Cyber is not just for Conflict: Lessons from Ukraine for Coordination & Resilience

AESCON, June 2023
Dr. Melanie Garson

Cyber Policy Lead
Acting Director, Geopolitics
Tony Blair Institute for Global Change
Ukraine & the World Remains Under Attack

Cyber Attacks Russia-Ukraine Q1 2023
New cyber actors are tipping the balance of power

How the cloud saved Ukraine’s data from Russian attacks
Microsoft gives away "$400m in cloud support' to Ukraine
Ukraine government is seeking alternatives to Elon Musk’s Starlink, vice PM says
Ukraine in direct contact with Musk amid Starlink drama
The Battle for Control Over Ukraine's Internet
The degrading treatment of Ukraine’s internet
And how the Ukrainians are responding

Satellite internet is a hot new commodity in Ukraine
Starlink is being used by the military and hospitals, but its signal is weaker on the front line

Disinformation fight goes beyond Ukraine war: Five of the most viral misinformation campaigns since the conflict began
Disinformation campaigns on Ukraine are complicated by their absence

Exclusive: Ukraine has started using Clearview AI’s facial recognition during war
Inside a US military cyber team’s defence of Ukraine
Platforms & hardware have led the discourse

Russia fights back in information war with jail warning

Source: Reuters
But private actors have been pivotal at every level
And are consolidating their geopolitical significance
Across a range of geopolitical crises
The More Capability = More Vulnerability
And cyber attacks are on the increase

Global attacks increased by 28% in the third quarter of 2022 compared to the same period in 2021. The average weekly attacks per organization worldwide reached over 1,130.
And will keep increasing

FIGURE 1 | Global Cybersecurity Outlook 2023: key findings

93% Cyber leaders

Business and cyber leaders believe global geopolitical instability is moderately or very likely to lead to a catastrophic cyber event in the next two years.

86% Business leaders

JANUARY 2023
With far-reaching implications

COSTA RICA DECLARED NATIONAL EMERGENCY AFTER MASSIVE HACK
So, what’s the problem?
Four key problems:

1. Clarity
2. Consistency
3. Coherence
4. Commitment
Coordinating with Tech Companies for the next cyber-enabled geopolitical crisis?

1. Formulate a robust & transparent geopolitical policy
2. Create an internal geopolitical crisis board
3. Build representation in key centres of geopolitical decisionmaking
4. Establish and join a self-regulatory geo-technology board
Contact us
Melanie Garson
Cyber Policy Lead
m.garson@institute.global