10

Imagining Cyber Peace

An Interview with a Cyber Peace Pioneer

Camille François and Christopher Ankersen

CHRISTOPHER ANKERSEN: What, to you, is cyber peace?

CAMILLE FRANÇOIS: For me, cyber peace is the set of norms and behaviors that we want democratic societies to observe in cyberspace, both below and above the threshold of armed conflict. It is a recognition that when we think about how to deploy cyber power, you also have to take into account what does it mean for democracy? What does it mean for human rights? It's a positive framework that talks about how you want to behave, and what you want to preserve, as you're thinking through deployment of cyber power.

CHRISTOPHER ANKERSEN: I think it's very interesting that you've connected cyber peace to the idea of democracy. Do you think, therefore, that it's not possible for other kinds of countries to play a role in this? Are they always going to be the "others" in this exercise?

CAMILLE FRANÇOIS: When I started working on cyber peace, my focus was working on both the US and the French approaches to cyber power. I was looking through historical records of how cyber power was defined, and it was very evident that cyber power was only defined in the context of warfare and conflict. Similarly, it was very obvious that cyber warfare was defined without its companion question, which is what is cyber peace? I thought that this was backwards; I thought that it was important for democracies, who are thinking through what cyber power is and how to deploy it, to have a positive vision of cyber peace, and you deploy cyber power outside the realm of war which, again, was a clear gap.

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

CHRISTOPHER ANKERSEN: It's very interesting to link it back to this idea of cyber power. Do you think then that cyber peace is a goal? What I mean is, countries are deploying cyber power in order to "do things." Is cyber peace, one of those things they're trying to do? Or do you think it's more like a precondition or even a collateral outcome?

CAMILLE FRANÇOIS: It's a necessary question for the societies to answer. Peace is a state of affairs that is much more common than war, which is what we want. And so it is interesting and somewhat baffling to me that most of the governments whose cyber theories we work on have spent all this time trying to work through the minutiae of how you deploy cyber power in wartime, which is important, but without ever touching on what the considerations are that you go through to get there. What are the appropriate sets of norms? How do you want to deploy cyber power in peacetime? And I think that this blind spot is detrimental to peace and stability.

When I started working on this, people were perhaps confused: it sounded like a "hippie" theory. But I think the past few years have demonstrated that the major cyber incidents do happen in peacetime and that the spectrum of conflict and conflict evolution doesn't allow these democratic societies to have a space for thinking how they deploy cyber power in peacetime. And this has to be a necessary democratic conversation.

CHRISTOPHER ANKERSEN: Can you go into a little bit more what you mean by people's reactions to cyber peace?

CAMILLE FRANÇOIS: So from a research perspective, I was looking at two bodies of conceptions on the role of the state in cyberspace. The first body of work that I was looking at was the cyber utopians. (It's the John Perry Barlow school of thought, to be brief.) And that's a really interesting body of work because, initially, it conceptually makes no room for state cyber power. The essence of the declaration says "you giants of flesh and steel have no room where we gather." A conception of cyberspace that makes no room for the deployment of state cyber power. And that's interesting. But it creates a huge gap between where we are and that initial conception. That

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

body of work is preoccupied with cyber security. It's also a school of thought that has thought a lot about encryption, but it kind of stops at actual cyber power. Because, again, it conceptually doesn't make room for that.

My other point of departure was actual military cyber theory, which is almost the radical opposite of where the cyber utopians are starting from. In it, cyber power deploys itself all over cyberspace, regardless of where we are on the spectrum of conflict and peace on wartime.

And so, looking at these two bodies of work, one says state cyber power is nowhere. The other one says state cyber power is everywhere. And for me it was self-evident that we were lacking the sort of rational approach that says today we are in a situation where states are building cyber power, they are building sort of military theories on how to express cyber power in cyberspace, and we need to have the in-between conversation, which is: What is the desirable use of that power? What is the responsible use? What is the democratic use of cyber power in peacetime?

And that was my point of departure – being stuck in between these two bodies of work, seeing the obvious gap, the conversation that has not happened.

CHRISTOPHER ANKERSEN: It's quite fascinating that the utopians saw cyberspace as almost anarchic, in a libertarian sense, where everything was possible. And we see this crop up over and over again: With the advent of social media, we had the same optimism. "Oh, great! Tahrir Square, uprisings across the Arab Spring, now we will know exactly what's going on. We won't have to worry about things being mediated!" But it really only took one contact with reality to see that wasn't exactly the case. Do you think, therefore, that this idea of cyber stability (as opposed to cyber peace) is a compromise, a way of trying to avoid the disappointment experienced before? Along the lines of "Well, let's not worry about peace, but can we at least have some kind of rules of the road so that we can have some reliability?" Do you think that stability is an ingredient towards cyber peace? Or is it a completely different approach?

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

CAMILLE FRANÇOIS: So it's a really interesting question, because one of the things I was circling around while working on cyber peace was also the question of what type of entities belong at the table when we talk about the reasonable deployment of cyber power in peacetime. When I started this body of research, I was at the Berkman Center for Internet and Society at Harvard (where I still am). I love the center: It's really grounded in the libertarian perspective. Working with one of my colleagues, I organized a meeting between the directors of the Berkman Center and the directors of the West Point Army Cyber Institute to talk about cyber peace. It must have been like 2013 or something. And it was this fascinating moment where it was evident that both parties at the table actually shared a lot of common ground. We're talking about the same thing, but with such radically different languages and concepts, and radically different perspectives.

And I think that is what I'm aiming for with this idea of cyber peace, which is, if you're going to talk about stability, that's fine, you can call it stability. But the normal parties that you would convene when you talk about rules of the road in peacetime have to be at the table for the debate to be meaningful. You have to have a consideration for the tension between cyber power and human rights in peacetime. You have to have corporations at the table. What is the role of the private sector in relationship to the deployment of cyber power in peacetime?

All these other types of conversations are now starting to progress. We finally saw the private sector say, okay, maybe we do have a role in preserving peace and stability in peacetime. And we do have some form of responsibility in the face of cyber power. But that took a very long time.

CHRISTOPHER ANKERSEN: One of the questions I had written down was exactly that. If we look at the analogue, the world peace movement from the 60s, it shares a lot of the same ideas with the cyber utopian side. And civil society was a big driver there: NGOs, ordinary people, churches, and community groups, and there was a dialogue of sorts between the people and the government. It was reluctant, but

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

it worked in a way: The disarmament movement was a bottom up affair and it forced politicians to engage. But who wasn't involved in that conversation? Weapons manufacturers like Dow Chemical (the makers of napalm) and Raytheon. They were implicated in that conversation, but they were not really parties to it. They were like, "well, we'll wait and see, do we get an order next week? Or do we not but we don't really have a role in doing anything. We're not going to cut back if Ronald Reagan wants to engage more for the SDI then full speed ahead. Let someone else drive the ship. And we'll just provide what's needed." But this seems slightly different now that companies, corporations, and firms seem to, as you say, understand, at least implicitly, that they have more of a role.

But we don't see as much civil society involvement. People aren't on the streets out there looking for cyber peace. Do you think that that makes cyber peace a different kettle of fish and that we can't necessarily draw on past practices?

CAMILLE FRANÇOIS: There are so many interesting questions in what you just put on the table, I'll take at least three of them. The first one is: What is the private sector in this context? There isn't really one private sector. And when you think about it, you know, the Raytheon example is interesting, because you have the part of the private sector that is manufacturing and selling elements of cyber power. So the sort of "hacking for hire" types. And here, the debate is one of regulation. What is the appropriate regulation for shops that develop "zero-days for hire"? And that is a conversation that really was late to the party. We've seen organizations like the NSO Group go back and forth on what that means for them to meaningfully respect human rights. I think they got a lot of that very wrong. At the same time, though, regulators have been slow to catch up with that.

So there's a private sector in that way, that is part of this conversation, because it's one of regulation. Now, there is another private sector, which sometimes intersects, but mostly doesn't, which is the private sector on which this conflict is being deployed.

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

And that raises a question of the role of a company like Microsoft, like Cloudflare, like Google, like Facebook. And here, what's really interesting is I have seen them be part of this conversation without acknowledging it, and therefore, we're missing the strategic guidance for it.

I'll give you a very bizarre, specific example, which is one that's really close to my heart. Ten years ago, Google launched my favorite feature anywhere on the Internet, which is the state sponsored warning. Google decided that its threat Intel team had the visibility to see when private citizens were being targeted by state sponsored actors on their services. And Google decided that it was worth telling these users and started rolling out a little message, initially in Gmail, that told its users "Google has reasons to believe that your account is being targeted by state sponsored actors." I spent a lot of time working on those features, and they are now replicated across the industry. Twitter's doing it, Facebook's doing it, and Microsoft's doing it. They're all saying not exactly the same thing and they're not all advising the same thing. But that is a hell of a recognition that in peacetime cyber power is deployed against the individual, and that there is a need to protect them and inform them.

CHRISTOPHER ANKERSEN: That is a great feature, but I would say most people don't know about it. Let's be honest, out of 7 billion people, probably less than 100,000 get that message, right? Because they're actually important enough in somebody else's ecosystem. And there are a few experts, such as yourself, who know about it, but that's what I mean. That's not the same as a peace symbol on a placard that a whole range of people might be attracted to and understand enough to, say, donate money to Greenpeace or actually go out and protest. It just seems to me that, in some sense, this is not a mass movement yet. There's a perfect example of technical capability to do it and some recognition among some people that it's necessary and possible. But does that include the people in the United States? Will Google warn somebody if they think the NSA or the FBI or someone is doing that? So few people know about that.

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

It's not like, "Hey, man, like, you know, did you get your warning yet? Are you on the warning list?"

CAMILLE FRANÇOIS: I've worked with the targeted communities and the users who get the warning, and talked them through it. What do you understand about it? What did it feel like? What are your questions?

The targeted communities, they're exactly who you would expect: Members of parliament, elected officials, journalists, activists. I remember I did a user interview with a journalist in cybersecurity who eventually got the warning, and he said, "I finally got it! It was my badge of honor. I was the last one of my friends to get it. Now I can brag at DEF CON!" So there are communities for whom this is a known entity. But then I also talked to users who were more unaware: "Oh, yeah, I see this stuff. I think it's just routine stuff that they send to everybody, to keep people on their toes." They fundamentally don't understand this is because of exactly what you're saying, which is that we don't have a movement to explain it. What does it mean? What does it look like? What are the moments to panic and the moments to stay calm? And the advocacy piece, the civil society piece of it, has been quite slow to develop.

CHRISTOPHER ANKERSEN: You were going to talk about a third piece of the private sector before I interrupted?

CAMILLE FRANÇOIS: I was going to talk about the third piece of your question about the private sector, which is civil society. Last year, I joined the board of Digital Peace Now Society; I'm super excited about what they do. Their mission is to build up advocacy. But to be honest, I think that the fact that the research has been lagging behind has also hampered the advocacy movement's ability to develop. And I think that what's happened with Solar Winds is a good example. If you look at the cyber conversation, what do you see? People yelling at one another because they can't define what constitutes an attack. Which is okay, I understand. But it's really interesting because you can see that despite years of work on cyber conflict, those important terminologies about what can be expected and what isn't an appropriate response are still in flux, and they

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

remain contentious points in the actual academic literature. I think that this is because the academic focus on cyber peace for so long has been lagging behind the focus on cyber war.

CHRISTOPHER ANKERSEN: Do you think that part of this lag is not just on the research side, but because people perceive this to be "ones and zeros" and hacking and geeky and green screens and just weird stuff that they don't think they understand? Whereas, let's be honest, nobody understood nuclear weapons either, but they understood them enough to know "it goes boom, kills people: got it." And that was enough for people to get informed and have this grassroots "we don't want it anymore" type movement. Whereas with cyber there's some feeling of "Well, we need it; I don't really understand it; somebody knows better than me, the experts must have a hold on this." And so, therefore, even the civil society groups tend to be more informed, like EFF. These groups are a subset of the "geek community" that get it and therefore have concerns.

CAMILLE FRANÇOIS: It is a really interesting example. And lobbyists have been working with them for a long time. That's a conversation I've been having with them for ten years. EFF always says that that part (cyber peace) of the overall question isn't in their scope. So if you look, for instance, at the EFF statement on the Tallinn manual – it doesn't exist. That's not part of their scope.

So it's interesting to see that we can have entire conversations on norms that are applied to state power both above and beyond the threshold of armed conflict without any meaningful consultation of civil society organizations. Even EFF, which, as you said, is super tech savvy, isn't around the table. As a result, Tallinn 2, which is preoccupied by conflict below the threshold of armed conflict, has a chapter on human rights that is significantly smaller than the chapter on the Law of the Sea! The way we've been engaging with these questions, the way we've been defining the scope of these questions, is backwards.

CHRISTOPHER ANKERSEN: I wonder if that's because it comes from this idea, as you say, that most of the movement has come from the cyber security perspective, as opposed to the cyber

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

peace or cyber utopia side. Therefore, they see this as about securing stuff, protecting stuff, as opposed to liberating and kind of offbeat, as defining what we're actually trying to do, which is have a place where we can get stuff done.

CAMILLE FRANÇOIS: Exactly. What you are describing is a very tech-centric definition of cyberspace, one of tech bits and systems, which is why you care most about things like encryption. That very tech centric definition of the space has long been a problem for our ability to address wider issues such as peace and stability. That is, the problem that we had in 2016, in the face of Russian Foreign interference: both Silicon Valley and Washington were so preoccupied *excluding* that piece from their definition of cyber security. Again, from a normative perspective, perhaps that is okay, but at the end of the day, concretely, it means that in Silicon Valley, you had entire cybersecurity threat intelligence teams with not a single person in charge of detecting the attack that was going to come their way. So yes, you can have whatever definitions you want from a normative perspective. But this trickles down into how peace and security are actually cared for, and how we do defensive work in a way that leaves blind spots open and is, ultimately, problematic for peace and security.

CHRISTOPHER ANKERSEN: That is fascinating because it's this self-defined issue. Privacy? People get that and the solution to that is, somehow, more tech. Get a password manager, get a VPN, don't do this, don't do that. And platforms like Facebook will have a "real world harm threshold," which is to say that if somebody says they're going to murder somebody, we'll take that as a threshold to actually do something about it. But beyond that, on things like false information actually going to sway something, perhaps there has been too much of a free hand given, allowing companies to self-define, and therefore, opt out of these conversations. So it's not just that they're not welcome at the table, but they're also not necessarily knocking on the door to get to the table, either. They can sit back and say "we got this little gap here fixed and we got this little gap here."

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press

But what about all "the rest of it"? And I think what you're saying is "all the rest of it" is cyber peace.

CAMILLE FRANÇOIS: Yes, it's not just hackers and "ones and zeros" everywhere. It's the unsexy but fundamental space where basic regulatory frameworks apply to protect peace and stability, how to define what's acceptable, what's not acceptable, who is in charge of defending it, and how we structure ourselves for it. What is the role of the private sector in that? What is the role of civil society? And what do we expect from our governments? Yes, it's not very sexy; it's not the hacker wars, but it represents the space where the vast majority of these incidents happen.

Because we're lacking this perspective, we're constantly getting blindsided by major events that after each of them, everybody says, "oh, how is it that we were possibly blindsided in this way?" My answer is that it's because our focus has been overly concerned with defining cyber war, the topic of countless doctrines, countless papers, and not focused enough on defining and organizing cyber peace.

CHRISTOPHER ANKERSEN: A last question then: What do you think the biggest threats are to this idea of cyber peace? Where would you say we were looking at the biggest barriers to actually getting to an idea of cyber peace?

CAMILLE FRANÇOIS: It's over indexing on offensive measures. It's that every incident that is getting in the way of peace and stability must be addressed by offensive measures, because our state of mind is that of cyber warfare and not that of cyber peace. Once you have a hammer, you have a hammer problem? What we need is a more positive, more defensive, broader understanding of cyber peace, across all of society. This last point is interesting because every time we confront a massive incident that was totally predictable, but yet not exactly in line with how we organize ourselves, one of the answers is, "oh, we need a whole of society response." That is true, but let's talk about why we don't have whole-of-society responses on things that touch cyber power.

https://doi.org/10.1017/9781108954341.010 Published online by Cambridge University Press