Enabling War Crimes?

Western-Made Components in Russia's War Against Ukraine

IPHR International Partnership for Human Rights

NAKO TI UKRAINE • TI-DS

Contents

Executive Summary 5

Part one 7
Suspected War Crime Case Studies

Part two 23
The Western Components at
the Heart of Russia's War Crimes

Part three 33
Tracking the Trade:
How Components Reach Russia

Recommendations 36

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

Legal Disclaimer

This document has been prepared for informational purposes only (the 'Permitted Purpose'). While all reasonable care has been taken to ensure the accuracy of information in this report (the 'Information'), we make no representations or warranties of any kind with respect to the Information.

You should not use, reproduce or rely on the Information for any purpose other than the Permitted Purpose stated above. Any reliance you place on the Information is strictly at your own risk. If you intend to use the Information for any other purpose (including, without limitation, to commence legal proceedings, take steps or decline to take steps or otherwise deal with any named person or entity), you must first undertake and rely on your own independent research to verify the Information.

To the fullest extent permitted by law, we shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of any of the Information by you or any third party.

The purpose of this report is to explain and illustrate how western made components are used in the Russian committing of suspected war crimes in Ukraine.

To achieve this, the 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 are 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 we 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 and/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.

The existence of counterfeit components is a recognised global problem. We recognise the possibility that components featuring the logos and/or branding of named entities may not have indeed been manufactured by said entities. However, given a) leaked Russian "shopping lists" showing the intent to acquire components manufactured by such companies in order to support its military[1], and b) the history of Soviet and Russian military procurement efforts targeting leading global technology companies, we have worked on the assumption that components we and third parties have identified are genuine.

Methodology

In preparing this report, a dataset of more than 170 individual components that had been found in Russian equipment and bore the branding or logo of foreign companies was compiled. This was sourced from open-source media, our own examination of components and expended equipment, and the research of 3rd party groups such as the Royal United Services Institute. This work provided a clear picture as to the equipment most reliant upon foreign components.

This was then married with a dataset of suspected war crimes committed by Russia in Ukraine. In each case, video and image evidence was documented, geolocated, and archived. The weapon understood to have been used in the attack was specified. Where ascertaining the weapon used could not be done with a high degree of confidence, the incident was removed from the dataset. Those suspected war crimes committed with weapons not found in our initial dataset were removed, resulting in over 400 examples of suspected war crimes committed using weapons understood to be, to varying degree, reliant upon foreign-made components.

Following this, specific case studies were selected for inclusion in this report, factoring in the available evidence.

Trade data was examined using open-source evidence. While trade data provides insight as to unit volume, value, and category, it cannot with precision determine the exact product(s) involved.

1 POLITICO, 'The chips are down: Putin scrambles for high-tech parts as his arsenal goes up in smoke', 5 September 2022. Available at: https://www.politico.eu/article/the-chips-are-down-russia-hunts-western-parts-to-run-its-war-machines/

Executive Summary

In the months following Russia's full scale invasion of Ukraine, we have worked to document hundreds of suspected war crimes and human rights atrocities carried out by Russian forces. Where suspected crimes are committed – whether the deliberate targeting of civilian infrastructure or attacks against residential areas – these are investigated thoroughly by analysts and researchers on the ground, and added to multiple databases. In many cases, it has even been possible to, through analysis of video footage, wreckage, and elements of expended munitions, ascertain the type of Russian weapon used in each attack. These facts too have been documented on an ongoing basis throughout the full scale invasion.

We have concurrently, alongside media organisations such as Reuters and other think tanks such as the Royal United Services Institute (RUSI), sought to uncover the extent to which these Russian weapons are reliant upon western-made components. Now one year on from the full scale invasion, it is clearer than ever that western-made components have and continue to be imported into Russia and be used inside weapons involved in the committing of suspected war crimes and human rights atrocities.

Analysing datasets of both suspected war crimes and components found in the weapons used to commit them, we have analysed the very fabric of a Russian attack, by first examining chosen case studies of suspected war crimes, followed by the weapon used in each case study, before finally identifying the components found in such weapons and the branding on them.

Where examining the branding of components, or analysing third party research, we have been mindful of the existence of counterfeits. We recognise the possibility that components featuring the logos and/or branding of named entities may not have indeed been manufactured by such entities. That said, given a) leaked Russian "shopping lists" showing the intent to acquire components manufactured by such companies in order to support its military[2], and b) the history of Soviet and Russian military procurement efforts targeting leading technology companies, we have worked on the assumption that components we and third parties have identified are genuine.

The suspected war crimes identified focus on the targeting of civilian infrastructure, such as residential buildings, power plants, businesses, and bridges. In each instance, we have explored the circumstances around the attack, the result of it, including the level of damage and casualties, and the means by which we have identified the weapon used to carry out such an attack.

We have then examined the extent to which each weapon involved in the suspected war crime is, 'under the hood', reliant upon western-made components in order to function. The result that follows is an uncomfortable truth for both businesses and corporations alike: western-made components have been and continue to be used within weapons involved in Russian suspected war crimes. The supply networks that facilitate this, while convoluted and deliberately opaque, are also becoming clearer.

2 POLITICO, 'The chips are down: Putin scrambles for high-tech parts as his arsenal goes up in smoke', 5 September 2022. Available at: https://www.politico.eu/article/the-chips-are-down-russia-hunts-western-parts-to-run-its-war-machines/

This report also examines trade data that evidences manufacturers exporting to Russia since the full scale invasion, in some cases to the tune of millions of dollars. While this trade data provides insight as to unit volume, value, and product category, it cannot with precision determine the exact product(s) involved. It is therefore not possible to analyse the legal background to continuing this trade. Rather, in light of the suspected war crimes detailed throughout this report and the weapons used, we query said manufacturers' ethical and moral judgement.

The beginning of the solution is to recognise that the problem exists. Up to now, businesses and policymakers alike have remained predominantly silent on this issue. This has been justified, at least in part, by the fact that the causes of the situation faced – western-made components being found in Russian equipment – 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

Suspected War Crime Case Studies

Part one
Suspected War Crime Case Studies

International humanitarian law (IHL) establishes several core principles aimed at protecting the civilian population, individual civilians and civilian objects during armed conflicts. The *principle of humanity* forbids the infliction of suffering, injury, or destruction not necessary for achieving a legitimate military purpose. The *principle of distinction* stipulates that civilian objects shall not be the object of attack or reprisals.[3] IHL defines civilian objects as all objects which are not military objectives,[4] including residential areas, dwellings, buildings, and houses.[5] Both deliberate[6] and indiscriminate[7] attacks against civilian objects constitute grave breaches of the Geneva Conventions and its Additional Protocol I,[8] and may be prosecuted as war crimes.[9] The authors of this report selected ten cases of attacks on civilian infrastructure by Russian guided missiles resulting in 70 civilian deaths and destruction or damage to more than 80 civilian objects, which may constitute grave breaches of IHL and war crimes.

Additional investigations would be required to corroborate these allegations to a judicial standard.

Attacks on civilian objects with Iskander missiles

Case study one

Date: 17 August 2022

Location: Kharkiv, Ukraine

Incident: Attack on a civilian dormitory

On 17 August 2022, the Russian army shelled civilian infrastructure in Kharkiv, Ukraine. The shelling damaged the cultural centre in the Kholodnogorsky district, a tram depot in the Slobodsky district and a civilian dormitory for people with hearing impairments in Saltivskyi district.[10] 18 civilians, including a 11-year-old child, were killed as a result of the shelling of the dormitory. Their bodies were found under the rubble[11].

The State Emergency Service of Ukraine discovered Iskander missile fragments on the site of the shelling[12]. Later, Kharkiv Police stated that it was able to confirm the use of the Iskander missile in tha

3 See Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts of 8 June 1977 ('Additional Protocol I'), Articles 51, 52, 57; ICRC, How Does Law Protect in War, Online Casebook. Available at: https://casebook.icrc.org/glossary/fundamental-principles-ihl
4 Additional Protocol (I) to the Geneva Conventions of 1977, Article 52(1).
5 Rule 9 of customary IHL.
6 To classify the perpetrator's actions as a deliberate attack against a civilian object, it is important to establish that the perpetrator carried out an attack against a civilian object; it was deliberate; and that the targeted civilian object was not a military objective. See: Elements of Crimes, Article 8(2)(b)(ix) War crime of attacking protected objects
7 Indiscriminate attacks are attacks that strike military objectives and civilian objects without distinction. Additionally, attacks which may be expected to cause incidental loss of civilian life, injury to civilians and/or damage to civilian objects which would be excessive in relation to the anticipated military advantage should also be considered indiscriminate attacks. See: Additional Protocol I, Article 51(4)(a)–(c); Article 57(2)(a)(iii); Article 85(3)(b).
8 Additional Protocol I, Article 85(3)(a).
9 ICC Statute, Article 8(2)(b)(iv) and Article 8(2)(b)(i)/(ii).
10 Suspilne.Media, 'People with hearing impairments lived in a Kharkiv dormitory hit by a Russian missile on August 17', 18 August 2022. Available at: https://archive.ph/1IOW6
11 Kharkiv City Council, 'At the site of the shelling of the dormitory on Akhiezeriv Street, rescuers today found three more bodies', 20 August 2022. Available at: https://archive.ph/7yTNP;
12 Suspilne.Media, 'Fragments of a Russian Iskander rocket were seized from under the rubble of a dormitory in Kharkiv: photo', 19 August 2022.

attack on the dormitory based on the marks discovered on the missile fragments found at the site. According to the Head of Kharkiv Police, the marks inspection also revealed that the missile was manufactured in Russia in 2020.[13]

The State Emergency Service of Ukraine removed the remnants of a missile from the territory of a dormitory in the Saltovsky district of Kharkiv. 19 August 2022. Source: Suspilne Kharkiv

Available at https://archive.is/TLnv3

13 Suspilne.Media, 'Police: Russia hit a dormitory in Saltivka in Kharkiv with Iskander', 18 August 2022. Available at https://archive.is/wSUXx

Case study two

Date: 26 September 2022

Location: Pervomayskiy, Kharkiv Oblast, Ukraine

Incident: Attack on private civilian houses

Russian armed forces carried out missile attacks on several districts in Kharkiv Oblast on 26 and 27 September 2022.[14] The most damaging of these attacks happened in Pervomayskiy, where a missile hit private homes in a residential area and killed seven individuals, including a 15-year-old child.[15]

Kharkiv Oblast police made an official statement, claiming that it discovered fragments of an Iskander M missile on the site of the attack, where rescuers found seven civilian bodies buried under the rubble.[16]

The fragments of the Iskander missile retrieved at Pervomayskiy, 26 September 2022. Source: Sergei Bolvinov, head of the investigative department of the National Police in the Kharkivs'ka oblast

14 CNN, 'At least 1 dead after Russian missile and artillery attacks in eastern Ukraine, Ukrainian officials say', 26 September 2022. Available at: https://archive.ph/rtg6X; Reuters, 'Explosions heard, power out in Ukrainian city of Kharkiv', 27 September 2022. Available at: https://archive.ph/VuGd9

15 Ukrainska Pravda, 'Attack on Pervomayskiy: 7 people killed', 26 September 2022. Available at: https://archive.ph/NaInK

16 Sergey Bolvinov, 'Russian servicemen launched a missile attack on a civilian infrastructure facility in the town of Pervomaisky', 26 September 2022. Available at: https://tinyurl.com/yer9xczu

Case study three

Date: 1-2 February 2023

Location of impact: Kramatorsk, Donetsk Oblast, Ukraine

Incident: Attack on eight apartment buildings

Over the period of 1 – 2 February 2023, Russian forces attacked residential buildings in the centre of Kramatorsk with missiles. In the afternoon of 2 February 2023, two more missile attacks followed.[17] Donetsk Regional Administration announced that on the night of the 1 February 2023, the city was attacked with an Iskander missile, and the next two attacks used S-300 missile systems.[18]

According to the police, the Iskander missile attack caused damage to eight civilian apartment buildings, three civilians were killed and 20 more were wounded.[19] The fragments of the Iskander missile were later retrieved by the rescuers from under the rubble.[20]

Fragments of the Iskander missiles near a residential building destroyed by the Iskander strike on Kramatorsk, 2 February 2023. Source: Radio Svoboda.

Potential legal classification

The three attacks analysed above were perpetrated against private civilian houses and apartment buildings located in residential neighbourhoods, claiming 28 civilian lives. The weapons used for these attacks were guided ballistic Iskander missiles. Iskander-M missiles have an accuracy range of 10 to 30 metres.[21] As such, Russian armed forces clearly intended to target these civilian objects. There is no information to suggest that the targeted private houses and apartment buildings or their vicinity were used by the Ukrainian military in any way. In the absence of a military objective,[22] the targeted buildings were civilian objects and fell under IHL protection. Considering the above, these three incident represent a grave breach of IHL[23] and may constitute war crimes of attacking civilians/civilian objects.[24]

17 Reuters, 'Russian missile destroys Ukrainian apartment building; at least 3 dead', 2 February 2023. Available at: https://archive.ph/emcf6
18 Pavlo Kirilenko, "The search and rescue operation on the ruins of a house in Kramatorsk", 3 February 2023. Available at: https://archive.ph/thfRy
19 The Police of Donetsk Oblast, 'More than 100 police officers are working at the scene of a missile strike in Kramatorsk', 2 February 2023. Available at: https://tinyurl.com/3z8ctzvt
20 RFE/RL, 'Iskander strike on a residential building in Kramatorsk: consequences', 2 February 2023. Available at: https://archive.ph/ayw3p
21 MDAA, Iskander-M (SS-26). Available at: https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/iskander-m-ss-26/
22 A military objective is any object that by its nature, location, purpose or use makes an effective contribution to military action and whose partial or total destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage. See: Additional Protocol (I) to the Geneva Conventions of 1977, Article 52(2).
23 Additional Protocol I, Article 85(3)(a).
24 ICC Statute, Article 8(2)(b)(i)/(ii)

Attacks on civilian objects with Kh-101 (X-101) missiles

Case study one

Date: 11 September 2022

Location: Kharkiv TEC-5 Power Plant, Podvirky, Kharkiv Oblast, Ukraine

Incident: Attack on Kharkiv TEC-5 Power Plant

On 11 September 2022, Russian forces attacked the TEC-5 power plant near Kharkiv. The attack resulted in widespread power outages in Kharkiv, Dnipro, Sumy and Poltava regions.[25] The attack damaged the building of the power plant and killed two power plant workers.

According to the Kharkiv police, it discovered Kh-101 missile remnants on the site of the attack.[26]

Kh-101 missile fragments retrieved by the Ukrainian police, 12 September 2022. Source: Serhiy Bolvinov/ Facebook.

25 The Guardian, 'Russian strikes knock out power and water in Ukraine's Kharkiv region', 11 September 2022. Available at: https://archive.is/IKpbd#selection-921.0-928.0; Slovo i Dilo, 'At the damaged power plant in the Kharkiv region the wreckage of the Russian Kh-101 missile was found', 12 September 2022. Available at: https://archive.ph/Ci8gz

26 Serhiy Bolvinov, 'As everyone knows, yesterday the Rashists shelled critical infrastructure facilities...',12 September 2022. Available at: https://tinyurl.com/ykfx3du3

Case study two

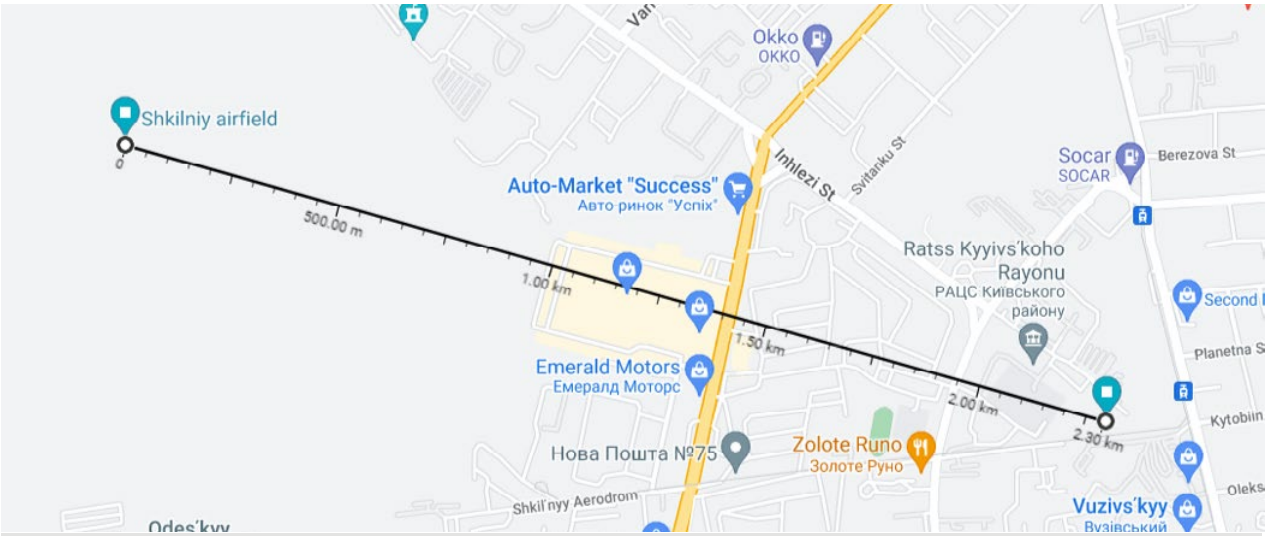
Date: 23 April 2022

Location: Odesa, Odesa Oblast, Ukraine

Incident: Attack on a 15-story apartment building

On 23 April 2022, Ukrainian authorities reported that Russian TU-95 bombers launched multiple Kh-101 and/or Kh-555 missile attacks on Odesa from the Caspian Sea.[27] The missiles hit a military facility and 15-story apartment building located more than two kilometres away from the facility.[28] The attack on the apartment building called Tiras killed eight civilians, including a 3-month-old baby, and injured at least 18 more[29]. At least 30 apartments were destroyed and 60 more damaged.[30]

Russia's Ministry of Defence stated the target was a 'logistics terminal at a military airfield,' which it claimed was holding a large shipment of foreign weapons.[31] The potential military target closest to the damaged Tiras apartment building is the Shkilnyi airfield (46°25'09.7"N 30°41'46.4"E) which, according to some media, was attacked on that day.[32] The airfield is located 2.3 kilometres away from the Tiras apartment building.[33]



Distance from the Shkilnyi airfield to the Tiras apartment building is approximately 2.3 kilometres.
Source: Google Maps

27 Kyiv Post, 'Russian missile strike on Odesa: residential district hit for first time, five dead', 23 April 2022. Available at: https://archive.ph/pk47p; See also: Air Command "South" Facebook announcement of 23 April 2022. Available at: https://tinyurl.com/3myvpv86

28 Tiras apartment block location: Akademika Korolyova Street 5/4 (46°24'49.3"N 30°43'30.3"E); The New York Times, 'Missiles hit a residential neighbourhood in Odesa, killing at least six, officials say', 23 April 2022. Available at: https://archive.ph/5nL0v; NV, "The only goal is terror." The Russian Federation launched missile strikes on Odesa - all that is known about the occupants' attack , which killed eight people, 23 April 2022. Available at: https://archive.is/BzECY

29 CNN, '8 dead in Russian missile strikes in Southern Ukraine, Odesa mayor says', 24 April 2022. Available at: https://archive.is/sMzb1

30 Odesa.Oficially, 'The occupiers hit a three-story residential building in Saltivka with a Russian Iskander missile', Telegram: @odesacityofficial, 20 May 2022. Available at: https://archive.is/SYfJH

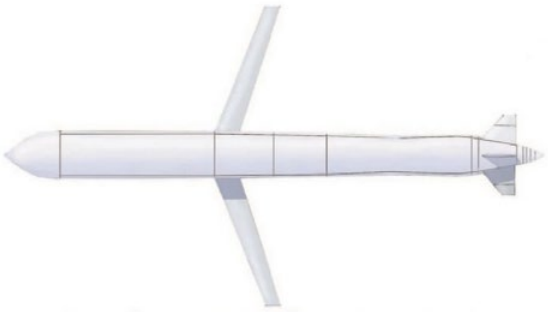
31 Interfax, 'The Ministry of Defense of the Russian Federation reported on strikes on a military airfield near Odesa', 23 April 2022. Available at: https://archive.ph/d1B1B

32 The Page, 'Rocket attack on Odesa: six dead, 18 injured (photo, video) – UPDATED', 23 April 2022. Available at: https://archive.is/DdahZ; Odessa. Officially, 'Official statement of the Operational Command "South":', Telegram: @odesacityofficial, 30 April 2022. Available at: https://archive.is/oLmDc

33 Odesa.Oficially, 'On April 23, two sections of the Tiras Residential Complex were damaged as a result of the missile attack on Odesa', Telegram: @ odesacityofficial, 20 May 2022. Available at: https://archive.is/SYfJH#selection-237.0-241.1; Suspilne.Media, 'As a result of the rocket attack, eight apartments were damaged in the Odesa residential complex. PHOTO', 25 April 2022. Available at: https://archive.is/nyRPU

Video footage posted on social media captured a missile with unfolding wings and tail parts flying in the sky above Odesa.[34] The missile's outline resembles a Kh-101 that hit the residential buildings.

The screenshot from a video of what matches the technical characteristics of a Kh-101 missile flying towards Odesa, 23 April 2022. Source: Ukraina Seichas[35]



Schematic representation of the X-101 missile. Source: Focus.ua

Photos of missile fragments were also published by Oleksiy Honcharenko, a member of the Ukrainian parliament.[36] The lower right corner of the missile fragment contains digits "...648382...". Conflict Armament Research has indicated in its report on Kh-101 missiles that all missiles that they studied were labelled with a number that contained either "648" or "263"[37] (see example below in Case study 3). Thus, it is highly likely that the missile used in the attack was Kh-101 and not Kh-555.

Fragment of the Kh-101 missile, Odesa, 23 April 2022. Source: Oleksiy Honcharenko.

34 Unian, 'The missile attack on Odesa: photos of the consequences and details have emerged', 23 April 2022. Available at: https://archive.ph/nUiV1
35 Ukraina Seichas, 'Sky over Odesa', 23 April 2022. Available at: https://archive.ph/wolDa. Archived video: https://tinyurl.com/yckwtbhj
36 Oleksiy Honcharenko, 'Rocket fragments landed in a cemetery in Odesa', 23 April 2022. Available at: https://t.me/oleksiihoncharenko/19785
37 Conflict Armament Research, 'Dating newly-produced Russian missiles used in Kyiv attacks', December 2022. Available at: https://archive.ph/6ZTRY

Case study three

Date: 10 October 2022

Location: Kyiv, Ukraine

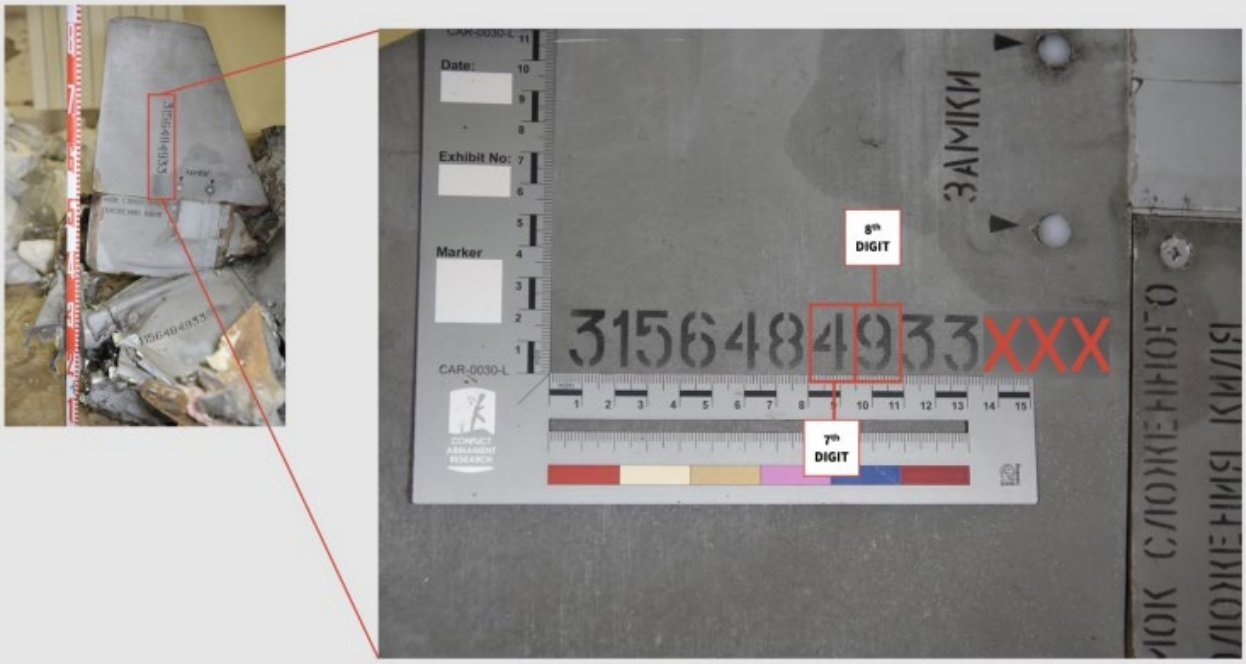
Incident: Mass attack on Kyiv civilian infrastructure

On 10 October 2022, Kyiv and a number of other Ukrainian cities were hit by a series of missile and drone strikes, leaving at least 23 civilians dead and more than 100 injured[38]. It was one of the largest missile attacks since the beginning of the Russian full scale invasion that targeted primarily civilian sites and energy infrastructure, which caused major power and water shortages across Ukraine[39]. In Kyiv alone, seven people were killed and 49 were injured. Vitaliy Klitschko, the Mayor of Kyiv, reported that 45 residential buildings, three schools, a kindergarten, five medical facilities, and the building that houses the German consulate were damaged[40]. These attacks were widely condemned by the international community.[41]

Ukrainian Air Force Command estimated that on that day, Russian forces launched 83 missiles including Kh-101, Kh-555, Kalibr, Iskander, S-300 and Tornado MRLS.[42] A Bellingcat investigation confirmed the use of Kh-101, Kalibr and Iskander missiles in the 10 October attacks.[43]

One of the missiles hit a pedestrian bridge in downtown Kyiv. The moment of the strike was captured by surveillance cameras. The video shows a civilian narrowly escaping the strike.[44] A Conflict Armament Research team that visited the site after the strike found and analysed fragments of the missile used in this attack and confirmed that it was a Russian-made Kh-101 missile, produced in 2018.[45]

38 Kyrylo Tymoshenko, "Civilian casualties as a result of the armed aggression of the Russian Federation on 10.10.2022", 11 October 2022. Available at: https://archive.ph/RLT1o
39 CBS News, 'Russia rains missiles down on Ukraine's capital and other cities in retaliation for Crimea bridge blast', 10 October 2022. Available at: https://archive.ph/hykrB
40 BBC, 'Russia has launched massive missile strikes throughout Ukraine', 10 October 2022. Available at: https://archive.ph/VL3oi
41 AP, 'UN, G7 decry Russian attack on Ukraine as possible war crime', 12 October 2022. Available at:https://archive.ph/J5hEn; Bloomberg, 'Biden Condemns 'Utter Brutality' of Russian Strikes on Civilians', 10 October 2022. Available at: https://archive.ph/qesht; Reuters, 'EU condemns 'barbaric' Russian missile attacks, warns Belarus', 10 October 2022. Available at: https://archive.ph/maQOV
42 Ukrainska Pravda, 'The Air Force clarifies what Russia used during 10 October attack', 10 October 2022. Available at: https://archive.ph/o8lx3
43 Bellingcat, 'The Remote Control Killers Behind Russia's Cruise Missile Strikes on Ukraine', 24 October 2022. Available at: https://archive.ph/5x5xy
44 BBC, 'Kyiv bridge: Near miss for pedestrian in missile strike', 10 October 2022. Available at: https://archive.ph/F0dsW
45 Conflict Armament Research, 'Dating newly-produced Russian missiles used in Kyiv attacks', December 2022. Available at: https://archive.ph/6ZTRY



Part of a Kh-101 missile recovered after the 10 October 2022 attack on Kyiv's Klitschko bridge. December 2022. Source: Conflict Armament Research.

Potential legal classification

The three 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 Ukrainian authorities and population. An attack on civilian infrastructure can only be justified if it 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[46] and amounts to a war crime.[47]

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".[48] However, by the end of November 2022, Russia had hit at least 200 energy infrastructure targets across the country, leaving up to 10 million households without power.[49] At least 77 civilians have died in these attacks and 272 more have been injured.[50] There is no evidence to suggest that all targeted infrastructure was linked to the Ukrainian military or decision-making centres. In addition to energy infrastructure, Russian armed forces have targeted residential buildings, schools and hospitals which on the face of it are not military objects.

Furthermore, comments by the Russian leadership and state propaganda suggest that the intention behind the attacks was to terrorise the civilian population, retaliate for Ukrainian counter-attacks

46 Additional Protocol I, Article 85(3)(a).
47 ICC Statute, Article 8(2)(b)(iv)
48 Ministry of Defence of Russia, statement of 18 November 2022. Available at: https://t.me/mod_russia/21855.
49 Human Rights Watch, "Ukraine: Russian Attacks on Energy Grid Threaten Civilians", 6 December 2022. Available at: https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians.
50 Human Rights Watch, "Ukraine: Russian Attacks on Energy Grid Threaten Civilians", 6 December 2022. Available at: https://www.hrw.org/news/2022/12/06/ukraine-russian-attacks-energy-grid-threaten-civilians

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".[51] His press secretary clarified that the attacks are part of Russia's negotiations tactics, stating: "The unwillingness of the Ukrainian side to settle the problem, to start negotiations, its refusal to seek common ground – this is their consequence".[52] Members of the Russian parliament were more candid, calling on Ukrainian civilians to "rot and freeze"[53] or describing the attacks as "necessary to destroy the Ukrainian state's capacity to survive".[54] State media personalities went further, admitting that the attacks are aimed at terrorising civilians.[55] Consequently, there is a reasonable basis to believe that these attacks are not aimed at a concrete military advantage, but rather at the civilian population.

IHL prohibits violence or threats, "the primary purpose of which is to spread terror among the civilian population."[56] Such tactics are also prohibited by the Russian Federation's Military Manual.[57]

The Kh-101 that was used in the analysed three cases is a high-precision guided missile. According to weapons analysts, the Kh-101 uses a Russian satellite navigation system for trajectory correction and has an accuracy range of five to six metres.[58] According to Bellingcat's findings, its flight path requires customised individual pre-flight planning, including simulation of the complete flight path from the launch site to the target.[59] Consequently, it is highly likely that the Russian attacks on the TEC-5 power plant in Kharkiv Oblast, the pedestrian bridge in Kyiv and the apartment building in Odesa were intentional.[60] These attacks targeted civilian objects and are therefore grave breaches of IHL.[61] Furtheremore, the attack on the TEC-5 power plant may constitute a war crime of excessive incidental death, injury or damage;[62] the attack on the apartment building in Odesa may constitute a war crime of attacking civilians/civilian objects;[63] and the attack on the pedastrial bridge in Kyiv may constitute a war crime of attacking a civilian object.[64]

Additionally, other Russian attacks on Kyiv civilian infrastructure of 10 October 2022, including 45 residential buildings, three schools, a kindergarten, five medical facilities, and the German consulate, which left seven civilians dead and 49 more injured, involved some or all of the following high-precision missiles – Kh-101, Kh-555, S-300, Kalibr, Iskander and Tornado missiles. Considering the above, these attacks represent a grave breach of IHL[65] and may constitute a war crime of attacking civilians/civilian objects.[66]

51 Russian President Vladimir Putin's public speech after 10 October 2022 mass attacks on Ukrainian energy infrastructure available at: https://t.me/RVvoenkor/28579.
52 The Moscow Times, "Civilians suffering as a 'Consequence' of Kyiv's Refusal to Negotiate", 17 November 2022. Available at: https://www.themoscowtimes.com/2022/11/17/civilians-suffering-as-a-consequence-of-kyivs-refusal-to-negotiate-kremlin-a79412.
53 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://twitter.com/francis_scarr/status/1596417788616536064
54 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://twitter.com/francis_scarr/status/1597149654793478144.
55 Russian Media Monitor, Russian lawmakers advocate freezing and starving Ukrainian civilians, turning them into refugees, 19 October 2022. Available at: https://www.youtube.com/watch?v=10AiNAsCnkw; Russian Media Monitor, Top Russian propagandists worry they might be tried at the Hague, 29 November 2022. Available at: https://www.youtube.com/watch?v=Fh06gMnt5Us
56 Article 51(2) of Additional Protocol I; Article 33 of Geneva Convention IV.
57 Russian Federation, *Instructions on the Application of the Rules of International Humanitarian Law by the Armed Forces of the USSR*, Appendix to Order of the USSR Defence Minister No. 75, 1990, § 5(n).
58 MDAA, KH-101/102. Available at: https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/kh-101102/; See also: Global Security, Kh-101 / Kh-102 / X-101/102 Air Launched Cruise Missile. Available at: https://archive.is/nii6A; Russia Beyond, Russia's most devastating sea, ground, and air missiles, 7 November 2017. Available at: https://archive.is/RSe4f
59 Bellingcat, The Remote Control Killers Behind Russia's Cruise Missile Strikes on Ukraine, 24 October 2022. Available at: https://archive.is/5x5xy
60 The pedestrian bridge – located in a park away from any military facilities or installations – was clearly not a legitimate military objective, but rather a symbolic retaliation for Ukraine's attack on the Krech bridge. Therefore, it was a civilian object protected by IHL from attacks.
61 Additional Protocol I, Article 85(3)(a).
62 ICC Statute, Article 8(2)(b)(iv).
63 ICC Statute, Article 8(2)(b)(i)/(ii)
64 ICC Statute, Article 8(2)(b)(ii)
65 Additional Protocol I, Article 85(3)(a).
66 ICC Statute, Article 8(2)(b)(i)/(ii)

Attacks on civilian objects with Kalibr missiles

Case study one

Date: 14 July 2022

Location: Vinnytsia, Ukraine

Incident: Attack on civilian infrastructure in the centre of Vinnytsia

On 14 July 2022, Russian forces carried out a massive missile attack on downtown Vinnitsa. [67] The missiles struck the 'House of Officers' concert hall (House of Officers) and a parking lot across the street,[68] and damaged the nearby medical centre, offices, stores and residential buildings.[69] The Russian Ministry of Defense stated that their intended target – the House of Officers – was hosting a meeting of the command of the Ukrainian Air Force and representatives of foreign arms suppliers, and that they were 'eliminated' as the result of the attack.[70] According to the Ukrainian government, UN and EU representatives, Russian attacks were directed purely against civilian infrastructure.[71]

The attack claimed 23 civilian lives including three young children.[72] More than 100 civilians were injured and at least 36 apartment buildings were damaged.[73]

Upon examination of the impact sites, the State Emergency Service of Ukraine announced that their experts extracted munition fragments of two Kalibr 3M-14 missiles.[74]

Fragments of Kalibr missile in Vinnytsia, 14 July 2022. Source: Vinnytsia City Council

67 Interfax-Ukraina, 'The Russians fired 4 Kalibr missiles at Vinnytsia, each weighing 1770 kg', 14 July 2022. Available at: https://archive.ph/Bqrwe
68 AP News, Russian missiles kill at least 23 in Ukraine, wound over 100, 14 July 2022. Available at: https://archive.is/QozgA
69 AP News, Russian missiles kill at least 23 in Ukraine, wound over 100, 14 July 2022. Available at: https://archive.is/QozgA
70 Reuters, Russia says building struck in Ukraine's Vinnytsia was military target, 15 July 2022. Available at: https://archive.is/gu9pf
71 AP News, Russian missiles kill at least 23 in Ukraine, wound over 100, 14 July 2022. Available at: https://archive.is/QozgA; European Union, Ukraine: Statement by High Representative Josep Borrell and Commissioner for Crisis Management Janez Lenarčič on Russian attacks against civilian targets, 14 July 2022. Available at: https://archive.is/aqZT9; Kyiv Post, Leaders Condemn Russian Missile Attack on Vinnytsia, 15 july 2022. Available at: https://archive.is/BxhFu
72 BBC, Ukraine war: 23 killed in Russian rocket attack on Vinnytsia, 14 July 2022. Available at: https://archive.is/EN5Ck
73 AP News, Russian missiles kill at least 23 in Ukraine, wound over 100, 14 July 2022. Available at: https://archive.is/QozgA
74 Vinnytsia City Council, 'Today, the Russians attacked Vinnytsia with 3M-14E Kalibr missiles',14 July 2022. Available at: https://archive.ph/YaY1F

Case study two

Date: 28 June 2022

Location: Dnipro, Ukraine

Incident: Attack on a car service station and two enterprises

On 28 June 2022, the Russian military attacked Dnipro with missiles, hitting the Avtodizel car service station in the western part of the city,[75] an industrial and a transport enterprise.[76] Railway infrastructure and several residential buildings were also damaged as the result of the attack.[77] After the attack on the Avtodizel car service station, two bodies of civilians were recovered from the rubble.[78] The State Emergency Service of Ukraine in the Dnipropetrovsk region released images of missile fragments confirming the use of the Kalibr missile in the attack on the civilian infrastructure.[79] The intermittent black stripes and the letters and digits "33-14.1" and "33-14.0" are the tell-tale signs of Kalibr missiles.

Fragments of Kalibr missile's sustainer stage in Dnipro, 28 June 2022. Source: Head office of the State Emergency Service of Ukraine in the Dnipropetrovsk region

For reference: Kalibr Missile shot down by the Ukrainian air defence in Vinnytsia, 23 June 2022. Source: General Staff of the Armed Forces of Ukraine

75 Valentin Reznichenko, the Dnipropetrovsk Regional State Administration, 'Bad news came this morning', 29 June 2022. Available at: https://archive.ph/tJMXJ; See also: Apostrophe, 'In Dnipro, people were killed in a missile strike: photos and new details', 29 June 2022. Available at: https://archive.ph/DkxMX

76 State Emergency Service of Ukraine in the Dnipropetrovska oblast, 'Enemy fired six missiles at Dnipropetrovshchina', 28 June 2022. Available at: https://tinyurl.com/2fw5jnyw

77 State Emergency Service of Ukraine in the Dnipropetrovska oblast, 'Enemy fired six missiles at Dnipropetrovshchina', 28 June 2022. Available at: https://tinyurl.com/2fw5jnyw; See also: Suspilne.Media, 'Our windows are broken. It was very scary." Missile strikes on the Dnipro on June 28: what eyewitnesses say EXCLUSIVELY', 29 June 2022. Available at: https://archive.is/lyuFX; Apostrophe, 'Rocket shelling of the Dnipro: it became known where the impact was'. Available at: https://archive.is/ukZDu

78 Valentin Reznichenko, the Dnipropetrovsk Regional State Administration, 'Bad news came this morning', 29 June 2022. Available at: https://archive.ph/tJMXJ; See also: Ukrainska Pravda, 'Two civilians killed in Russian attack on car repair service in Dnipro pulled out from under the rubble', 29 June 2022. Available at: https://archive.is/NU3Od

79 State Emergency Service of Ukraine in the Dnipropetrovska oblast, 'Enemy fired six missiles at Dnipropetrovshchina', 28 June 2022. Available at: https://tinyurl.com/2fw5jnyw

For reference: Kalibr Missile. Source: Missilery.info

Potential legal classification

Russian forces used Kalibr 3M-14 missiles in the two attacks analysed above. A single Kalibr 3M-14 missile carried a 450 kg warhead and has a satellite guidance system that gives it an accuracy of 3 metres.[80]

Russian authorities justified the attack in Vinnytsia by alleging that a military gathering was taking place in the House of Officers – the biggest concert hall and the main space for other cultural events in Vinnytsia and the wider region.[81] Kalibr 3M-14 missiles hit the House of officers and damaged the nearby medical centre, offices, stores, and residential buildings. Their impact caused 120 civilian casualties (dead and wounded) and mass destruction of civilian infrastructure. Even if Russian authorities were operating on the belief that a military gathering was taking place at this location, the means employed to carry out this attack were disproportionate to the military objective sought, and caused excessive death and damage. Therefore, the Russian Kalibr missile attack on the House of Officers and the surrounding civilian infrastructure in the centre of Vinnytsia is a grave breach of IHL[82] and may constitute a war crime of excessive incidental death, injury, or damage.[83]

The attack in Dnipro was perpetrated against civilian businesses, claiming at least two civilian lives. Russian armed forces clearly intended to target this civilian area as they used high-precision Kalibr 3M-14 missiles. There is no information to suggest that this area was used by the Ukrainian military in any way. In the absence of a military objective,[84] the targeted civilian commercial district was a civilian object and fell under IHL protection. Considering the above, this incident represents a grave breach of IHL[85] and may constitute a war crime of attacking civilians/a civilian object.[86]

80 MDAA, 3M-14 Kalibr (SS-N-30A). Available at: https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/ss-n-30a-kalibr/
81 Myvin, Concert hall 'House of Officers'. Available at: https://www.myvin.com.ua/catalogs/160-budynok-ofitseriv
82 Additional Protocol I, Article 85(3)(ba).
83 ICC Statute, Article 8(2)(b)(iv).
84 A military objective is any object that by its nature, location, purpose or use makes an effective contribution to military action and whose partial or total destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage. See: Additional Protocol (I) to the Geneva Conventions of 1977, Article 52(2).
85 Additional Protocol I, Article 85(3)(a).
86 ICC Statute, Article 8(2)(b)(i)/(ii)

Attacks on civilian objects with Tornado-S multiple rocket launchers

Case study one

Date: 9 July 2022

Location: Kryviy Rih, Dnipropetrovsk Oblast, Ukraine

Incident: Attack on a residential neighbourhood in Kryvyi Rih

On 9 July 2022, Russian forces shelled Inhulets, a residential neighbourhood in Kryvyi Rih suburbs.[87] Several apartment buildings, a school and a kindergarten were damaged.[88] Two civilians died as the result of shelling and three more were wounded.[89] According to the Ukrainian Prosecutor's Office, Kryvyi Rih was hit by a Russian Tornado-S multiple rocket launcher system with cluster munitions.[90] According to the Prosecutor's Office, there were no military facilities in the area.[91]

The remnants of the Tornado S missile in Kryviy Rih, 9 July 2022.
Source: Prosecutor's Office of Dnipropetrovsk oblast

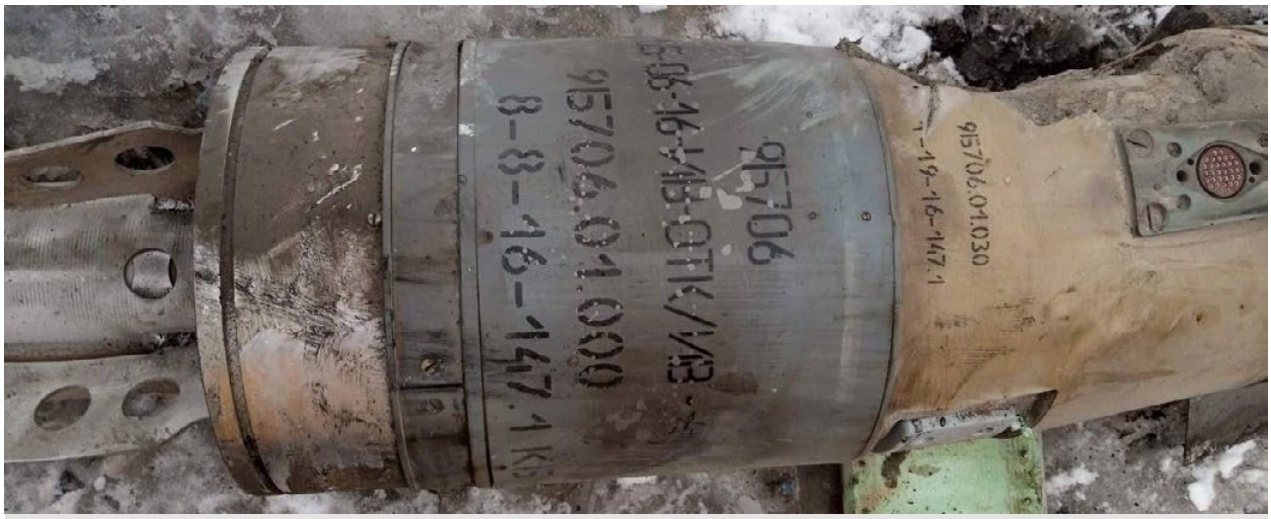
Case study two

Date: 3 March 2022

Location: Pokrovsk, Donetsk Oblast, Ukraine

Incident: Attack on a residential area with private homes

On 3 March 2022, Ukrainian military reported that Russian forces shelled a residential area in Pokrovsk, hitting private homes. There were no casualties as the shells did not explode.[92] Donetsk Regional State Administration stated that remnants of a Tornado-S cluster shell were discovered at the impact sites.[93] Conflict Intelligence Team experts confirmed that the residential buildings were hit by a Tornado-S munition.[94]



The remnants of the Tornado-S missile in Pokovsk, 4 March 2022. Source: Head of the Donetsk Regional State Administration.

Potential legal classification

The two attacks analysed above were perpetrated against residential neighbourhoods, claiming at least five civilian lives. The weapons used for these attacks were Tornado-S MLRS carrying cluster munitions. Cluster munitions are weapons consisting of a container that opens in the air and scatters large numbers of explosive submunitions or bomblets over a wide area, according to the International Committee of the Red Cross.[95] The use of cluster munitions in a residential area is inherently indiscriminate, and therefore can be considered a deliberate attack on civilians. In the absence of a military objective,[96] the targeted residential area was a civilian object and fell under IHL protection. Considering the above, these incidents represent grave breaches of IHL[97] and may constitute war crimes of attacking civilians/civilian objects.[98]

87 Ukrainska Pravda, 'Woman killed in Kryvyi Rih as Russian forces shell residential areas with Grad multiple rocket launchers', 9 July 2022. Available at: https://archive.is/JUIvO;
88 Prosecutor's Office of Dnipropetrovsk Oblast, 'Missile attack on Kryvyi Rih', 9 July 2022. Available at: https://archive.ph/qfFJP
89 Ukrainska Pravda, 'Shelling of Kryviy Rih by Russia: the number of casualties has increased'. 9 July 2022. Available at: https://archive.ph/FRPq8; Prosecutor's Office of Dnipropetrovsk Oblast, 'Missile attack on Kryvyi Rih', 9 July 2022. Available at: https://archive.ph/qfFJP
90 Prosecutor's Office of Dnipropetrovsk Oblast, 'Missile attack on Kryvyi Rih', 9 July 2022. Available at: https://archive.ph/qfFJP
91 Militarny, 'In Kryvyi Rih, after the shelling, new control units for the Tornado-S missiles were discovered', 9 July 2022. Available at: https://archive.is/7X9NF
92 RFE/RL, 'The headquarters of the Joint Forces Operation reported that Pokrovsk was shelled with cluster shells', 4 March 2022. Available at: https://archive.is/dMECA#selection-1035.1-1035.62; 06239, 'The aftermath of the yesterday's shelling in Pokrovsk', 4 March 2022. Available at: https://archive.ph/BMD28;
93 Russian President Vladimir Putin's public speech after 10 October 2022 mass attacks on Ukrainian energy infrastructure available at: https://t.me/RVvoenkor/28579.
94 Conflict Intelligence Team, 'Russian troops shelled the city of Pokrovsk, Donetsk region, with the guided cluster rockets MLRS Tornado-S', 4 March 2022. Available at: https://archive.ph/BEafv; See also: Bellingcat, 'These are the Cluster Munitions Documented by Ukrainian Civilians', 11 March 2022. Available at: https://archive.is/0XucO
95 International Committee of the Red Cross, 'Cluster munitions: what are they and what is the problem?', 1 August 2010. Available at: https://www.icrc.org/en/doc/resources/documents/legal-fact-sheet/cluster-munitions-factsheet-230710.htm
96 A military objective is any object that by its nature, location, purpose or use makes an effective contribution to military action and whose partial or total destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage. See: Additional Protocol (I) to the Geneva Conventions of 1977, Article 52(2).
97 Additional Protocol I, Article 85(3)(a).
98 ICC Statute, Article 8(2)(b)(i)/(ii)

Part two

The Western Components at the Heart Of Suspected Russian War Crimes

Part two
The Western Components At The Heart Of Suspected Russian War Crimes

Disclaimer: *Where examining the branding of components, or analysing third party research, we have been mindful of the existence of counterfeit components. We recognise the possibility that components featuring the logos and/or branding of named entities may not have indeed been manufactured by said entities. However, given a) leaked Russian "shopping lists" showing the intent to acquire components manufactured by such companies in order to support its military[99], and b) the history of Soviet and Russian military procurement efforts targeting leading global technology companies, we have worked on the assumption that components we and third parties have identified are genuine.*

For the avoidance of doubt, we do not allege any legal wrongdoing on the part of the companies who manufacture the components and we 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 and/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.

For all of the above weapons used in the suspected commission of war crimes by Russian forces, western-made components have been identified. Our research, in addition to previous revelations including the Royal United Services Institute's (RUSI) August 2022 report – 'Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine' – sheds light on the extent to which these weapons are reliant on such components.

It is also becoming clearer which companies manufacture the components most prevalent in Russian equipment.

According to RUSI's August 2022 report, of the 450 foreign-made unique components RUSI identified in its examination of 27 different Russian military systems, more than a quarter bore the branding or logo of Texas Instruments and Analog Devices, two US based manufacturers.

Analysis of expended Kalibr missiles conducted by NAKO also found multiple components bearing the branding or logo by Texas Instruments were present.

99 POLITICO, 'The chips are down: Putin scrambles for high-tech parts as his arsenal goes up in smoke', 5 September 2022. Available at: https://www.politico.eu/article/the-chips-are-down-russia-hunts-western-parts-to-run-its-war-machines/

Meanwhile across the Atlantic, Harting, a German-based technology company, manufactures ethernet cables used in the Zarya computer, a signal processing system within the Iskander missile, according to RUSI's August 2022 analysis.[100]

Most concerningly, new trade data has revealed that, despite Russia's full scale invasion, a Harting subsidiary continues to export to Russia. Since 24 February 2022, Harting LLC has exported 2,851 shipments to Russia with a total value of more than $16m USD. While this trade data provides insight as to unit volume, value, and category, it cannot with precision determine the exact product involved. It is therefore not possible to analyse the legal background to such exports. Rather, in light of the suspected war crimes detailed throughout this report, we query said manufacturers' ethical and moral judgement.

What follows paints an urgent picture: the weapons used by Russia in perpetrating its suspected war crimes are reliant on components made by western companies.

Iskander (9K720 Iskander)

9T250-1 Iskander-M

Iskander is a surface-to-surface short-range ballistic missile**,** capable of carrying either a nuclear or conventional warhead. It uses inertial and optical guidance systems and has a range up to 500 km. The missile is also specifically designed to overcome air defence systems through its use of supersonic speed, extreme manoeuvrability and through releasing decoys. The Iskander has been used for hundreds of strikes on Ukraine since the full scale invasion, including strikes on civilian objects detailed above.[101]

100 RUSI, Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine, 8 August 2022. Available at: https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine
101 https://twitter.com/oleksiireznikov/status/1611449870040109058/photo/1

Iskander (SS-26 "Stone") at a Glance	
ORIGINATED FROM Russia	**POSSESSED BY** Russia, Algeria, Armenia
ALTERNATE NAMES Stone, Tender, 9M720, 9M723, 9M723-1	**CLASS** Short-Range Ballistic Missile (SRBM)
BASING Road-mobile	**LENGTH** 7.3m
DIAMETER 0.92 m	**LAUNCH WEIGHT** 3,800-4,020 kg
PAYLOAD 480-700 kg, 480 kg (export variant)	**WARHEAD** High-explosive, submunition, earth-penetrator, thermobaric
PROPULSION Single-stage solid propellant	**RANGE** 400-500 km, 200 km (export variant)
STATUS Operational	**IN SERVICE** 2006

Main characteristics of Iskander missile. Source: Missile Defense Project, "9K720 Iskander (SS-26)," Missile Threat, Center for Strategic and International Studies, 27 September, 2016, last modified 2 August, 2021, https://missilethreat.csis.org/missile/ss-26-2/

In August 2022, the Royal United Services Institute released a landmark report – Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine – revealing that several western-made components were found to be present inside the Iskander missile.[102] Specifically, these components were found inside the missile's signal processing computers and its sensors: the digital signal processors, flash memory modules, static RAM modules, and ethernet cabling that had been manufactured by US, Swiss, and German companies.

Processors, flash memory, ethernet cabling, and microchips bearing the logo or branding of the following companies were found inside the missile:

Country of origin	Company
USA	Texas Instruments
	Integrated Device Technology
	Advanced Micro Devices
	Cypress Semiconductor
	Spansion Inc
	Microchip Technology
	Altera
	Xlinx
	M-Tron
	Mini-Circuits
Germany	Harting
Switzerland	Traco Power Company

102 Silicon Lifeline: Western Electronics at the Heart of Russia's War Machine, RUSI, available at: https://rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine

Kh-101

The Kh-101 is an air-launched cruise missile with an estimated range of 2,500km to 2,800km, although the Russian military has claimed it is capable of reaching distances of up to 4,500km.[103] It has a multi-faceted guidance system and low flight pass (at tree level in terminal stage) in order to avoid radars and air defence systems. The missile is equipped with a GLONASS navigation system which guides it to the target, as well as GPS.

The missile entered service in 2012, and has been used by Russia's air force several times in combat since. Launched from aircraft including the TU-160 Blackjack, it is fired without a booster, using the aircraft's momentum at release to give it initial velocity.

Kh-101 / Kh-102 at a Glance	
ORIGINATED FROM Russia	**POSSESSED BY** Russia
CLASS Air-launched Cruise Missile (ALCM)	**BASING** Tu-160 Blackjack, Tu-22M3/5 Backfire C, Tu-95MS16 Bear-H, and Su-27IB
LENGTH 7.45m	**DIAMETER** 0.51 m
PAYLOAD 450 kg	**WARHEAD** HE, fragmentation, submunition (kh-101), 250 kt nuclear (Kh-102)
PROPULSION Turbofan	**RANGE** 2,500-2,800 km
STATUS Operational	**IN SERVICE** 2012

Main characteristics of Kh-101 missile. Source: Missile Defense Project, "Kh-101 / Kh-102," Missile Threat, Center for Strategic and International Studies, October 26, 2017, last modified 31 July, 2021, https://missilethreat.csis.org/missile/kh-101-kh-102/

103 https://eng.mil.ru/en/news_page/country/more.htm?id=12132186@egNews

Components bearing the logo or branding of companies based in the US, Netherlands, Switzerland, and Taiwan have been found in the Kh-101, according to RUSI's August 2022 report. Similar to the Iskander missile, these components included circuits, microprocessors, switches, memory, and oscillators.

Country of origin	Company
USA	Microchip Technology
	Spansion Inc
	Linear Technology Corporation
	Zilog
	Intergrated Device Technology
	Texas Instruments
	Xlinx
	Anderson Electronics
	Intel
	Analog Devices
	Vicor
	Motorola
	Cypress Semiconductor
The Netherlands	Philips Semiconductor
	Nexperia
Switzerland	STMicroelectronics
Taiwan	VBsemi

Kalibr (3M-14 Kalibr (SS-N-30A))

Kalibr is a sea launched land-attack cruise missile. With a range of between 1,500km and 2,500km, it is believed to be a "mainstay in the Russian Navy's ground-strike capabilities", according to the Center for Strategic and International Studies.[104]

Kalibr SS-N-30A at a Glance	
ORIGINATED FROM Russia	**POSSESSED BY** Russia
ALTNERNATE NAMES 3M-54, Kalibur	**CLASS** Sea-launched Land Attack Cruise Missile
BASING Ship/submarine based	**LENGTH** 6.2 m
PAYLOAD 450 kg warhead: High explosive, possibly nuclear capable	**PROPULSION** Turbojet
RANGE 1,500-2,500 km	**STATUS** Operational
IN SERVICE 2015	

Main characteristics of Kalibr missile. Source: Missile Defense Project, "3M-14 Kalibr (SS-N-30A)," Missile Threat, Center for Strategic and International Studies, 11 August, 2016, last modified March 7, 2022, https://missilethreat.csis.org/missile/ss-n-30a/

104 https://missilethreat.csis.org/missile/ss-n-30a/

New analysis of expended Kalibr missiles conducted by NAKO, now being made public for the first time, has revealed that components in its satellite navigation system, guidance computer, and altimeter bear the logo or branding of companies based in the US, Switzerland, and Taiwan:

Country of origin	Company
USA	Cypress Semiconductor
	Texas Instruments
	Altera Corporation
	HALO Electronics
	Motorola
	Spansion
	Integrated Device Technology
	Linear Technology
	Marvell Technology
Switzerland	STMicroelectronics
Taiwan	VBsemi

Tornado S 9K515 MLRS

Tornado S

Tornado S is a 300 mm multiple launch rocket system with GPS satellite navigation systems to launch both guided and unguided rockets. It has a range of 120km and the latest modification of guided missiles is precise down to between five and ten metres. The GLONASS system allows Tornado S to hit a group of targets at distance from each other in one salvo. According to some publications, the system can automatically receive and process information from reconnaissance vehicles or drones without the operator's interference.[105]

Tornado S at a Glance	
ARMAMENT 12 launch tubes 300 mm caliber	**ARMOR** No armor protection
COUNTRY USERS Russia	**VEHICLE WEIGHT** ?
DESIGNER COUNTRY Russia	**TRUCK SPEED** 60 km/h
ACCESSORIES Computerised firing control system with GPS, GLONASS satellite navigation system, NBC protection system	**TRUCK RANGE** 850 km
CREW 3	**DIMENSIONS** Length: 12.37 m; Width: 3.1 m; Height: 3.1 m

Main characteristics of Tornado S MLRS. Source: https://www.armyrecognition.com/russia_russian_army_vehicles_system_artillery_uk/tornado-s_9k515_mlrs_300mm_multiple_launch_rocket_system_data_fact_sheet.html

105 Russia Boasts 1-Meter Accuracy for New GLONASS-Guided, 200-Km Range Missile Squadrons. Inside GNSS, 24 September 2020. Available at: https://insidegnss.com/russia-unveils-new-glonass-guided-200-km-range-missile-squadrons/

RUSI's August 2022 report revealed that rockets fired by the Tornado system contained a gyroscope featuring a field-programmable gate array (FPGA) bearing the name of Altera Corporation. This gyroscope allows the rocket to correct and alter its course during flight. In December 2015, Intel announced that it had entered into an agreement to acquire Altera.[106]

Separately, the report revealed that memory modules inside the rocket's satellite navigation and computing units bore the name of Cypress Semiconductor, another US based company.

106 Intel Acquisition of Altera, Intel, 28 December 2015. Available at: https://newsroom.intel.com/press-kits/intel-acquisition-of-altera/

Part three

Tracking the Trade: How Components Reach Russia

Part three
Tracking the Trade: How Components Reach Russia

Our analysis has found that western-made components have continued to reach Russia long after its full scale invasion of Ukraine, raising moral and ethical concerns for the companies involved.

Indeed, new trade data has revealed that three western technology companies – two of which make components being sought by Russia to manufacture and repair its military equipment, and one of which makes a variety of a specific component needed by the Russian military – continue to export thousands of components worth millions of dollars to Russia as recently as November 2022. While the trade data cannot accurately reveal the exact components included in such shipments and therefore provide insight as to the legalities of them, the data nonetheless poses questions as to the moral direction of the companies.

The businesses, Harting, Trimble, and TE Connectivity, all manufacture components which continue to be imported by Russia, either through official distributors for the companies, or third countries such as Hong Kong and Turkey.

In September 2022, POLITICO reported on a leaked Russian "shopping list" of components the Kremlin had identified as needing in order to sustain its war effort.[107] This list included 24 components made by Harting and two made by TE Connectivity. Also featured on the so-called shopping list were components made by Altera, Cypress Semiconductor, Marvell, Texas Instruments, and Analog Devices, all companies whose branding or logos have been found on components in weapons used in the suspected committing of the war crimes documented here.

Trimble meanwhile continues to manufacture GLONASS enabled components, the Ukrainian Directorate of Intelligence stated in November 2022.[108] GLONASS is a navigation system used in many of the weapons explored throughout this report. The trade data cannot provide insight as to whether the Trimble components being imported by Russia are GLONASS enabled, however the Directorate of Intelligence cautioned: "Foreign companies should realise the direct impact of their products on Russia's defence capabilities, stop producing chips with GLONASS support and remove the function of supporting this navigation system from all their devices."

In December 2022, the Royal United Services Institute (RUSI) and Reuters released a joint investigation revealing that at least $2.6 billion of computer and other electronic components had flowed into Russia in the seven months to 31 October, Russian customs records showed. At least $777 million of these products were made by Western firms whose components had previously been found in Russian weapons systems.[109]

In many cases, components reach Russia via a complex network of subsidiaries and distributors. In the case of Harting for example, Harting LLC, the company's Russian subsidiary, has continued to import components to Russia from Harting Technology Group in Europe and Asia since Russia's full scale invasion. The last registered import data was recorded on 29 November 2022. Since 24 February 2022,

107 The chips are down: Putin scrambles for high-tech parts as his arsenal goes up in smoke, POLITICO, available at: https://www.politico.eu/article/the-chips-are-down-russia-hunts-western-parts-to-run-its-war-machines/
108 Foreign Companies Help Guide Russian Missiles to Ukraine, Defence Intelligence of the Ministry of Defence of Ukraine, 25 November 2022. Available at: https://gur.gov.ua/en/content/inozemni-kompanii-dopomahaiut-skerovuvaty-rosiiski-rakety-na-ukrainu.html
109 https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-tech-middlemen/

Harting LLC has exported 2,851 shipments to Russia with a total value of more than $16m USD.

Harting Electric Stiftung Co. Kg From Vinges Terminalas Lvtr 1000, Vilnius was the largest supplier, responsible for 21.38% of these imports.

The supplier addresses for the imports are predominantly Harting offices in Germany.

Harting did not respond to a request for comment.

Prosoft LLC meanwhile, an official distributor of Harting products, has carried out 894 imports since Russia's full scale invasion. These imports also included products manufactured by Trimble, TE Connectivity, Texas Instruments and Infineon Technologies, all companies whose logo or branding has been found on components identified in weapons used in the suspected committing of the war crimes documented here.

In Trimble's case, trade data shows that it has been the supplier of 81 imports to Russia with a total value of more than $2.4m USD since the start of the full scale invasion. Trimble Europe BV was the biggest supplier followed by Cxo Logistics C/O Trimble. While Trimble appears to have stopped supplying to Russia in June 2022, its products appear to still be being imported through a different supplier, namely Prosoft Systems LLC.

Responding to the data, a Trimble spokesperson said: "The implication that Trimble supports military GLONASS based operations, or other Russian military operations, is simply false."

Finally, TE Connectivity has been the supplier of 479 imports to Russia with a total value of more than $1.8m USD since the start of the full scale invasion. It appears to have ceased supplying directly to Russia in May 2022, however its products appear to still be being imported through different suppliers via Turkey, Taiwan, Morocco, and India.

A TE Connectivity spokesperson said: "TE Connectivity complies with all export controls that apply to its business globally and has fully complied with all sanctions imposed on Russia following the Russian invasion of Ukraine. Additionally, TE has not shipped any product from any TE location to Russia since the sanctions were imposed, beginning in March 2022.

"TE is firmly committed to its policy of no direct or indirect shipments of its products to Russia and will continue to communicate this policy with distribution partners, and expect them to comply."

The trade data does not specify exact product codes for shipments into Russia. It is therefore not possible to ascertain whether such shipments are in breach of any legal or sanction obligations, and ascertaining such is outside the scope of this report. It is clear however that the suspected war crimes documented in Ukraine, coupled with the clear evidence of western-made components being found in Russian weapons, should present grave ethical concerns for businesses involved in the manufacturing of such components.

Shortcomings in existing regulation and sanctions have also been identified as a root cause in Russia's continued supply of western made components. In October 2022, StateWatch, a Ukrainian think tank, identified 24 Russian arms manufacturers who had not been sanctioned by the United Kingdom, European Union, or United States.[110] While some of these arms manufacturers have, at the time of writing, now been sanctioned, more than ten remain free of sanctions in the UK, EU, and US.

110 https://statewatch.org.ua/en/publications/tens-of-russian-weapons-manufacturers-have-escaped-western-sanctions-new-trap-aggressor-research-reveals/

Recommendations

Recommendations

As detailed throughout this report, Russian weapons containing western-made components have been used to carry out what are suspected to be war crimes in Ukraine. Moreover, as Russia seeks to obtain critical components amid international scrutiny and sanctions, trade data now reveals the extent to which such components have continued to flow into the country, long after the invasion.

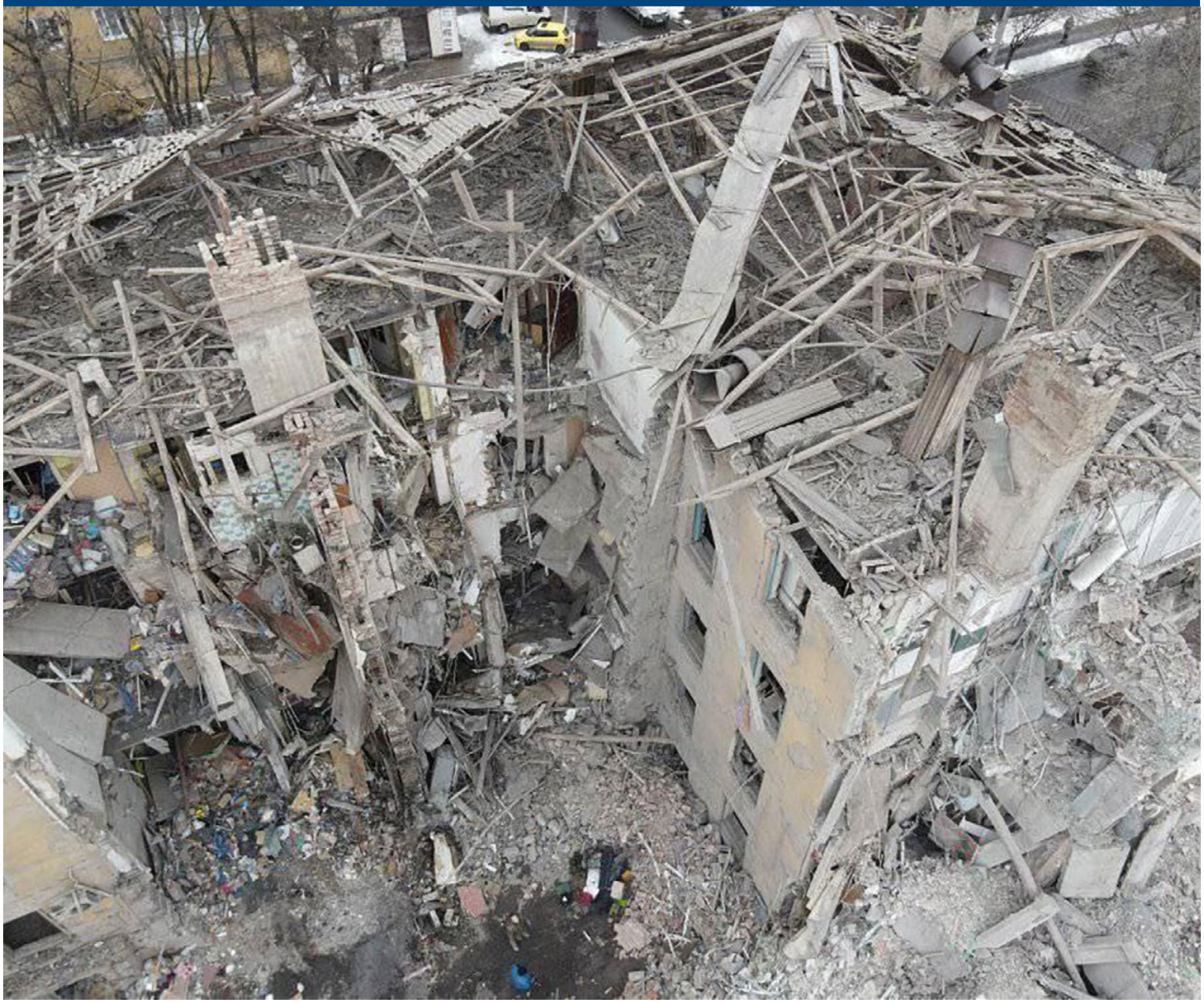
Restricting Russia's access to such components would have a devastating and immediate effect on its war effort. Operating at a high tempo requires an equally high resupply and replenishment rate: Russia's drones, missiles, communication systems, and other equipment all require repairing, maintaining, and restocking – all processes that require such components. If the supply was to dry up, it would only be a matter of weeks before that was felt on the battlefield.

The supply and maintenance of its weapons is a key vulnerability of the Russian war machine. It is the duty of policymakers and businesses to exploit this vulnerability. A crucial first step in this process is to **recognise that a problem exists**. Stakeholders have, up to this point, not commented in depth on these issues. An open and frank acceptance that more must be done to stem Russia's access to western-made technology is needed as a matter of urgency.

This requires 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.

The revelation that companies making components that are actively sought by the Kremlin, according to POLITICO's leaked "shopping list", continue to supply to Russia as recently as November 2022, evidences that existing regulatory and sanctions measures are inadequate. A **thorough and holistic review of existing sanctions and export control measures** should therefore be conducted, reflecting on the issues raised by this report.

Finally, **businesses must enhance their due diligence, 'know your customer', and end-user surveillance** to ensure their products are not being used in ways that do not align with their ethical and legal commitments. Ignorance as to a product's end-user should not be relied upon as a moral or legal defence.

IPHR International Partnership for Human Rights

NAKO TI UKRAINE • TI-DS