

Ron Nersesian,  
Executive Chairman,  
Keysight Technologies, Inc.  
1400 Fountaingrove Parkway  
Santa Rosa, CA 95403

CC: Keysight Executive Team and Board

02/11/2022

RE: Keysight Technologies' business operations in Russia

Dear Mr. Nersesian,

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 conversation regarding potential inconsistencies between Keysight Technologies' (Keysight) stated human rights policies and the company's ongoing operations and relationships in Russia that may contribute to, or be linked with, human rights harms.

Keysight's Human Rights Policy formalises the company's commitment to respecting the fundamental principles contained in the Universal Declaration of Human Rights, the tenets of the UNGPs, core International Labour Organisation Conventions, and the laws of countries in which it operates.<sup>1</sup> Further, the policy is supported by Keysight's Standards of Business Conduct, Supplier Code of Conduct, supplier audits, Purchase Order Terms and Conditions, human rights impact assessments, and its disclosures under the Global Reporting Initiative, the Sustainability Accounting Standards Board, and its Corporate Social Responsibility Report.

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 committing war crimes, crimes against humanity, and 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 disasters and refugee crises of modern times.

---

<sup>1</sup> Keysight Technologies, "Human Rights and Labor Policy," <https://www.keysight.com/de/de/assets/3120-1572/exhibits/Keysight-Technologies-Inc-Human-Rights-and-Labor-Policy.pdf> (accessed October 26, 2022).

On September 21, President Vladimir Putin further 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 1,500 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.<sup>2</sup> 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.<sup>3</sup> Companies may also be exposed to financially material risks through operational restrictions, such as limitations on future government contracts.<sup>4</sup>

In response to this unprovoked and unjustified war<sup>5</sup> many companies have left Russia. Prior to Russia’s invasion of Ukraine, Keysight’s Russian sales represented 1 percent of the company’s total revenue and Keysight maintained operations within the country, including overseeing offices and

---

<sup>2</sup> Federal Law No. 31-FZ of February 26, 1997 "On mobilisation training and mobilisation in the Russian Federation" (as amended), <https://base.garant.ru/136945/> (accessed October 26, 2022).

<sup>3</sup> The new legislation creates significant risk of international companies violating sanctions regimes as providing direct services and goods to Russian actors involved in executing the invasion will likely involve transacting with sanctioned individuals or entities. Furthermore, several domestic civil and criminal cases against companies involved in violations of international law, including supporting governmental war crimes and crimes against humanity, demonstrate the risk of significant liability for facilitating state-sponsored human rights abuses abroad (e.g., Lafarge case, Lundin case, Castel Group indictment, Amesys Indictment, Nevsun holding, and Dassault Aviation, Thales, and MBDA France criminal complaint.) See, “French court upholds Syria ‘complicity in crimes against humanity’ charge against Lafarge,” *France 24*, May 18, 2022, <https://www.france24.com/en/live-news/20220518-paris-court-upholds-charges-of-complicity-in-crimes-against-humanity-linked-to-lafarge-s-cement-plant-in-syria> (accessed October 26, 2022); 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 October 26, 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 October 26, 2022); “French technology firm charged over Libya cyber-spying,” *RFI*, July 2, 2022, <https://www.rfi.fr/en/business-and-tech/20210701-french-tech-firm-charged-over-libya-cyber-spying> (accessed September 26, 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 September 26, 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 October 26, 2022).

<sup>4</sup> 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 October 26, 2022).

<sup>5</sup> 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.”

employees.<sup>6</sup> Furthermore, Keysight's manufacturing test and measurement equipment and software has previously been sold to public and private Russian entities in violation of US regulations. In 2021, Keysight settled charges with the U.S. Department of State for violations of International Traffic in Arms Regulations based on the unlawful export to Russia of electronic warfare simulation software.<sup>7</sup> In addition, Keysight 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.<sup>8</sup>

In response to an increase in sanctions and export controls, Keysight claims that it has discontinued its operations in Russia, which included writing down \$3 million in assets and incurring "asset impairment charges of \$7 million and other liquidation-related expenses, including employee severance."<sup>9</sup> However, questions remain regarding the manner in which Keysight exited the Russian market, which Russian customers maintain access to Keysight's technologies, the extent to which Keysight is still providing services to pre-existing customers/contracts, and the status of Keysight's former assets and employees. As mentioned above, Keysight has already provided Russian entities with technology that could further the war effort. However, it remains to be seen how Keysight's products that are still in the Russian market will be further implicated, transferred, or accessed through the partial mobilisation, creating 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 Keysight has conducted and continues to conduct heightened Human Rights Due Diligence, 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 Keysight's ongoing business decisions. 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 conversation with Keysight's relevant senior management and staff to discuss the company's remaining risks in the Russian market, associated risks to the people of Ukraine and the company, and potential steps to prevent or mitigate these risks. Please contact Eleanor Nichol at [enichol@businessforukraine.info](mailto:enichol@businessforukraine.info) to schedule a call. We kindly ask for your response by 5:00pm CET, 16 November 2022.

---

<sup>6</sup> Keysight Technologies, "Form 10-Q - Quarterly Report," August 30, 2022, <https://www.sec.gov/Archives/edgar/data/1601046/000160104622000066/keys-20220731.htm> (accessed October 26, 2022).

<sup>7</sup> U.S. Department of State, "U.S. Department of State Concludes \$6.6 Million Settlement of Alleged Export Violations by Keysight Technologies, Inc.," August 9, 2021, <https://www.state.gov/u-s-department-of-state-concludes-6-6-million-settlement-of-alleged-export-violations-by-keysight-technologies-inc/> (accessed October 26, 2022).

<sup>8</sup> Andrei Soldatov and Irina Borogan, "How Western tech companies are helping Russia censor the Internet," *Washington Post*, December 21, 2021, <https://www.washingtonpost.com/opinions/2021/12/21/how-western-tech-companies-are-helping-russia-censor-internet/> (accessed October 26, 2022).

<sup>9</sup> Keysight Technologies, "Form 10-Q - Quarterly Report," August 30, 2022, <https://www.sec.gov/Archives/edgar/data/1601046/000160104622000066/keys-20220731.htm> (accessed October 26, 2022).

We very much look forward to speaking with you.

Sincerely,

Eleanor Nichol  
Executive Director  
The B4Ukraine Coalition