression would be deterred and punished through collective security. Specifically, the decisions of the UN Security Council on economic sanctions and military interventions supersede any neutral duty. However, as the Security Council is not always effective at stopping international armed conflicts, the law of neutrality has remained applicable. Moreover, its application has been extended beyond its legal source domains of land and sea to airspace. In the last two decades, many have argued that international humanitarian law, including the law of neutrality, also applies to the cyber domain.

The hacker collective anonymous declared "cyberwar" on Russia on February 24. *Michael Treu / Pixabay*

Under the Hague Conventions, neutrals have several duties. First, they must prevent the movement of belligerent troops across their territory. Second, neutrals can allow exports of war materiel by private companies. However, neutrals must have impartial export control rules, and the government itself is not allowed to export "war materiel of any kind" to belligerents in order not to militarily favor either side. Third, neutrals can allow individuals to cross their borders and join the conflict. However, they must prevent the organized recruitment of volunteers ("corps of combatants") on their territory. In return, neutrals also have rights. Most importantly, the belligerents have a duty to respect the territorial sovereignty of neutrals. This means they are not allowed to attack targets on neutral territory or conduct attacks from or through neutral territory. This includes an obligation not to interfere with trade between neutrals and belligerents.

Originally, belligerent and neutral were the only two legal statuses of states in an international armed conflict. Consequently, by default, any state that is not a belligerent can be considered a conflict neutral.[1] A formal declaration of conflict neutrality only has the effect of making the neutral status better known. However, many legal scholars have argued that today a third status of non-belligerency exists (also called qualified or benevolent neutrality). Non-belligerency is an intermediate position between belligerent and neutral in which a state understands itself as not bound to the neutral impartiality duty but still refrains from an armed attack with the aim of not becoming a co-belligerent. The reasoning for this is that the UN Charter prohibits wars of aggression and allows collective self-defense measures against them. In the case of Russia's invasion of Ukraine, there are two belligerents, about 30 non-belligerents, and more than 150 UN-recognized states that are (undeclared) conflict neutrals.

In the popular discourse, the term neutral is primarily associated with permanent neutrals. This status only applies to a handful of states, including Switzerland, that have declared that they will remain neutral in all future conflicts, either through domestic law or an international treaty. These states cannot make commitments during peacetime that would render it impossible to fulfill neutral duties in a future conflict. Most importantly, they cannot join an alliance with a collective defense clause, such as NATO, without losing their status as a permanent neutral. Beyond this minimum requirement, permanent neutrals also have a neutrality policy. This refers to self-imposed restrictions to maintain the perception and external credibility of being a permanent neutral. For example, during the Cold War, Switzerland refused to join the United Nations and to engage in economic sanctions based on its neutrality policy. While the law of neutrality applies to all conflict neutrals, permanent neutrals have a particular interest in developing its rules, as they have renounced the option of choosing non-belligerency in any individual conflict.

Cyberneutrality

Scholars and legal manuals, such as the Tallinn Manual on the International Law Applicable to Cyber Operations, have translated the rules in the Hague Conventions that refer to the information and communication technology of 1907 (telegraphs, radiotelegraphs, and telephones) to rules for modern computer networks. However, it is important to point out that there is not yet a firm consensus on many questions. Ukraine has not published any views on how international law applies to cyberspace. Russia has published its views; however, it has not discussed the applicability of international humanitarian law. Given this ambiguity, the observed practice during international armed conflicts can have a strong impact on how rules are developed.

The basic neutral duties in cyberspace are to abstain from engaging in acts of cyber hostility against belligerents and from providing them with military assistance. This in-

cludes a ban on the governmental export of "cyber weapons" and other war materiel. Second, a neutral state has a duty to prevent both the recruitment of a corps of combatants and cyberattacks originating from its territory and infrastructure. This duty is not absolute, but it means that the neutral state needs to take actions to stop such activities if it is informed of them. For example, a neutral state would face such an obligation if Russia were to provide credible evidence that individuals were directly participating in hostilities from its territory. Third, a neutral state can restrict computer networks or private exports. However, it must do so impartially, meaning that the same restrictions apply to all belligerents. It also needs to ensure that restrictions to private communication networks are applied impartially. In return, belligerents are forbidden from carrying out any hostile conduct against a neutral state's cyberinfrastructure.

The two aspects in which cyberneutrality is currently most relevant in the conflict in Ukraine are the role of volunteers and the generation of intelligence of military value through satellites (see further readings). Dozens of non-state groups are involved in the cyber conflict, most of them on the side of Ukraine. Furthermore, on February 26 the Ukrainian Ministry of Digital Transformation announced the formation of the IT Army, which directs the efforts of global volunteers and publicly distributes targets to volunteers through their Telegram channel. The provision of remote sensing imagery may be viewed as "war materiel of any kind" that falls under the neutral impartiality duty. At least five Western commercial firms provide satellite intelligence to Ukraine. Further, the New York Times writes "in Washington and Germany, intelligence officials race to merge satellite photographs with electronic intercepts of Russian military units, strip them of hints of how they were gathered, and beam them to Ukrainian military units within an hour or two."[2] This is legally non-consequential in the sense that the affected states already deliver physical war materiel to a belligerent from government stocks and do not view themselves as bound by neutral duties in this conflict.

Further Reading

Sean Cordey / Kevin Kohler, **"The Law of Neutrality in Cyberspace,"** *CSS Cyberdefense Report* (2021).
Provides an overview of the legal opinions of states and scholars on if and how to apply the law of neutrality to cyberspace.

Nils Melzer, **"Keeping the balance between military necessity and humanity – A response to four critiques of the ICRC's interpretive guidance on the notion of direct participation in hostilities,"** *New York University Journal of International Law and Politics* 42:3 (2010), 831–916.
Explores the reasoning for and consequences of classifying volunteers in cyber conflict either as combatants or civilians directly participating in a conflict. Links to the debate on this issue between the ICRC and US-aligned scholars such as Michael Schmitt.

Charles Dunlap, **"Are commercial satellites used for intelligence-gathering in attack planning targetable?"** *Lawfire,* 05.03.2021.
The former deputy judge advocate general of the US Air Force expands on the issue of commercial satellites that provide intelligence to a belligerent in an international armed conflict and US policy options.

A More Permissive Operating Environment

A consequence of the war in Ukraine may be a permissive operating environment for ransomware gangs and an increased intensity of "persistent engagement" that is likely to continue even if the intensity of the kinetic conflict were to decrease after a ceasefire. Yet, if the operating environment is permissive towards cyberattacks, then why have we not seen widespread damage from Russian cyberattacks beyond Ukraine in 2022? In testimony to the US Senate, NSA director General Paul Nakasone has explained this as a mix of the Russian strategic calculus, hardening measures on the defensive side, and pro-active measures to disrupt offensive capabilities. However, he emphasized that it was still the early days of the war and that continued vigilance was essential, particularly highlighting the threats of a NotPetya-like attack and the Russian use of criminal ransomware groups as proxies.[3]

In the 2017 NotPetya attack, the Russian military intelligence agency GRU released a quickly developed, self-propagating malware that deleted data on infected machines. This attack was aimed at Ukraine but spread to many global firms, causing more than 10 billion USD in damages. Ransomware gangs have been largely responsible for the strong increase in cybercrime and cyber-insurance premiums in the last few years[4] and have the capacity to mount serious attacks on critical infrastructure, as evidenced by the attack on Colonial Pipeline in 2021, which shut down the largest oil pipeline in the US for about a week. Furthermore, due to sanctions, Russia is increasingly decoupled from the Western economies and hence would be less affected by attacks that cause economic damage in the West.

Western powers like the United States and the United Kingdom are likely to assert their interests in such an environment through a mix of deterrence through the threat of punitive offensive cyber operations and the pro-active disruption and harassment of potential attackers. However, this is not a realistic

option for most states in terms of both capacity and political will. For these states, reparations for neutrality violations may offer a softer tool to mitigate the impact of cyberattacks and to influence the behavior of belligerents.

The Case for Financial Compensation

The main goal of financial compensation for collateral damage on neutral territory would be to influence the belligerent trilemma for cyber operations. This term refers to the tradeoffs that actors engaged in cyber operations face among control, speed, and impact, in which optimizing for one factor negatively affects the other factors.[5] An example of a cyber operation that had control and impact but required many years of research and preparation was Stuxnet, the joint US-Israeli attack on centrifuges in the Natanz nuclear facilities in Iran. Even though the Stuxnet worm infected more than 200,000 computers to get to the facility, it only had a negative effect on a very targeted set of machines. In contrast, if a belligerent wants to create a lot of damage and fast, it will likely compromise on its control over the operation. A good example of this is NotPetya. Cyber operations with a high degree of control can have a de-escalatory effect. Stuxnet provided an alternative to a kinetic airstrike that would have destroyed the facility, killed people, and could have caused a war. In contrast, cyber operations with high impact and low control have the potential of leading to a horizontal escalation of a conflict.

With regard to airspace, there is a well-established state practice of financial compensation for damages caused by accidental bombings on neutral territory, which was a common prospect back when pilots strongly relied on visual navigation and target identification. The practice was established through bilateral diplomacy between neutrals and belligerents, and in the absence of any international agreement on how exactly to apply neutrality to airspace. Furthermore, there is evidence that the insistence by neutrals on their right to territorial inviolability has encouraged at least some operational restraint on the side of belligerents. For example, in the Second World War the United States prohibited aerial bombings within 50 miles of Switzerland without positive identification, which was eventually extended to 150 miles to limit the number of accidental bombings.[6]

Extending a similar logic to the application of neutrality in cyberspace, states that are neutral in the war in Ukraine should consider demanding financial compensation for collateral damage from any cyberattack that can be attributed with reasonable certainty to one of the belligerent states. They should consider declaring this intention pre-emptively. Collateral damage on neutral territory from belligerent cyberattacks violates the neutral right to inviolability even if the attack remains below the threshold of an armed attack. First, this would help to reimburse businesses for the fallout of the conflict. Cyberinsurance usually explicitly excludes, and will likely refuse to cover, damages occurring from cyberattacks related to a war. Second, in the case at hand, it might be possible to get financial compensation for a hypothetical attack from Russia, even if Russia would refuse to acknowledge responsibility. The reason for this is the vast amounts of Russian assets that are frozen outside of Russia. Third, establishing the general state practice that belligerents are held accountable for collateral damage from cyberattacks in neutral countries provides an incentive for more control in the belligerents' trilemma for cyber operations in (future) conflicts and thereby also decreases the inadvertent horizontal escalation risk for other actors.

Selected sources

1. ICRC, *Commentary on the Second Geneva Convention: Article 5 – Application by Neutral Powers,* 2017.
2. David Sanger et al., "Arming Ukraine: 17,000 Anti-Tank Weapons in 6 Days and a Clandestine Cybercorps," *New York Times,* 06.03.2022.
3. "Intelligence Directors Testify on National Security Threats and Ukraine," *C-SPAN,* 10.03.2022.
4. Eric Cho, "Why the hardening cyber market benefits all," *Munich RE,* 29.10.2021.
5. Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46:2 (2021), 51–90.
6. Jonathan Helmreich, "The Diplomacy of Apology: US Bombings of Switzerland during World War II," *Air University Review* 28:4 (1977), 19–37.

Kevin Kohler is a Senior Researcher in the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

Policy Perspectives is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy.

Series Editor: Brian G. Carlson
Issue Editor: Linda Maduz
Layout: Miriam Dahinden-Ganzoni

Feedback welcome: PolicyPerspectives@sipo.gess.ethz.ch
More issues and free online subscription:
css.ethz.ch/en/publications/css-policy-perspectives

Most recent editions:
Europe: Greater Autonomy, Better Allies (9/10)
The Role of Value Systems in Conflict Resolution (9/9)
Redesigning Nuclear Arms Control for New Realities (9/8)
NATO's Strategic Concept: Three Do's and Don'ts (9/7)
Nord Stream 2: It's Time to Change Perspective (9/6)
European Drone Clubs Stall Strategic Autonomy (9/5)

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000548707