THE NATIONAL INTEREST

Why Can’t Cyber Scholars Move Beyond the Basics

By Brandon Valeriano

August 7, 2022

Instead of pushing knowledge forward, the field of cybersecurity in geopolitics has mostly become about explaining why something didn’t happen rather than why it did.

The most exciting part of the scientific process and research is the process of discovery and figuring out something that you did not know before. Being a scholar and researcher is about feeling stupid from time to time, scratching at the edges of knowledge to push the field further. The struggle for many observers and scholars in the cybersecurity community is that it’s difficult to feel stupid. There are few challenging questions in cybersecurity, rather, the truly remarkable thing about cybersecurity is the complete lack of novelty. The questions are always the same and rarely evolve. Is this a cyber war? Can cyber deterrence work? Will cyber operations help states during wars and change the nature of warfare?

Instead of pushing knowledge forward, the field of cybersecurity in geopolitics has mostly become about explaining why something didn’t happen rather than why it did. The entire concept of cyber war has been inflated to such a point that every modern movie seems to include the necessary shot of the hacker winning the day.

Science is about feeling stupid about what you don’t know, not looking around the room constantly wondering why you think every other research question on offer is blitheringly simple or represents a dream for the future.

The Lack of New Ideas

How does a major form of interaction that has certainly changed twenty-first-century life, the internet, lead to a stagnant research field that appears no different over decades? Why are there no new ideas in cybersecurity?

After nearly five months of a reckless and norm-busting conventional war in Ukraine, the cybersecurity community is still asking when the cyber war will start. When a cyber conflict did not materialize, pundits fell back on the typical claim that it was really happening, but we just couldn’t see it. The cyber war is mainly fought in the shadows, or perhaps the "Upside Down" like in *Stranger Things*. It's all there, we just don’t know where to look, apparently.

For all the reported success of Ukrainian resistance, precision targeting, and coordination between forces to deny the Russians any advantage, a team of NATO scholars had the complete inability to recognize hyperbole when they claimed that "cyber-operations have been Russia's biggest military success to date in the war in Ukraine." Cybersecurity has main character syndrome, a term used to describe the lust for attention in the new generation, with cyber playing a key role in every story about the future of geopolitics.

This need to be the main character in a devastating war of conquest is no more apparent than in Microsoft's series of cybersecurity reports. They note that cyber war is happening and that there is coordination between military and cyber action, with Microsoft standing as the defender between chaos and order in Ukraine.

Unfortunately, it is still not clear how Microsoft defines cyberattacks. Coordination is never demonstrated beyond a correlation between an event one day and another the next day, providing no evidence that these events are connected and centrally directed. Instead of noting the importance of the defense and providing lessons for the community, Microsoft hunts for answers to questions they presume we are asking, such as where is the cyber war?

Overcoming the Challenge

This article presents a challenge to the cybersecurity community to develop new and interesting questions. If we were playing bingo with old and discredited concepts such as cyber privateers, building public-private partnerships, offensive advantage, or the need to enable deterrence, every observer would be waving their winning card in the air. The field of cybersecurity has the strange inability to develop new questions while at the same time making "cyber" the hero of every story.

Progress only comes through new explorations of unconventional ideas. For example, instead of focusing on rural access to broadband and increasing diversity in the field, why not put things into action by trying to solve the digital redlining issue which limits access? Digital redlining is when poor and minority communities in major urban areas have limited access to broadband, severely constricting educational opportunities and creating workforce pipeline issues in the first place.

Instead of focusing on the need to achieve coercive effects in cyberspace suggesting that the cyber offense has the advantage, how about we study the impact of cyber actions on behavior first before providing strategic solutions? Precision is needed in research; investments should only come through clear evidence of an impact, all hallmarks of social science.

Without novelty, cybersecurity will continue to fail as a field. There is no progress in cybersecurity. Instead, there are frequent setbacks and academic arguments that go in circles with no clear resolution. It would be nice to feel stupid from time to time when reading the next emerging generation of cyber security scholarship. Progress here will require throwing off the shackles of expectation and searching for novelty.

Brandon Valeriano is a senior fellow at the Cato Institute and a distinguished senior fellow at the Marine Corps University.