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 – Myriam Dunn Cavelty

https://www.e-ir.info/2024/06/09/interview-myriam-dunn-cavelty/

E-INTERNATIONAL RELATIONS, JUN 9 2024

Dr. Myriam Dunn Cavelty is Senior Scientist and Deputy for Research and Teaching at the Center for Security Studies (CSS) at ETH Zurich. For more than twenty years, she has published on the intersection between technology and security, more specifically on how digital technologies influence political behaviour and societal values and on how and why specific arrangements to govern the use of digital technologies emerge. Since September 2023, she is one of the editor-in-chiefs of the journal *Contemporary Security Policy*. Her latest book *The Politics of Cyber Security* is forthcoming from Routledge this summer.

Where do you see the most exciting research/debates happening in your field?

Two distinct yet interconnected trends are particularly noteworthy in the field of cyber security research. Firstly, there is a surge of interest in integrating critical approaches from security studies into cyber security studies. This includes feminist perspectives, post-colonial lenses, innovative attempts to queer cyber security, and the application of Science and Technology Studies (STS) perspectives. In line with this, the use of ethnographic methodologies to study cyber security practices is unravelling some of the black boxes and myths surrounding the topic. The positive aspect of these developments is that these approaches, which focus on deconstructing traditional power structures, norms, and assumptions, help to make cyber security more accessible by lowering the perceived barriers to entry. I think this research shows that you do not need specialized technical knowledge to make important contributions.

Secondly, there is a compelling focus on scrutinizing the limits of cyber operations in a different segment of the field. In many ways, this continues work that criticized the “hype” around cyberspace and its game changing nature for national security in the 2000s. However, this time the critique is not from a securitization or discursive angle but more from a technological-material perspective, where the functioning of computing machines is at the centre of thought. Insights from the technically-oriented threat intelligence community have significantly enriched this understanding, fostering a more holistic comprehension of the evolving cyber conflict landscape. Overall, the convergence of diverse forms of knowledge facilitates interdisciplinary collaborations and paves the way for transdisciplinary explorations, which I believe are the future of cyber security research in many ways.

How has the way you understand the world changed over time, and what (or who) prompted the most significant shifts in your thinking?

The field of cyber security studies has itself profoundly shaped my understanding of the world, continuously challenging complacency and expanding my knowledge through “incidents”—disruptions to the normal functioning of computers and networks. These incidents offer glimpses into a normally hidden world due to the secrecy surrounding cyber operations. The landscape of cyber security underwent a significant transformation during the latter half of the 2000s, driven by evolving threat perceptions, emerging opportunities, and broader geopolitical and domestic issues. This transformation intertwined cyber security with broader strategic and political contexts, shaping major power dynamics and introducing a new form of competition.

From these experiences, several key takeaways have emerged, fundamentally altering how I study international cyber security politics. Firstly, viewing cyber incidents as isolated technical events overlooks their broader socio-political underpinnings and their role as instruments of foreign and security policy. Understanding cyber-attacks

requires contextualizing them within larger political forces. Secondly, these incidents have spurred new avenues of inquiry while posing fresh challenges for researchers, necessitating evolving research methodologies to address the complexities of cyber security.

A critical realization has been that focusing solely on visible policy overlooks the impactful practices of hidden security actors. This has shifted the entire field towards the role of creators (mostly private entities) and exploiters (sub-, semi-, and non-state actors) of digital technologies. Furthermore, recent research increasingly recognizes that the political reading of cyber security cannot be divorced from knowledge practices in different communities. This has led to a growing focus on the role of cyber security companies and their influence on policy and practice.

Cyber-security has quickly risen to the forefront of international politics. What are the salient dynamics driving the sudden rise in importance of cyber-security? Are there any particular aspects in this rapid development of cyber-security which is still lagging?

There is a confluence of diverse factors that have propelled cyber security to the forefront of international politics. The twin concepts of "vulnerability" and "dependency" are at the core of cyber-threat-frames, and they develop their mobilizing power especially when they are put in interaction: Computer networks are demonstrably full of primary vulnerabilities that can be exploited by malicious actors, feeding into a secondary vulnerability brought on by increasing dependency of society on computers. Moreover, the increasing involvement of nation-states in cyber operations for espionage, sabotage, and geopolitical influence has escalated cyber security concerns further and have demonstrated the potential for cyber operations to disrupt economies, undermine democratic processes, and compromise national security.

However, critically reflecting on these narratives reveals a multidimensional "securitization" dynamic that we need to critically dissect as scholars. Cyber security is often portrayed as a completely novel issue that fundamentally departs from the past, driven purely by technical innovation. The dominant view is that technologies are a primary driving forces behind change in the international system. This way, an independent "power" is attributed to them, existing outside of social interactions. This analytical fallacy is known as "technological determinism" imbues the political discourse with a sense of inevitability that overlooks the complex interplay between technology and society.

While the cyber realm does possess distinctive characteristics such as rapid technological advancements, short innovation cycles, and significant influence wielded by private actors in the tech sector, it is essential to recognize that fundamental principles of human societies, rooted in social, political, and cultural structures, persist even amid technological evolution. Recognizing the reciprocal relationship between technologies and society, and acknowledging how they mutually influence and transform each other, is crucial.

In "Making Cyber Security More Resilient: Adding Social Considerations to Technological Fixes" you propose that re-conceptualising cyber security as a "social problem + technology" would improve cyber resilience. What is the prevailing ideology of resilient cyber-security? How would this re-conceptualisation address the current ideology's shortfalls?

The prevailing ideology predominantly focuses on technical problem-solving. This approach views technologies as distinct entities that can be fixed or managed, often overlooking the socio-technical nature of cyber-security. Adding social aspects to technological understandings may sound a little banal, but the paper speaks to an engineering and risk analysis community for whom such perspectives are not yet mainstream.

We show that focusing too much on technology ignores three crucial aspects of cyberspace. First, like every technology, it is entirely built by humans. This means that people and their interests and ideas shape the development and design of technologies decisively. Technologies do not hold meaning on their own or act by themselves – they are part of an assemblage of people, discursive processes and other material or immaterial things. Second, cyberspace is not an independent system. It is intertwined with other systems, such as the energy network. In turn, many critical systems depend on communication infrastructure, creating co-dependency. All of these infrastructures and their respective interdependencies matter because they are crucial for societal functioning. Third,

cyberspace consists of multiple interactions between the underlying technology and its human users and operators. It is their interaction with technology – and with each other by means of technologies – that creates cyberspace in the first place. This is even truer for cyber security (or the lack thereof), which is only relevant with respect to its effects on people and what they value.

These three aspects make cyberspace a socio-technical system, where human and societal actions, motivation and interests, plus technologies, and the interaction of these different parts, make up the system. In the article, we advocate for importing concepts from disaster resilience research in the debate to gain a better understanding of the socio-technical dimensions of vulnerabilities and uncertainties.

What kind of role does the private sector play in policymakers' cyber-risk management plans? Do cyber incidents in either the private or public sector often pose a contagion risk to the other?

The private sector plays a crucial role in policymakers' cyber risk management plans, given its substantial ownership and operation of critical infrastructure, technological innovation, and cyber security expertise. Private companies often hold the key to vital data and control over essential services, making them indispensable partners in formulating and implementing cyber risk management strategies.

Private sector involvement includes sharing threat intelligence, developing and deploying advanced security technologies, and providing critical incident response capabilities. Collaborations between public agencies and private companies are essential for enhancing situational awareness and fostering a coordinated response to cyber threats. These partnerships help bridge gaps in resources and knowledge, ensuring that both sectors are better equipped to mitigate cyber risks.

Cyber incidents in either the private or public sector can indeed pose a contagion risk to the other due to the highly interconnected nature of modern digital ecosystems. For instance, a cyber-attack on a private company's supply chain can disrupt essential services that public institutions rely on, leading to widespread implications. Conversely, a breach in a government system can compromise private sector partners through shared data and interconnected networks.

In "Goodbye Cyberwar: Ukraine as Reality Check" you highlight there is a common overestimation of the current capabilities and strategic value of cyber operations in warfare. Why is the utility of cyber operations overestimated? How do you foresee the role of cyber operations in warfare changing in the future?

In that policy brief, we highlight that the common overestimation can be attributed to several fallacies that ignore the complex interaction effects between technology and politics. In short: Technology constrains political possibilities, and politics constrains technological use, explaining why some types of cyber-operations are more prevalent than others.

- The "vulnerability" fallacy assumes that vulnerabilities in computer systems will always be exploited, disregarding the strategic calculus and timing of adversaries.
- The "the hack is the success" fallacy equates network intrusion with operational success, ignoring the political or strategic effects achieved.
- The "cheap and easy" fallacy assumes that cyber tools are low-risk weapons, disregarding the complexity and risk involved in targeted attacks.
- The "just pull the trigger" fallacy assumes that cyber operations are as easily deployable as conventional arms, ignoring the extensive planning and integration required.

When going beyond technical imperatives, it becomes clear that we need to look at the challenges, costs, and risks associated with different cyber operations. Not least, we have enough evidence now that cyber operations are not effective in fundamentally altering warfare elements such as permanently disabling or degrading enemy conventional forces and occupying and controlling territories. The damage inflicted by cyber attacks is often transient and

reversible, necessitating additional resources to maintain their effects. Additionally, there is always uncertainty regarding the success of cyber attacks and whether the desired effect can be achieved.

Drawing from decades of cyber security politics and available knowledge, it's reasonable to assert that the use of cyber operations in warfare will be governed by political considerations, context-specific factors, and primarily play a supporting rather than decisive role in military operations. The maturity of offensive and defensive cyber capabilities, external support received by nations, and learning from previous exposure to cyber operations will all be crucial considerations in future conflicts.

You also have an upcoming book publication *The Politics of Cyber-Security* which will deconstruct the intricacies of cyber-security's relationship with conflict and international order. What are the most important distinctions that separate politics and the politics of cyber-security?

I argue that it's impossible and unwise to separate politics from the politics of cyber security. Despite the rapid pace of technical innovation, cyber security fundamentally shares characteristics with other political issues. Regardless of shifts in the scale, scope, and speed of information flows and digital computations, enduring principles rooted in social, political, and cultural structures persist. The politics of cyber security emerges from the interplay between digital technologies, political processes, and the interpretation of incidents.

Therefore, the aim of the book is to show that enduring human dynamics influence how societies organize, govern, and interact within the evolving landscape of the cyber era. It emphasizes that cyber security is not solely about technology but also about intentional social interactions, compelling us to contextualize cyber security politics within appropriate historical frameworks and to comprehend technological advancements as interconnected with human deliberations and choices. This perspective also counters overly alarmist accounts of the disruptive nature of emerging technologies.

In line with this, I suggest that scholars and policymakers should refrain from adopting oversimplified conceptualizations merely for the sake of convenience. Instead, they should always strive to place the dynamics of "co-shaping" at the core of their deliberations. Recognizing the reciprocal relationship between technologies and society, and acknowledging how they mutually influence and transform each other, is crucial for comprehensive and nuanced analyses of the complex interplay between technology and human affairs.

How developed is the current framework for international cyber-security norms? Does it allow for sufficient flexibility to stay ahead of a rapidly changing cyber-threat landscape?

The current framework for international cyber security norms is still in its nascent stage and faces numerous challenges. Diplomatic efforts were initiated in the late 1990s to address the threat of "cyber doom" (destructive attacks on critical infrastructures with war-like consequences), but a significant portion of unfriendly actions occur outside the scope of existing norms. This is especially true for activities conducted during peacetime and in secrecy by intelligence entities, which lack comprehensive regulation under international law. This absence of regulation creates a grey area where deliberate ambiguity prevails, allowing many cyber operations to evade clear normative boundaries.

In the absence of strong norms, the establishment of red lines often involves a process of trial and error. Responses to violations vary, with some red lines being met with consequences while others are not. This continuous interplay of actions and consequences serves as a parallel, messy process of norm-setting. Ideally, this process would eventually lead to an equilibrium in the form of an "agreed competition," a situation resting on a tacit understanding among key actors about what constitutes acceptable and unacceptable behaviour, what moves are within the rules, and what actions are considered escalatory. For an understanding of the norms space, it is important to look at both international (multilateral) diplomacy as well as state-driven (unilateral) strategies in addressing cyber threats, because they often co-evolved.

What is the most important advice you could give to young scholars of International Politics?

The most important advice I could give to young scholars of International Politics is to maintain intellectual curiosity and remain open to diverse perspectives. International Politics is a dynamic and multidisciplinary field that encompasses a wide range of topics. Embrace the complexity and interdisciplinary nature of the field by engaging with different theories, methodologies, and perspectives. Additionally, don't shy away from challenging assumptions and questioning established paradigms. Critical thinking is essential in International Politics, where issues are often multifaceted and contentious. Be willing to examine issues from multiple angles, and don't hesitate to explore unconventional or innovative approaches to research. In your journey as a scholar, remember to be kind to yourself and others. Know yourself, your strengths, and your limitations, and strive for balance in all things. Take care of your physical and mental well-being, and don't hesitate to seek support when needed. And as you progress in your career, remember to become the mentor you (wish you) had. Pay it forward by offering guidance and support to those who are following in your footsteps.