INTERVIEW WITH CHRISTOPHER PAINTER

CHRISTOPHER PAINTER
Mr. Painter has been on the vanguard of cyber issues for over twenty-five years. In his current role as the Secretary's first Coordinator for Cyber Issues, Mr. Painter coordinates and leads the United States' diplomatic efforts to advance an open, interoperable, secure and reliable Internet and information infrastructure. He works closely with components across the Department, other agencies, the White House, the private sector and civil society to implement the President's International Strategy for Cyberspace and ensures that U.S. foreign policy positions on cross-cutting cyber issues are fully synchronized.

Mr. Painter is a recognized leader in international cyber issues. He has represented the United States in numerous international fora, including chairing the cutting edge G8 High Tech Crime Subgroup from 2002-2012. He has worked with dozens of foreign governments in bilateral meetings and has been a frequent spokesperson on cyber issues around the globe.

Sir, first of all, thank you for finding time for this interview. I strongly believe that it is crucial to start talking about cybersecurity in an international context, especially that a lot of important processes are currently underway, influencing the international community to a great extent. Based on the decision of the UN General Assembly, a new UN Group of Governmental Experts (GGE) will start its work soon. What kind of an outcome and findings do you expect out of the work of the experts?

To begin with, let me put some context around that. This will be the fifth GGE and I think that the last two in particular have shown a notable progress on a number of issues, the key matter being the applicability of international law in cyberspace as a foundational matter. At the last GGE, a particular importance was paid to the elucidation of what we call "peak time" norms – norms of behaviour of states below the threshold of an armed conflict or, for that part, of international law plug-ins. Those were pretty tremendous achievements, given the core active membership of that GGE. Even more so, in the GGE, there were expert groups in a number of different areas, and the cyber group has become one where it has really been a crucible for producing these very valuable results: the framework that we have championed for some time, international law as the foundation of norms of behaviour, voluntary norms of behaviour, and confidence-building measures. I think that has been a real success.

Even this year we have had it go well beyond the GGE and have the GGE report affirmed in the G20 declaration that came out just a few months ago now. That really shows this has become a real global issue – an important issue. Now, on that foundation, we want to continue with the mandates the GGE has. The focus is predominantly on the international security aspects, so we would like to see a further elucidation on how international law applies to cyberspace, a further discussion of the norms and how we implement those, and also of confidence-building measures, which I should say is beyond the GGE. But I think one of our chief goals over the next

period of time is to do that work in the GGE, and also to get a wider number of countries all over the world, even those outside the GGE, to affirm and to embrace this framework as well as the framework of international law, the framework of norms of behaviour (the ones that we have elucidated), and confidence-building measures. That is a key part of what we want to do. The first meeting of the new GGE will be in August. There are 25 members this year. Some are different than last time, and some are the same, so we are looking forward to that.

I would also like to underline, with respect to the things that have come out of the GGE on this framework in the past, especially confidence-building measures, that we have been making progress in other forms on that. We are doing some efforts to take those forward particularly in the Organization for Security and Cooperation in Europe (OSCE), but also in the ASEAN regional forum. We are both concentrating our efforts on the GGE, but also looking globally to gain a wider acceptance of this framework and do some more practical work on it.

You said that you were looking for a practical implementation of confidence-building measures in different formats and on various regional fora. Do you have any plans to push forward more practical talks, for example, within the framework of the OSCE?

Yes, within the OSCE, we have been doing a lot of work on confidence-building measures recently. About two and a half years ago, we had the first set of 11 confidence-building measures that came out from the OSCE. Just last year, the last additional 5 of confidence-building measures were added to that. The OSCE has been looking at how to implement things like exchanging doctrine among countries, or setting up points of contact, i.e. a number of really practical elements. Confidence-building measures from the OSCE make a lot of sense. Within the OSCE, a lot of its work over the years has been done on these kinds of practical, confidence-building measures, albeit in another context, so it is a perfect venue to discuss these issues.

The Department of State undertakes many actions to implement President's International Strategy for Cyberspace. Could you please describe or elaborate on the greatest achievements so far?

There is a broad sweep of what the international strategy is. It is not just a strategy about cybersecurity. It is a strategy about all the aspects in cyberspace because even though they are distinct, they are also in a relation. So the strategy talks about freedom of expression and human rights in cyberspace, about Internet governance issues and economic issues, about capacity building, cybersecurity, cybercrime, and international security. So there are many achievements in each of those areas and I hesitate to prioritize one of the areas over another because they are so important and they are all different. They also happen to differ between communities. Having that said, I would like to underline that not just creating, but pushing and getting pretty strong acceptance in a short period of time within this international security framework I just talked about – international law, confidence-building measures – is a really big achievement. Diplomacy often moves slowly, but this has been done pretty quickly, hence it is something I would highlight.

I also believe that some organizational things like Internet freedom, the creation and expansion of the Freedom Online Coalition has been very important. In the context of cybercrime, there are a number of new countries who joined the Budapest Convention, and many countries who came up with good cybercrime laws and have increased international collaboration. In cybersecurity, it is worth mentioning due diligence, as we call it. There are many countries now that have created national strategies for cyberspace and

CERTs, and are now collaborating internationally. There are other economic achievements in terms of Internet governance and maintaining the multi-stakeholder system, which has been quite important. So really, across all those pockets, there have been some real achievements I think.

I would like to give an overall comment on some international aspects. Just a few years ago, although I have been doing the job for 24 years now in different capacities, this was seen very much as a boutique or a technical issue, and not so much as a policy issue. But now, firmly in the U.S., but also in more and more countries around the world, this has become a key issue of a national security policy, a human rights policy, an economic policy, and a foreign policy. And we have seen that play out in a couple of different ways. For example, just yesterday we had the Singaporean Prime Minister in town, and the declaration that came out of his visit with President Obama had a very significant statement in respect to cyber issues. Virtually every time our president now meets with a foreign leader, there is a significant statement on cyber issues.

I started this office 5 years ago, and we were the first in the world to have a foreign ministry post in office dedicated to the issues. There are now about 22 around the world. There are dialogues between countries and governments around the world to try to break down the barriers between the different agencies and parts of a country and their private sector from civil society. And that is a huge change in a very short period of time. I think there have been both procedural changes and real substantive achievements. That does not mean, however, that we are done yet. I think that we are still fairly near the beginning of this road and there is a lot more work to be done. Nevertheless, it is heartening to see the level of interest and understanding that we see around the world.

This is exactly why we have decided to create the European Cybersecurity Forum, just to promote the idea that cybersecurity is not purely an IT issue, but a strategic challenge that also needs to be understood from the policy-making perspective. We truly admire your work in this field and your efforts to promote this kind of attitude, and we are doing whatever we can to motivate the CEE region to look at cybersecurity exactly from this perspective.

To illustrate that, for a long time, within governments, there would be a technical minister, or a person in the ministry of communications who would get involved in cybersecurity. But what you see in almost every country now is that a communications minister might have a part, the interior ministry might have a part, the justice system will be involved, the same with the foreign ministry and the defence ministry. So even within governments it is important to see the different aspects. This is a challenge.

Exactly. Sir, you mentioned the promotion of cybersecurity due diligence as one of the areas where your focus is. All nations have responsibility to protect their own networks and information infrastructure, and your department supports these efforts. One of the main pre-conditions of cybersecurity in general is well-working private-public cooperation, so my question is: do you have any advice on how to build solid cooperation between the private and the public sector?

I think there are several things that are important here. Many countries now have and many more are developing national strategies. And with national strategies, we think the best practice of doing those is to consult with the private sector and civil society. It is not just a government issue – it is larger than that. We also have countries that are establishing national CERTs, and those national CERTs obviously plug in with the private sector as well. Even in our own country, when we did our

National Incident Response Plan, for instance, we built it with the private sector from the beginning because they own a lot of important infrastructure. There have been a lot of developments in the U.S., even recently, in terms of engaging the private sector in these issues. We had a summit with the private sector out in Stanford about a year and a half ago. We passed legislation in our Congress to allow better information sharing between the public and the private sector, and took down some barriers. That is important and that is something we promote as we go around the world and say it is crucial to have that engagement with the private sector and civil society.

In addition, we have done a lot of capacity building, particularly in Sub-Saharan Africa, but also in other parts of the world. The OAS in our region has done it in Latin America as well. And we do not just go as the government. We also have private sector representatives who are there talking to countries, so they can understand that it is part of the best practice of how you build it. These are operational issues which are about making sure you are sharing information between the private sector and the government, so you are better able to defend your networks and respond to incidents. There is also the larger policy if the government takes care of designing their policy. The private sector should be someone in our group. It is not monolithic. There are many different parts to the private sector, just like there are many different parts of civil society, or the government. But really having that engagement is important.

My next question is related to the issue that unfortunately has recently become extremely important for Europe, namely a growing risk coming from the use of the Internet for terrorist purposes. In your opinion, how can we fight this problem, this risk, without violating human rights and fundamental freedoms, including privacy? I know the question is very complex and hard to answer, but could you just share your thoughts on that?

We have a very extensive first amendment protection in our system, and all other like-minded countries have freedom of expression as something that the courts value. It is obviously a concern that terrorists are using the same networks as we are to communicate, to plan, to recruit, and to get funded. Now, some of those activities are illegal in our system: if someone is providing material support for terrorism and is funding terrorism – that is something we will go after. But, generally, what we have not seen terrorists do as of yet is to launch attacks against critical infrastructure using cyber means. They have mostly used the Internet to spread their war and communicate plans. What we have been trying to do is to counter the terrorist message: to get to the root cause and counter this very negative message with positive messages, and try to reach that community they are trying to reach. This is here at stake at the Global Engagement Center, and there are also a number of countries doing this together. This countering might not need to be from the government. It might be from other sources, from people within the community of people who are exposed to it. That is something that the State Department has spent a lot of time focusing on, and that is what we will continue to do.

Now I would like to touch upon the Report to Congress on the International Cyberspace Policy Strategy. The document summarises the involvement of the Department of State in the implementation of your international strategy. In this document we can read that countries like Russia or China advance alternative visions for international stability in cyberspace. So could you please explain how this vision differs from the ideas that the U.S. promotes, and how do you deal with this issue? How do you try to resolve the differences?

It is not going to come as a big surprise that there are other countries that have a very different view of cyberspace overall. For example, when Russia uses terms like “information security” and “end-

to-end cyber security", what they are saying is that they want to control information. They often see information itself as a threat, so a lot of their policies will go on that. When you look at Internet governance for instance, if countries want a more state-centric control, they want to do that because they think that it is a better chance of controlling what they think is destabilizing information.

You have command of, from the human rights' and the government's perspective, that absolute sovereignty that we see Russia and China arguing for in a number of different forms. Sovereignty exists in cyberspace. Certainly, there are sovereign aspects of cybercrime – servers are located in countries, etc. But you cannot take sovereignty too far. Sovereignty is not absolute. Things like universally recognized human rights transcend sovereignty. I believe, therefore, we should emphatically counter different approaches. We deal with countries who disagree with us on a number of things. We are having dialogues with China about some of the international security issues, about the theft of intellectual property issues, and cybercrime. It is important to have those dialogues. Nevertheless, I think the big thing for us is that a lot of like-minded countries around the world believe, as we do, that the Internet needs to remain open and uncapped. Adopting a more repressive view of controlling everything is not the way to go.

There are also a lot of countries who are trying to decide what their future is, especially in the developing world. As they get more connectivity, I think it is incumbent on us and other like-minded countries to work with those countries because they understand that there are huge economic and social benefits to the vision that we are promoting over the visions that some more repressive countries are providing. So that is the challenge where we have done a good job so far. And it is not a battle that is going to go away – it will continue to be an issue.

Thank you for pointing this out. I believe that countries like Poland should strongly support all of your efforts aimed at promoting open, secure, and interoperable Internet.

One big signal is that it does not mean we cannot try to find areas of common ground. The GGE report, for instance, reflected the ground that included Russia and China as well as a number of other countries. You have to look for common ground, but you also have to be clear about the differences and highlight why those differences are important and where you want to go.

Confidence-building measures, especially those related to critical infrastructure protection, are one of the examples where countries with different opinions on some of the issues should focus on and seek common ground.

I think the fact we got agreement on some of those norms means that even countries that often disagree with us also see the value in them. But those are not ideologically-based issues. Those are based on a real desire not to have an invert escalation. They are practical and they are meant to be practical.

Thank you so much for your time and answering our questions. It was a huge honour and pleasure talking to you. I hope we will see each other during the next CYBERSEC.

The pleasure is all mine and I very much hope to make it to the next one. ■

Questions by:
Dr Joanna Świątkowska
The Kosciuszko Institute