TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

Software and Hard War: Building Intelligent Power for Artificially Intelligent Warfare

PETE FURLONG
MELANIE GARSON
JEEGAR KAKKAD

Contents

Published at https://institute.global/policy/software-and-hard-war-building-intelligent-power-artificially-intelligent-warfare on November 18 2022

Executive Summary

The conflict in Ukraine has played out in ways that few predicted at the outset, with the Russian military seemingly outmanoeuvred by a Ukrainian defence that is more adaptable and better equipped than anticipated. Ukraine's performance has highlighted the gaps in operational capacity in even the most advanced militaries, providing lessons for emerging digital economies as well as established military powers on how to work with tech companies for more agile access to the most cutting-edge capabilities.

While the outcome of the war may still be far from guaranteed, the combat so far demonstrates the clear links between technology policy and military strategy. This conflict, which was predicted to be the first cyber war, has brought to the fore a new, more intricate and holistic theatre of war in which the lines between the civilian and military-industrial complex have become blurred, where commercial entities fill resource gaps faster than countries, where semiconductor engineers are the new rocket scientists and where data security can tip the balance of power.

The multistakeholder approach to arming the Ukrainian and Russian armies is heralding a new age of "drone diplomacy". Alongside the commercial entities that have been filling the gaps, countries such as Iran and Turkey are vying to leverage their geopolitical influence, benefitting from fewer regulatory limitations than the EU or US. Ukraine, in turn, is making appeals to foreign nations including Israel to provide specific weapons and technologies.

In the private sector, too, this approach to combat is recasting established patterns and relationships. The privatisation of military contracting coupled with the emergence of large tech firms as military suppliers has blurred the lines between technologies designed for the military and those used by hobbyists, consumers and industry.

At the heart of navigating this tech-enabled warfare are two fundamental levers: rapid access to commercial technology and continued access to communications infrastructure. Ukraine is exceeding expectations because it is able to process and share information gathered from drones to reshape its operational strategy. Without access to a stable communications infrastructure to enable the software underpinning or informing these weapons, Ukraine would likely not have been as successful in resisting the Russian offensive.

However, with each escalation in smart and interconnected capability comes increased vulnerability. Informal, benevolent relationships with commercial entities can prove feeble, and hobbyists and hacktivists, like Ukraine's 400,000 strong IT Army, can have malleable allegiances. Tools built on open-source platforms can be easily exploited by malicious actors. Keeping the networks free from physical sabotage and cyber-attacks requires constant vigilance and innovation.

Incremental innovations in technology have repeatedly reshaped warfare throughout the history of human conflict. However, innovation alone cannot revolutionise military affairs. Production capacity, integration of parts and people, organisation, and leadership create the impact. The contrast between the Russian and Ukrainian approaches to development, procurement, deployment, integration and coordination on the battlefield suggests that 21st-century defence requires a more sophisticated, open and forward-looking approach to leveraging tech for more intelligent power.

Innovating Warfare

There has always been a question about the complex causal link between innovation in tech and warfare. Do new technological advances make warfare or does warfare make technological advances? Much of the tech that is so commonplace today, from radar to the internet, is the product of wartime innovation and defence needs. Many other technologies, such as aircraft and trains, were developed to meet peacetime needs but dramatically altered the nature of warfare. Technology does not create war, but it can amplify and intensify warfare and, in turn, reshape the course of a conflict.

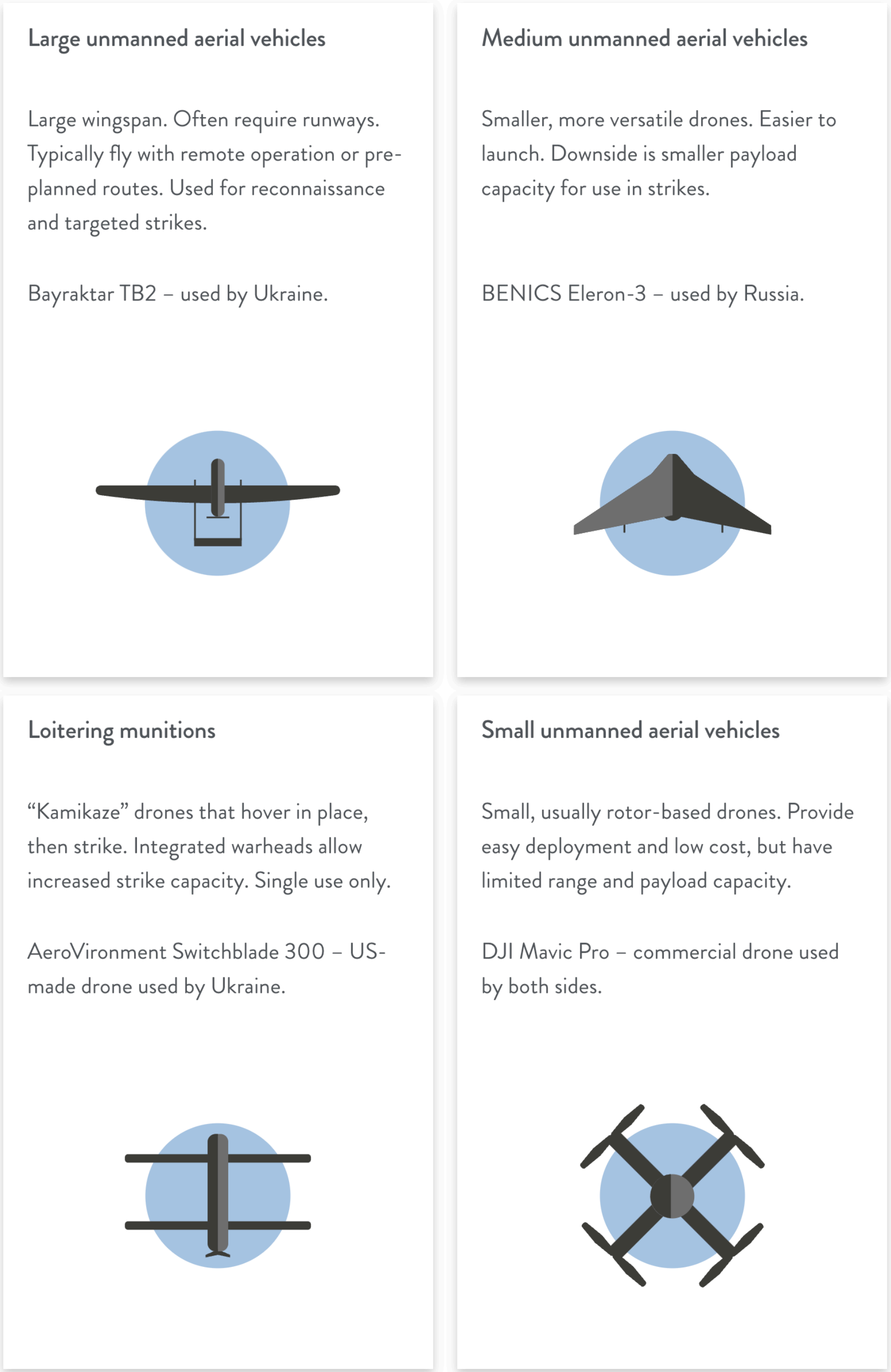
Traditional military-investment models that rely on capital-heavy hardware with long production lines are challenged in the new, integrated domains of war. The modern battlefield encompasses arenas beyond the physical domain – the on-the-ground conflict most people imagine when they think of war. Success or failure now also depends on deterring and defending in the virtual domain. Militaries must prevent malicious cyber operations on critical infrastructure and systems as well as manage the cognitive domain – the use of social media, networking, messaging and interference that distorts thinking, influences action and hinders decision-making. This type of warfare requires access to technologies that can be rapidly deployed across these multiple domains.

Militaries like those in the US and the UK typically depend on subsystems of operational technologies known collectively as C4ISTAR

The Hardware–Software Balance of Power in the Ukraine Conflict

The critical shift in the multi-domain battlefield in Ukraine is the increasingly symmetric use of unmanned aerial vehicles (UAVs): drones and anti-drones. This is heralding a new age of "drone diplomacy" with Iran and Turkey, both of whom benefit from fewer regulatory limitations than the EU or US as to which government clients they can sell technology to; both countries are vying to leverage their geopolitical influence alongside the commercial entities that have been plugging the supply gaps in the interim. There are rumours of Iran supplying its Fateh-110 and Zolfaghar ballistic missiles to Russia, prompting Ukraine's repeated request for Israel to supply its defence systems, in particular: Iron Beam, Barak 8, Patriot, Iron Dome, David's Sling, and Arrow Interceptor.

Figure 1 – The different types of UAVs



Large unmanned aerial vehicles

Large wingspan. Often require runways. Typically fly with remote operation or pre-planned routes. Used for reconnaissance and targeted strikes.

Bayraktar TB2 – used by Ukraine.

Medium unmanned aerial vehicles

Smaller, more versatile drones. Easier to launch. Downside is smaller payload capacity for use in strikes.

BENICS Eleron-3 – used by Russia.

Loitering munitions

“Kamikaze” drones that hover in place, then strike. Integrated warheads allow increased strike capacity. Single use only.

AeroVironment Switchblade 300 – US-made drone used by Ukraine.

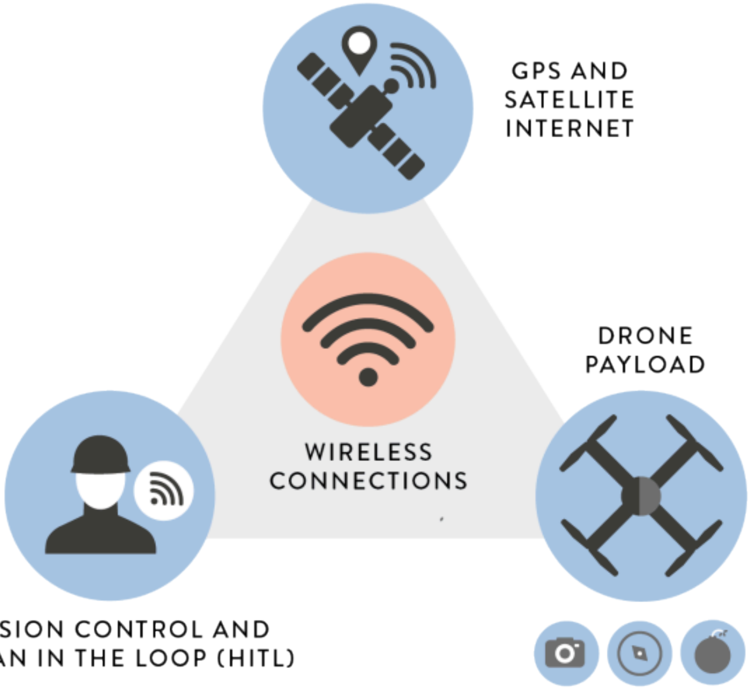
Small unmanned aerial vehicles

Small, usually rotor-based drones. Provide easy deployment and low cost, but have limited range and payload capacity.

DJI Mavic Pro – commercial drone used by both sides.

Source: TBI

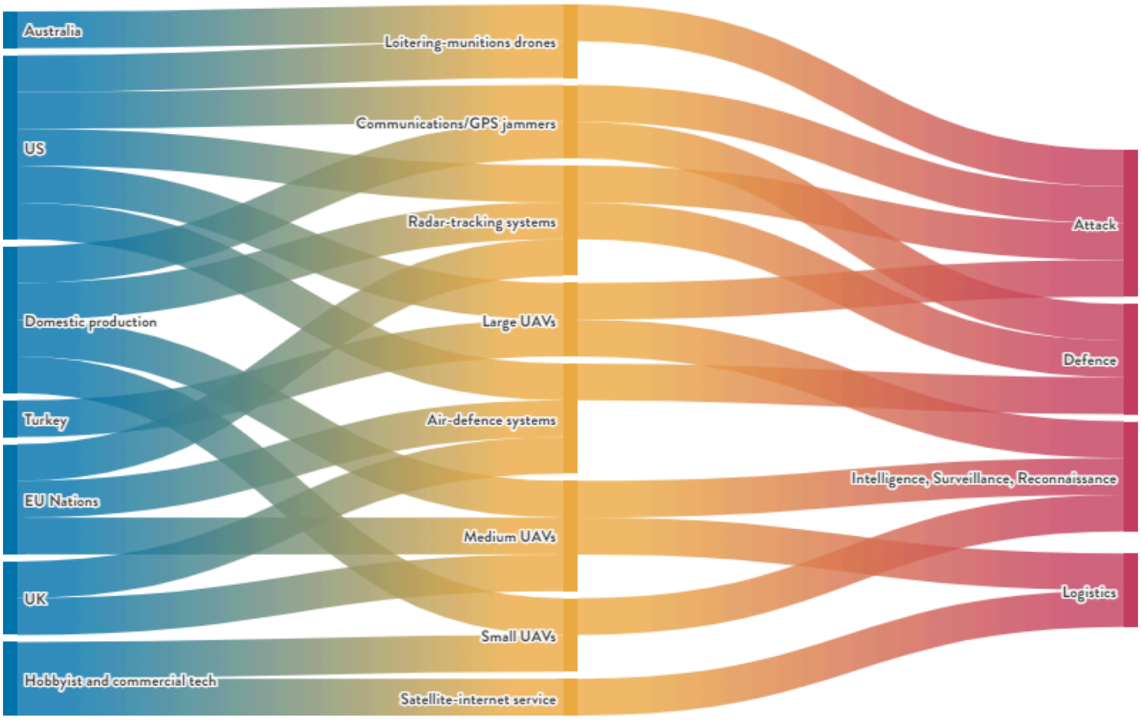
Figure 2 – UAVs and sustainable internet connectivity



Source: TBI

Figure 2 illustrates the importance of the ability to seamlessly weave the multiple flows of disparate civilian and military technology across the physical, virtual, and cognitive domains so that they can work together and integrate into the battlefield workflow. Having access to a single, stable internet source that allows all these elements to connect delivers invaluable strategic advantages.

Figure 3 – Flow of technology to Ukraine's military

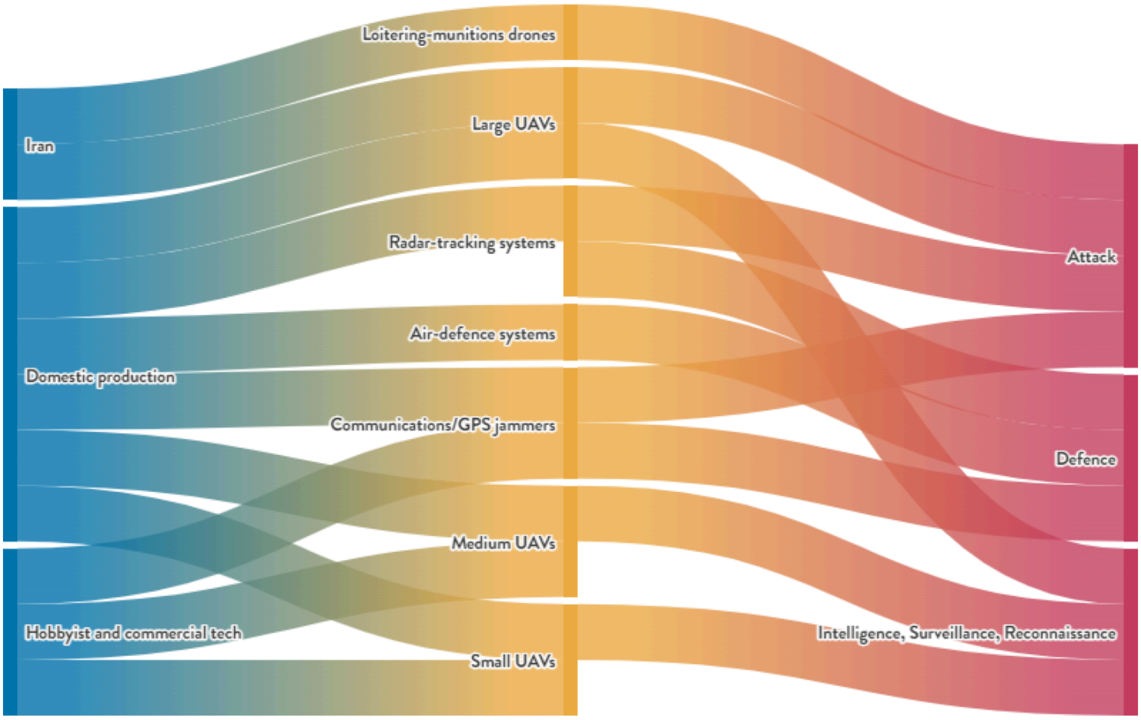


Source: TBI

Ukraine's access to a diverse range of cyber-warriors and hacktivists, tech companies, hobbyists, semi-conductor engineers and platforms is helping tip the hardware-software balance of power in its favour. Ukrainian President Volodymyr Zelensky's platform to address US weapons manufacturers combined with private donors such as Cyprus-based Swarmly drones providing equipment has presented Ukraine with an unprecedented advantage. Russia does not only have to beat Ukraine and its Western weaponry but must also counter new battalions of highly creative commercial companies and individuals.

Russia, on the other hand, despite the influx of Iranian technology, is heavily reliant on its own technology and has only limited access to international support and commercial technology. With sanctions driving a reduced supply chain, Russia is purportedly having to buy commercial jammers, which interrupt the operation of Ukrainian drones, from the Chinese online retailer AliExpress. With its steady and diversified stream of technology that is easily integrated into a stable communications system, Ukraine is creating a new brand of intelligent power that is more suited to the holistic battlefield.

Figure 4 – Flow of technology to Russia's military



Source: TBI

Increased Capability = Increased Vulnerability

With each step taken towards an increasingly intelligent and interconnected capability, myriad vulnerabilities present themselves. Much of the technology is built on open-source platforms, blurring the lines between hobbyist, consumer, commercial and military tools. The fact that many of the tools necessary for effective military capability are produced by private companies leaves countries beholden to tech corporations that may not have the same long-term vision. And technology alone is not enough to fully tip the balance of power without the trained users to operate it.

Open Risks

Open-source projects are foundational to digital technology – and military technology is no exception. This includes Linux, which is fundamental to the operation of most computer chips and operating systems, and essential for almost any device with an embedded computer. Control software and hardware as well as communications protocols for UAVs are based on existing open-source projects such as PX4, ArduPilot, Pixhawk and MAVLink. Python and other programming languages are maintained by a broad base of contributors and open-source committees. Military user interfaces for mission planning and situational awareness leverage open-source projects co-developed by militaries, such as the Android Team Awareness Kit (ATAK) app.

Military researchers, defence firms and subcontractors actively contribute to open-source projects as it is often a more effective way for the military to engage with and maximise the benefits of technical tools and research than if they were to seek to develop these capabilities themselves: not everyone wants to work directly for the military or government. This builds a symbiotic relationship, with the wider community supporting each other's research – particularly academic researchers who often work extensively in open-source projects, which can inevitably tie military research to open-source software. However, academic researchers and open-source communities are becoming more wary of this relationship and beginning to restrict the use of their tools, implementing licensing restrictions which state that the technology cannot be used to cause harm or breach the Universal Declaration of Human Rights.

While these are the best available technical tools, their vulnerabilities are also open to exposure and exploitation. Last year's exploitation of Apache Log4J, which affected 44 per cent of corporate networks globally, including Adobe and IBM, exposed how vulnerable many of the internet's tools are to flaws in open-source projects. This extends to military tech as well. Malicious actors could target projects frequently used by the military. In the US, the Defence Advanced Research Projects Agency (DARPA) is investigating how the dynamics of Linux's development could impact military security. For example, does it matter if sanctioned organisations and individuals are contributing to an open-source project that is, in effect, critical infrastructure for the military?

Credible Commercial Commitment

The privatisation of military contracting coupled with the emergence of large tech firms as military suppliers has blurred the lines between technologies designed for the military and those intended for the use of hobbyists, consumers and industry. Many technologies are also increasingly dual use: satellite internet and drones can be of value in the cornfield and on the battlefield. The rapid escalation of the war in Ukraine has meant both sides are quick to fill resource gaps with consumer-grade equivalents as well as to take advantage of commercial companies to deploy communications systems at speed and scale to underpin the connected military.

Both Ukraine and Russia have been documented using consumer and commercial drones for reconnaissance sourced from the company DJI, a consumer-facing supplier of UAVs. And Ukraine has leveraged Starlink from SpaceX for connectivity as well as cybersecurity and communication resilience from Microsoft, Google, Cloudflare and others to remain in operation amid attacks on its internet infrastructure. Starlink has not only provided the infrastructure but was also able to resist electro-jamming attacks at a pace that even shocked the US military.

However, as we highlighted in our report Disrupters and Defenders: What the Ukraine War Has Taught Us About the Power of Global Tech Companies, there are no clear guarantees as to the long-term engagement of large tech companies and their role in bolstering power in the conflict. Their withdrawal of commitment could come as easily as their engagement and could therefore materially disrupt the course of the war. This vulnerability has been exacerbated recently as Elon Musk threatened to stop paying for Starlink in Ukraine, despite the Ukrainian army's reliance on the service. There is no viable alternative that could be implemented within a year. Similarly, DJI has condemned the use of its drones by both sides, halting sales in Ukraine and Russia. This means that national sovereignty could become dependent not just on access to a specific technology but also on the whim of an individual CEO.

A Specialised Workforce for Intelligent Power

While countries might be able to access technology, gaps in training can limit its usefulness. Some of the world's best hackers and drone pilots aren't associated with the military and are often hobbyists. While they have been leveraged to good effect in Ukraine's IT Army, the piloting of sophisticated drones can be complex and requires training. Aerorozvidka, an NGO in Ukraine, promotes local drone training and development in support of the Ukrainian army: Ukraine's requests for weaponry are often accompanied by the requirement for operator training. Training on sophisticated systems and their best use has been crucial to enabling Ukraine to move away from Soviet-style strategy and tactics and to maximise the benefits of intelligent power.

This reflects the wider competition between militaries for the world's top technical talent, and not only during wartime. After the second world war, the US and Soviet Union competed for rocket and nuclear scientists. Recently tightened US restrictions on semiconductor exports to China may force US citizens working in the industry in there to leave their posts or risk losing citizenship. Geopolitical powers increasingly compete not just over technological resources, but also over the required expertise.

Intelligent Power for Intelligent Warfare

Even as the bombs and bytes continue to fly, the conflict in Ukraine has highlighted the gaps in operational capability in the most advanced militaries, providing lessons for emerging digital economies on how to work with tech companies for more agile access to the most cutting-edge capabilities. As Russia's recent withdrawal from Kherson shows, its Hail Mary reliance on new supplies of 1,700 Iranian "suicide" drones alongside a steady narrative of strategic uncertainty may not be enough to decisively shift the trajectory of the conflict. Bolstering defensive and offensive capabilities in this hybrid physical, virtual and cognitive battlefield relies on a shift from "dumb" brute force to "intelligent" denial and retaliation. Such adaptability is becoming hardwired into Ukraine's approach; Russia is likely to continue to find it a challenge.

Defence and strategic stability are no longer just about spending but also about fostering an environment where the military can act coherently across the physical, cognitive and virtual domains. This requires a whole-nation approach that closes the gap between government and industry so that resource needs can be quickly met and the conceptualisation of the army of 2040 does not wait for the technology of 2040 to arrive but is developed alongside new disruptive technologies. The new technology gateway that is part of the US Department of Defence's redirected Project Convergence is designed to incorporate new technologies into the process. Similarly, in October 2022, NATO held its first Annual Data & AI Leaders' conference, highlighting the that the alliance's success depends on being more agile and more able to work at the accelerated pace of digital transformation.

The ability to rise to this challenge is not determined by a country's size. Israel, which has a defence budget of one-thirtieth that of the US, is able to achieve maximum impact through its innovation by maintaining close relationships between the operational military, military R&D and commercial-technology communities. Its ecosystem that integrates academia, the military and industry has been key to maintaining the country's advantage. NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) project works to build innovation ecosystems that draw together the "triple helix" of government, the private sector and academia to help ensure all countries across the alliance have a strong procurement pipeline of the best technologies to meet the challenge of multi-domain warfare. Rapidly digitalising nations are leapfrogging to this type of procurement pipeline. For example, Rwanda's Fourth Industrial Revolution Strategy is fostering relationships with critical defence-technology companies, such as Israel's Elbit Systems, to help maintain the country's edge and build its talent pipeline.

The ability to integrate the knowledge of all these communities simultaneously and have access to a continuous stream of innovation will enable countries to develop intelligent power. The recent US National Defence Review 2022 highlights that building enduring advantage requires increased support for research institutions as well as working with innovative tech firms and increased collaboration in the private sector.

Access to a stable and resilient communications infrastructure is crucial. Even though the war has not played out in the cyber domain as anticipated, the Russian cyber-attack on Viasat one hour before invading Ukraine and the 196 per cent increase in cyber-attacks on Ukrainian military and government targets in the first three days of the war highlight the importance of ensuring access to an alternative communications facility and the means by which to secure the communications themselves. As the US Department of Defence's Cybersecurity and Information Systems Information Analysis Centre (CSIAC) recently stated: "Whether it be deterrence in the early competition phase or dominance throughout conflict, the invisible, complex, and congested electromagnetic spectrum will be where future battles are won or lost." This has been reflected in the newly released US National Defence Strategy that calls for greater "strength and capability" for resilient command and control to meet the demands of the fast-paced battlefield and ensure "effective coordination of distributed forces."

Tech companies' dominance of the communication infrastructure as they diversify through the internet stack, from devices to subsea cables, allowed for the crucial cooperation to plug the holes in the digital frontier of the conflict. From cybersecurity to relocating critical data, Russia found itself facing not only the brightest military cyber-minds but also the might of the global commercial cyber-community. Creating the mechanisms to call upon this power is the key to accessing the software to win the hard war.

As the character of warfare evolves once more there are several steps that countries and the global order can take to access or facilitate the intelligent power required to prevail on the multi-domain battlefield:

Ensure access to a diversified and resilient supply chain and communications infrastructure: We have previously advocated for a Digital Infrastructure Defence Alliance (DIDA) – a practical mechanism for states to coordinate on regulatory and internet infrastructure issues. This mechanism should also include commitments to plug holes in the critical-tech supply chain and network architecture of members and allies, either individually or in concert with commercial companies.

Encourage and equip tech companies to have a robust and transparent policy for engagement in international crises: With tech companies able to tip the balance of a conflict through their collective engagement, greater transparency is needed with regard to their decision-making about intervention and withdrawal. As heroic as Starlink's initial intervention was, negotiating military agreements on Twitter can reverse gains and lead to strategic vulnerability. Creating a geopolitical crisis board of experts and key policymakers that can provide clear guidance on a company's priorities and commitments as the conflict shifts is vital to long-term strategic stability.

Foster close-knit tech ecosystems that allow mutually beneficial circulation of innovation between sectors: Countries with siloed tech ecosystems are finding themselves ill-equipped to respond to the demands of the hyperconnected battlefield. Fostering innovation for this context requires a tech ecosystem where, similar to countries like Israel, there is a close nexus between the military and commercial tech companies. This increased collaboration with tech companies is crucial for long-term advantage on the future battlefield.

Integrate tech expertise into foreign policy: Leveraging successful relationships and partnerships on global tech issues with states and companies requires states to build a capacity in which tech is fully understood and plays an active part in its foreign-policy agenda. From educating diplomats on emerging technologies to ensuring representation in key tech hubs and shaping global tech norms, states will be able to amplify their intelligent power on and off the battlefield.

FOLLOW US

facebook.com/instituteglobal
twitter.com/instituteGC
instagram.com/institutegc

GENERAL ENQUIRIES

info@institute.global

FIND OUT MORE
INSTITUTE.GLOBAL