October 21
What should the main goals of Internet governance be now and in the future?

First of all I would like to thank distinguished co-facilitators for helping us to reach constructive conclusions in this very important WSIS+10 review process.

Regarding the question what should be the main goals of internet governance we align ourselves with the statement by EU representative. In addition I would like to offer the following contribution to the drafting process of the review document.
The current multistakeholder model of Internet governance has proven to be very successful and the underlying reason for it is that it reflects decentralized architecture of the Internet. There is no central Internet exchange point in the world and there should not be centralized Internet governance authority, technical nor political.
The main goals of Internet governance are: ensuring the stability, resilience, trust and openness of global internet as an undivided, free, pluralistic, neutral, secure, global platform for developing worldwide information society. Building on the work of UNESCO let me say that Internet governance should ensure Internet universality.
Regarding paragraph 36, I would like to note that there is a number of member states that have called not to establish international legal framework and we align ourselves with that calls. Internet governance is one of many topics addressed within this review process and we see no reason to elevate this particular topic to the level of debating here separate legal framework for it.
Poland appreciates the decision to renew the IGF mandate as written in zero draft review document. However it appears that 5 years is too short to effectively start and finish a process of improving IGF. We call for 10 years extension of IGF mandate if we really want this organization to produce even better results.

Thank you.

October 22
How should human rights issues related to ICTs be addressed in the zero draft?
How should the outcome document handle present and emerging concerns about cybersecurity?

Thank you co-facilitators.

First of all I would like to emphasize that we align ourselves with the EU statement in that regard and I must confess that I appreciate very much the constructive dialog, the constructive debate to which I am listening with great interest and learning about important issues.

First, I would like to say something about the structure of the document. I think that current link, what appears as a close link between the human rights issues and cybersecurity issues creates a risk to lead us to the false dichotomy, false dichotomy between human rights and security, false dichotomy between freedom and security or between privacy and security. So I think, that chapter on human rights should be separated from the chapter on security.
Regarding the issues of cybersecurity, of course it is very important and there are many voices on that and I guess nobody disagrees but I have an impression that in some instances it is treated as all-encompassing basket. I think this holistic approach to security creates certain risks.
Let me first, take a step back and building upon what distinguished representative of the United States said – and others, - let me enumerate few distinct aspects of cybersecurity that require dedicated, highly professional in-depth discussion and that cannot be combined into one basket. For example, we should separately talk about so called cyber war, about cybercrime, about cyber

sabotage, about privacy violations, about software and hardware assurances or about international law applicability to cyber operations and each of those topics requires separate in-depth debate and that debate in many cases takes place, whether in intergovernmental forums like GGE for example, or multistakeholder or private sector forums especially regarding software, hardware assurances.
So I think, if we would try holistically - I understand this might be tempting and on the surface level seems like a reasonable intention - but if we try to take holistically all of this within the WSIS, then not only we risk being superficial but also we risk losing solid and long lasting attempts to solve those problems – those attempts that are happening in other forums, many of them at UN, for example UN Group of Governmental Experts that was mentioned many times here.
So I think let's be more constructive and focus on those aspects of cybersecurity that are directly related to development of information society. Things like education and public awareness of citizens – there is a great role for governments here, – capacity building like development of Computer Security Response Teams and similar.
Thank you.

October 22
What would be the ideal periodicity and formats for follow-up and review?

Thank you co-facilitators.

Regarding the issue of high level review or summit proposal I think we need more clarification of the rationale for that. It is true of course, we see it every day, that ICT technology progresses and I follow that as closely as I am able to. I have not seen in the developments so far, neither in the near future predictions any so far reaching, nor so far ground breaking developments in ICT that would require redrafting, renegotiating, modifying the WSIS action lines.
In Poland, we think that current WSIS action lines are general and broad to the extent that they cover the entire impact of ICT on social and economic life today and we expect this for near future to be true as well. So I think, on this very important, very profound matter whether to meet on very high level as some advocate we really need more clarification At this point in history as we are today we do not support calls for any high level meeting that would reconsider, that would assess either new legal instruments or open the Tunis Agenda for negotiations.