The Henry Jackson Society - Written evidence (IUD0008)

The Henry Jackson Society (HJS) is a trans-Atlantic defence, security and foreign policy, think tank in Westminster, UK. The society drives initiatives for the pursuit of a robust foreign policy, and clear universal principles, such as the global promotion of the rule of law, liberal democracy, civil rights, environmental responsibility and the market economy.

Implications of the war in Ukraine for UK Defence.

The Henry Jackson Society has an established record of analysis and expertise on the Russia's invasion of Ukraine and the resulting implications for the future of warfare and UK defence and security. The content of this submission includes our recent research and therefore specific expertise on the questions raised by the committee in this inquiry.

Recent research that will be included in this written evidence includes:

The Centre for the Future of Warfare:

A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare. Megan Gittoes, March 2024.
Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience. David Kirichenko, February 2024.

The Centre for Russia and Eurasia Studies:

Ukraine's Nuclear Shadow: National Security Implications for NATO and the UK. Dr Bahram Ghiassee, December 2023.

The Centre for Social and Political Risk:

Winter is Coming: How the UK Should Respond to Russia's Weaponisation of Energy Sources This Winter. Dr Helena Ivanov, August 2023.

1. **What does the war in Ukraine tell us about the changing character of warfare? To what extent are the lessons from the war in Ukraine applicable to UK Defence?**

The war in Ukraine makes one lesson very clear. The nature of warfare is extending beyond the boundaries set by traditional, anachronistic perspectives. Since Russia's invasion on 24th February 2022, the ongoing conflict has highlighted three key elements that distinctively represent how warfare currently plays out and how it will evolve moving forward.

1. Use of proxies and increase in conflict-related sexual violence (CRSV)

In 2022, the United Nations Security Council held their 9378th meeting and confirmed the disturbing upward trend of CRSV, in part due to the rise of global militarisation and arms proliferation.[1] Not only does this connection identify another

[1] Megan Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," Henry Jackson Society, 19 March 2024, 11, https://henryjacksonsociety.org/publications/a-

complexity of modern warfare, illustrating the need for more nuanced responses by the West, but showcases the ties between increased militarization contributing to the prevalence of non-traditional forms of violence like CRSV.[2]

How CRSV unfolds denotes a further development of modern-day warfare: the use of proxies. The use of proxies to wage war in Ukraine exemplifies the evolving proxy-sponsor relationship. The diminishing level of state control over armed conflicts coupled with the increased prevalence of non-state actors introduces a phenomenon that represents the changing character of warfare.[3] The Wagner Mercenary Group (WMG), a Russian proxy private military company,[4] is an example of how the use of proxies that employ CRSV as a tool to further a government's political, economic and military goals, severely exacerbate the conditions of armed conflict. In the case of the WMG, who have posted videos of the human rights abuses in Ukraine, like what other proxies have done in recent conflicts such as from Hamas following the events on 7th October 2023, illustrate a pattern of non-state actors using online platforms that clearly depict breaches of international law.[5] Furthermore, this displays how as the nature of warfare evolves, the responsibility of government continues to lessen. The WMG has allowed a level of deniability, an intrinsic problem of proxy warfare, for the Russian government in terms of criminal activities and human rights abuses, fostering a culture of impunity and further friction within the international community on how to hold perpetrators accountable.[6]

The situation of rising CRSV in Ukraine signals a need for the UK to have a more profound examination of the evolving character of warfare entrenched in its defence policy. A central problem, aside from the human rights abuses and the undermining of Ukrainian sovereignty, is the further development of a culture of impunity therefore it is not only up to the UK to make swift changes in preventing and addressing CRSV. For the UK in particular, a few steps should be made moving forward:

- The presence of proxies, such as the WMG, increases the total number of participants in a conflict zone, and many of them employ indirect methods of warfare like terrorism, posing significant military, political, financial, and legal challenges for redress. Given this, non-state actors now have transnational reach through online communications and recruitment, as well as benefiting from global arms proliferation and militarisation, which is inherently tied to rising rates of CRSV. Countering their activities necessitates intricate and expensive international cooperation across diplomatic, legal, military, intelligence, and humanitarian domains. Integrating this understanding into defence planning is essential for effectively addressing contemporary security threats.[7]

---

culture-of-impunity-understanding-conflict-related-sexual-violence-in-contemporary-proxy-warfare/.
[2] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 11.
[3] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 16.
[4] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 26.
[5] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 29.
[6] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 26.
[7] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 20.

- Understanding how proxies are employed to achieve strategic objectives, such as the WMG to further Russia's goals of expansion and undermining Ukrainian sovereignty, is relevant for analysing the changing character of warfare and informing UK Defence strategies in countering similar tactics employed by adversaries.[8]

2. The era of cyber wars

24th February 2022 marked the start of the first all-out cyber war between two countries, as Russia attempted to integrate cyberattacks with physical strikes. This underscores the evolution of warfare, particularly in the cyberspace domain. The integration of cyberattacks alongside traditional military actions represents a significant shift in the character of warfare, calling for strengthened cyber capabilities in modern conflicts.[9] Improved cyber defences are unquestionably needed going forward as cyber warfare illuminates a pivotal point in the changing character of warfare: the lines between combatants and non-combatants are now blurred.[10] As civilians can now unwillingly become part of cyber conflicts, along with increased globalization of shared digital platforms, this demonstrates how quickly cyberattacks can be disseminated globally and extends the battleground beyond physical spaces and the countries waging war into a conflict with a global scope.

Given the emergence of cyberwarfare and its potential devastating effects, both the UK and the international community need to adjust their defence strategies to encompass both physical and cyber domains, reflecting a clear departure from traditional perspectives on warfare.[11] For the United Kingdom, this emphasizes the importance of strategic alliances and ongoing investment in cybersecurity capabilities to protect critical infrastructure and national security interests.[12]

Key Lessons for UK Defence:

- Improve coordination between the private and public sectors to develop robust processes that effectively mitigate cyber threats.[13]
- Invest in creating stronger security mechanisms to protect critical infrastructure, given the devastating Russian cyberattack on Kyivstar, Ukraine's biggest mobile network operator.[14]
- Like the US, provide technical assistance in the form of financial support for Ukraine's cyber defence.[15]

---

[8] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 26.
[9] David Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," Henry Jackson Society, 20 February 2024, 5, https://henryjacksonsociety.org/publications/lessons-from-the-first-cyberwar-how-supporting-ukraine-on-the-digital-battlefield-can-help-improve-the-uks-online-resilience/.
[10] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 10.
[11] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 6.
[12] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 28.
[13] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 25.
[14] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 22.
[15] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help

- Provide Ukraine with more intelligence on Russian vulnerabilities to enable Ukraine to conduct cyber offensives to support its ground campaign.[16]
- UK Defence must prepare for cyber threats from a diverse range of actors, given the increased relevance of non-state actors and hacktivist groups, not just traditional adversaries.[17]
- Invest in training more of Ukraine's military personnel for both cyber defence and offensive capabilities.[18]
- Back the International Committee of the Red Cross in its mission to have existing international humanitarian law extended to protect civilians (non-combatants) and civilian infrastructure within the realm of cyber warfare.[19]

3. Global Nuclear Threat

While the presence of nuclear weapons is not new nor isolated element to the war in Ukraine, the global risks associated with nuclear confrontation are unprecedented. From the start, the conflict has been fought under the long shadow of nuclear weapons and the escalation of which could lead to the deployment of tactical nuclear weapons resulting in catastrophic implications for Ukraine, neighbouring countries, European members of NATO and the UK.[20] When coupled with the rising rates of CRSV and proxies operating unchecked by the international community, as well as the growing use of cyberattacks, any escalation in this new era of warfare could trigger a nuclear response. This highlights how quickly a conflict can spiral out of control now that warfare is no longer confined to its traditional definition.

Ukraine not only underscores the imminent threat of nuclear confrontation, but exposes related risks, such as radiological terrorism and its impact on surrounding societies if the conflict escalates. Based on reports of Russia's potential nuclear attacks at the Zaporizhzhia nuclear power plant (NPP),[21] experts have identified that the catastrophic impacts on critical infrastructure, public health, food security and energy security would have immense implications on the national security of not only Ukraine, but the rest of Europe and the UK.[22]

As nuclear threats and radiological terrorism underpin the tumultuous nature of the current geopolitical landscape, UK Defence will not be successful making changes to their procedures and responses without international cooperation and collaboration. This looming nuclear threat requires the full commitment of NATO. The UK and other NATO members should lend their diplomatic, political, and financial support to the International Atomic

---

Improve the UK's Online Resilience," 27.
[16] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 5.
[17] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 5.
[18] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 38.
[19] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 11.
[20] Dr Bahram Ghiassee, "Ukraine's Nuclear Shadow: National Security Implications for NATO and the UK," Henry Jackson Society, 11 December 2023, 9, https://henryjacksonsociety.org/event/ukraines-nuclear-shadow-national-security-implications-for-nato-and-the-uk/.
[21] *Reuters*, "Ukraine Says Russia Considering Nuclear Plant 'terror' Attack, Moscow Denies It," 22 June 2023, sec. Europe, https://www.reuters.com/world/europe/ukraine-says-russia-considering-terror-attack-zaporizhzhia-nuclear-plant-2023-06-22/.
[22] Ghiassee, "Ukraine's Nuclear Shadow: National Security Implications for NATO and the UK," 11.

Energy Agency (IAEA) to help accelerate its efforts to establish a 'nuclear safety and security protection zone' around the nuclear power plants in Ukraine, in particular the Zaporizhzhia NPP.[23]

8. What role has the space domain, including satellite communications, played in the war in Ukraine, and how has this differed from previous conflicts? What are the implications for the UK Armed Forces.

The war in Ukraine has highlighted the emergence of the space domain in contemporary warfare. Cyber warfare aims to achieve political and strategic objectives through cyberspace, extending the battleground beyond physical spaces. Through this extension, the space domain blurs traditional lines between combatants and non-combatants, as civilians can both willingly and unwittingly become part of cyber conflicts.[24]

Unlike previous conflicts, communication in the Ukraine military relies heavily on satellite networks, which was Russia's primary target with their goal of disrupting Ukrainian military communications at the onset of the invasion.[25] The role of satellite communications in Ukraine and Russia's goal of hindering their defensive capabilities prior to invading illustrates a fundamental difference in modern conflict, one that requires a strategic and modernized response. Ukraine's use of satellite networks has played a crucial role in sustaining military operations and being able to maintain communications across the country.[26]

One hour before the invasion on 24th February 2022, Russia launched a cyberattack, with a wiper malware called AcidRain, on the American commercial satellite internet company Viasat, erasing all the data on its systems.[27] This marked one of the most damaging attacks of the war as Russia attempted to knock out vital communication systems on Ukraine's telecom provider, Kyivstar.[28] Not only does this initial cyberattack reflect the military's unprecedented reliance on satellites, but showcases the vulnerability of satellite communications and the critical part they play in modern warfare.[29]

The impact of these attacks differed from expectations. Unlike previous conflicts where cyberattacks might have had a crippling effect, Russia's attempt to disable Ukrainian communication through Viasat proved temporary and minimally impactful. This highlights the growing sophistication of cyber defences, forcing both adversaries and allies of Ukraine to shift tactics.

The grey area in cyber warfare not only raises concerns over current responses from the UK Armed Forces as well as other allies of Ukraine but brings to light legal questions about the boundaries of acceptable conflict behaviour. Despite theoretical advancement in

[23] Ghiassee, "Ukraine's Nuclear Shadow: National Security Implications for NATO and the UK," 7.
[24] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 10.
[25] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 22.
[26] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 30.
[27] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 22.
[28] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 5.
[29] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 5.

recent years, the institutional framework and international legal procedures are entrenched in an outdated view of warfare.[30]

Current responses to Russia's attacks in Ukraine may be inadequate to address the complexities of satellite communications showcasing the need for UK Armed Forces to continually update their cyber satellite communication systems to mitigate potential attacks. Some experts suggest a shift towards physically destroying satellites in future conflicts, as opposed to cyberattacks.[31] Others are calling for the purchasing of different satellite systems to allow armed forces to be more mobile and wide reaching in their approach to thwarting cyberattacks.[32] The suggestions raise serious concerns about the weaponization of space and the urgent need for international regulations to govern these actions. The UK should work with allies to establish clear regulations governing cyberwarfare to prevent further weaponization of the space domain.

While Ukraine is the epicentre for Russia's cyber aggression, the impact of the cyber war in Ukraine is global.

9. What lessons have the UK and NATO learned from the war in Ukraine about the management of escalation of force?

In the era of modern warfare responses towards managing escalation can no longer solely focus on traditional military force. The complex interplay of cyberattacks, disinformation, and the emergence of non-state actors demands a multifaceted approach to prevent conflict from further escalation that results in devastating outcomes.

The war in Ukraine has underscored three crucial lessons for the UK and NATO when it comes to managing the escalation of force:

1. <u>The Complexities of Hybrid Warfare</u>

   The war in Ukraine has exposed a new front: decentralised cyberwarfare, which is quickly becoming a core element of military operations. Leading up to 24th February 2022, there was a significant surge of 450% in cyberattacks originating from Russia, which continued after the invasion with a dramatic rise in DDoS attacks against US national security targets.[33] Investing in robust cyber defences for critical infrastructure and government systems, collaborating with allies to develop international frameworks for addressing cyberattacks and holding these perpetrators accountable are all guidelines that should be considered when formulating effective responses to prevent further escalation.[34]

[30] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 20.
[31] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 30.
[32] Dr Stepan Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," Henry Jackson Society, 5 October 2022, 33, https://henryjacksonsociety.org/publications/securing-uk-defence-procurement-to-meet-21st-century-challenges-from-present-threats/
[33] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 31.

2. Looming Shadow of Nuclear Weapons

The UN Secretary General has noted that, "the prospect of nuclear conflict, once unthinkable, is now back within the realm of possibility."[35] The deployment of tactical nuclear weapons has been an element of concern since the outset of the war, and as the conflict continues along with the supply of advanced weapons by the West to Ukraine and increased Russian losses, these all point to the potential of the Russian Federation deploying its "battlefield" tactical nuclear weapons.[36] Not only would nuclear weapons have catastrophic results for the national security of Ukraine and its neighbouring countries, but is relevant to European NATO members as well. Under NATO's Article 5, the deployment of nuclear weapons could trigger a wider conflict. Several UNSC members have expressed their concern that Russia's allegations in 2022 against Ukraine developing a 'dirty bomb' could be a pretext for escalation of the military conflict, and Moscow's actual deployment of a dirty bomb in Ukraine.[37]

The constant threat of nuclear weapons hanging over the conflict raises the stakes to an unprecedented level and underscores two key takeaways for the UK and NATO:

1. Deterrence Strategies: Strengthening conventional defences and deterrence capabilities to discourage nuclear escalation in the first place.
2. De-escalation Mechanisms: Developing clear protocols for managing potential incidents and preventing a spiral towards nuclear war.

3. Use of Non-State Actors

The last decade the world has experienced a particular increase in militarisation and illicit arms proliferation, involving coups, unconstitutional militia and insurgent-led military takeovers that are often exacerbated by state actors exploiting the unrest to fulfil their geopolitical objectives.[38] In terms of the war in Ukraine, the WMG's actions not only exhibit how acting on behalf of a state escalates political and security crises, but inevitably results in human rights violations. The UN has failed to publicly condemn member states for the actions of their proxies. This creates a culture of impunity at the global level that emboldens states to commit atrocities at one remove without fear of repercussions, as evidenced by the escalation in the last two years.[39]

The current anachronistic view of warfare fails to incorporate the rise of non-state actors and how detrimental their actions can be. For the UK and NATO, the need to acknowledge how the use of proxies is influencing escalation.

---

[34] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 5.
[35] Ghiassee, "Ukraine's Nuclear Shadow: National Security Implications for NATO and the UK," 9.
[36] Ghiassee, "Ukraine's Nuclear Shadow: National Security Implications for NATO and the UK," 18.
[37] Ghiassee, "Ukraine's Nuclear Shadow: National Security Implications for NATO and the UK," 11.
[38] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 18.
[39] Gittoes, "A Culture of Impunity: Understanding Conflict-Related Sexual Violence in Contemporary Proxy Warfare," 35.

From cyberattacks to potential dirty bombs, the UK and NATO need strategies to address these threats directly, not just through traditional state-to-state responses.

The UK and NATO must prioritize building cyber resilience, fostering international cooperation to address cyber threats, and developing capabilities to identify and hold attackers accountable. By taking these steps, the UK and NATO can navigate the complexities of modern warfare and deter adversaries in this new era.

10. Is the hybrid threat to the UK posed by Russia evolving as a result of the war in Ukraine, and if so, how?

The interconnected nature of the geopolitical landscape undoubtedly precipitates shared risks. Western support to Ukraine since Russia's invasion on 24th February 2022 has unsurprisingly triggered numerous consequences for both nation-states and individuals alike. For the UK, providing continual support to Ukraine outlines clear benefits and drawbacks moving forward.

Many agree on the principle that the more support the UK provides to Ukraine, the more cyberattacks Russia will conduct against the country. Russia has previously been implicated in a series of cyberattacks against the UK, including spear phishing attacks on parliamentarians from 2015 onwards, hacks of UK–US trade documents ahead of the 2019 general election, and breaches of think tanks and civil society organisations.[40] Russia's track record of aggression against the UK coupled with the increasing digital interdependence of our world point to an escalation of the hybrid threat the UK is presently facing.

In January 2024, the UK signed an unprecedented security agreement with Ukraine and provided a £2.5 billion military aid package. As a result of being one of the biggest donors of military aid to Ukraine, the UK has also become the third most targeted country in the world, after the US and Ukraine, for cyber-attacks.[41] While the UK has backed Ukraine since Russia's first invasion in 2014, the war in Ukraine combined with the grey areas of cyber warfare heightens the hybrid threat posed by Russia.

Russian aggression in Ukraine is a direct threat to the UK as it has destabilised the world markets and forced a mass displacement of people in Europe, something that has not been seen since the Second World War,[42] illustrating how the hybrid threat to the UK is continuously evolving as the war unfolds. With that in mind, as the war in Ukraine grinds more into a stalemate, Russia will explore new methods to target Ukraine's allies, namely increasingly the already present critical infrastructure attacks in the UK

`The debate of whether to continue to support Ukraine in fears of UK insecurity remain consistent. While the rapidly changing nature of warfare invites unprecedented risks, such as the use of proxies to advance state interests,[43] the UK's continuous support of Ukraine on both digital and physical fronts will protect the Western world. The interconnectedness of our world and digitised societies points to the argument that protecting Ukraine's digital

[40] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 19.
[41] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 30.
[42] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 37.
[43] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 29.

network simultaneously protects the West's.[44] Achieving the West's security interests are dependent on giving Ukraine the arms to reinforce their cyber capabilities and not only addresses immediate threats but also strategically curbs Russia's capabilities.[45]

When Vladimir Putin invaded Ukraine, he hoped to weaken the Western response by holding over Europe its dependence on Russian energy imports. In September 2022, he warned that price caps on Russian gas would leave Europe to "freeze, freeze." Yet Europe imposed unprecedented sanctions on Russian energy and survived the winter of 2022 with its resolve intact.

This proved a particular challenge in the UK. Despite its relative lack of reliance on Russian gas, the UK has been among the most severely impacted European countries when it comes to soaring energy bills and gas prices.[46] Russia's use of hybrid warfare to influence Europe's political decisions proved ineffective but demonstrated how wildly exposed we were.

11. What other lessons can we draw from the war in Ukraine for UK Defence? What are the implications for the UK's defence priorities, including manpower?

The previous questions have covered a wide array of evidence in Ukraine illustrating the changing character of warfare as well as lessons for UK Defence. Yet, other crucial areas for improvement remain and serve as a stark wakeup call that continuous adaptivity in a time of global conflict is essential.

Manpower and arms sustainability should be a paramount priority for UK defence, as evidenced by Ukraine's struggle to maintain fresh and experienced troops to carry a decisive offensive. This is such a critical lesson as the Russian forces increased manpower and equipment reserves, even if outdated, set the two nations apart.[47] A Ukrainian military victory is possible with unwavering and extensive support from more technologically advanced states, like the UK and NATO members, that are currently at peace and capable of providing arms.[48]

Subsequently, the war in Ukraine has also exposed the danger of maintaining a low quantity stock of expendable arms as despite Britain sending over 6,900 units of the next-generation light anti-tank weapon (NLAW) anti-armour portable missiles, 16,000 shells for artillery pieces, with a further 50,000 on the way, it takes years to replace these weapons considering how quickly the stock is depleted in its use against Russian forces.[49]

Aside from manpower and arms supply, maintaining a physical presence in regions of potential conflict is key.[50] This is due to Article 5 of the North Atlantic Treaty, aligning with the proposal of some experts that the UK should have a physical presence in areas of conflict to act as a deterrent. The presence of British troops in regions of focus for national security and defence has to be achieved through international agreements and frequent

---

[44] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 5.
[45] Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," 6.
[46] Dr Helena Ivanov, "Winter is Coming: How the UK Should Respond to Russia's Weaponisation of Energy Sources This Winter". The Henry Jackson Society, 1st August 2023. https://henryjacksonsociety.org/publications/winter-is-coming-how-the-uk-should-respond-to-russias-weaponisation-of-energy-sources-this-winter/
[47] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 7.
[48] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 7.
[49] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 21.
[50] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 34.

joint exercises which the UK should lead and encourage.[51] Alongside this point, the UK has a prominent role on the world stage, evident by its position in the UNSC and the G7, therefore needs to shift from a subordinate position of reliance on the US to other, more local, partnerships as well as accept greater personal responsibility.[52]

Finally, supporting allies like Ukraine goes beyond arms supply and manpower. Given the broadening nature of warfare, specifically beyond the physical battlefield and into the space domain, the UK must consider broadening the kind of resources we provide. Aside from traditional weaponry, advanced cyber capabilities to bolster Ukraine's defence and offensive strategies in the digital realm to ensure a more robust and adaptable defence posture.[53]

Principle Recommendations:

Lessons from the Ukraine war and the changing character of warfare:

- Lead international diplomatic efforts to forge a coalition against the use of proxy warfare that contributes to human rights abuses; Call on the United Nations (UN) to establish a special proxy force monitoring and reporting mechanism. This dedicated body within the UN would be tasked with monitoring, reporting and responding to incidents of human rights abuses including CRSV – which is rising as a result of proxy warfare. This mechanism should have the authority to investigate allegations through state sponsorship of non-state actors and to publish its findings to the UN.
- Ensure protocols are established by the Ministry of Defence for the prevention of human rights abuses perpetuated by UK-sponsored proxy forces. UK Armed Forces must incorporate CRSV prevention knowledge, awareness, training and practice when training proxies and in peacekeeping missions.
- Improve coordination between the private and public sectors for shoring up cyber defences and invest in creating stronger security mechanisms to protect critical infrastructure.

Impacts of space domain on the UK Armed Forces:

- The UK should work with allies to establish clear regulations governing cyberwarfare to prevent further weaponization of the space domain.
- Enhance satellite systems to allow armed forces to be more mobile and wide reaching in their approach to thwarting cyberattacks

UK & NATO:

- The UK and NATO must prioritize building cyber resilience, fostering international cooperation to address cyber threats, and developing capabilities to identify and hold attackers accountable.
- The war in Ukraine has also exposed the danger of maintaining a low quantity stock of expendable arms. NATO must do more to encourage its member states to commit to 2% of their GDP.

[51] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 34.
[52] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 9.
[53] Stepanenko, "Securing UK Defence Procurement to Meet 21st Century Challenges from Present Threats," 29.

- The presence of British troops in regions of focus for national security and defence has to be achieved through international agreements and frequent joint exercises which the UK should lead and encourage.
- The UK and NATO to initiate the drafting and adoption of an international legal instrument in relation to the safety and security of nuclear and radiological facilities during armed conflict.
- The UK and NATO to lend their diplomatic, political, and financial support to the IAEA in establishing a 'nuclear safety and security protection zone' around the NPPs in Ukraine.

Evolving threat of Hybrid Warfare on UK:

- Aside from manpower and arms supply, maintaining a physical presence in regions of potential conflict is key for UK soft-power and the balancing act between Russia and the West that is being played during elections across Europe this year.

Additional Research:

As a prominent voice on this subject HJS has additional recent research relevant to this inquiry but not referenced in this submission, as the below publications did not explicitly answer the questions posed by the committee:

The Centre for Russia and Eurasia Studies:

Drawing the Line: Declaring Putin Illegitimate as a Step Towards Future-Russia. Dr Stephen Hall, March 2024.
Russia and the Anti-Western Axis Must be Militarily Defeated: Shifting the Western consensus toward ending Russia's military threat to Ukraine and the West. Dr Taras Kuzio, October 2023.
Why Still Pro-Russia? Making Sense of Hungary's and Serbia's Pro-Russia Stance. Dr Helena Ivanov and Professor Marlene Laruelle, January 2023.
Opening a Second Western Front Against Putin: Russia's Latin American Proxies. Peter Young, November 2022.

Centre on Social and Political Risk:

Winning the Peace: Why Britain and the West Must Act Now to Help Rebuild Ukraine. Dr Helena Ivanov and Marc Sidwell, May 2023.

24 April 2024