Bits, Bytes and Bombs: Power, War and Conflict in the Age of Technology

An Interview with Dr. Sulmeyer

As we enter an increasingly multipolar world, traditional definitions of conflict, power and war are being fundamentally reshaped by rapid technological advancement, expanding competition beyond conventional battlefields into cyberspace, data infrastructure, AI and digital supply chains. In this evolving landscape, both state and non-state actors are leveraging technological capabilities to assert influence, disrupt adversaries and redefine deterrence, with intensifying competition between the US and China illustrating how control over critical technologies has become central to geo-political strategy. This year's edition of the Fletcher Security Review seeks to explore how emerging technologies are transforming the nature of power and conflict and the following questions aim to unpack these shifts and interrogate how we are navigating this era.

1. Much of the post-Cold War security architecture was designed around a unipolar moment - American technological supremacy, NATO interoperability standards, and the assumption that the United States could dominate the cyber domain much as it dominated the air and sea. Now, as we are moving into what many scholars describe as an emerging multipolar order, China has been fielding offensive cyber capabilities that rival or exceed those of many Western states and Russia has demonstrated a willingness to use cyberattacks as instruments of coercive statecraft short of war. Do you think the strategic logic of cyber operations has fundamentally changed? Do you believe the doctrinal frameworks the United States developed during the post-Cold War period are still adequate for the current environment?

Powerful question you ask and there's a lot there. On the U.S. side, I think the last big shift or change was in and around 2018. Three developments unlocked that change. First, you had the first Trump Administration announcing a cyber strategy for the Department of Defense called "Defend Forward." This gave a strategic context and rationale for not just building a force-in-waiting, but to set the conditions for disrupting adversary cyber efforts. Second, you had a statutory change by the U.S. Congress in the National Defense Authorization Act that clarified that cyber operations could be – and this is a term of art – traditional military activities. This may seem obvious now, but at the time, this was key to unlocking some intra-U.S. government friction. And third, the mid-term elections that year showed the power of the partnership between the National Security Agency and U.S. Cyber Command in protecting the country from foreign threats to U.S. elections.

If there is to be another big shift, it will probably be due more to the fast-paced developments of artificial intelligence. The traditional race between offense and defense has been accelerated, and it will be for decision-makers to decide how much autonomy they are comfortable with delegating on offense and on defense to keep competing in that race. It is also possible that AI unlocks the potential of truly strategic cyber attacks – attacks that we have not really seen historically. NotPetya caused something like $10B in financial damage, but in some sense that can be viewed as an attack that got out of hand by the perpetrators. The concern is that what's coming could make NotPetya look tactical by comparison.

2. From your vantage point, did the rise of a genuinely capable Chinese cyber apparatus change perceptions of risk tolerance, escalation management, and the relationship between offensive cyber operations and broader deterrence strategy?

We wonder this particularly due to China's approach to cyberspace seemingly blending civilian, commercial, and military actors in ways that make traditional deterrence frameworks (built around attributable state actors) enormously difficult to apply.

Deterrence as an approach to managing international conflict obviously has a deep history in theory and practice. And for whole-of-nation efforts to deter our adversaries from engaging in certain activities, it's wise to include cyber capabilities in the arsenal of tools that can help. But cyber operations do not on their face represent the kind of strategic capability that nuclear weapons did at the dawn of the Cold War. So while discussions about deterrence should include cyber operations, I think we have to look beyond deterrence to deal with the evolution of malicious cyber activity against the United States and our allies and partners.

I think the challenges of attribution for purposes of international statecraft are often overstated, and so in that regard, there's less of an obstacle for deterrence frameworks. Determining that there's a connection to a particular China-affiliated or Russia-affiliated group is not so much of an issue. Nor do I think the escalation concerns I recall from 10-15 years ago are as prevalent today, mostly because there's a lot of evidence now that shows cyber attacks have not proven to be all that escalatory. Whether states should or shouldn't react the ways they have to cyber attacks is a different question, but the record has been, to my mind, pretty clear.

3. Arms control has historically depended on verification, transparency, and a shared interest in avoiding mutual destruction. Cyberspace seems to resist almost all those conditions (capabilities are largely invisible, attribution is contested, and there is no agreed-upon threshold that separates an act of war from an act of espionage). Do you think any meaningful cyber arms control regime is achievable between great and rising powers in a multipolar world? If not, what does that mean for long-run strategic stability?

It's a great question to tie in the strategic frameworks from the Cold War to today's emerging technologies. The part I appreciate is the recognition that developments in one domain or through one technology can have outsized "destabilizing" effects on broader international relations. But based on how things have been and where I think they are going, I don't see most states having a lot of interest in an arms control regime. Even putting the issues of verification and transparency aside, I think the dual-use nature of the technology, among so many reasons, does not create a lot of incentive for states to pursue an arms control agenda for cyber capabilities.

4. Current technological competition is no longer just a story about state actors. The private sector now controls national security infrastructure in ways that governments did not anticipate and still struggle to govern. States like Russia, Iran, China, and North Korea are actively courting, coercing, and in some cases absorbing private technology firms into their national security apparatus. What are the governance challenges for democracies as they attempt to compete in the battle for the 21st-century technological revolution?

I think it begins with having more national security leaders of the future gain more exposure to these private firms so there's a little more fluency in public service about what they do and how they operate. That's a big opportunity for Fletcher and other programs to consider from a career development perspective what kinds of opportunities they could promote. I think it would be a good thing if we saw on people's

resumes some time spent at a frontier AI lab or a startup that aims to contribute to national security before they end up in public policy. Not a requirement, but not something to be discouraged.

I'm a believer in public-private partnerships, but I remember a lesson Joe Nye taught me at Harvard years ago. He cautioned me that a lot of folks will come out of the wood-work to "partner" with me. He advised discretion and encouraged me to look at those partnerships where 1+1 equals more than 2. Most of the time, he said, if you're lucky, a partnership is just 1+1=2. At worst, it's less than that because of the friction and process tax you pay. But those rare partnerships where what you achieve can only be had through the power of the partnership, that's where I'd focus and be most excited about.

"...cyber defense does matter: it's not hopeless."

5. The war in Ukraine has served as a kind of laboratory for cyber operations in conventional conflict, and the results have been surprising. The anticipated cyber catastrophe largely did not materialize in the way many predicted, even as kinetic warfare has caused devastation on a scale not seen in Europe since 1945. At the same time, the conflict has revealed an extraordinary degree of private sector involvement in the cyber defense of a sovereign state, with companies like SpaceX, Microsoft, Google, and Amazon playing roles that blur the line between commercial support and active participation in the war. What has Ukraine taught us about the relationship between cyber operations and conventional warfare in a modern great power conflict? Are these lessons analogous to a potential conflict scenario in the Indo-Pacific, where the geographic, infrastructural, and political conditions are radically different?

It is important for the audience to distinguish between cyber operations, information operations, and electronic warfare. I think there's been quite a lot of information operations and electronic warfare. The challenge with "knowing" about the cyber operations is that not all will be so public like the compromise of Viasat at the beginning of the war. Because cyber operations are a vehicle for other outcomes (such as reconnaissance) it is possible that there's been a lot of cyber activity between Ukraine and Russia but it is for intelligence and other more subtle purposes.

I also think one of the important take-aways is that cyber defense does matter: it's not hopeless. A lot of folks get frustrated and extremely pessimistic thinking that they have to secure everything perfectly all the time while the offense only has to be right once. To that I would say, like a good law school graduate, it depends. I think the Ukraine example shows us that the right investments in cyber defense can be quite helpful for protecting one's crown jewels. But that's not to say that cyber defense translates so clearly to territorial outcomes on a battlefield.

6. Artificial intelligence is one of the primary elements of modern military competition. The United States, China, Russia, among other states, are racing to successfully integrate AI into intelligence collection, targeting, logistics, and autonomous weapons systems. Each state is doing so with varying institutional, strategic, and civil-military cultures, and as well as different tolerances for algorithmic risk. Where do you see the greatest risks of AI-enabled instability or miscalculation in a potential conflict scenario? Do you believe there is a realistic pathway toward the development of "rules of the road" for military applications of AI?

I think the Glasswing Project that Anthropic

catalyzed is a novel development in the "field" of cyber policy. For the first time that I can recall, a company has deliberately held back the release of a product from a mass audience and instead made it available only to those whose scale is large enough to have a multi-national impact on cybersecurity. But for that, a new model as powerful as Mythos out in the wild could be very destabilizing. So it was a stabilizing move, I would submit, to manage the access to Mythos as Anthropic has.

One of the big open questions remains: how much autonomy will we be comfortable assigning a model for the purposes of cyber defense? It's a different debate about autonomy that tends to happen in military and national security circles, but this is an important one too because there is plenty of evidence that our nation's chief competitors are experimenting with using AI to aid in their cyber attacks. What will our decision-makers need to know to be comfortable with different degrees of autonomy to defend against these attacks?

7. Looking back across the arc of cyber policy, how well do you think Western policy and national security communities anticipated how computing technology would reshape power and conflict? What does this track record suggest we should be most concerned about getting wrong in the next ten to twenty years as technology evolves in quasi-unpredictable ways?

One of the hardest challenges is anticipating not just developments in technology, but also evolutions in the international system. Nations still operate in cyberspace to achieve certain goals, but if you are merely looking at these developments in terms of cyberspace, you miss the broader connection of what drives states to do what they do. Being slow to respond to geopolitical forces can be problematic alongside missing the next great technology. That's why I encourage students to study emerging technologies, but also to explore a particular country or region to understand the political dynamics outside of technology.