TERROR IN THE DETAILS:

Western-made Components in Russia’s Shahed-136 Attacks
LEGAL DISCLAIMER

This report identifies several companies and governments who are believed to be involved in the manufacturing of components which have been acquired by the Russian military and used in their military hardware.

For the avoidance of doubt, we do not allege any legal wrongdoing on the part of the companies who manufacture the components and do not suggest that they have any involvement in any sanctions evasion-related activity.

Furthermore, we do not impute that the companies which make the components are involved in directly or indirectly supplying the Russian military or Russian military customers in breach of any international (or their own domestic) laws or regulations restricting or prohibiting such action.

Where a link is drawn between manufacturers and the weapons being used in suspected war crimes, this is done solely to highlight ethical and moral concerns.
<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Part one: what are IHL violations and war crimes?</td>
<td>7</td>
</tr>
<tr>
<td>Part two: suspected war crimes carried out by the Shahed-136 in Ukraine</td>
<td>10</td>
</tr>
<tr>
<td>Part three: the Shahed-136 and its reliance on western components</td>
<td>30</td>
</tr>
<tr>
<td>Recommendations</td>
<td>37</td>
</tr>
<tr>
<td>About the authors</td>
<td>40</td>
</tr>
</tbody>
</table>
INTRODUCTION

The Shahed-136 is an Iranian loitering munition that targets stationary ground objects guided by a sophisticated navigation system. Described as “ingenious in its simplicity” by Dr Uzi Rubin, the former Director of the Israel Missile Defense Organization, it flies low and slow towards a target and detonates on impact. It is both ruthlessly accurate and inexpensive.

This report analyses ten suspected Russian war crimes carried out using the Shahed-136. The attacks targeted residential buildings, power plants, businesses, a school and a children’s summer camp. In each instance, we have explored the circumstances around the attack, the presence of military objects or activity in the vicinity of targeted objects, the result of the attacks, including the level of damage and casualties, and the means by which we have identified the Shahed-136 as being used.

We find that Russia’s attacks are, on the face of it, intentionally aimed at the civilian population and infrastructure, with no tangible military advantage gained as a result of them. These are fundamental conditions that must be met in order for an attack to be assessed as a war crime, and in each case study, we examine the legal background behind our assessment.

This report also explores the Shahed-136’s documented reliance upon Western-made components, and in so doing, calls into question the effectiveness of sovereign export controls and corporate due diligence processes. Since Russia’s February 2022 invasion, Western governments have worked to supply the Ukrainian armed forces with equipment, support, and training, but have done little to exploit the Russian military’s Achilles heel: its reliance upon Western components.

In total, components from 16 companies based in the US, Japan, Canada, and Switzerland have been found inside the Shahed-136, ranging from microprocessors and semiconductors to batteries and memory.
These findings are consistent with a wide range of existing research, including our previous report – ‘Enabling War Crimes? Western-Made Components in Russia’s War Against Ukraine’ – that has explored the extent to which the weapons at the heart of Russia’s committing of atrocities are, ‘under the hood’, reliant upon Western-made components in order to function.

Restricting Russia’s access to such components would have a devastating and immediate effect on sustaining its war effort. Operating at a high tempo requires an equally high level of resupply and replenishment: Russia’s drones, missiles, communication systems, and other equipment require regular repairs, maintenance, and restocking – all processes that require, to varying degrees, Western components. It would be just weeks before Russia’s supply of these components dried up, which would have significant consequences on the battlefield.

This report serves two purposes. Firstly, to illustrate Russia’s continued unlawful and barbaric assaults on the Ukrainian population, judged to be in conflict with International Humanitarian Law. Secondly, to sound the alarm as to the Russian military’s reliance on Western-made components in its war against Ukraine and the urgent need to restrict the continued supply of such components.

The beginning of the solution is to recognise that the problem exists. Up to now, businesses and policymakers alike have remained predominantly silent on the issue of Russia’s reliance on Western-made components. This has been justified, at least in part, by the fact that the causes of the situation – including the Russian military’s supply chain – are difficult to track and as such, a challenge to put right. The reality, however, as this report demonstrates, is that civil society organisations and research groups can, using open-source intelligence, expose and trace these causes with immense precision. Lack of evidence or lack of understanding can no longer be used as a justification for inaction.
PART ONE: WHAT ARE IHL VIOLATIONS AND WAR CRIMES?
PART ONE: WHAT ARE IHL VIOLATIONS AND WAR CRIMES?

What is an IHL violation?

International Humanitarian Law (IHL) is a set of rules and principles that seeks to protect persons who are not or no longer directly or actively participating in hostilities and imposes limits on the means and methods of warfare. An IHL violation is a violation of this set of rules, which can be found in the four Geneva Conventions of 1949, the Hague Conventions of 1907 and customary international law, which are the core sources of modern IHL. IHL is part of public international law, which is made up primarily of international treaties (formed by states parties), customary international law (formed by “a general state practice accepted as law”) and general principles of law (legal norms existing among the majority of nations). IHL applies once the conditions for an armed conflict are factually met on the ground. For international armed conflicts, these conditions consist of one or more states' use of armed force against one or more other states, and for non-international armed conflicts. Armed confrontation between governmental armed forces and one or more non-state armed groups, or between such groups, may amount to non-international armed conflict and thus be governed by IHL if it reaches a certain level of intensity and organisation of non-state parties involved.

What is a war crime?

The core principle behind the concept of war crimes is that individuals can be held criminally accountable for serious violations of IHL.

A serious IHL violation that amounts to a war crime must include one (or several) of the following three types of conduct:

1. Endangering protected persons, e.g. willful killings, torture, intentional attacks on civilians, killing of combatants rendered hors de combat (incapable of fighting);
2. Endangering protected objects, e.g. intentionally attacking civilian objects including civilian dwellings, hospitals, schools, and

---

3 Article 38, the Statute of the International Court of Justice.
5 ibid.
6 ICC Statute, Article 8(2)(a)(i)
7 ICC Statute, Article 8(2)(a)(ii)
8 ICC Statute, Article 8(2)(b)(i)
9 ICC Statute, Article 8(2)(b)(vi)
10 How law protects in war?, Hors de combat, available at: https://casebook.icrc.org/a_to_z/glossary/hors-de-combat
11 ICC Statute, Article 8(2)(b)(ii)
3. Breaching important values even without physically endangering persons or objects directly, e.g. declaring that no quarter will be given,\(^\text{12}\) subjecting persons to humiliating treatment,\(^\text{13}\) violating the right to a fair trial\(^\text{14}\).

Currently, the most comprehensive list of examples of serious violations of IHL (war crimes) is contained in Article 8 of the Rome Statute of the International Criminal Court.\(^\text{15}\)

War crimes, together with crimes against humanity, genocide, and the crime of aggression, are four core international crimes.\(^\text{16}\) These crimes are considered to be of such gravity that they have no statute of limitation under international criminal law,\(^\text{17}\) meaning that those committing the crimes can be brought to justice no matter how much time has passed since their commission.

The implementation of IHL is primarily the responsibility of states. They must respect, and ensure respect for, these rules in all circumstances.\(^\text{18}\) IHL is universal: all parties fighting in a conflict are obliged to respect it, be they governmental forces or non-state armed groups\(^\text{19}\). The responsibility to prevent and punish IHL violations also belongs primarily to states. IHL requires states to investigate serious violations and, if appropriate, prosecute the suspects. This means that appropriate steps must be taken to implement the legal framework for criminal prosecution of IHL violations into a state’s domestic criminal law. As a complement to domestic trials, internationally established criminal justice mechanisms, including the International Criminal Court (ICC), may promote greater respect for IHL by ensuring that the most serious IHL violations, e.g. war crimes, do not go unpunished.\(^\text{20}\)

**Who can prosecute IHL violations and war crimes?**

States must adopt legislation and regulations aimed at ensuring full compliance with IHL. Additionally, states must investigate war crimes committed by their nationals or armed forces or on their territory and, if possible, prosecute the suspects.\(^\text{21}\) Some states have also adopted national legislation allowing the prosecution of war crimes in their national courts, irrespective of the nationality of the offender.

---

\(^{12}\) IHL prohibits using this procedure, that is, ordering that there shall be no survivors, threatening the adversary therewith, or conducting hostilities on this basis. For more information, see How law protects in war?, Quarter, available at: [https://casebook.icrc.org/a_to_z/glossary/quarter-denial](https://casebook.icrc.org/a_to_z/glossary/quarter-denial); ICC Statute, Article 8(2)(b)(xii); Hague Regulations (1907), Article 23(d); AP (I) 1949, Article 40; AP (II) 1949, Article 4(1).

\(^{13}\) ICC Statute, Article 8(2)(b)(xxi)

\(^{14}\) ICC Statute, Article 8(2)(a)(v)


\(^{16}\) European Union Agency for Criminal Justice Cooperation. Core international crimes., available at: [https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/core-international-crimes]; ICC. About the Court., available at: [https://www.icc-cpi.int/about/the-court](https://www.icc-cpi.int/about/the-court)


\(^{18}\) Article 1 common to the four Geneva Conventions.


\(^{20}\) Ibid.

\(^{21}\) Geneva Convention (III), art. 129; Geneva Convention (IV), art. 146; Additional Protocol I, art. 88.
or the place where the violations were committed (universal jurisdiction). Domestic prosecution is, however, often impossible during or in the aftermath of an armed conflict if the regime that perpetrated the crimes retains power and is unwilling to prosecute its own representatives.

Over the past 30 years, the international community has stepped in on several occasions to bridge the impunity gap created by the failure of domestic accountability by creating international ad hoc tribunals (ICTY/R), hybrid tribunals (ECCC, SCSL, STL) and the ICC. The latter is a permanent international judicial body with jurisdiction over any core crime committed on the territory of its 123 member states or by its nationals, and, in some cases, when a situation is referred to the Prosecutor of the ICC by the UN Security Council or a country submits a declaration with the Registrar of the ICC accepting the exercise of the ICC’s jurisdiction, non-member states. Ukraine did not ratify the Rome Statute but recognised the jurisdiction of the ICC over international crimes committed on the territory of Ukraine from 21 November 2013 by submitting two declarations of the Verkhovna Rada of Ukraine to the ICC in 2014 and 2015. After Ukraine recognised the ICC’s jurisdiction, the Office of the Prosecutor of the ICC (OTP) conducted a seven-year-long preliminary examination and, in 2022, opened an investigation into the situation in Ukraine. On 17 March 2023, the OTP issued arrest warrants for Russian President Vladimir Putin and Russian Commissioner for Children’s Rights Maria Lvova-Belova for their alleged responsibility for the war crime of unlawful deportation of children and the unlawful transfer of children from occupied areas of Ukraine to the Russian Federation.

These and other suspected perpetrators can be tried by ICC and, if found guilty, sentenced to up to 30 years in prison or to a term of life imprisonment when justified by the extreme gravity of the crime and the individual circumstances of the convicted person.

---

23 Trial International, What are war crimes?, available at: https://trialinternational.org/topics-post/war-crimes/
26 ICC, The International Criminal Court, available at: https://www.icc-cpi.int/
28 ICC Statute, Article 12(3), 13(b).
31 ICC Statute, Article 8(2)(a)(vii)
32 ICC Statute, Article 8(2)(b)(viii)
34 Ibid.
PART TWO: SUSPECTED WAR CRIMES CARRIED OUT BY THE SHAHED-136 IN UKRAINE
PART TWO: SUSPECTED WAR CRIMES CARRIED OUT BY THE SHAHED-136 IN UKRAINE

Russia's full-scale invasion of Ukraine is the first international armed conflict involving the use of unmanned aerial vehicles (UAVs) as weapons at this scale. Between September 2022, when Russia first began using widespread UAV attacks, and May 2023, it launched more than 1,000 UAVs to attack Ukrainian critical energy and civilian infrastructure.

By the end of 2022, Russian attacks on energy infrastructure had left millions of Ukrainians without heating, electricity, water and other vital services during the cold winter months. As of 31 January 2023, at least 116 civilians have been killed, and at least 379 more have been injured in such attacks.

In May 2023, Russia intensified its aerial attacks against Ukrainian cities, launching at least 20 waves of UAVs and missiles. On the night of 28 May 2023, Kyiv alone was attacked by 54 Shahed 136/131, making it the largest Russian UAV attack to date.

As demonstrated throughout this report, there is no evidence to suggest that Russian aerial attacks have affected the Ukrainian military or decision-making centres significantly. Instead, these attacks are part of the broader pattern of the Russian military’s intentional terror campaign against the Ukrainian people.

The authors of this report documented 25 Russian UAV attacks on Ukraine between September 2022 and May 2023. Cases were discarded where there was insufficient information to establish the target’s status (military/civilian), the level of damage caused, or the model of the UAV used in the attack. Ten attacks were then selected for inclusion in this report, on the basis that they caused serious damage and civilian casualties, and used the Shahed-136.

---


36 Euronews, Russia using drones to save ammunition in Ukraine, available at: https://www.euronews.com/2023/04/20/russia-using-drones-to-save-ammunition-in-ukraine#:~:text=The%20Institute%20for%20the%20Study,their%20ammunition%20since%20September%202022

37 Ukrainian government figures compiled by IPHR


39 Kyiv Post, ‘Russia’s Month of Missile Madness: 90% of Projectiles Failed, $1.7 Billion Spent’, 31 May 2023, available at: https://archive.ph/zrij8


41 According to IPHR’s internal database on Russian attacks on Ukraine based on information from open sources.
The attacks documented in this report killed 15 civilians and injured another 42. In addition, they destroyed or damaged nine critical infrastructure objects, 13 civilian houses and four other civilian objects.

The Shahed-136 is considered to be a guided weapon. It navigates using a combination of GPS and GLONASS, while a commercial-grade digital communication chip within it allows for a target’s location to be updated mid-flight, or even for the intended target to be changed entirely while still in the air.

Targets are selected and struck with precision, and it is therefore reasonable to assume that in the case studies below and the plethora of other strikes in recent months, the Shahed-136 is impacting its intended target, rather than experiencing any level of deviation.

The ten attacks analysed in this report may constitute grave breaches of IHL and war crimes of directing attacks against protected civilian objects and directing attacks against civilians. Additional investigations would be required to corroborate these allegations to a judicial standard.

Case Study No. 1

DATE: 11 OCTOBER 2022
LOCATION: LADYZHYN, VINNYTSIA OBLAST
INCIDENT: ATTACK ON ENERGY INFRASTRUCTURE

On 11 October 2022, Russian forces attacked energy infrastructure across six regions in western, central and southern Ukraine. According to the Ukrainian military, the attacks were carried out using Kh-101 missiles and Shahed-136 UAVs.

One of the Shahed-136 attacks damaged a thermal power plant in Ladyzhyn, Vinnytsia Oblast. A second strike, following shortly after the first one, injured six emergency workers who were responding...
to the first attack.\textsuperscript{47} The attacks caused severe damage to the Ladyzhyn power plant, leaving some 18,000 civilians without heating for at least two months during winter.\textsuperscript{48}

\textsuperscript{47} DTEK Ladyzhynska TPP, ‘The Ladyzhynska TPP was hit again by Russian terrorist forces’, 11 October 2022, available at: https://archive.ph/5HPZ1.

\textsuperscript{48} Ukrainska Pravda, ‘Vinnytsia Oblast: TPP attacks create emergency situation in Ladyzhyn’, 28 November 2022, available at: https://archive.ph/AGXgt; Vinnytsia Regional Military Administration, ‘Restoration of heat supply in Ladyzhyn, limitation of electricity consumption, the state of the medical system of the region - the key issues of the meeting of the Head of RMA Serhiy Borzov with the heads of structural divisions’, 23 January 2023, available at: https://archive.ph/qoOXa; Serhiy Borzov, ‘Heat supply has been restored in Ladyzhyn’, 1 December 2022, available at: https://www.facebook.com/borzov.s/posts/pfbid0348nKL5zJ4gV2yhe735rCSiwBcgKwemjMRrgbBgRAKTLAxpcXSVuowKj8XpsCmZ9l.
On the morning of 17 October 2022, Russian forces attacked Ukrainian cities with missiles and UAVs, directing some 28 UAVs at Kyiv. The first attack took place at around 7 a.m. and targeted an office building in Shevchenkivskyi District, setting it on fire and damaging several nearby residential buildings. The use of the Shahed-136 was confirmed by both the US Defence Intelligence Agency and the General Staff of the Armed Forces of Ukraine. The Mayor of Kyiv, Vitaliy Klitschko, published a photo of one of the UAV's remnants; this can be identified as the Shahed-136.

The second attack followed an hour later. Four UAVs targeted several energy infrastructure facilities and an apartment building in downtown Kyiv. The attack on the apartment building killed five people.
civilians, including a pregnant woman. Three people, including two rescue workers, were hospitalised with injuries. As a result of the attack, the 120-year-old apartment building – which was part of Kyiv’s historical downtown – was damaged beyond repair.

UAV and missile attacks on Kyiv, Sumy and Dnipropetrovsk regions that day caused black-outs in hundreds of settlements across the regions.

Sources: https://t.me/vitaliy_klitschko/1555; https://t.me/V_Zelenskiy_official/3675


60 State Emergency Service of Ukraine, ‘Russian attack on the capital in the morning of 17 October’, 17 October 2022, available at: https://archive.ph/q8plE; Tymoshenko Kyrylo, ‘Kyiv. As of now, 19 people have been rescued, 4 were injured, and 2 people died’, 17 October 2022, available at: https://archive.ph/FqWq0.

61 Kyiv City Council, ‘Vitaliy Klitschko: As a result of the kamikaze drone attack in the capital, four people died. Three Kyiv residents were hospitalised. Two of them were lifeguards’, 17 October 2022, available at: https://archive.ph/0iaES.

62 Suspilne.Media, ‘Kamikaze drones hit a residential building in Kyiv, there are dead people. What is known about the Russian forces attack’, 17 October 2022, available at: https://archive.ph/25Ujm; Vitaliy Klitschko, ‘The body of a dead woman was recovered from the rubble of a house in Shevchenkovskyi district, where an explosion occurred as a result of a drone attack’, 17 October 2022, available at: https://archive.ph/OXnkS.

63 Tkachenko Oleksandr, ‘Russia continues to terrorise the civilian population’, 17 October 2022, available at: https://archive.ph/h9TE; Map of Renovation, ‘In the morning, Russia again attacked the center of Kyiv’, 17 October 2022, available at: https://archive.ph/RU66e.

On the night of 9 November 2022, Russian forces launched a UAV attack on a storage facility used by the Nova Poshta delivery company in Dnipro.\textsuperscript{65, 66} The fire caused by the attack significantly damaged the building and destroyed most of its equipment and parcels.\textsuperscript{67} Four Nova Poshta employees were hospitalised with severe injuries.\textsuperscript{68}

Local authorities published pictures of Shahed-136 remnants discovered at the scene. The Russian Ministry of Defense described this attack as “the destruction of the ammunition of the Armed Forces of Ukraine.”\textsuperscript{69} The Office of the Prosecutor of Dnipropetrovsk Oblast said however that there were no military targets in the area that was attacked.\textsuperscript{70} No military personnel were killed or wounded.\textsuperscript{71} Additionally, the company's Terms and Conditions prohibit the shipment of any weapons\textsuperscript{72} and there is no evidence of any direct cooperation or relationship between the Armed Forces of Ukraine and Nova Poshta.

\textsuperscript{65} Coordinates of the impact site: 48.47155079634144, 35.116388223042435.
\textsuperscript{67} Nova Poshta, ‘One of our depots in Dnipro was destroyed tonight as a result of a drone attack’, 9 November 2022, available at: https://www.facebook.com/nova.poshta.official/posts/pf7id0U4wob03yJnS0PEVfHvWsb1FNuBhbmF8xBn7pWjhgQuaqS8gQodgyRldjAr3WkKl; Mykola Lukashuk, ‘Full-scale military invasion of the Russian Federation in Ukraine, day 259’, 9 November 2022, available at: https://archive.ph/R2gc.
\textsuperscript{68} Nova Poshta, ‘One of our depots in Dnipro was destroyed tonight as a result of a drone attack’, 9 November 2022, available at: https://www.facebook.com/nova.poshta.official/posts/pf7id0U4wob03yJnS0PEVfHvWsb1FNuBhbmF8xBn7pWjhgQuaqS8gQodgyRldjAr3WkKl; Dnepr Operativ, ‘Night attack on Dnipro: fire, injured people and destruction’, 9 November 2022, available at: https://archive.ph/dTDgy; Fakty, ‘Drone attack: the Russian Federation targeted an enterprise in Dnipro. Four workers are in the hospital’, 9 November 2022, available at: https://archive.ph/HKaA.
\textsuperscript{70} Office of the Prosecutor of Dnipropetrovsk Oblast, The Russian military attacked the city of Dnipro with kamikaze drones - an investigation has been launched, 9 November 2022, available at: https://archive.ph/6sWea.
\textsuperscript{71} Nova Poshta, ‘One of our depots in Dnipro was destroyed tonight as a result of a drone attack’, 9 November 2022, available at: https://www.facebook.com/nova.poshta.official/posts/pf7id0U4wob03yJnS0PEVfHvWsb1FNuBhbmF8xBn7pWjhgQuaqS8gQodgyRldjAr3WkKl.
On 10 December 2022, Russian forces launched a UAV attack on two energy infrastructure facilities in Odesa Oblast.\textsuperscript{73} It took firefighters more than four hours to extinguish the fire started by the attack.\textsuperscript{74}


\textsuperscript{74} Our Odessa, ‘About 4-4:30 hours have already passed from the moment of attack, but it still not possible to extinguish it’, 10 December 2022, available at: https://archive.ph/IqziJ.
The attack caused a total electricity blackout in Odesa and Odesa Oblast, which affected some 1.5 million residents. The next day, 300,000 people were still without electricity. Local authorities had to mandate restrictions on energy use in the region for the following five days as a result of the damage reducing the network's ability to fulfil demand.

The Odesa Regional Prosecutor’s Office confirmed that Russian forces used the Shahed-136 to carry out the attack.

Source: Odesa Region Prosecutor’s Office

---

75 Suspilne Odesa, ‘After a night strike by drones, more than one and a half million people in Odesa remain without electricity’, 10 December 2022, available at: https://archive.ph/C20yw; DTEK Odesa Electricity Networks, ‘Power engineers of DTEK and NEC Ukrenergo are restoring the region’s energy infrastructure after an enemy attack’, 10 December 2022, available at: https://www.facebook.com/dtekoem/posts/pfbid0Zm6pYmvWCTc6wM25QT5gwB9iHoTc0i9Egs31K84oo4u1Z1AH4r8xbYfRnyhXE8sI

76 Suspilne.Media, ‘300,000 people in Odesa remain without electricity’, 11 December 2022, available at: https://archive.ph/6n05A; Suspilne Odesa, ‘Odesa is without electricity after the drone attack: all the sockets in the shops are in use’, 11 December 2022, available at: https://archive.ph/qKvwh.


DATE: 28–29 DECEMBER 2022
LOCATION: KHARKIV
INCIDENT: ATTACK ON ENERGY INFRASTRUCTURE

On the night of 28–29 December 2022, Russian forces attacked critical energy infrastructure in Kharkiv with 13 UAVs. 11 of them were shot down by Ukrainian Air Defence while two hit critical infrastructure, leaving some 1,000 civilian homes without heating.79

The General Staff of the Armed Forces of Ukraine and the Kharkiv Regional Prosecutor’s Office reported that the UAVs used in the attacks were Shahed-136.80

Source: Kharkiv Region Prosecutor’s Office


Case Study No. 6

**DATE:** 10 FEBRUARY 2023  
**LOCATION:** SHEPETIVKA, KHMELNYTSKYI OBLAST  
**INCIDENT:** ATTACK ON ENERGY INFRASTRUCTURE

On 10 February 2023, Russian forces launched a massive attack on Ukraine with 20 Shahed-136/131 UAVs and 71 Kh-101, X-555 and Kalibr missiles. Local authorities reported Shahed-136/131 attacks in Khmelnytskyi Oblast and Dnipropetrovsk Oblast.

One UAV damaged a critical infrastructure facility in Shepetivka, Khmelnytska Oblast, causing a fire and a two-day blackout.

The local authorities reported that the Ukrainian Air Defence shot down four Russian Shahed-136/131 that were trying to target energy infrastructure facilities in Dnipropetrovsk Oblast.

**Sources:** https://t.me/shepetivka/18011; https://t.me/khmelnytskaODA/1356

---


82 Like Shahed-136, these missiles contain Western components. Russia uses them in its systematic attacks on civilian objects in Ukraine. For more information, see: Enabling War Crimes? Western-Made Components in Russia’s War Against Ukraine, Joint report by NAKO and IPHR, available at: https://www.iphronline.org/wp-content/uploads/2023/02/Enabling-War-Crimes-report-final.pdf


86 City of Shepetivka, ‘Power engineers managed to stabilise the situation with the supply of electricity in the region’, 11 February 2023, available at: https://archive.ph/EmPLf.

87 Chas.News, ‘Kamikaze drone attack. Three aerial targets were shot down over Mykolaiv Oblast’, 10 February 2023, available at: https://archive.ph/CiBQ.
On the night of 8–9 March 2023, Russian forces attacked Ukrainian civilian infrastructure across Ukraine with eight Shahed-136/131 UAVs and 81 missiles,\(^8^8\) including Kh-101 and Kalibr.\(^8^9\) \(^9^0\)

In Zhytomyr Oblast, a UAV hit an energy infrastructure facility, leaving 150,000 civilian users without electricity and water until the evening.\(^9^1\)

Dnipropetrovsk Oblast meanwhile was attacked by UAVs, missiles and artillery fire, causing significant damage to the energy infrastructure and killing one civilian.\(^9^2\) Other UAVs were shot down over Kyiv and Sumy Oblast.\(^9^3\)

---


Case Study No. 8

DATE: 18 MARCH 2023
LOCATION: NOVOMOSKOVSK, DNIPROPETROVSK OBLAST
INCIDENT: ATTACK ON ENERGY INFRASTRUCTURE AND CIVILIAN HOUSES

On the night of 18 March 2023, Russian forces launched an attack with five UAVs on Novomoskovsk, Dnipropetrovsk Oblast. Two UAVs hit and significantly damaged a critical infrastructure object with oil products, destroyed four nearby civilian houses and damaged another six.

The General Staff of the Ukrainian Armed Forces confirmed that the attack was launched by a Shahed-136 UAV.

Sources: https://t.me/dneproperatyv/58470; https://t.me/dneproperatyv/58216

Case Study No. 9

DATE: 22 MARCH 2023
LOCATION: RZHYSHCHIV, KYIV OBLAST
INCIDENT: ATTACK ON TWO DORMITORIES AND A SCHOOL

Sources: https://t.me/dneproperatyv/58470; https://t.me/dneproperatyv/58216
On the night of 22 March 2023, Russian forces attacked Kyiv Oblast and Zhytomyr Oblast with 21 Shahed-136/131 UAVs. In Rzhyshchiv, Kyiv Oblast, the UAVs hit a school and two adjacent dormitories. Nine people were killed, and 29 more were injured, according to local officials. The attack partially destroyed one of the school buildings and the two dormitories, causing a massive fire. As a result of the attack and the fire, more than 200 people had to be evacuated from the area.

Source: Головне управління ДСНС України у Київській області


99 Coordinates of the impact sites: 49.965932798542696, 31.025156529844455.

100 The main department of the State Emergency Service of Ukraine in the Kyiv region, 'Work on the demolition of debris on the territory of the Rzhyshchiv Vocational Lyceum has been completed'; 23 March 2023, available at: https://kv.dsns.gov.ua/uk/pres-centr/news/nadzvicaini-podyi/roboti-po-razboru-zavaliv-na-teritoriyi-rzishhivskogo-profesiinogo-liceiu-zaverseno; Tsaplienko, 'Consequences of the attack in the Kyiv region'; 22 March 2023, available at: https://archive.ph/6jDGA.

101 NV, 'Details of the night attack near Kyiv. Russia hit dormitories and a school in Rzhyshchiv, three dead persons, people under the rubble'; 22 March 2023, available at: https://archive.ph/2Yk5; The main department of the State Emergency Service of Ukraine in the Kyiv region, 'Work on the demolition of debris on the territory of the Rzhyshchiv Vocational Lyceum has been completed'; 23 March 2023, available at: https://kv.dsns.gov.ua/uk/pres-centr/news/nadzvicaini-podyi/roboti-po-razboru-zavaliv-na-teritoriyi-rzishhivskogo-profesiinogo-liceiu-zaverseno; The main department of the State Emergency Service of Ukraine in the Kyiv region, 'At 12:52 on 23 March, work on the demolition of debris on the territory of the Rzhyshchiv Vocational Lyceum was completed'; 23 March 2023, available at: https://archive.ph/0wEe.

102 Andrii Nebytov, '9 dead persons, 9 injured and another 20 people were taken to the hospital with minor injuries'; 23 March 2023, available at: https://archive.ph/IEMD.


104 Suspilne.Media, 'The rescuers finished dismantling the rubble in Rzhyshchiv. What is known about the Shahed attack on Kyiv and the Kyiv region'; 23 March 2023, available at: https://archive.ph/Vwzu; Andrii Nebytov, 'Three people died, 7 people were injured as a result of drones hitting a dormitory building in one of the districts of Kyiv region'; 22 March 2023, available at: https://archive.ph/KMjPN.
DATE: 19–20 APRIL 2023
LOCATION: ODESA
INCIDENT: ATTACK ON A CHILDREN’S SUMMER CAMP

On the night of 20 April 2023, Russian forces attacked Odesa with 12 UAVs. Two drones targeted a children’s summer camp, causing a fire in one of its buildings. Odesa District Military Administration and Ukrainian air defence confirmed the use of the Shahed-136 UAVs, the remnants of which were found at the impact site.

Sources: https://t.me/odesacityofficial/16526; Operational Command “South” Facebook page

---


106 Coordinates of the impact site: 46.37653580320062, 30.73649621962206

107 Operational Command “South”, ‘At night, the enemy attacked Odesa with Shahed-131/136 kamikaze drones’, 18 April 2023, available at: https://archive.ph/LWuoA


Potential legal classification

The ten cases of Russian attacks on Ukrainian civilian and energy infrastructure analysed above are part of the broader pattern of Russian forces’ intentional terror campaign against the Ukrainian population. An attack on civilian infrastructure can only be justified if it is proved to represent a concrete military advantage. Even where a military objective is identified, the attack’s lawfulness is a question of proportionality – measured by pitting the concrete military advantage being sought against the harm that the attack causes to the civilian population. Where harm is disproportionate to the advantage being sought, the attack violates IHL and may amount to a war crime.

The Russian High Command has claimed that its attacks on civilian infrastructure are aimed against the “military command system of Ukraine and related energy facilities.”

The Ukrainian government, Ukrainian army representatives, and national and international military experts have said however that the Ukrainian Armed Forces are energy-autonomous and the Russian attacks on Ukrainian energy infrastructure do not affect either Ukrainian military capacity or its progress/advances on the battlefield. Thus, Russian attacks on Ukrainian energy infrastructure provide the Russian armed forces with very little, if any, military advantage.

As of February 2023, Russian forces have attacked some 250 energy facilities, mostly cogeneration plants and electricity substations, leaving more than ten million households without power. As of 31 January 2023, at least 116 civilians have been killed, and at least 379 more have been injured in

---

111 Additional Protocol I, Article 51(5)(b), Article 57(2)(a)(iii), Article 85(3)(a).
112 ICC Statute, Article 8(2)(b)(iv).
113 Ministry of Defence of Russia, statement of 18 November 2022, available at: https://t.me/mod_russia/21855.
115 Deputy Ministers of Defense, Hanna Malya, ‘The vast majority of enemy missile strikes have recently been aimed at energy infrastructure facilities’, 23 November 2022, available at: https://t.me/annamaliar/447
116 Focus, ‘Strikes on the power system: at the front, they know how to act - an expert’, available at: https://focus.ua/uk/voennye-novosti/534133-udyary-po-energosisteme-na-fronte-znayut-kak-deystvovat-expert
117 The Guardian, Kremlin decision to target Ukraine's cities was political, not tactical Dan Sabbagh Defence and security editor, 10 October 2022, available at: https://www.theguardian.com/world/2022/oct/10/kremlin-decision-to-target-ukraines-cities-was-political-not-tactical ; NYT, Kremlin decision to target Ukraine's cities was political, not tactical Dan Sabbagh Defence and security editor, 10 October 2022, available at: https://www.nytimes.com/2022/10/10/world/europe/russia-missiles-ukraine-civilians.html; NTA, ‘The main missile terror of Russia will begin when the real cold comes. Analyst thai Levin’, 1 November 2022, available at: https://www.nta.ua/igolovnyj-raketnyj-teror-rosiya-mozhe-pochaty-koly-pryjde-spravzhnij-holod-analityk-igal-levin/
these attacks. Without electricity, water and fuel, hundreds of healthcare facilities were unable to operate to their full capacity and the power outages posed severe risks to the lives of their patients, especially those dependent on electric life-support machines. As a result of Russian attacks on critical infrastructure, millions of people were at times deprived of access to clean water, heating and the ability to cook hot meals.

In addition to energy infrastructure, Russian armed forces have targeted residential buildings, a school, a children's summer camp and a delivery business, which on the face of it, are not of any military value. These attacks have claimed 14 civilian lives and injured at least another 36.

Comments by the Russian leadership and state propaganda illustrate that the attacks have aimed to terrorise the civilian population, retaliate against Ukrainian counter-attacks and put pressure on Ukrainian authorities to abandon their resistance. According to President Putin, attacks on the energy infrastructure will be “commensurate with the level of threat to the Russian Federation”. His press secretary later clarified that the attacks are part of Russia’s negotiation tactics, adding: “The unwillingness of the Ukrainian side to settle the problem, to start negotiations, its refusal to seek common ground – this is their consequence”. Members of the Russian parliament were more candid, calling on Ukrainian civilians to “rot and freeze” and describing the attacks as “necessary to destroy the Ukrainian state’s capacity to survive”. Consequently, there is a reasonable basis to believe that these attacks are aimed not at a substantial military advantage but at the civilian population. At the very least, the Russian attacks cause disproportionate harm to the civilian population to the military advantage being sought – harm which the Russian military and civilian leadership appear to disregard and even encourage.

IHL prohibits violence or threats, “the primary purpose of which is to spread terror among the civilian population.” Such tactics are also prohibited by the Russian Federation’s Military Manual.

The Shahed-136 is considered to be a guided weapon. It navigates using a combination of GPS and GLONASS, while a commercial-grade digital communication chip within it allows for a target's location to be updated mid-flight, or even for the intended target to be changed entirely while still in the air.

---


124 Ibid.

125 Russian President Vladimir Putin’s public speech after 10 October 2022 mass attacks on Ukrainian energy infrastructure available at: [https://archive.ph/02ZuU](https://archive.ph/02ZuU).


127 Francis Scarr, [@francis_scarr], I missed this last week: Russian MP Boris Chernyshov (who’s also one of the Duma’s deputy speakers) celebrating the “holy hatred” of missile strikes on Ukraine’s critical infrastructure and calling for ordinary Ukrainians to “freeze and rot” in their homes, Twitter, 26 November 2022, available at: [https://archive.ph/dhvTB](https://archive.ph/dhvTB).

128 Francis Scarr, [@francis_scarr], Russian MP Andrei Gurulyov says his country will “finish off” Ukraine’s power grid and then target its banking system “If we bomb the centre of their banking operations, they won’t be able to transfer anything anywhere, cards won’t work and people won’t get their paychecks”, Twitter, 28 November 2022, available at: [https://archive.ph/6IOK5](https://archive.ph/6IOK5).

129 Article 51(2) of Additional Protocol I; Article 33 of Geneva Convention IV.

Targets are selected and struck with precision, and it is therefore reasonable to assume that the case studies show the Shahed-136 impacting its intended and premeditated target, rather than experiencing any level of deviation.

In conclusion therefore, the Russian attacks on eight energy infrastructure objects across seven Ukrainian regions, ten residential buildings in Novomoskovsk, an office in Kyiv, a school in Rzhyschiv, a children’s summer camp in Odesa and a delivery business in Dnipro, on the face of it, represent grave breaches of IHL and may amount to the war crime of directing attacks against protected civilian objects.

Additionally, Russian attacks on some of these objects, particularly, energy infrastructure in Dnipropetrovsk and Vinnytsa regions, an apartment building in Kyiv, two dormitories in Rzhyschiv and a delivery business in Dnipro, which left 15 civilians dead and 42 more injured may amount to the war crime of directing attacks against civilians.

---

131 Additional Protocol I, Article 85(3)(a).
132 ICC Statute, Article 8(2)(b)(ii). The attack on a school in Rzhyschiv should be additionally qualified as an attack on specially protected object under Article 8(2)(b)(ix).
133 ICC Statute, Article 8(2)(b)(i).
PART THREE:

THE SHAHED-136 AND ITS RELIANCE ON WESTERN COMPONENTS
PART THREE: THE SHAHED-136 AND ITS RELIANCE ON WESTERN COMPONENTS

Usually given the name ‘Geranium’ inside Russia, the Shahed-136 is an Iranian-made ‘one-way attack’ (OWA) UAV, meaning each aircraft is used once to fly towards a designated target, detonating on impact. Amid Russia’s ongoing difficulties maintaining high-tempo missile strikes, the Shahed-136 has proved a key weapon in its arsenal. It is believed to have a range of up to 2,500km, using a combination of Global Navigation Satellite System and GLONASS to reach its intended target, while its warhead, at between 40 and 50 kg, is effective against soft, unprotected targets.

Dr Uzi Rubin, the former Director of the Israel Missile Defense Organization, previously described the Shahed-136’s “simplicity, combined with its almost uncanny accuracy, long range and low cost” as making it entirely unique as a strategic standoff weapon.

As RUSI has noted, this precision and range, combined with a small yet powerful warhead, renders the Shahed-136 for all practical purposes a “propeller-driven cruise missile”.

The origin of the Shahed-136 is uncertain, but Iran has been employing drones in its military operations since the 1980s. In recent decades, a range of new UAVs have been exhibited during annual Iranian military parades and the country is known to manufacture several types of drones. It has been alleged that the Shahed-136 was developed with Russian assistance and components.

| THE HESA SHAHED-136 AT A GLANCE |
|-------------------------------|------------------|
| Originated from               | Possessed by     |
| Iran                          | Iran, Russia     |
| Alternative names             | Class            |
| Geran-2/Geranium-2 in Russian possession | Loitering munition |
| Guidance system               | Length           |
| GNSS, INS                     | 3.5m             |
| Basing                        | Weight           |
| Rocket-assisted take-off       | 200 kg           |
| Wingspan                      | Range            |
| 2.5 m                         | allegedly 2,500 km |
| Speed                         | Engine           |
| 185 km/h                      | MD550 / 3W motors |
| Payload                       | In service       |
| ≈50 kg                        | 2019-2020        |
| Status                        | Operational      |

The origin of the Shahed-136 is uncertain, but Iran has been employing drones in its military operations since the 1980s. In recent decades, a range of new UAVs have been exhibited during annual Iranian military parades and the country is known to manufacture several types of drones. It has been alleged...
that these drones are then supplied to various groups including Hezbollah in Lebanon and Houthi rebels in Yemen. According to the Pentagon, Iranian-allied forces have utilised these drones in attacks against US military personnel in Syria, including one such attack in August 2022 against the US-run base at Tanf.\(^\text{135}\)

The Shahed-136, the most advanced of these drones, was first publicly named by Israel’s Prime Minister Naftali Bennett in September 2021.\(^\text{136}\) In July 2022, US National Security Advisor Jake Sullivan said the White House believed Iran was preparing to provide Russia with hundreds of drones, adding that Iran would also train Russian military personnel to use them.\(^\text{137}\)

In October 2022, the United States National Security Council told reporters that “a relatively small number” of Iranian trainers and technicians were in Crimea “to help the Russians use [the drones] with better lethality.” Russians remotely piloted the aircraft with Iranian personnel “assisting”.\(^\text{138}\)

While it is not known precisely how many Shahed-136s have been supplied to Russia, Ukraine’s intelligence services have claimed that Russia ordered approximately 2,400 of the type.\(^\text{139}\)

NAKO’s analysis of two different Shahed-136s, downed in Odesa and Cherkasy in 2022, revealed them as having a range of Western components originating from the US, Japan, Canada, and Switzerland. The type of components found inside the Shahed-136 vary, but it’s clear they provide a genuine and substantial contribution to its overall capability.


\(^{138}\) [https://www.washingtonpost.com/national-security/2022/10/20/russia-iran-kamikaze-drones/](https://www.washingtonpost.com/national-security/2022/10/20/russia-iran-kamikaze-drones/)

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>COMPANY</th>
<th>COMPONENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>Adesto Technologies</td>
<td>SPI Serial Flash Memory with Dual-I/O and Quad-I/O Support</td>
</tr>
</tbody>
</table>
|         | Analog Devices | RF Transceivers  
AD 12-Output Clock Generators with 2.8GHz VC  
Linear CMOS regulators with low drop  
16-bit analog-to-digital converters  
Output voltage/current drivers with output signal range |
|         | Freescale Semiconductor | Microprocessor |
|         | Hemisphere GNSS | Unidentified semiconductor |
|         | Hitec USA Group | High Voltage Giant Torque Servo |
|         | International Rectifier | Integrated circuit, buffer/line driver |
|         | Marvell Technology | Ethernet Transceivers |
|         | Maxim Integrated | Multichannel RS-232 Line Drivers and Receivers |
|         | Micrel Semiconductor | Low dropout linear regulators |
|         | Micron Technology | Parallel NOR Flash Memory  
Multilayer ceramic chip capacitor |
|         | MinMax Technology | Non-Isolated DC/DC Converter |
|         | ON Semiconductor | High speed CMOS octal bus buffer |
|         | Texas Instruments | Instrumentation amplifiers  
Microcontrollers  
Digital signal processors  
Dual output low dropout voltage regulators  
3- to 5.5-V single channel RS-232 line driver/receiver  
Dual-channel low-dropout voltage regulators  
Power modules |
| Japan   | Murata Manufacturing | Integrated circuits  
Point-of-load converters  
EMI/RFI Filters  
Non-Isolated DC/DC Converters |
| Canada  | Tallysman | GLONASS, GPS Ceramic Patch RF Antenna |
| Switzerland | STMicroelectronics | Microcontrollers  
Linear regulators |
All companies named above were invited to respond to concerns around the supply of their products to Russia and Iran.

A spokesperson for **Analog Devices** said: “As a global public company, Analog Devices is committed to complying with all applicable laws and regulations in the countries where we operate.

“Following Russia’s invasion of Ukraine, and in compliance with U.S. and EU sanctions, Analog Devices ceased business activities in Russia, and in the Russian-backed regions of Ukraine and Belarus, and promptly instructed all of our distributors to halt shipments of our products into these regions. Any post-sanctions shipment into these regions is a direct violation of our policy and the result of an unauthorized resale or diversion of ADI products.”

A spokesperson for **NXP Semiconductors** said: “We do not tolerate the use of our products in Russian or Iranian weapons, or any other application our products were not designed or licensed for. We continue to comply with export control and sanctions laws in the countries where we operate and we
do not support any business in or with Russia, Belarus, and other fully embargoed countries, including Iran. Our team is in ongoing contact with regulators around the world on this issue, as we explore additional measures to help neutralize illegal chip diversion.”

Micro-components made by Hemisphere GNSS, a US manufacturer based in Arizona.

A High Voltage Giant Torque Servo, a form of ultra-precise and efficient electrical motor, manufactured by Hitec USA Group.

Buffer line driver manufactured by International Rectifier, now part of Infineon.

Our previous report – ‘Enabling War Crimes? Western-Made Components in Russia’s War Against Ukraine’ – identified components bearing the name of Cypress Semiconductor, another company that has been acquired by Infineon, inside the Iskander, Kh-101, and Kalibr missiles.

Ethernet transceivers, allowing for point-to-point network and data transfer, manufactured by Marvell Technology. Components bearing the name of Marvell have previously been identified in Russia’s Kalibr cruise missile.
A spokesperson for Marvell said: “Marvell is appalled that any of its products are used in Russian weapons. Marvell does not sell to the Russian military or government. We have a strong export compliance program and have no knowledge how these parts have found their way into Russia.”

Microchip said: “Microchip does not sell products into countries where our technology is prohibited from sale such as Iran, Russia, Belarus, or sanctioned regions in the Ukraine. We condemn the illegal use of our products. We take our responsibility as a good corporate citizen seriously, and comply with applicable laws, including export controls and trade sanctions. We take care to maintain supply chain integrity by various methods including screening customers against restricted party lists. We also partner with government authorities and law enforcement, as necessary.

Microchip is a leading provider of smart, connected, and secure embedded control solutions with more than 120,000 customers across the industrial, automotive, consumer, aerospace and defense, communications, and computing markets. Our products have many possible customer applications. Distributors also sell our products into the marketplace.

Diversion of legally sold products is an industry-wide issue. Microchip is participating in a U.S. Industry Working Group led by the U.S. Department of Commerce Bureau of Industry and Security to further discuss these matters. For more information, see the Semiconductor Industry Association (SIA) statement titled Semiconductor Industry is Committed to Combatting Illicit Chip Diversion. Microchip is a member of SIA and our CEO is on the SIA board of directors.”
A spokesperson for Texas Instruments said: “TI is not selling any products into Russia, Belarus or Iran. Ti stopped sales to Russia and Belarus at the end of February 2022, and we no longer support sales there. TI complies with applicable laws and regulations in the countries where we operate. We do not support or condone the use of our products in applications for which they weren’t designed.”
A spokesperson for Tallysman said: “We were made aware and agree that some of our components have been misused in sophisticated military guidance systems in Ukraine. Tallysman is 100% committed to supporting Ukraine in the face of Russian aggression. Tallysman produces GNSS (also known as GPS) patch elements, that are highly desired globally for positioning, navigation, and timing systems. The Tallysman ceramic patch antennas recovered are typical of what can be found in a consumer Satnav device. They are normally used for survey equipment, precision agriculture, timing systems, fleet management, and many other applications. Tallysman has been and will continue to be fully compliant and cooperative with all Canadian and international agencies and export controls. Unfortunately, products like antennas, printed circuit boards, semiconductors, resistors, capacitors, screws, wires, etc., with significant engineering effort can be used for malevolent purposes and unintended applications. To the extent possible for a product sold globally, we examine and review end customer identities and intended end uses. We are hyper vigilant about what products we sell to whom.”
RECOMMENDATIONS
RECOMMENDATIONS

As detailed throughout this report, the Shahed-136, containing Western-made components, has been used to carry out what are suspected to be war crimes in Ukraine. The supply and maintenance of Russia’s weapons is a key vulnerability in its campaign against Ukraine, and it is the duty of policymakers and businesses to exploit this vulnerability.

In light of this report’s findings, the authors offer the following recommendations:

1. **Sanctions and embargoes**: Countries should consider implementing further targeted sanctions or embargoes on specific individuals, entities, or sectors involved in the transfer of Western components to Russia’s military-industrial complex. These measures should be implemented in coordination with like-minded countries to maximise their impact.

   Moreover, it is clear that such sanctions require greater monitoring and enforcement in order to truly be effective. This is an area where governments can cooperate effectively with civil society, NGOs, and think tanks. Western companies and NGOs have easily available open-source intelligence tools at their fingertips, whether they are commodity trading platforms or automatic identification system-based vessel tracking websites. These tools empower watchdog organisations and risk assessment committees in governmental and non-governmental organisations to monitor malign transfers of products and technologies that would undermine sanctions efficacy.

2. **Strengthen export controls**: Countries should enhance their export control mechanisms and regulations to restrict the transfer of sensitive military technology and components to Russia. This includes stricter scrutiny of export licences and a comprehensive review of end-user certificates. These countries should also study the supply chain to prevent the export of Western components from third countries to Russia.

3. **Company due diligence**: Companies must exercise greater diligence in assessing the ultimate purpose for which their products are utilised, as emphasised in the United Nations Guiding Principles on Business and Human Rights. It is strongly recommended that companies carefully consider the conclusions presented in these reports and acknowledge the possible material risks associated with future products.

For companies engaged in cross-border transactions involving items that are restricted under Russia-related export controls, it is prudent to implement a compliance policy reasonably designed to prevent, deter, and detect violations. Such a policy and related procedures should cover:

- Screening of counterparties against U.S. sanctions- and export control-related restricted party lists;
- Identification of export-controlled products and implementation of related internal controls;
- Training of employees; and
- Periodic testing of the functionality of the compliance program.140

---

140 TechCrunch, Western sanctions against Russia: Tips for tech companies managing compliance risk, 08 May 2023, available at: https://techcrunch.com/2023/05/08/western-sanctions-against-russia-tips-for-tech-companies-managing-compliance-risk/
Regarding third-party diversion risk in particular, companies can take the following steps:

- Conduct reasonably robust due diligence on third parties such as resellers, distributors, and sales agents;
- Obtain from counterparties “end-user certificates,” confirming the intended end-use and end-user of the products;
- Incorporate compliance-related terms into contracts with counterparties; and
- Conduct periodic audits of sales/distribution channels.141

Ignorance as to a product’s end-user should not be relied upon as a moral or legal defence.

4. **Diplomatic efforts:** An international, and solution-focused conversation to examine ways in which the flow of western-made components can be ceased. Governments, political leaders, and businesses alike have a duty to engage with this conversation and explore solutions.

---

141 TechCrunch, Western sanctions against Russia: Tips for tech companies managing compliance risk, 08 May 2023, available at: https://techcrunch.com/2023/05/08/western-sanctions-against-russia-tips-for-tech-companies-managing-compliance-risk/
ABOUT THE AUTHORS

IPHR

International Partnership for Human Rights (IPHR) is an independent, non-governmental organisation founded in 2008. With a presence in Brussels, Kyiv, and Tbilisi, IPHR works closely with civil society groups in Eastern Europe, South Caucasus, and Central Asia to raise human rights concerns at the international level and promote respect for the rights of vulnerable communities. IPHR has been documenting atrocity crimes committed in the context of Russia’s war on Ukraine since 2014 and has been using collected evidence for accountability purposes.

www.iphronline.org

NAKO

The Independent Anti-Corruption Commission (NAKO) is a voluntary, non-profit, non-partisan organisation pursuing the goals of minimising opportunities for corruption in Ukraine’s defence sector through strong research, effective advocacy, and increased public awareness. NAKO was established as a program of the Transparency International Defence and Security program in 2016 and since then has evolved as a self-standing organisation within the Transparency International global movement.

www.nako.org.ua

TRUTH HOUNDS

Truth Hounds is a team of experienced human rights professionals documenting war crimes and crimes against humanity in conflict contexts since 2014. Truth Hounds fights against impunity for international crimes and grave human rights violations through investigation, documentation, monitoring, advocacy and problem solving for vulnerable groups. Truth Hounds documenters mobilise all available resources and documentation methodology to create a systemic approach to its documentation work, and promote accountability for grave human rights abuses and international crimes.

https://truth-hounds.org

GLOBAL DILIGENCE

Global Diligence LLP is a partnership of established international lawyers with practical experience of living and working in high-risk areas. Global Diligence team advises and represents States, businesses, organisations, or individuals on international criminal law and human rights. Focused on challenges in unstable and conflict-affected regions, Global Diligence provides mapping, training, and project management for capacity building programs.

https://www.globaldiligence.com