This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Interview - Daniel Moore

https://www.e-ir.info/2018/11/11/interview-daniel-moore/

E-INTERNATIONAL RELATIONS, NOV 11 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.

Daniel Moore is a PhD researcher at King's College London's Department of War Studies where he focuses on the application of network operations to military doctrine and strategy. Daniel has experience both in the public and private sectors, having previously served as a lieutenant in the Israel Defense Forces and later working in companies such as IBM. Alongside his academic research, Daniel works as a lead threat intelligence engineer.

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

A few people had significant impact on me throughout my life. My mother is a well-published sociology professor, and as I grew up her passion for research was infectious. I was hands-on with computers early on and was very eager to learn by breaking things and experimenting. During my BA, I had one lecturer in political philosophy – a topic normally way outside my comfort zone – who was unbeknownst to him, really inspiring me by making the topic so fascinating. But probably the biggest nudge came a few years later when I noticed that my MA at King's College London's offered a cyber security module. I was pretty experienced with the practical aspects of cyber security by then, so, I was very curious to see what the academic side of it looked like. Professor Thomas Rid, who was teaching the class at the time, painted an image of a nascent field with a lot of unrealised potential and a strong need for some inter-disciplinary scepticism. He was inclusive and encouraging, which eventually led to me pursuing the PhD with him as my supervisor at the department a couple of years later.

What would indicate a state of war between states in relation to cyberwarfare?

The classic notion of a "state of war" is generally eroding in modern conflict. Many of the key international players are investing resources in these sub-warfare scenarios that still look like war, if you take a hard-enough look. For example, despite overwhelming evidence, Russia maintains a narrative that it is not at war with Ukraine. At the same time, the war that tore Syria apart is an absolute nightmare of competing powers, regional or otherwise; yet the story of a Syrian civil war persists. It's now common to undertake operations that skirt the classic definitions of inter-state war.

Offensive cyber capabilities play naturally into this narrative. Attacking adversary networks is a convenient way to reduce the overtness of hostile intent. We see this already, especially in operations undertaken by Russia against various Ukraine networks and infrastructure. So, while we can't say necessarily what leads to a "state of war", nations can establish strongly communicated and enforced red lines which would incur consequences if overstepped. It's less about defining a state of war, and more about defining the boundaries of acceptable operations in and against networks. We reluctantly have to accept that network-based espionage will always exist but attacking critical infrastructure or breaching national sovereignty by compromising elections has to elicit stronger responses against the parties who do so.

What effects do you think the stronger offensive network capabilities of a state can have on inter-state conflict?

It strangely makes it both more surgical and more indiscriminate at the same time. Network operations allow nations to carefully craft attacks over many months, traversing networks, identifying the specific targets and desired effects. In some cases, such as Stuxnet or the Ukrainian energy grid attacks, a network attack enabled focused operations that would largely be impossible by a conventional attack without triggering all-out war. That's significant for the countries who capitalise on that potential. Successful offensive network operations can create a controlled specific impact that would be difficult to create otherwise. They also allow doing so at range, so targeting adversaries around the world becomes a more plausible possibility.

On the other hand, the potential for rampant collateral damage has never been more significant. As we saw with the NotPetya worm which crippled commercial and public entities around the world despite (seemingly) targeting Ukraine, things can quickly get out of hand. With everyone so reliant on the same global internet, destructive network attacks can easily extend beyond their targets to have uncontrollable and unpredictable effects.

Considering the increase in the weaponization of cyber capabilities, do you think an arms control system for cyber-weapons is possible?

This comes up quite often and has been advocated by some. I personally do not think it's realistic. I'm certainly not a counter-proliferation or arms control expert, but these normally require transparency, enforcement, and clarity of definition that are rather difficult for offensive cyber capabilities. Considering their intangibility, hiding their existence or the efforts to create them is far easier than with chemical, biological, nuclear, or even ballistic capabilities. Maintaining an inventory of "cyber-weapons" is rather meaningless, and inspections are improbable. Allowing external inspection of offensive network capabilities inherently risks compromising them, unlike missiles or the payloads they deliver.

This becomes even harder when considering intelligence collection tools. Implants or platforms used to compromise adversary networks for espionage are effectively identical to those meant for attacks. To simplify, the main difference is often in the actual payload delivered to the target – is it an information extraction tool or a destructive one? Considering the legitimacy of maintaining an array of intelligence collection capabilities, nations could easily dodge any control mechanism by hiding offensive payloads and declaring the tools themselves as "intelligence capabilities".

Do you think the involvement of private intelligence companies is advantageous or disadvantageous especially in cases where a state level infrastructure is affected or compromised by malware?

Both. It is a little unusual that companies now have business models that leverage exposing national intelligence operations. In some cases, overzealous public reports can cause reverberating effects that the report-writers have no way of knowing about. The exposed parts of online cyber operations often mask a great deal of context. Every one of these operations happens within a broader narrative. Why were they initiated? Were they supporting some broader operational need? How will the affected agency or unit respond once compromised? Will this have broader political impact? At the same time, these companies can play a key role in protecting individuals and organisations against threats. Considering private companies cannot always rely on resource-limited law enforcement to protect them and their assets against compromise, it's natural for companies to step in and address the gaps.

What are you currently working on?

I'm currently working on completing my thesis on military offensive network operations, and how they can be better integrated into military doctrine. My thesis tries to combine technical, operational, and academic analysis to comment on the complexities of these operations, their potential contribution to the overall strategic effort, and how nations can do better to incorporate them into their planning.

What advice would you give to young scholars?

Don't fret too much on having answers upfront. That's one crucial aspect of academic research that is glossed over, especially in bachelor's degrees. Identifying the questions that matter and how you'd go about answering them is in

some cases equally important. Be critical, of yourself and everyone else. Never take anything you read at face value, assessing the credibility of sources is important. At the same time, allow yourself room to grow and improve, which requires both self-criticism and accepting it from others. Look for people that will help you grow. There are so many horror stories about difficult supervisors or destructive influences for young academics. Try to identify those people who would help you with constructive criticism, and then push them to give it. This is true both for peers and superiors, no one is an expert in everything. Networking is important. Even if it doesn't come naturally, it's important to connect with people to identify opportunities, create relationships, and build up your career. Early on, look for events that would help this along, either by presenting, participating in workshops or roundtables, or even just chatting people up in coffee breaks.