International Pugwash Workshop: Cyberwar & Cyberpeace

Dimensions of Cyber Challenges

Berlin, 23 October 2015

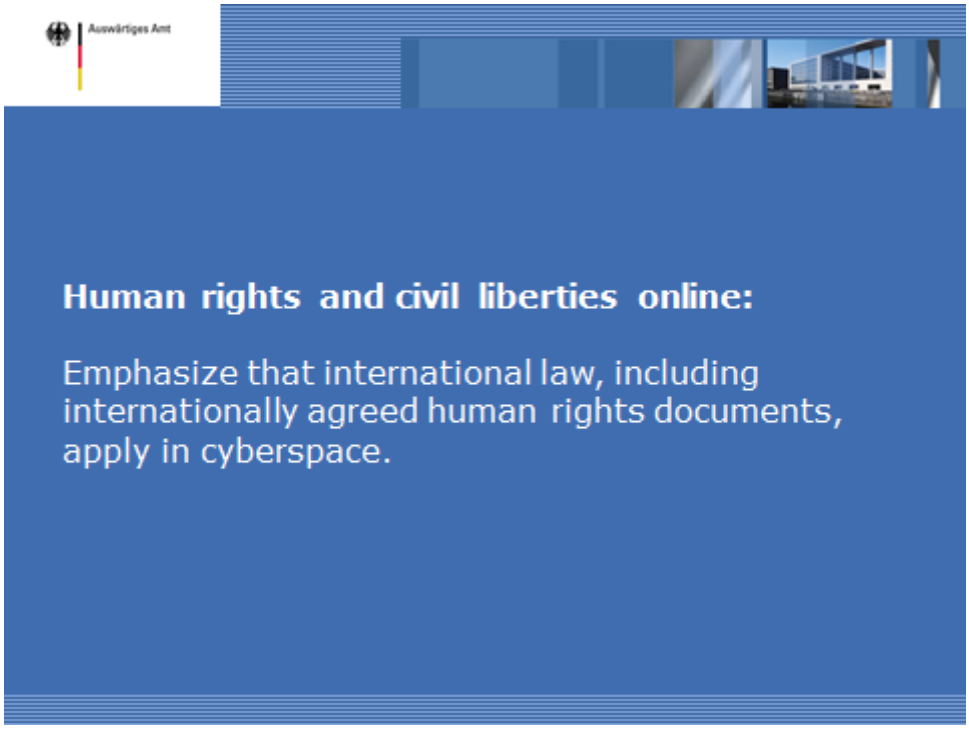
We may wish for a future characterized by global norms adherence, rainbows and funny cats. However, this is not realistic.

A better goal for our cyber diplomacy may be maintaining the c*yber status quo*. This status quo is messy: On important issues such as internet governance, cyber and international security, fundamental rights online, there is no single, stringent, international line of action. Instead, we are witnessing a "muddling-through" approach, where multiple, not always consistent decisions are taken in competing forums by a variety of actors – not all with the same claim to legitimacy. Regardless, the "net community" is putting into question traditional patterns of international decision-making. Conversations on international cyber affairs often sound like alphabet soup: We discuss NGO participation at the IGF and WSIS; compare ICT4D to ICT4P; or find that the UN GGE has informed the discussions not just at the OSCE IWF, but also in the ARF and possibly even OAS and EAC. And we have not even turned to the questions of IANA transition and ICANN accountability. There are code-words like "rough consensus" and "Budapest article 32 b".

No single individual, no single institution can claim to have even a rough overview – not to speak of a comprehensive understanding – of all current dimensions of cyber challenges. However, this multitude of parallel forums, actors and conversations has served us quite well so far. The Internet, for all its complexity and hap-hazard development, is certainly no bad thing that has moved humanity backward. It continues to have tremendous potential for the exchange of information, for education and science, for economic growth and development and for democracy. We need to maintain a free, safe, reliable and accessible Internet. I would add that the "messy" cyber status quo not only reflects the gradual, piecemeal and largely uncoordinated development of the Internet since a few U.S. universities started to exchange data packages over telephone lines. The large variety of stakeholders and institutions, the complexity of the system itself has also greatly contributed to the stability of

the Internet. Think of it as a haystack: You can pull out a lot of hay before the whole thing collapses.

Nevertheless, hay is constantly being pulled from the barn. There are multiple international challenges against the cyber status quo, to which our diplomacy must find answers. Here are a few:



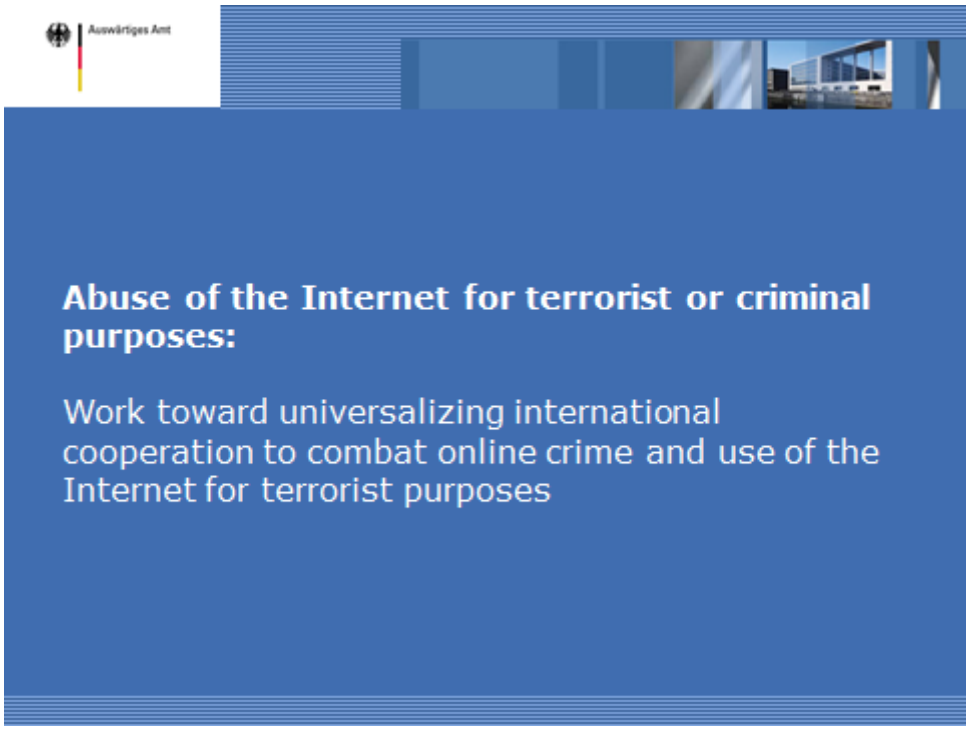
Human rights and civil liberties online: Many countries – not only authoritarian regimes – harbor fears that online communication can be destabilizing. One reflection of this can be found in the Russian-Chinese proposal for a "Code of Conduct", containing multiple provisions that aim at restricting freedom of speech and information online. Even among NATO allies there are varying views e.g. on hate speech online, use of the Internet for terrorist propaganda and recruiting, the use of social media for organizing and mobilizing political opposition, and also the right to privacy in the digital age. **In the face of these challenges it is important to emphasize that international law, including internationally agreed human rights documents, apply in cyberspace.** We need to maintain a clear, coherent and coordinated narrative on this point. One important point of this narrative has to be that individuals enjoy the same universal human rights "offline" as "online". This includes the freedom of expression -- including the freedom to seek and impart information --, the freedom of assembly and association, and the right to privacy, as the UN General Assembly and the UN Human Rights Council have unanimously confirmed.

This latter issue – the right to privacy – has proven particularly thorny. The discussion comes down to the question, whether the state has the right to collect unlimited electronic data on individuals, and moreover, whether the state has the right to insist that the business community, i.e. private IT service providers, assist in doing so. On the other hand: The very essence of democracy requires that every person retains a personal space free of state surveillance and interference. If such a space is missing, if every message we write, every phone-call we make, even every step we take are recorded, how can opinions be formed, controversies fought out?

The European Court of Justice laid down some important markers in its 8 April 2014 decision on the *European Data Retention Directive*. The Court made clear that within its jurisdiction – the 28 Member States of the European Union – *the retention of personal data, when it is wide-ranging and particularly seriously interfering with fundamental rights, needs to be sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary*. In its 6 October 2015 decision in the case of *Maximillian Schrems v Data Protection Commissioner*, the Court added that *legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life*. Likewise, the Court observed that *legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law*.

If all this seems too complex to retain, my personal summary is as follows: Data privacy is an issue of personal freedom. Those who sacrifice personal liberty for the sake of safety will end up with neither. This, of course, is a line stolen from Benjamin Franklin.

Internet governance: The multi-stakeholder system of internet governance is under challenge from countries that feel it is dominated by the West. Calls for a more "multilateral" system of internet governance, in which all *states* would have an equal say, abound in a variety of fora, including the UN and the ITU. On the other hand, large parts of the "*internet community*" are highly skeptical of the state, which they criticize as steeped in hierarchy and insufficiently flexible to accommodate rapid technological change. They would like to reduce states' role in internet governance, preferring discursive processes in large networks and "broad consensus" over rules-based governance and clear decisions. **We need to maintain unity that in cyberspace governments, as well as private sector, civil society and the United Nations and other international organizations all have an important role and responsibility, as appropriate, in decision-making processes. Building a people-centered Information Society is a joint effort which requires cooperation and partnership among all stakeholders.** It is important to draw in new allies on this point, including emerging leaders in the global South.



Abuse of the Internet for terrorist or criminal purposes: This is potentially one of the greatest threats to cyberspace. A study published in 2014 by the Center for International Security Studies estimated that the United States lost about $100 billion to cybercrime and economic espionage last year. Germany was second with $60 billion, and China followed with $45 billion. In both the United States and China, these losses represent about 0.6 percent of their economies, while Germany's loss is 1.6 percent. As online crime, including intellectual property theft, does ever greater damage to modern economies, and as fears of terrorist abuse of the Internet mount, governments as well as private users may decide that the cost of the free and borderless Internet use outweighs its benefits. **We should work toward universalizing international cooperation to combat online crime and use of the Internet for terrorist purposes.** The members of the Council of Europe and 21 other states – from Argentina to the USA – have agreed a Convention on Cybercrime. It is open for others to sign. Yet, a number of countries argue that this so-called Budapest Convention should be replaced by an UN instrument. This would be a step back: It would take many years to duplicate the work already done, and there are doubts if

some of the more forward-leaning clauses, such as the authorization to access data in third countries without their government's consent (article 32 b), could be replicated. We must resist the temptation of sacrificing progress attained in the interest of efficient law enforcement for the sake of universalization. And we need to balance freedom and security. That balance needs to be reasonable, and the instruments of security need to be proportional to the costs they impose on our privacy.

International Security: Given the ever increasing availability of malicious cyber tools for use by both state and non-state actors, the danger is growing of an incident in cyberspace escalating into conflict between states. Rules for responsible state behavior in cyberspace, transparency and confidence-building serve to reduce this risk. Important work in this respect is being done in the United Nations. Since 2005, the United Nations General Assembly has mandated a series of groups of governmental experts (GGE) to work on this issue. The 2014/2015 GGE completed its work in June 2015. In its report to the UN Secretary-General, it offered a list of non-exhaustive views on how

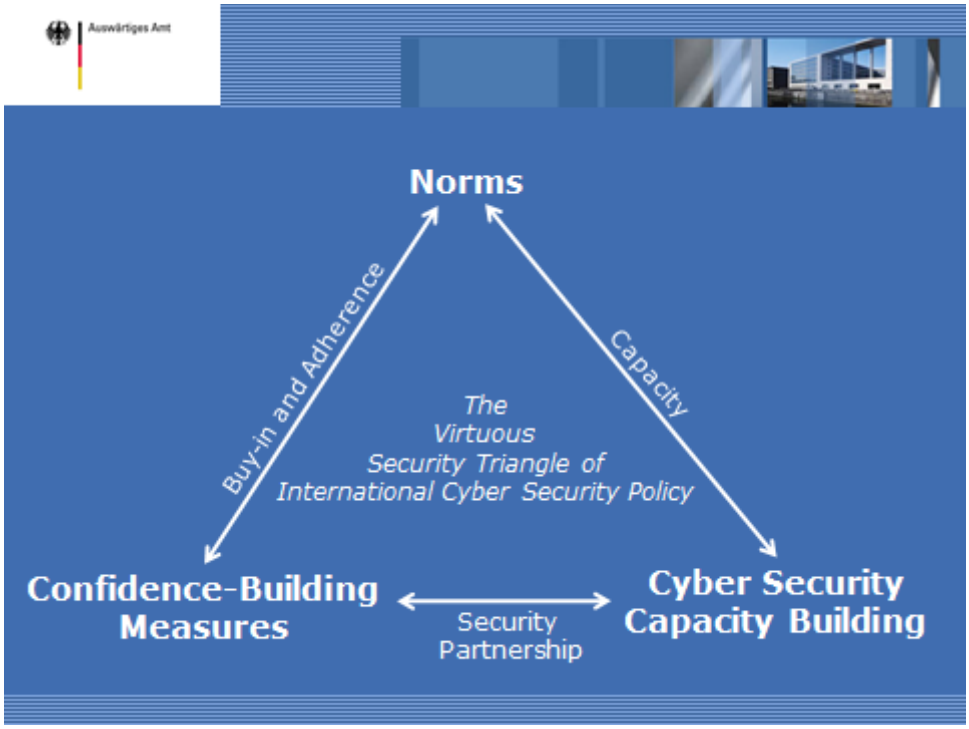
international law applies to the use of ICTs by States. The GGE also agreed a number of voluntary, non-binding norms of responsible State behavior. Such norms do not seek to limit or prohibit action that is otherwise consistent with international law; they reflect the international community's expectations, set standards and allow the international community to assess the activities and intentions of States.

Rules under international law and norms of responsible state behavior are of limited value, however, without actors' confidence that states will respect these rules. Such confidence is best built through transparency and confidence-building measures. Much of this work is taken forward in regional organizations, as they bring together those states that are most likely to have difficult relations: It is far more likely that two neighbors share a dispute over a border area, the delineation of a sea border, or the use of natural resources than that two far-away countries are in conflict. Regional organizations provide a forum for such neighbors to talk, and, ideally, to resolve their grievances. This is especially valuable regarding cyber incidents. Since the perpetrators of hostile cyber action are difficult to identify, a state that falls victim to such action in most cases has to guess who is responsible. Chances are that suspicions will fall on a neighbor with whom relations are strained.

In Europe -- or rather: in the area ranging from Vancouver to Vladivostok -- OSCE Participating States have decided to take up these recommendations in a three-step approach: In December 2013, we agreed a set of cooperative measures aiming at transparency-building. Since last year, while engaging in the implementation of these measures, an informal OSCE working group has been discussing a second set, aiming at trust-building and cooperation. And in the longer term, we hope to arrive at a third set that would be geared toward increasing risk-reduction and stabilization. As it assumes the chairmanship of

the OSCE next year, Germany is looking forward to deepening and widening the OSCE work on cyber.

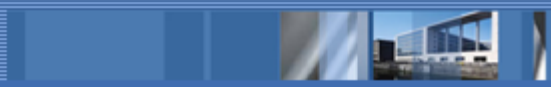
The OSCE is only one of many regional organizations. Germany is engaging with other regional organizations as well, such as EADC, UNASUR, the OAS and the ARF, supporting their work on enhancing cyber stability.



Another element in ensuring that rules under international law and norms of responsible state behavior are respected is building capacity in to do so. Cyber security capacity building can help build international understanding for the challenges cyber capabilities pose to international security, and to the importance of rules-based behavior, transparency and confidence-building in mitigating these challenges.

Adherence to rules for responsible state behavior in cyberspace is related to inter-state transparency and confidence, as well as to cyber security capacity-building. We should recognize this link.

Auswärtiges Amt



Thank you for your attention.