Center for Strategic and International Studies

Online Event

"International Security in Cyberspace - New Models for Reducing Risk"

RECORDING DATE:
Monday, October 19, 2020 at 3:30 p.m. EDT

FEATURING:
Dr. Christopher Ford,
Assistant Secretary of State for International Security and Nonproliferation

CSIS EXPERT:
James Andrew Lewis,
Senior Vice President and Director, Technology Policy Program, CSIS

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

James Lewis: Good afternoon and welcome to CSIS. Today's topic is International Security in Cyberspace – New Models for Reducing Risk. Our speaker is Dr. Christopher Ford, who was the assistant secretary for international security and nonproliferation. And he's been delegate – almost exactly a year ago the authorities and functions of the undersecretary for arms control and international security at the State Department, T for those of you who know that. Before coming to State, Dr. Ford served at the National Security Council. He has deep experience in arms control, nonproliferation, and intelligence, worked on a number of Senate committees, and was a senior fellow at the Hudson Institute.

So, a great background for this. Thank you, Chris, for doing it. Let me quickly tell people what the agenda is. Dr. Ford will open with remarks that will be on the record, right? Then we will, to the extent we have time, to questions. But those will be Chatham House. So, a quick switch of the rules – on the record remarks, Chatham question – Chatham House questions. You can submit your questions either through the Q&A function or through the chat function. We'll try to get to as many of them as we can. But with that, Chris, over to you.

Christopher Ford: Thank you very much. Good afternoon, everybody, and thanks for having me participate in this event. You guys have no actual reason to know this, but I actually got my start in the think tank business at CSIS many years ago as an Africanist, as an intern working for Helen Kitchen in the African Studies Department back a very, very, very long time ago. I can see, Jim, from your face you're realizing how long ago that is. 1990, maybe, or something like that? It was my first introduction to what a think tank is, and to what a think tank does. And I guess I have to thank you guys for that formative impression. You didn't scare me away from think tankery, by a long shot.

Now, of course, back then when I was working for Helen none of us imagined that something called cyberspace would be such – or, would exist at all, let alone be such an important piece of the 21st-century international security environment. But of course, here we are. But I guess that's why I should really start my remarks by thank you, Jim, on behalf of the department for your role – indispensable role – as rapporteur for several successive groups of governmental experts at the U.N., where some really, really important work was done in articulating standards of responsible behavior in cyberspace.

I don't think there are that many folks around who can lay claim to having personally had such a formative influence on an entire area of diplomacy, as you have in the cyber arena. So, on behalf of the department, let me say thanks. And it makes it all the more special for me to be able to be here and talk to you guys today. So, congratulations on all that, and thanks for having me.

James Lewis: Thank you.

Christopher Ford: For my part, I'd like to say a few words about what we're doing currently in the U.S. government, and particularly in the State Department, from the perspective of cyberspace security diplomacy. This is a critical time, of course, but it's also true that all this other real-time swirl of headlines and the oncoming U.S. presidential election, you know, make – there are lots of reasons to perhaps be distracted from these things. I think it's vital not to lose sight of the fact that important policy initiatives in this arena continue to advance, and there really is a great deal of really very, very valuable continuity and evolutionary progress in U.S. cyber diplomacy.

Now, of course, why we should need to pay attention to these things is unfortunately pretty obvious. In an ever-more interconnected age, it's no surprise that cyber threats continue to increase. The indispensable all these types of connectivity are to everyday life – commerce, communications, innumerable aspects of how it is that we live in the modern world – all these things – the more these increase, the more that malicious actors see or hope to see opportunities for themselves to steal or to hold hostage the information that is the lifeblood of this modern economy.

But I want to stress that the problems that we face today go beyond just the sort of, you know, ordinary – if you will, ordinary criminality of cybertheft and fraud, and beyond even the traditional sort of cyberespionage that states engage in. As we sit here, the current challenges of great-power competition have especially raised the stakes in the cyber arena. So adding to the problems that we already faced from cyber criminality, we must also now address that additional layer of geopolitical threat from the revisionist powers of the PRC and Russia, states that, of course, use cyber tools to steal technology to build up their military capabilities, to prepare for devastating attacks upon our critical infrastructure in the event of crisis or armed conflict, and to carry out disruptive cyberattacks and destabilizing our allies and partners, and to influence and manipulate our own electoral processes.

So, this shift in the threat from a criminality and espionage frame to also a full-spectrum global great-power competition sort of frame is a shift of huge, huge magnitude and one to which the non-authoritarian world is really only in the early stages of trying to develop effective responses.

Your audience, Jim, needs no primer on the particular threats that we face from cyber-facilitated technology transfer, on the one hand, potential disruptive cyberattacks against critical infrastructure as well, and thirdly, from cyber-facilitated political manipulation.

But what I'd like to do today is say a few words about what we are doing, at least in my own piece at the State Department from this perspective, in responding to those threats. But I guess before I talk about what we're doing, I should say a couple of words about what we are, I guess, not doing.

Christopher Ford (continued):

What we are not doing is reflexively changing solutions that just simply can't address the problems that we face in cyberspace today. Effective risk reduction in cyberspace is challenged by several important characteristics of that domain. It will be no surprise to any of you all listening, I suspect.

First of all, malicious cyberactivity can be carried out across a spectrum that spans activities both above and below the legal threshold for a use of force, and indeed, arguably, in some sense, a continuum across that space.

Secondly, impending cyberattacks offer few external observables, getting little strategic or tactical warning in many cases, and complicating the ability to attribute responsibility for an incident or to verify compliance with accepted norms of behavior.

And the third factor is that the technologies involved in cyberoperations and the ubiquity of these technologies – and they're often dual-use nature, not to mention their possession by both state and nonstate actors – all this makes cyberspace tools rather difficult to define or to control, but raising the possibility that efforts to achieve that kind of control could have severe repercussions for innovation and economic development.

So, I would say that together – and this has very much been the understanding in the U.S. government for quite a long time – effective arms control, as it is traditionally understood, is greatly problematized by all of these factors. This is – really any kind of a protean, rapidly moving, evolving, high-technology domain like cyberspace, it's very hard to make those traditional concepts work.

I've said this about outer space as well. And I think, in both of these contexts, if one aims to sort of limit or to ban what we define as weapons, in this case in cyberspace, in the traditional way that one tries to address other dangerous tools through the prism of traditional arms control, it's all but impossible to come up with a good definition of what a weapon is.

I don't see any way to avoid being either damagingly overinclusive, in ways that would also prohibit technologies that are, in fact, essential to civilian – peaceful civilian and scientific uses, or to be dangerously underinclusive by perhaps missing entire categories of potential weaponry or, in fact, to do both at the same time, which is very possible as well. And even if you could define the problem, no one, to my eye, has ever been able to offer an intelligible scheme for verifying any such prohibition.

So I would say that cyberspace, like outer space, is a domain in which technology are evolving so quickly, private and governmental actors are so intertwined, and definitions of what can be a weapon are so vague, that it is hard to see how traditional rules-based and legally binding prohibitory approaches common to traditional arms control really could work in this arena.

Christopher Ford (continued):

So, it's for those reasons that the U.S. has long rejected efforts to impose traditional arms control on – arms-control measures on offensive cyber capabilities. And I think it's particularly important to hold that line, given the degree to which Russian and PRC campaigns to promote arms control in cyberspace have, in fact, focused less on actual measures to reduce the risk of conflict that involves tactical cyber operations, then they have focused upon efforts merely to sort of co-opt the rhetoric of arms control in support of campaigns by those authoritarian governments to legitimize oppressive controls over the political content of internet communications.

So, as is often the case in diplomacy, I guess, not doing dumb things is half the battle. So, we continue to resist the temptation to engage in quixotic arms-control efforts in cyberspace, especially when such proposals originate from the dictatorial regimes who are themselves responsible for some of the most egregious cyber behavior in the world today. So that's what we're not doing.

But let me talk about what we are doing, which is actually much more interesting and fun. One critical plank of the U.S. agenda is to promote – as I have sort of suggested before, to promote clear understandings of what constitutes responsible state behavior in cyberspace. This is something that Jim knows extremely well from his service as rapporteur and actually helping to bring into being those articulations of norms in a really successful way.

As I have explained elsewhere and I'd like to stress, U.S. diplomats for many years now – more than a decade, in fact, and across three different U.S. presidential administrations, which very significantly indicates a strong bipartisan continuity here that is worth remembering as we move forward this year – U.S. diplomats have been working with their counterparts from around the world to articulate and to promote such voluntary and nonbinding norms. One of these key principles – and I think in some ways one of the most important ones – is that international humanitarian law and international human rights law, and indeed the charter of the U.N. itself, all apply in cyberspace in the event of an armed conflict. Led by the U.S., a broad coalition of diplomats carried the day on this at the 2013 GGE. And Jim, you were there; I was not. And that GGE articulated by consensus the idea that international law, and in particularly the Charter of the United Nations, is applicable and is essential to maintaining peace and stability, and to promoting an open, secure, peaceful, and accessible cyberspace environment. This conclusion was reiterated in a subsequence GGE in 2015, and both reports have been endorsed by U.N. member states.

Christopher Ford (continued):

Now, Russia, to be sure, has recently started to try to walk back its commitment to this principle, which is very disturbing. We must all join in condemning and holding a line against that. But the achievement of the U.S. and its GGE partners in this in making these points clear I think was a huge step forward for cyber diplomacy.

And beyond articulating just the applicability of international law, the U.N. cyber GGEs have also spelled out voluntary nonbinding norms of responsible state behavior that apply short of armed conflict, as well. That consensus 2015 report that I mentioned a moment ago, for instance, recommended among other things that states should not conduct or knowingly support cyber activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public. The U.N. General Assembly has by consensus called on all states to be guided by these norms.

So, these are, of course, you know, voluntary nonbinding norms and not legally-binding requirements. But I do think that they are a major step forward in creating expectations of responsible behavior in the cyber domain to help guide state actions and to encourage restraint and prudence in cyber operations.

And that brings us to one of our – one of the – of our more recent innovations in this realm. Understandings of responsible behavior of the sort that I was referring to before are really critical not just in their – for their own sake, but also in helping define what is irresponsible behavior. Because if you can understand what irresponsible behavior is, that opens up really important possibilities for efforts to make that kind of irresponsibility increasingly unattractive to its would-be perpetrators. This is the burgeoning areas of cyberspace deterrence.

And to be sure, explicit strategies of deterrence are only relatively recent additions to our cyberspace diplomacy. For a while, the U.S., it seemed, almost seemed to hope that the mere example of its good-faith engagement with malicious cyber actors such as Russia and the PRC might be on its own terms enough to persuade them to rein in their bad acts. In 2013, for instance, the Obama administration established a new communications channel for addressing cyberspace problems that connects today the U.S. State Department to the Ministry of Defense in Moscow. Now, this kind of direct domain-specific communication channel I think can, indeed, provide a really valuable means with which parties can communicate about emergent issues in ways that could help manage crises and prevent inadvertent escalation.

Christopher Ford (continued):

But while this is an important step forward, that link by itself cannot represent an adequate answer, because U.S. policy at the time seemed – well, seemingly ignored the element of deterrence. The approach then seem to rest on the idea that communication alone, in some sense, could help address the growing cyberspace threats that we face – as if the Kremlin's malicious cyber activities were just some kind of miscalculation or mistake that could be stopped if we – that would be stopped if simply we pointed it out.

Now, that pure communication approach collapsed in response to Moscow's efforts to influence the 2016 U.S. elections, because the Russian activity in question, of course, was not a misunderstanding or error that might be corrected by having attention drawn to it, but in fact a deliberate policy choice. But we learned the lessons from that in our diplomacy and have built upon what has come before to more explicitly incorporate elements of deterrence in our cyberspace security diplomacy as well.

So, the lessons of the last few years have made clear that having some kind of a framework if responsible behavior is not, by itself, enough. You need also to have there be some kind of consequences for violations of those norms. And so in the 2018 National Cyber Strategy in the U.S., it made very clear that as the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners.

According to the strategy: The United States will launch an international cyber deterrence initiative, to build a coalition of states and develop tailored strategies to ensure adversaries understand the consequences of their own malicious cyber behavior. The United States will work with likeminded states to coordinate and support each other's responses to significant malicious cyber incidents – including human intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.

That's a long quote, but it's actually, I think, a really important piece from the cyber strategy. And it's the framing construct for what we have tried to do thereafter. Now, in this, the State Department has played a really important role, in particular through taking the lead role in building that aforementioned Cyber Deterrence Initiative, or CDI. On one hand, we have of course continued the work that I referred to already in describing our work to build acceptance of and to promote adherence to U.S.-developed frameworks of responsible state behavior in cyberspace.

But at the same time, we have also worked within the U.S. government and with our interagency partners and international partners, to build a shared capacity to swiftly impose consequences when our adversaries transgress this framework.

Christopher Ford (continued):

So, working with interagency colleagues, for example, we have developed policies, processes, and response options, including templates, to allow us to act quickly. We worked with likeminded countries to build a flexible model for how we organize cooperative responses to cyber problems. And we have engaged in what I call attribution diplomacy, which is a critical part of this work as well.

It used to be thought – and as a sort of cyber layman years ago I assumed, as many people did – it used to be assumed that cyber attribution was essentially impossible. Thankfully, of course, that's not true. It's not easy to do, of course, but it's hardly impossible. And we are getting better, not just at doing attribution ourselves, but at mobilizing partners in order to condemn malicious cyberactivity as well. And this is a critical component of our cyberspace diplomacy today.

Just to give a few examples, in September of 2019, 28 states joined in a joint statement on advancing responsible state behavior in cyberspace, which included our commitments to work together on a voluntary basis to hold states accountable when they act contrary to this framework. Accordingly, in February 2020 – just earlier this year – 28 individual states and the European Union as a whole, making a very considerable number altogether, although there's some overlap and I've forgotten the exact number – but they all joined together in condemning the destructive cyberattack against the country of Georgia that was mounted in October of 2019 by the Russian GRU military intelligence service.

In April 2020 moreover, the U.S. and several other likeminded countries issued coordinated statements in response to an alert issued by the Czech Republic about its detection of an impending cyberattack targeting its health sector, warning that such an attack, if it were to occur, would result in consequences. This, I think, was the first time that likeminded countries had ever come together to warn against a specific future cyberattack. And we believe our warning did, indeed, having an effect. Despite preparatory work by the would-be perpetrators, no major cyberattacks ultimately occurred in that case.

This isn't just a question of diplomacy and bring our friends together to condemn things. We are also, of course, in the U.S. interagency imposing more concrete consequences as well. You may have seen in the news today, for example, that a number of indictments have come down from the Department of Justice in the U.S. today against members of a GRU unit that has been responsible for all sorts of horrible mischief, including going after the Ukrainian power grid, the enormously destructive NotPetya virus, and other mischief of that sort.

Christopher Ford (continued):

And you may be familiar with what the Defense Department sort of coyly refers to as defend-forward activities. Now, naturally I will not be talking about those here today, but I want to make the point that this is a whole-of-government effort. And we, as diplomats, have our piece to play in it. We've been working very aggressively to play that role as effectively as possible, so reinforced not just by U.S. increasing role with sanctions and penalties of that sort, but also now by European sanctions for the most egregious cyber events. This cyberspace security diplomacy is helping to increase the costs and the risks that are faced by the perpetrators of malicious cyberactivity.

Now, there's a lot we still have to do and there's a long way to go. I won't deny that in the slightest. But we have been making some very important strides. And this is a really important growth area right now for the department and for the U.S. interagency.

So, as a final note, let me say that we are also working in the department finally to organize ourselves for success in this arena as well. As far as I can tell, it's all but universally agreed that the State Department badly needs a full-time – needs a bureau, the full-time job of which is to address cyberspace, security and emerging-technology issues. Such points have been made by the National Security Commission on Artificial Intelligence, the Cyberspace Solarium Commission, and by world-class think tanks such as you guys.

We agree completely about the importance of having that kind of organization in the department. And that is why Secretary Pompeo notified Congress in June of 2019 of our intention to create a new Bureau of Cyberspace Security and Emerging Technologies, or CSET, as we call it.

Our move to create CSET is based upon the idea that in addition to the need to ensure that the department is fully staffed and prepared for the ongoing challenges of cyberspace security diplomacy, such as the things that I'm talking about already, we also need full-time specialist expertise to address the security challenges presented by rapid developments in emerging-technology areas, among them artificial intelligence and machine learning, quantum information science, nanotechnology, biological sciences, hypersonic systems, outer-space technologies, additive manufacturing and direct energy.

These and other areas are extremely important, and we need to have specialists who are working on these issues for the Department of State on a full-time basis, concerned with the security challenges that they present. The 2017 National Security Strategy that we put out early in this administration acknowledges that maintaining a competitive edge in emerging technologies is critical to our national-security interests and to our economic growth. Our strategic competitors certainly think this, and they're working as fast as they can to organize and seize advantage in those areas. And we must not allow ourselves to be left behind.

Christopher Ford (continued):

Here too, no single bureau at State has been responsible for ensuring that the department develops and implements coordinated diplomatic responses to the national-security-related aspects of cyberspace and the – and of current and future emerging technologies. So, we intend to fix that.

According to the Undersecretary for Arms Control and International Security, CSET will finally allow the State Department to be properly organized to handle these various security challenges. So, we're excited about that, but getting to that implementation has certainly been hard – needlessly so, I would argue.

Secretary Pompeo, as you will recall, as I said, notified Congress of our intent to create this new bureau in the summer of 2019. I think it was June 3, if I recall correctly. Thanks to the refusal, at this point, merely of two members of Congress who have kept holds upon our creation of this new bureau, however, CSET still does not exist nearly a year and a half later. Our adversaries are surely delighted by this, of course, for their activities against the United States have faced no hold. And indeed, those activities are accelerating.

So, I do hope this roadblock will be quickly overcome, for the department badly needs to posture itself against the security challenges that this country faces in cyberspace and in connection with emerging technologies. We badly need to reorganize and to resource our diplomats while other countries, of course, have already been – both partners and adversaries have moved forward with their own analogous organizations while we have remained held back by those two members of Congress.

So, there is hope here. Within the department we have long done good work in coordinating across multiple bureaus in addressing these challenges, but we can do better. And with CSET, we will do better.

So, in conclusion, let me just say that the breadth and the severity of the cyberspace challenges and the cybersecurity threats we face today, they are great, and they are growing. But the U.S. government is firmly committed to moving forward to mount ever-more-effective responses, and we are doing good work to that end. And we hope very much to be able to work with folks such as you all in making sure that our policy initiatives are responsive to these challenges on an ongoing basis moving forward. We do this on an interagency basis, but we also do it specifically here at State. And it's been a pleasure and a delight to be able to be part of that for this last year or so.

This is, of course, a really challenging arena. There's a lot of hard work and a lot of attention that will need to be paid to this in years ahead, but I do think we're on the right path. We're making good progress. And I thank you for the chance to have the opportunity to talk about it a bit.