Interview - Peter W. Singer

https://www.e-ir.info/2013/12/30/interview-peter-w-singer/

E-INTERNATIONAL RELATIONS, DEC 30 2013

Peter W. Singer is Senior Fellow and Director of the Center for 21st Century Security and Intelligence at the Brookings Institution. He is one of the world's leading experts on changes in 21st century warfare, and has written about the privatized military industry, child soldiers, robotics and other new technologies of war. His forthcoming book *Cybersecurity and Cyberwar: What Everyone Needs to Know*, co-authored with Allan Friedman, is an easy-to-read yet informative overview of the cutting-edge issue of cybersecurity (it is also available for preview on CourseSmart).

Singer has been named by Defense News as one of the 100 most influential people in defense issues, and placed as one of the Top 100 Global Thinkers in Foreign Policy Magazine. In his personal capacity, Singer served as coordinator of the Obama-08 campaign's defense policy task force. He has also worked as a consultant for the US Department of Defense and the FBI. He has also advised various TV series, and the video game series Call of Duty. Prior to his current position, Dr. Singer was the founding Director of the Project on U.S. Policy Towards the Islamic World in the Saban Center at Brookings, where he was a founding organizer of the U.S.-Islamic World Forum, a global leaders conference. He has also worked for the Belfer Center for Science and International Affairs at Harvard, the Balkans Task Force in the U.S. Department of Defense, and the International Peace Academy. Singer received his Ph.D. in Government from Harvard University and a BA from the Wilson School of Public and International Affairs at Princeton University.

Peter W. Singer discusses his forthcoming book *Cybersecurity and Cyberwar*, emerging global security threats, and how parenthood has changed his perspective of international security.

—

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

I'm located in the part of the field where policy and research cross, so what fascinates me is how there are a range of new debates and areas of research, but in many ways they echo back to dilemmas that have been with us from the start. For instance, the questions that surround China's political, economic, and military rise will shape everything from 21st century geopolitics to the future of the Internet. And so while some parts entail information gathering and discussions possible in no prior century, other parts involve applying theories and lessons that Thucydides would be quite at home talking about.

Similarly, the issues in the realm of cybersecurity have been seemingly limited to the "IT Crowd" and yet the questions of where the public and private sphere begin and end are both research and philosophic ones that have been with us for the ages.

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

I know I should make some kind of statement about the rise of the internet or the end of the Cold War or 9-11, but for me it was parenthood. As one joked it is like being a Secret Service bodyguard to a suicidal president. But more seriously, it heightens your sense of both optimism and pessimism in the directions the world is headed, and desire to do something about both.

What do you think is the most important emerging global security threat today? Are policymakers equipped to understand and respond to it?

The incredible lowering of the barriers to entry in the tools of war. Like in the past, there are a series of new "gamechangers" when it comes to how we fight, and the ripple effects that result for politics, law, ethics, etc. This is the pattern of disruption that links gunpowder to the steam engine to the atomic bombs, etc. But what is different is that the new wave (from robotics, to cyber to 3D printing etc.) is not something that requires huge amount of resources and bureaucracy to build and utilize, and thus in turn, reinforced the power of the state. That is, when I was in graduate school we learned Charles Tilly's famous lesson that "War made the state, and the state made war." But today, this truth may no longer hold….

Policymakers are woefully equipped to understand these issues. Woefully trained and even worse, many take pride in their lack of understanding or use of the new. Take cybersecurity. In our book we explore how the Secretary of Homeland Security, the agency in charge of civilian side of cybersecurity, didn't even use email, not because she saw it as insecure, but because she thought email was a waste of time. 8 of the 9 Supreme Court justices, the body that will decide many of the key legal questions, similarly don't. This problem is not just one at the peaks of power. Indeed, you can find the same lack of understanding of core issues and technologies we use everyday in the academy, media, business, etc. Indeed, one study found that 70% of business executives have made a cybersecurity decision for their organization, and yet no major MBA program teaches it. The same goes for law, the military and yes, political science.

Your forthcoming book *Cybersecurity and Cyberwar: What Everyone Needs to Know* seeks to explain the dynamics of cybersecurity to a broad audience. What motivated you and your co-author Allan Friedman to write the book? What do you hope it will accomplish?

Cyber issues have not only dominated recent headlines, but have more broadly evolved from a technology matter into an area that we all need to understand. To put it another way, cybersecurity and cyberwar has shifted from a "need to know" issue into one everyone now needs to know more about, whether working in academics, politics, business, military, law, etc. or even just as a good citizen or parent. The goal of the book is to help fill that gap, by providing an easy-to-read guide to the key questions, with a tone that moves the issue from histrionics to explanation.

Written in a lively, accessible style, filled with engaging stories and illustrative anecdotes, the book is structured around the key questions of cybersecurity: how it all works, why it all matters, and what we can do. Along the way, we try to take readers on a tour of the important (and entertaining) issues and characters of cybersecurity, from the "Anonymous" hacker group and the Stuxnet computer virus to the new cyber units of the Chinese and US militaries. The overall concept is that Cybersecurity and Cyberwar can serve as the resource book for the rest of us to understand, while also pushing some new lessons and concepts for the field.

Beyond its relation to various fields of research (and for IR, it connects everything from geopolitics to future of war), our hope is that the book will also prove especially useful for academic courses across a number of disciplines. It is written in a style that reflects not just the latest rigorous research, but is flavored with contemporary references, anecdotes, and explanations that today's students might find accessible. In addition, we have created a website for the book, that includes various teaching resources for involving students to a greater degree, including a discussion guide to use for classroom settings/essay assignments, as well as a music list for their further engagement. Finally, the paperback and e-book prices are set to be of special appeal to student budgets.

In the book, you warn of the dangers of "cyber proliferation" and a kind of cyber security dilemma, in which the more cyber capabilities states acquire, the less safe they feel. Will traditional IR concepts like the security dilemma help us to understand emerging security issues like cybersecurity, or does the IR discipline need to develop entirely new theories to explain and understand such issues?

Yes, and that is part of how the book goes about telling the story of cybersecurity and how to better understand it. We look at everything from offense-defense dilemmas to proliferation theories to the rise of norms in other fields and domains. The idea is not only that you can make the tale a bit more interesting by flavoring it with things like the rise of the real pirates of the Caribbean or some of the more zany (and scary) episodes of the Cold War, but that you can use these lessons from IR and history to better understand where we are now, where we might be headed, and what we can do to head off some of the bad paths we are now on.

The Center for 21st Century Security and Intelligence at the Brookings Institute, which you direct, works on emerging issues in defense, arms control, intelligence, and cybersecurity. What is the story behind the founding of the Center? What are they key issues that exist across these emerging security threats that unite them under the heading of "21st century security" issues?

The Center was created to address the key issues shaping security policy over the coming decades. It seeks to answer the critical questions emerging in defense, cybersecurity, arms control, and intelligence in an all-encompassing manner, seeking not just to explore important new policy challenges but also how they cross traditional fields and domains. To put it another way, while the policy and research sides are often stovepiped, the real world is not.

We have scholars who range from young academics to mid-career military officers to recently retired Ambassadors and Generals. While we, of course, wrestle with the issues of today, be it defense budgets to Afghanistan, our hallmark is also looking at the trends that will shape the issues of tomorrow. We also stand out in an increasingly partisan and co-opted thinktank community by leading with the question first, not the answer.

Your book *Wired for War* examines the ways the robotics and drones are changing battlefield conditions and challenging the laws of war. Do you see evidence today that the US is falling behind in this technological revolution, as you predicted in the book? And what implications does this have for the future of warfare?

The US is not falling behind so much as the rest of the world is catching up. We remain the leader in military unmanned systems, and darn well should given that we spend just under half the defense dollars in the world each year. Yet, there are now at least 87 other countries also now playing in this field, building, buying and/or using military robotics. And beyond these, there are a host of non-state actors, from Hezbollah's use in the Lebanon war, to potentially soon Amazon at an upcoming Christmas. To connect back to the earlier question, what is fascinating, and so challenging to the US, is that the technology is civilianizing. Akin to what happened with computers, the military will not solely "spin out" the technology to the private sector, but is already wrestling with how to "spin in" the technology into its operations. Again, it is not just software that has gone open source, but also warfare. That doesn't mean the big boys don't matter, but they don't have the same old monopoly that too many assume.

What is the most important advice you could give to young scholars of international politics and security?

When thinking about what to write on, triangulate. What will be important to the field? What will be important to the real world? And what will be interesting to you? If the topic falls in the space of these three questions, it's a winner.

—

This interview was conducted by Alex Stark. Alex is Features Editor of the website and a director of e-IR's editorial board. She is a PhD student in International Relations at Georgetown University.