Cyber conflict as an academic discipline: it’s no all doom-and-gloom

Collier, J.; Kaminska, M.

COUNCIL on FOREIGN RELATIONS

from Net Politics *and* Digital and Cyberspace Policy Program

Cyber Conflict as an Academic Discipline: It's Not All Doom-and-Gloom

Although there are challenges facing the study of cyber conflict, they are not insurmountable.

Rick Collins/University of the Fraser Valley via Flickr

Blog Post by Guest Blogger for Net Politics

September 18, 2018 2:45 pm (EST)

Jamie Collier and Monica Kaminska are PhD students at the University of Oxford. You can follow them at @TheCollierJam and @monica_kaminska.

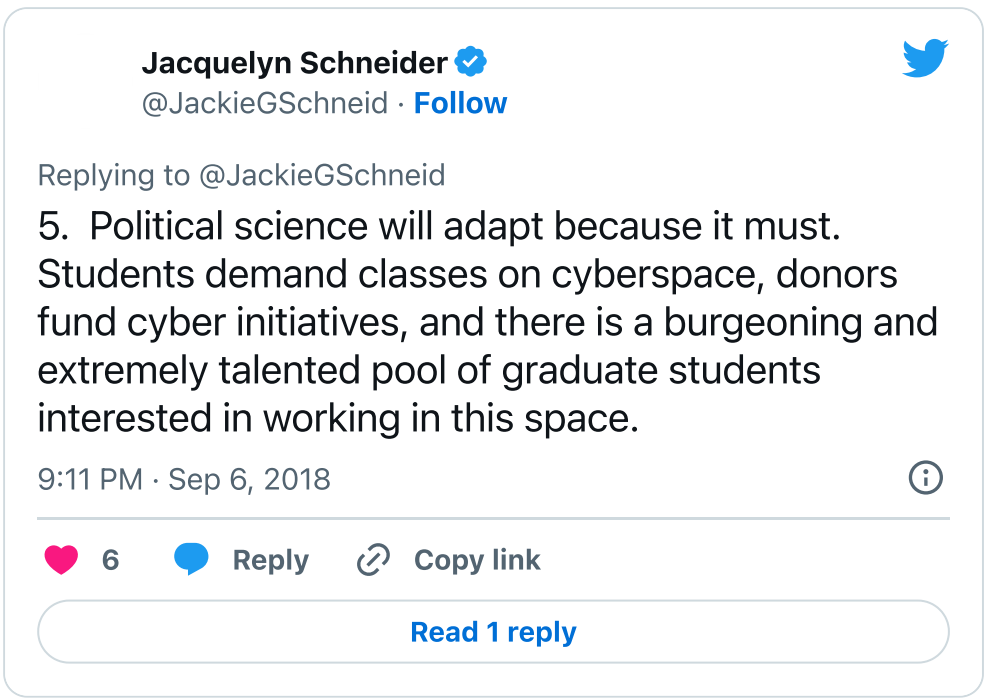
As few weeks ago on *Net Politics*, Melissa K. Griffith laid out the challenges facing academics who want to study cyber conflict. She highlights the start-up costs young academics face, the scare availability of data, and the barriers to publishing. Her post sparked a lively discussion on Twitter.

We are slightly more optimistic at the prospects of studying the intersection of politics and cyber conflict.

Although Melissa is right that there may be no single foundational cybersecurity text as there might be in the study of nuclear weapons, a solid base of literature is now emerging. The first major debate in the field considered the disruptive capacity of the new technology and its implications for international security, with works by Martin Libicki, John Arquilla, Lucas Kello, Thomas Rid, and Jon Lindsay forming the essential reading. The field has largely now moved past these first-order questions and onto exciting fertile ground with topics including the applicability of deterrence to cyber conflict, its escalatory dynamics, the role of proxy groups, and the mechanics of cyber capability proliferation. Scholars have also looked at the construction of the cyber threat in national security policies, public-private dynamics and the cultivation of norms.

Another issue that is frequently brought up is the shroud of secrecy that cloaks cyber operations, making it difficult for academics build datasets. Yet, the nature of the technology means that knowledge of individual cases often finds its way into the public domain. This is helped by the growing number of competent cybersecurity journalists and threat intelligence companies that are constantly monitoring the landscape for new malware and publicising state-sponsored operations. While large-n quantitative analyses of the cyber domain may therefore obscure more than they illuminate, qualitative approaches can yield important insights into the significance of cyber operations for international order. Political science has a long tradition of adapting to imperfect datasets—cyber conflict should be no exception.

There is also much to be positive about the structure of the discipline. The high interest levels amongst the public, relevance to current affairs and shortage of qualified thinkers provide opportunities for younger academics to accelerate their careers and publication records. Outlets such as the Journal of Cybersecurity offer prospects for meaningful interdisciplinary research, and political science outlets are not always as conservative as may appear. Individual scholars are developing new methodological approaches to adapt to the unique challenges the field faces, as Danny Moore and Thomas Rid have done to search the dark web.



The outmoded distinctions that have been historically established between various academic disciplines often fail to reflect contemporary reality. Cybersecurity is one topic that stumbles into various university departments and puts political science and international relations into an identity crisis of sorts. There are certainly some very traditional political science issues to explore in cybersecurity (many of which do not require a technical background): the role of norm entrepreneurship, the way various international organizations compete to capture the cybersecurity remit, and the nature of cybersecurity governance. Yet, operational areas often sit awkwardly with political science. For many cyber campaigns, it is not always clear how these areas fall into broader understandings of the international system. This might mean developing new conceptual models within political science, yet there is also a compelling case for studying such topics from a different perspective. As Jon Lindsay noted on Twitter, intelligence and counterintelligence studies offers a fruitful, albeit neglected, framing for studying a great deal of today's cyber activity.

Of course, many political science publications lack an appreciation for technical issues that might be necessary to publish on certain cybersecurity issues. Technology-focused boot camps would be one welcome initiative. But tooling-up political scientists is not a silver bullet. Cybersecurity requires an eclectic range of skill sets—ranging from malware analysts and penetration testers to strategists and policy experts—and it is impossible to assume someone to have a mastery in all these skill sets. Political scientists, from professors to PhD students, would benefit from closer collaboration with colleagues in other disciplines. The Oxford University Centre for Doctoral Training in Cyber Security provides one interesting model by building an interdisciplinary cohort that enables political scientists to connect and collaborate with those more technically-minded. (Full disclosure: we are affiliated with the centre).

Finally, academics studying cyber conflict need to think much more radically about bridging gaps with other cybersecurity communities. FireEye offers a wealth of insight in understanding emerging threat actors; adversary hunter Joe Slowik has

brought much-needed nuance to the offence-dominance debate; while few political scientists have written as eloquently on attribution as security researcher Juan Andres Guerrero-Saade. There is a broader information security community out there; political scientists would do well to acknowledge it.