Technology and Geopolitical Crisis – A New Compact for a New World Order

Pete Furlong, Tony Blair Institute for Global Change, United States (p.furlong@institute.global)
Melanie Garson, Tony Blair Institute for Global Change, United Kingdom (m.garson@institute.global)

Abstract

The Ukraine War has exposed the sensitive role the global internet plays in crises across the world. Governments need to improve their capacity to engage on tech issues through the allocation of dedicated tech diplomats and the education of foreign service officials on tech policy. Tech companies need better access to the international community to formulate clear policy based on global norms to respond coherently to geopolitical crises. A new compact that combines geopolitical understanding with the might and creativity of the tech sector will bring a new commitment and energy to the UN SDGs.

The internet is the foundational backbone of our 21st century life. However, as geopolitical divides threaten its integrity, tech companies are stepping in to fill the void with immense power over key resources, wielded both for manipulation and stabilisation. Ensuring that they and digital technologies remain a "force for good" as this new world order navigates this era of "polycrisis" requires a new compact.

New Guardians of Internet Resilience

Internet usage in the Global South is growing but the provision of secure infrastructure by states is "lagging" (Calederaro & Craig, 2020), and states alone may be unable to guarantee the stable and reliable access to global connectivity as articulated SDG 9C. The "quality, reliant, sustainable and resilient infrastructure" for economic development and human well-being (SDG Target 9.1) depends on a complex interaction of multiple layers spanning from submarine cables to satellites, many of which now lie in the hands of private tech companies.

Diversified and consolidated, through the internet stack, tech companies are now the guardians of global connectivity and the underwriters of internet infrastructure resilience. While this may offer the advantage of agility, they sometimes lack the geopolitical expertise and incentives to always act responsibly. This requires not only new transnational approaches to infrastructure resilience but a new compact for transnational public-private partnership.

The Ukraine War

The conflict in Ukraine has brought sharply into focus the power of internet access and by extension the internet itself to fundamentally alter the trajectory of the war.[1] This in turn has depended on layers of tech companies, including:

Internet platforms such as the messaging apps Telegram and Signal which both saw massive spikes in installation, in Ukraine and Russia at the outset of the war, have provided crucial access for the dissemination of information.

Critical hardware and devices manufacturers that provide the semiconductor chips, sensors, and computers underpinning cell phones used by soldiers for communications on the battlefield to civilian use of personal devices for threat alerts,

Essential Internet Services and Access Control providers such as Microsoft and Cloudflare that have been instrumental in protecting citizens and government with cybersecurity and cloud infrastructure.

Internet Infrastructure and "Backbone" providers such as Starlink, that has enabled Ukraine to communicate on the battlefield despite the devastation of infrastructure through Russian bombing.

Lack of Clarity for Complexity

Whilst the response of tech companies has been unprecedented states and companies have struggled to engage effectively. This has led at times to a lack of coherence across policies. From diplomacy by Twitter to more traditional avenues political pressure, sanctions regimes, and new legislation, there have been conflicting messaging over key objectives that could undermine internet resilience. The sanctions regime threatened the rights of ordinary Russian to have universal access to connectivity. Exemptions to sanctions on Russia for basic internet connectivity were

[1] *See* Furlong & Garson (2022) "Disrupters and Defenders: What the Ukraine War Has Taught Us About the Power of Global Tech Companies."

not immediately granted and required significant lobbying efforts from civil society organisations. However, this came too late for some organisations such as Cogent Communications and Lumen who had already pulled out of Russia, partly due to the lack of clear policy (Access Now, 2023) .

Tech companies have also wavered in their commitments. Private alternatives to connectivity, have been vital in counteracting Russia's deliberate strategy of cutting internet access. Yet, this new dependency has also caused instability. Starlink. despite their importance to Ukraine's defence has threatened to stop funding, and restrict use of SpaceX for drones, possibly putting Ukraine at greater risk.

In an era of increasing converging crises, the risks exposed by the Ukraine War are not fading. Ukraine benefited from strong Western support, both politically and in the public sphere, making the case for tech company action relatively clear. In other contexts, it may not be so straightforward. Tech companies have struggled to balance their engagement in more complex crises such as Myanmar and Ethiopia, and the closure of international offices as part of the tech downturn, such as that of Twitter's only African office could leave it ill-prepared to address global challenges. And it is still not clear how they will fully address the crisis-inducing potential of generative AI systems and similar emerging technologies that could be exploited in misinformation campaigns, reduce the barrier to generating synthetic media, deep fakes, and malicious content.

Defenders in the Firing Line?

Tech companies have taken on crucial roles as active defenders, particularly in their provision of cybersecurity and defensive cyber tools from the first moments, and even before, the invasion of Ukraine. However, this convergence of actors on the front line of defence places tech companies on the front line for retaliatory cyberattacks and offensive action from nation states. Private company engagement could find themselves legally participants to the conflict (Zetter, 2022).

While Microsoft has been clear that it's support is entirely defensive as any offensive action would violate its pledge made as a part of the "Cybersecurity Tech Accord,"(Zetter, 2022) Google's Threat Assessment Group (TAG) anticipates Russian cyber attacks expanding to NATO partners as the conflict continues (Google, 2023).

Similarly, with the lines between consumer and military tech blurry, and many militaries relying on consumer tech for military use,[2] could find themselves construed as participants to the conflict.

Towards a New Compact for A New World Order

A resilient and stable global internet is fundamental to steady progress on the SDGs. With increased dependency of tech companies to provide this, a new holistic compact is needed that:

1. Increases state capacity and channels for engaging with tech providers
2. Incentivises coherent private company approaches and processes for handling geopolitical crises
3. Builds greater coordination between stakeholders.

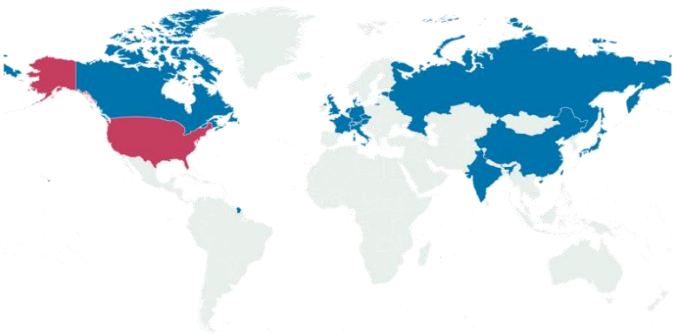
States need increased tech foreign policy capacity:[3]

All nations must improve their capacity to engage with tech and tech providers on key foreign policy and geopolitical issues. This will close the knowledge gap on ICTs and provide for more nuanced specialised diplomatic engagement in key multilateral processes including the Group of Government Experts and Open-Ended Working Groups.

Countries are increasingly appointing dedicated tech diplomats and focusing foreign policy resources on how they engage on tech issues. This rollout has been unequal, however, particularly lacking nations from Africa, and providing a lack of nuanced global voices at the table on emerging governance on key tech issues. Countries need to be supported in building a new tech-forward foreign-policy to be able to fully leverage the possibilities of tech partnerships for digital resilience.

[2] *See (*Garson, Furlong, & Kakkad, 2022) Software and Hard War: Building Intelligent Power for Artificially Intelligent Warfare,.
[3] *See* (Erze & Garson, 2022) A Leader's Guide to Building a Tech-Forward Foreign Policy.

Figure 2. Countries that appointed a dedicated office or team within foreign-affairs ministries



Data Source: Tony Blair Institute for Global Change

Companies need new models for self-governance and engagement in geopolitical crises:

Tech companies need a robust and transparent geopolitical policy for their engagement in crises. As the Ukraine War enters its second year, support has required sustained effort from companies, something that's not always considered when getting involved. Private companies need to balance their obligations to the international community and internet resilience with their obligations to shareholders. This could lead to tensions as a conflict becomes longer and intractable. A clearly established policy would help manage expectations and increase stability in future crises.

However, belt-tightening at many tech companies threatens the prospects for geopolitical policy initiatives. This is even more pronounced at smaller tech firms. Governments will need to provide the support and incentives to ensure that tech companies are able to fully contribute where needed in crises.

Coordination across stakeholders to ensure resilient internet infrastructure:

Cyber defence informal collaboratives provide good examples of constructive mechanisms for collaboration and facilitation of strong communication and trust among stakeholders. The United States Cybersecurity and Infrastructure Agency (CISA)"s Joint Cyber Defence Collaborative, aligns capacity between US federal cyber officials and top cyber firms. Modelled on this the Cyber Defence Assistance Collaborative has played a crucial role in support of Ukraine and could be a strong model for future crises.

NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) also provides a model for building opportunities for strategic alignment between tech development and NATO's objectives.

However, continuous coordination is needed to preserve global internet resilience in peacetime as much as during conflict. This requires engagement with global forums with multistakeholder representation.

Tech companies should seek representation and presence at existing global forums, such as the UN. While Microsoft has opened an office at the UN, this may be out of the reach of smaller companies and a new mechanism is needed for tech companies to have more consistent observer status at the UN.

Conclusion

The free, secure, open and interoperable internet is the heart of human security and global digital prosperity. Increased private and corporate control of the internet may provide the agility to intervene rapidly however it carries risks. Adequate resources and mechanisms must exist to align tech company actions with globally agreed-upon values and objectives, such as the SDGs, universal internet access, and democratic principles. Crucially in a world of polycrisis, amplified by tech, it is time for new compact with tech companies to underwrite the resilience of the internet for good.

References

Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Furlong, P., & Garson, M. (2022). *Disrupters and Defenders: What the Ukraine War Has Taught Us About the Power of Global Tech Companies*. Tony Blair Institute for Global Change. https://institute.global/policy/disrupters-and-defenders-what-ukraine-war-has-taught-us-about-power-global-tech-companies

Access Now. (2023). *Weapons of Control, Shield of Impunity: Internet shutdowns in 2022*. https://www.accessnow.org/cms/assets/uploads/2023/03/2022-KIO-Report-new.pdf

Zetter, K. (2022, Dec 7). Security Firms Aiding Ukraine During War Could Be Considered Participants in Conflict. *Zero Day*. https://zetter.substack.com/p/security-firms-aiding-ukraine-during

Google Threat Assessment Group. (2023). *The Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

Furlong, P., Garson, M., Kakkad, J. (2022). *Software and Hard War: Building Intelligent Power for Artificially Intelligent Warfare*. Tony Blair Institute for Global Change. https://institute.global/policy/software-and-hard-war-building-intelligent-power-artificially-intelligent-warfare

Erzse, A., & Garson, M. (2022). *A Leaders' Guide to Building a Tech-Forward Foreign Policy*. Tony Blair Institute for Global Change. https://institute.global/policy/leaders-guide-building-tech-forward-foreign-policy