Interview - Andreas Haggman

https://www.e-ir.info/2018/06/03/interview-andreas-haggman/

E-INTERNATIONAL RELATIONS, JUN 3 2018

This interview is part of a series of interviews with academics and practitioners at an early stage of their career. The interviews discuss current research and projects, as well as advice for other young scholars.

Andreas Haggman is a PhD researcher at the Centre for Doctoral Training in Cyber Security at Royal Holloway University of London. His thesis investigates the use of tabletop wargames for cyber security education. Andreas' wider research interests lie in non-technical cyber security topics and he has published on national cyber security strategies, cyber deterrence, and offensive cyber. Andreas received BA (Hons) and MA degrees from the Department of War Studies at King's College London and has professional experience in video games, retail management, the defence industry, and scenario development. He can be followed on Twitter @Andreas_Haggman.

What (or who) promoted the most significant shifts in your thinking or encouraged you to do research?

I really stumbled into my PhD thesis by accident. As part of the training programme at the Centre for Doctoral Training (CDT) in Cyber Security at Royal Holloway University of London, all students are required to complete a 'summer project' at the end of their first year (equivalent to a Masters-level dissertation). For my project, I wanted to work with an external company and partnered with professional services firm KPMG, who supports the CDT. Rather than prescribing a project, the company preferred that I suggest some ideas and I had seen wargaming mentioned on one of KPMG's blogs. Despite having no formal background in wargaming, I pitched this topic, along with a selection of others. KPMG responded that they had someone in the company who was keen to work with me on wargaming; this person happened to be David Ferbrache (at the time on secondment to KPMG from his day job as Head of Cyber and Space for the MOD). David was keen to create something "actionable", which really inspired me, and the project was a success in that it created a useful game prototype which was well-received in the wider wargaming community. I took all this enthusiasm as a vote of confidence in the subject and decided to continue with wargaming for my thesis, which is not at all what I expected when starting the PhD programme!

Your thesis focuses on the use of wargames to analyze cyber-attacks. What are the advantages and limitations of the use of wargaming in relation to cyber-attacks?

My specific approach is to use manual tabletop wargames – not a computer in sight here! – but this can have some drawbacks because cyber security is inherently a computerised topic. Notably, there are three limitations with manual games when it comes to modelling cyberspace. Firstly, there is the issue of visibility. Translating a non-spatial concept into a two-dimensional game board can be tricky, and accurately representing information disparities between different actors can involve complicated gameplay mechanics. Secondly, time flows are not straightforward. Cyber operations shift in pace throughout their lifecycle, from months or years in planning and preparation to milliseconds in actual execution, after which protracted investigation and repercussions phases can last months and years again. In board games, we ideally want a game turn to represent the same amount of real time, yet the time flows associated with cyber-attacks can make this difficult. Finally, there are constraints on determining capabilities. Cyber capabilities do not physically manifest themselves like tanks or cruise missiles. So, perceiving and measuring the capabilities of any given actor is very difficult. This problem is exacerbated by the often secretive and classified nature of cyber capabilities, which often complicates research and makes it difficult to accurately portray actors' capabilities in a game.

Counteracting all of this, the primary advantage of using manual games is their flexibility. Rather than trying to accurately model the world and grappling with the problems outlined above, my approach has been to create a game model *inspired* by the real world. As players engage with the game, it is then up to them to identify the inaccuracies of the model and explore the nuances of cyber security through discussion. By giving players a flexible game model, they can make modifications simply and quickly to reflect their interpretation of the world. Because the game is analogue rather than digital, no programming or graphics skills are required to make these alterations, just imagination and creativity (and maybe some rudimentary arts and crafts).

Since Stuxnet, many governments have resorted to cyber-attacks to either complement or replace conventional methods of achieving their political or military objectives. Do you believe establishing a system of deterrence to mitigate the consequences of cyber-attacks is possible?

I have been sceptical of cyber deterrence elsewhere and remain unconvinced that pure cyber deterrence is viable. There are fundamental problems with credibility (how you can prove you definitely will retaliate) and attribution (although the UK and other states have been more amenable to pointing fingers lately), and the kind of red lines required to establish norms of behaviour are not straightforward. There have been suggestions that we move the thinking away from deterrence by threat (classical nuclear deterrence) to deterrence by denial (have such strong defences that any attack would be unsuccessful) and this to me seems like a more promising approach. In cyberspace, the difficulty is that the attacker is normally regarded to have the upper hand. So, establishing strong enough defences may be an impossibility.

Given the inherent uncertainties of cyber-space what are key issues governments should consider while establishing their cyber-security strategies?

That depends on what their policy goals are. Strategy is traditionally understood as the link between ends and means. Accordingly, any strategy must have a clear conception of what the government wants to achieve and what levers (economic, diplomatic, military) it has at its disposal. Having said that, a couple of issues are prevalent in cyberspace that will invariably affect any cyber security strategy. The first is instability. Cyberspace is a domain of constant hostile activity, by both state and non-state actors, and no one is immune. Therefore, no cyber security strategy should be formulated in an imagined vacuum where the focus can simply be on economic growth and prosperity; it must also actively tackle threats. Secondly, global international consensus on cyberspace does not exist. International agreements have proven notoriously difficult to establish (look at the failure of the UN GGE process) and the Western view of cyberspace is not necessarily shared by other influential actors, notably Russia and China. Seeking solutions that are using old governance structures is therefore unlikely to work, and how we go forward establishing new structures will be a major challenge in the coming years. Indeed, the whole question of governing cyberspace is up for a debate and cyber security strategies should be cognisant of the different views on this issue.

Compared to conventional methods, the enhancement of cyber capabilities is relatively easy for small states or non-state groups to achieve. Do you think this could cause a shift in the balance of power in relation to conventional or cyber warfare?

I agree that it is easy to gain basic disruptive cyber capabilities, anyone can download the Low Orbit Ion Cannon and launch DDoS attacks. Additionally, cyber espionage capabilities with low-to-moderate sophistication have allowed some small states like North Korea to achieve outsize effects such as hack of Sony Pictures. However, this becomes less true when we look at high-end cyber capabilities which have physical effects. The likes of Stuxnet (targeting the Natanz Iranian nuclear facility) and Black Energy (affecting the Ukrainian electricity grid) require considerable effort to acquire, often involving months of painstaking technical research backed by a comprehensive intelligence machinery. Cyber capabilities should not be viewed as isolated from conventional capabilities. Existing economic and military clout often translates directly into cyber prowess, just as it does conventional prowess. We may see a shift in the balance of power because some big states like Russia and China seem more adept at harnessing cyber capabilities to greater effect, but I do not think small states and non-state actors can rise to prominence based solely on possession of cyber capabilities. Furthermore, in warfare, geography still matters: physical control of an area cannot be achieved through cyber means. Conventional capabilities will therefore have an important role to play in conflict going forward. Just like air power did not obviate the need for armies and navies, cyber capabilities will not obviate the need for conventional forces.

What are you currently working on?

Primarily, I am finishing off my thesis but as always there are far too many exciting things to get involved in (like this interview!). I am currently working on a short article about how ‘medium powers’ can use cyber capabilities to enhance their conventional capabilities – very related to the question above. In the near future, I will also be producing one or two journal articles based on thesis chapters.

What advice would you give to young scholars?

Network, network, network. Unfortunately, the old adage holds true that opportunities come from who you know, not what you know. My thesis journey has taken me to some fascinating places to meet some fascinating people, but none of it would have happened if I wasn’t willing to go to events and get my work out there. Even the most brilliant research can fail to gain traction unless it is actively promoted at conferences and workshops and, perhaps more importantly, in the coffee breaks at these events. If you are not confident presenting or comfortable networking, your university likely has training courses to help you develop these skills, so take advantage of these.

–

This interview was conducted by Kübra Öztürk. Kübra is an Associate Features Editor for E-IR.