B4Ukraine

Chuck Robbins
Chair & Chief Executive Officer
170 West Tasman Dr.
San Jose, CA 95134
USA

CC: CISCO Executive Team and Board

02/11/2022

RE: Cisco business operations in Russia

Dear Mr. Robbins,

We write to you as a coalition of Ukrainian and international civil society organizations working to curtail the financial resources enabling the Russian invasion of Ukraine. In the spirit of respect for the fundamental rights of all people, the rules-based international order, and a prosperous global economy, we expect companies to demonstrate public support for the people, democracy, and territorial integrity of Ukraine, opposition to Russia's war of aggression, and alignment with the UN Guiding Principles on Business and Human Rights (UNGPs).

We request an urgent dialogue regarding potential inconsistencies between Cisco Systems' (Cisco) stated policies on Russian aggression and human rights more broadly and the company's ongoing business operations and relationships in Russia that may contribute to, or be linked with, human rights harms.

Cisco's Global Human Rights Policy formalises the company's "long-standing commitment to uphold and respect human rights for all people" and "reflects fundamental standards for business conduct and human rights, provides a cornerstone for Cisco to identify and manage its human rights impacts, mitigate risks, and fosters collaborative and transparent engagement with our stakeholders and investors." Further, the policy is applicable to all employees, partners, suppliers, and contractors. Finally, we note that the company's Human Rights Due Diligence (HRDD) policy is "grounded in the [UNGPs]" and the approach allows the company "to identify actual and potential human rights risks, strategies for addressing those risks, [track] the effectiveness of our response, and [communicate] about how the impacts are addressed."

It has been eight months since Russia invaded Ukraine and the devastating impacts continue to shock the global conscience and shake the global economy. Russia is violating international humanitarian law (IHL), including war crimes and crimes against humanity, through attacks on civilians and civilian infrastructure (e.g., mass executions, sexual violence, torture, and forcible transfer of civilians). More than 15,000 Ukrainians have been killed and injured and millions more have been forced to flee their homes, creating one of the largest humanitarian and refugee crises of modern times.

On September 21, President Vladimir Putin escalated the war by announcing a "partial mobilisation" of the Russian population. The accompanying legislation (Article 9 of Federal Law No. 31-FZ)

mandates all organisations, including more than 1500 international companies that are currently operating on a full or limited scale in Russia, to conduct military registration of the staff if at least one of the employees is eligible for military service.[1] They must also assist with delivering the military summons to their employees, ensure the delivery of equipment to assembly points or military units, and provide information, buildings, communications, land plots, transport, and other material means of support to the war effort.

This legislation entails new and significant legal risks for companies remaining in Russia, including potential civil and criminal liability under comprehensive sanctions regimes and recent international jurisprudence holding corporations and their officers responsible for human rights abuses abroad.[2] Companies may be exposed to financially material risks through operational restrictions, such as limitations of future government contracts.[3]

In response to this unprovoked and unjustified war[4] many companies have left Russia. According to the respected Kyiv School of Economics Institute's #LeaveRussia company tracker, Cisco announced in March that it would be "stopping all business operations, including sales and services, in Russia and Belarus for the foreseeable future" and further committed to "begin an orderly wind-down of our business in Russia and Belarus" in June 2022. While we commend these statements, our research indicates that Cisco has not met its stated commitments.

In the years following Russia's 2014 occupation of Crimea, Cisco gained a significant share of the Russian market. By 2021, Cisco's 266 staff members were providing the products and services upon which nearly 20 percent of all network infrastructure operates and generating $800 million in revenue. Today, the company appears to maintain certain business activities in Russia, including the continued sales and services by Cisco and its licensed distributors with over 500 transactions in

---

[1] Federal Law No. 31-FZ of February 26, 1997 "On mobilization training and mobilization in the Russian Federation" (as amended), https://base.garant.ru/136945/ (accessed November 2, 2022).

[2] International companies remaining in Russia are now at a greater risk of violating sanctions regimes as implementation of the legislation will likely involve transacting with sanctioned individuals or entities. Furthermore, new domestic civil and criminal cases against companies involved in violations of international law demonstrate the risk of significant liability for facilitating state-sponsored human rights abuses abroad (e.g., LafargeHolcim [Syria], Lundin Energy [Sudan], Castel Group [Central African Republic, Nevsun [Eritrea], and Dassault Aviation, Thales, and MBDA France [Yemen].) Victoria Riello and Larissa Furtwengler, "Corporate Criminal Liability for International Crimes: France and Sweden Are Poised To Take Historic Steps Forward," *Just Security*, September 6, 2021, https://www.justsecurity.org/78097/corporate-criminal-liability-for-human-rights-violations-france-and-sweden-are-poised-to-take-historic-steps-forward/ (accessed November 2, 2022); The Sentry, "Breaking: France Opens War Crimes Inquiry Focused on Iconic Food and Beverage Conglomerate," July 1, 2022, https://thesentry.org/2022/07/01/7216/breaking-france-opens-war-crimes-inquiry-focused-iconic-food-beverage-conglomerate/ (accessed November 2, 2022); Preston Lim, "Canadian Supreme Court Allows Corporate Liability for International Law Violations," *Lawfare*, March 12, 2022, https://www.lawfareblog.com/canadian-supreme-court-allows-corporate-liability-international-law-violations (accessed November 2, 2022); Sherpa, "Aiding and abetting war crimes in Yemen: Criminal complaint submitted against French arms companies," June 2, 2022, https://www.asso-sherpa.org/aiding-and-abetting-war-crimes-in-yemen-criminal-complaint-submitted-against-french-arms-companies (accessed November 2, 2022).

[3] Venable LLP, "Do You Contract with State Governments? If So, Beware of Emerging State Sanctions' Obligations Related to Russia and Belarus," *JD Supra*, June 3, 2022, https://www.jdsupra.com/legalnews/do-you-contract-with-state-governments-6537229/ (accessed November 2, 2022).

[4] The UN General Assembly condemned Russia's "aggression against Ukraine" and demanded that Moscow "unconditionally withdraw all of its military forces from the territory of Ukraine within its internationally recognized borders."

August,[5] use of equipment and services that support the Russian payment system MIR (introduced following Visa and Mastercard's termination of operations) and data centers belonging to the sanctioned Sberbank,[6] and ongoing educational programs by the Cisco Networking Academy.[7] A *New York Times* investigation also revealed that Cisco equipment was used to connect Russia's internet to the SORM system, which is used by Russian authorities to surveil and censor internet traffic in Russia and occupied Ukrainian territory.[8]

These activities risk enabling and financing Russia's violations of IHL and human rights law during the ongoing invasion and occupation of Ukraine and violating Cisco's Global Human Rights Policy and the company's stated commitment to abiding by the UNGPs. It remains to be seen how directly Cisco will be impacted by the partial mobilisation and the heightened legal, regulatory, operational, and financial risks associated with companies being required to provide direct support to the internationally sanctioned Russian military.

We seek to understand how Cisco has conducted and continues to conduct heightened HRDD, per its stated policy and the UNGPs concerning due diligence in conflict-affected areas, and how the findings of such a process has resulted in these continued business activities and relationships. As noted by the UNGPs:

> …the more severe the abuse, the more quickly the enterprise will need to see change before it takes a decision on whether it should end the relationship. In any case, for as long as the abuse continues and the enterprise remains in the relationship, it should be able to demonstrate its own ongoing efforts to mitigate the impact and be prepared to accept any consequences – reputational, financial or legal – of the continuing connection.

With the above points in mind and in consideration of B4Ukraine's Declaration, we request an urgent dialogue with Cisco's relevant senior management and staff to discuss the company's ongoing activities and relationships in Russia, associated risks to the people of Ukraine and the company, and potential steps to prevent/mitigate these risks.Please contact Eleanor Nichol at enichol@businessforukraine.info to schedule a call. We kindly ask for your response by 5:00pm CET, 16th November 2022.

Please do not hesitate to get in touch if you require any further information

Sincerely,

---

[5] James Rogers, "Cisco gear is being shipped into Russia from China and other countries, leaked customs database shows," *MarketWatch*, October 17, 2022, https://www.marketwatch.com/story/cisco-gear-is-being-shipped-into-russia-from-china-and-other-countries-leaked-customs-database-shows-11666013986 (accessed November 2, 2022).

[6] Anton Shvets, "Technogiant CISCO continues business in Russia despite announcing pullout," *EuroMaidan Press*, May 20, 2022, https://euromaidanpress.com/2022/05/20/cisco-continues-business-in-russia-after-announcing-pullout/ (accessed November 2, 2022).

[7] RosTender, "Tender: Information, technical and organizational support for the school's participation in the Cisco Networking Academy program," April 14, 2022, https://rostender.info/region/moskva-gorod/59619346-tender-informacionno-tehnicheskaya-i-organizacionnaya-podderjka-po-uchastiyu-shkoly-v-programme-setevoj-akademii-cisco (accessed November 2, 2022).

[8] Adam Satariano, Paul Mozur, and Aaron Krolik, "When Nokia Pulled Out of Russia, a Vast Surveillance System Remained," *New York Times*, March 28, 2022, https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html (accessed November 2, 2022); Matt Burgess, "Russia is Taking Over Ukraine's Internet," *Wired*, June 15, 2022, https://www.wired.com/story/ukraine-russia-internet-takeover/ (accessed November 2, 2022).

Eleanor Nichol
Executive Director
The B4Ukraine Coalition