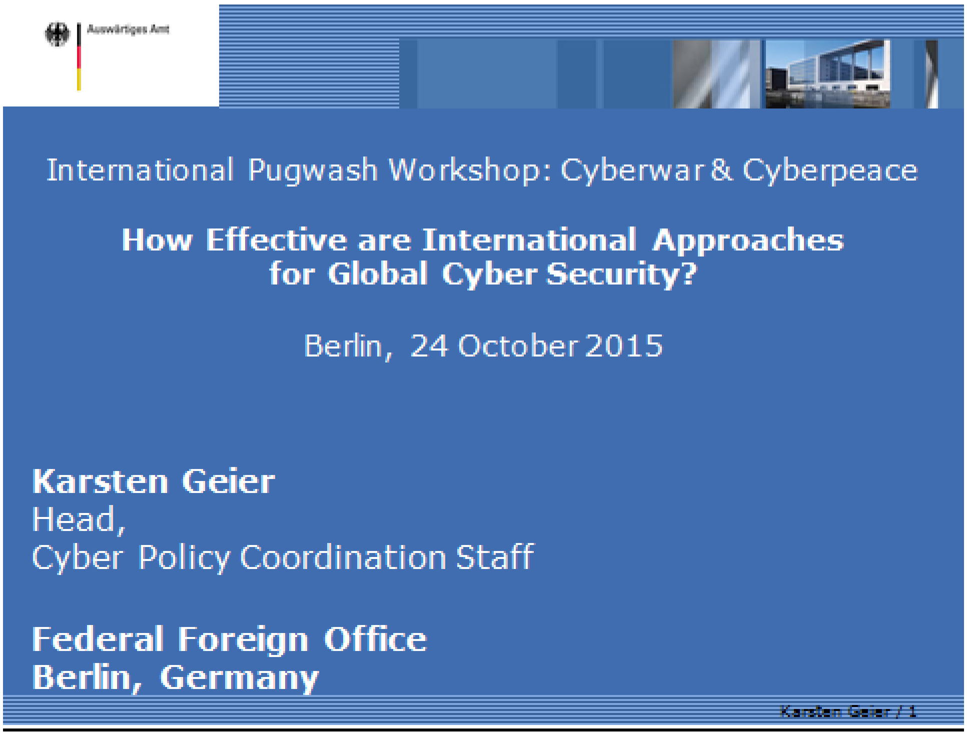
International Pugwash Workshop: Cyberwar & Cyberpeace

How Effective are International Approaches for Global Cyber Security?

Berlin, 23 October 2015



Auswärtiges Amt

International Pugwash Workshop: Cyberwar & Cyberpeace

How Effective are International Approaches for Global Cyber Security?

Berlin, 24 October 2015

Karsten Geier
Head,
Cyber Policy Coordination Staff

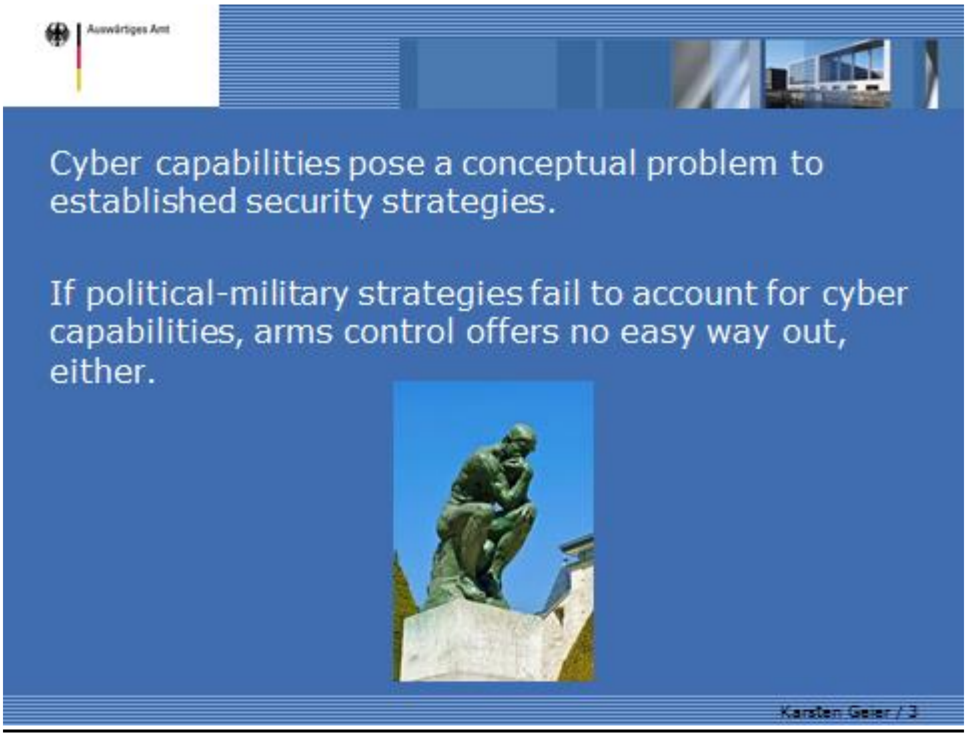
Federal Foreign Office
Berlin, Germany

Auswärtiges Amt

Cyber action is not limited to cyber space. It can create real damage in the physical world.

Diplomats and international security experts have to ask themselves how to respond.

Numerous states are pursuing military cyber-capabilities. The United Nations Institute for Disarmament Research, in its 2013 Cyber Index, found on the basis of publicly available information that there were 114 national cyber security programs world-wide. According to this index, forty-seven states have cyber-security programs that give some role to the armed forces. These cyber capabilities are affecting international security. They can create real damage in the physical world. In the interest of international peace and security, diplomats and security experts have to ask themselves how to respond, and how effective their approaches to global cyber security are.



Auswärtiges Amt

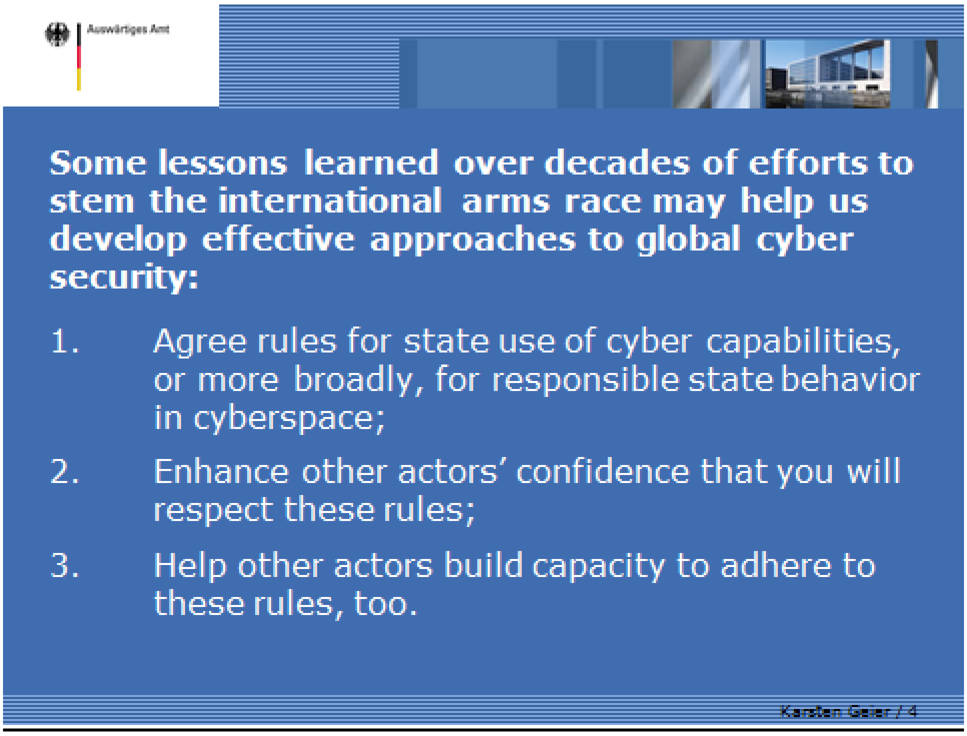
Cyber capabilities pose a conceptual problem to established security strategies.

If political-military strategies fail to account for cyber capabilities, arms control offers no easy way out, either.

Karsten Geier / 3

Cyber capabilities pose a conceptual problem to established security strategies. Traditional political-military strategies predate the existence of the internet. During the Cold War, the opposing parties built their defense on the idea that the best defense is to deter an enemy state from attacking. Deterrence requires that the consequences of any attack be clearly and credibly communicated *ex ante* to any potential adversary. This may not hold in cyber-space: Perpetrators show great skill in hiding or confusing their targets, using botnets, convoluted routings, delayed messaging and other techniques. They may not even be states. The effort required to attribute cyberattacks, the limits on forensic capabilities, and the absence of cooperation and collaboration between nations tax the credibility of attribution. Consequently, uncertainty about the origin of hostile cyber-action is a characteristic of cyber-incidents. This makes it difficult for states to threaten negative consequences of such action. Under such circumstances, deterrence may not work.

<u>If political-military strategies fail to account for cyber capabilities, arms control offers no easy way out, either</u>: Arms control treaties are typically concluded between a finite number of state-actors on a definable military good. By comparison, it seems next to impossible to negotiate an arms control or even disarmament treaty for “cyber-weapons”, given the potentially unlimited number of actors, state and non-state, that can develop, procure and proliferate computer malware. Also consider the difficulty of defining a “cyber weapon” in the first place: For some, this might be computer malware which allows an intrusion into another party’s computer system, either with the purpose of conducting cyber espionage, or for cyber sabotage. Others prefer talking about “information weapons”, a much wider term that covers the capacity to threaten destroy or otherwise affect individuals, society, the state and their interests. A common understanding of what we are talking about remains elusive.



Auswärtiges Amt

Some lessons learned over decades of efforts to stem the international arms race may help us develop effective approaches to global cyber security:

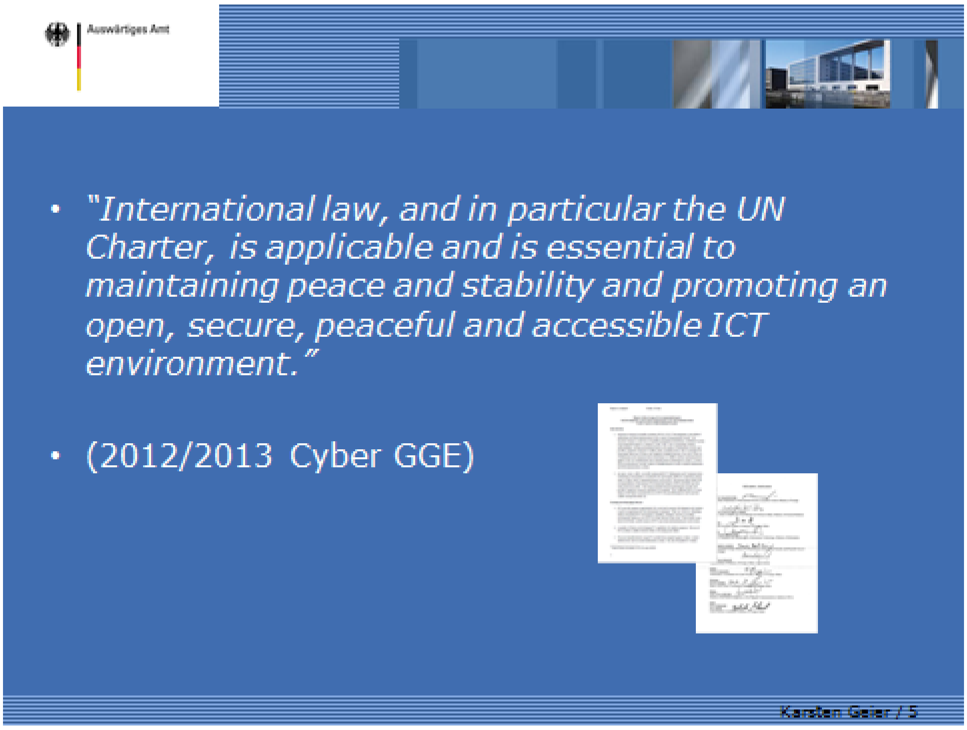
1. Agree rules for state use of cyber capabilities, or more broadly, for responsible state behavior in cyberspace;
2. Enhance other actors' confidence that you will respect these rules;
3. Help other actors build capacity to adhere to these rules, too.

Karsten Geier / 4

Nevertheless, some lessons learned over decades of efforts to stem the international arms race may help us develop effective approaches to global cyber security. I believe there are three lessons in particular states should heed:

1. Agree *rules* for state use of cyber capabilities, or more broadly, for responsible state behavior in cyberspace;
2. Enhance other actors' *confidence* that you will respect these rules;
3. Help other actors *build capacity* to adhere to these rules, too.

The first line of action -- **agreeing rules for state use of cyber capabilities, or more broadly, for responsible state behavior in cyberspace** -- is the domain of the United Nations.

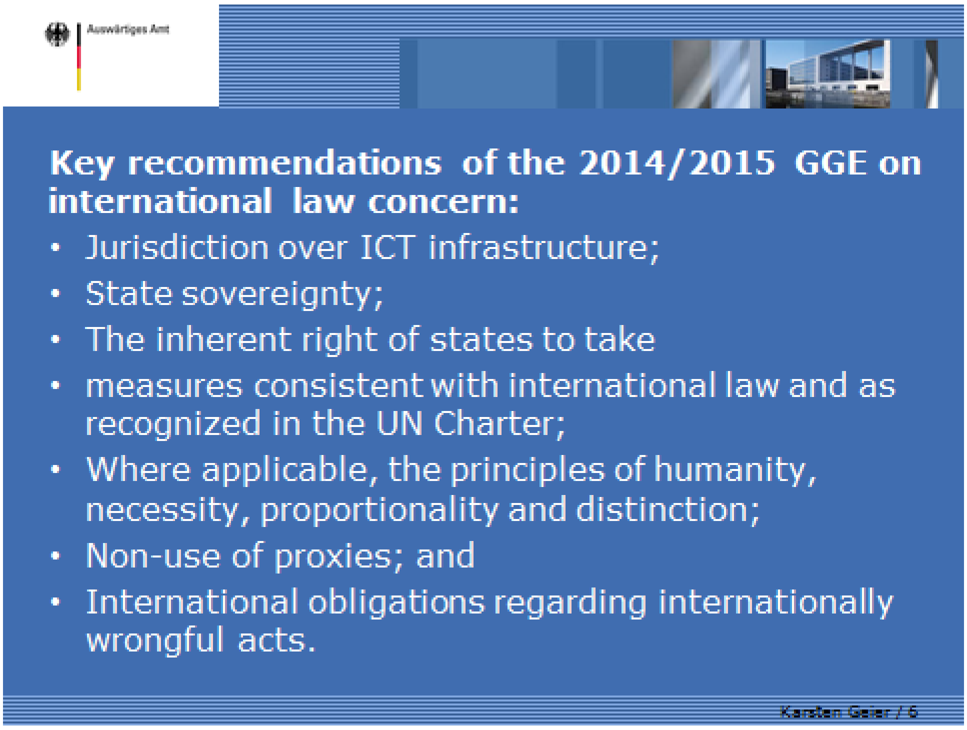


Auswärtiges Amt

- *"International law, and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."*
- (2012/2013 Cyber GGE)

Karsten Geier / 5

Since 2005, the United Nations General Assembly has mandated a series of groups of governmental experts (GGE) to work on this issue. The key point of the 2012/2013 Cyber GGE was the following: *"International law, and in particular the UN Charter, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."* On this basis, the General Assembly requested another GGE in December 2013 "*to study, with a view to promoting common understandings, existing and potential threats in the ICT sphere and possible cooperative measures to address them, including norms, rules or principles of responsible behavior of states and how international law applies to the use of ICT by states*".



Auswärtiges Amt

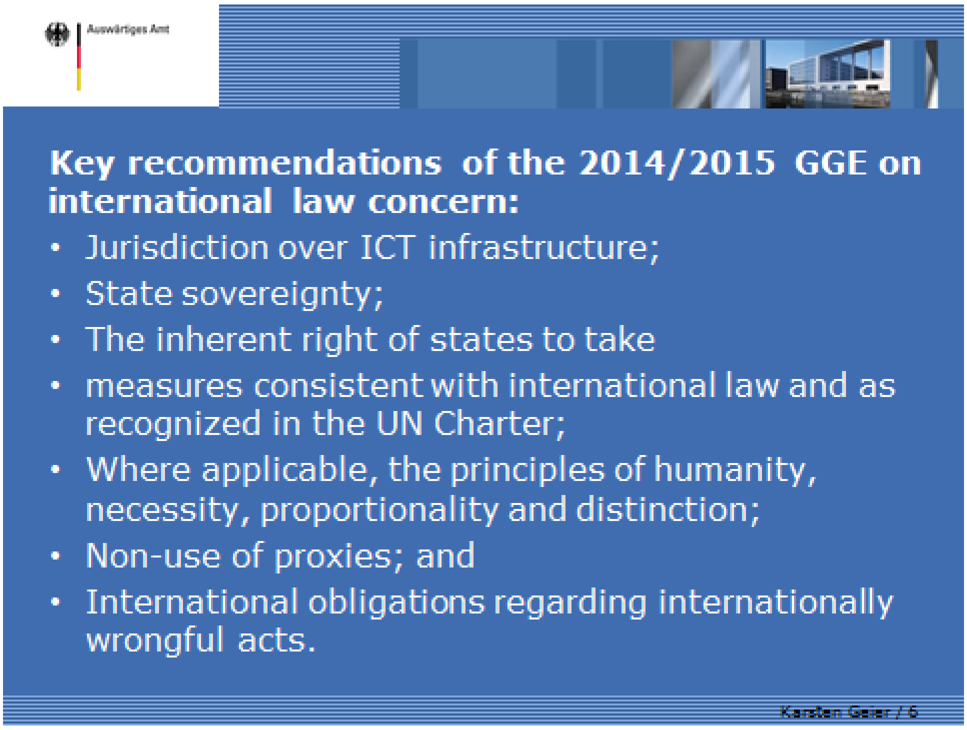
Key recommendations of the 2014/2015 GGE on international law concern:

- Jurisdiction over ICT infrastructure;
- State sovereignty;
- The inherent right of states to take
- measures consistent with international law and as recognized in the UN Charter;
- Where applicable, the principles of humanity, necessity, proportionality and distinction;
- Non-use of proxies; and
- International obligations regarding internationally wrongful acts.

Karsten Geier / 6

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. This list addresses, inter alia, issues of

- Jurisdiction over ICT infrastructure;
- State sovereignty;
- The inherent right of states to take measures consistent with international law and as recognized in the UN Charter;
- Where applicable, the principles of humanity, necessity, proportionality and distinction;
- The use of proxies; and
- International obligations regarding internationally wrongful acts.



Auswärtiges Amt

Key recommendations of the 2014/2015 GGE on international law concern:

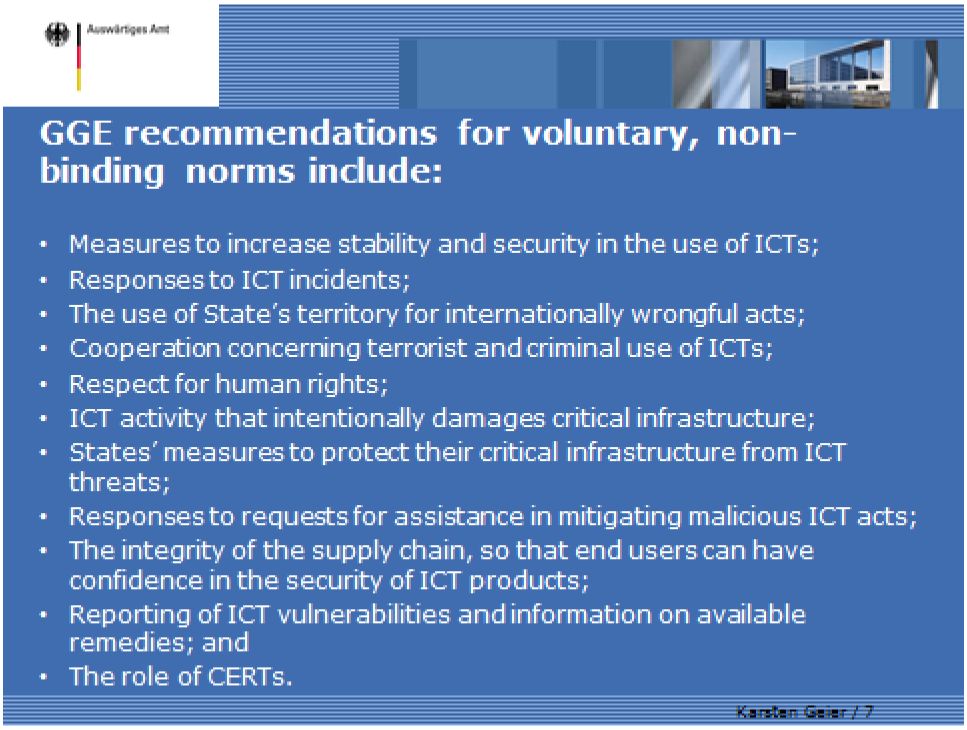
- Jurisdiction over ICT infrastructure;
- State sovereignty;
- The inherent right of states to take
- measures consistent with international law and as recognized in the UN Charter;
- Where applicable, the principles of humanity, necessity, proportionality and distinction;
- Non-use of proxies; and
- International obligations regarding internationally wrongful acts.

Karsten Geier / 6

The GGE also recommended a number of voluntary, non-binding norms of responsible State behavior for consideration by States. 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. The GGE recommendations include norms on

- Cooperation to increase stability and security in the use of ICTs;
- Responses to ICT incidents;
- preventing of the use of a State's territory for internationally wrongful acts;
- Cooperation concerning terrorist and criminal use of ICTs;
- Respect for human rights while ensuring the secure use of ICT;
- not conducting or allowing ICT activity that intentionally damages critical infrastructure;

- States’ measures to protect their critical infrastructure from ICT threats;
- Responses to requests for assistance in mitigating malicious ICT acts;
- The integrity of the supply chain, so that end users can have confidence in the security of ICT products;
- Reporting of ICT vulnerabilities and information on available remedies; and
- The role of CERTS.



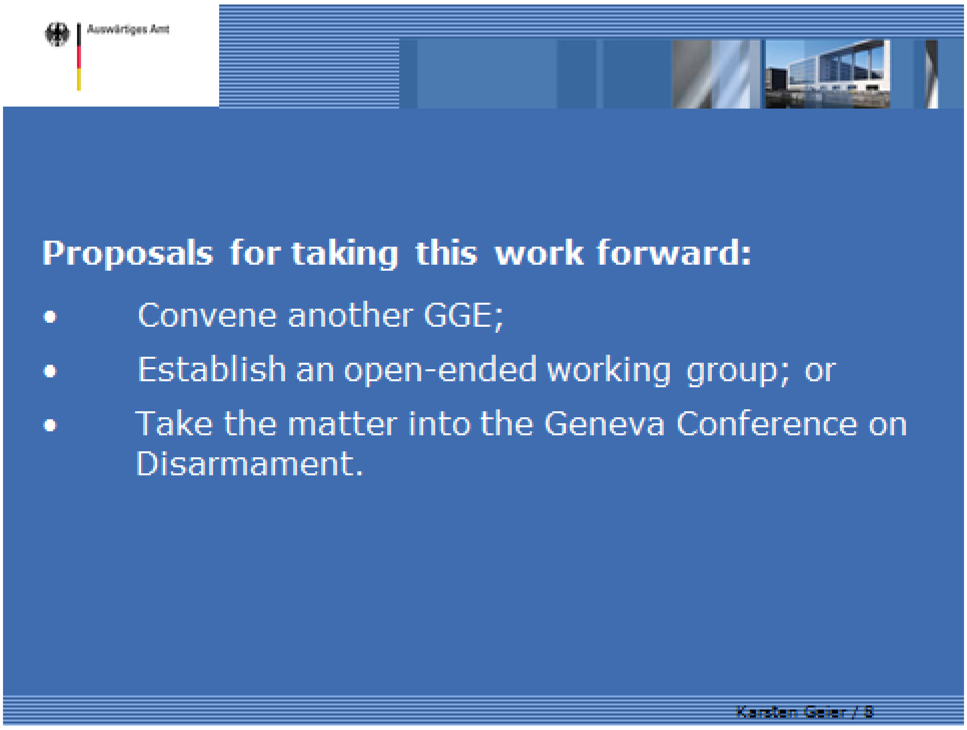
Auswärtiges Amt

GGE recommendations for voluntary, non-binding norms include:

- Measures to increase stability and security in the use of ICTs;
- Responses to ICT incidents;
- The use of State’s territory for internationally wrongful acts;
- Cooperation concerning terrorist and criminal use of ICTs;
- Respect for human rights;
- ICT activity that intentionally damages critical infrastructure;
- States’ measures to protect their critical infrastructure from ICT threats;
- Responses to requests for assistance in mitigating malicious ICT acts;
- The integrity of the supply chain, so that end users can have confidence in the security of ICT products;
- Reporting of ICT vulnerabilities and information on available remedies; and
- The role of CERTs.

Karsten Geier / 7

In addition to these norms, the GGE proposed a list of voluntary confidence-building measures to enhance trust and cooperation and reduce the risk of conflict.



Auswärtiges Amt

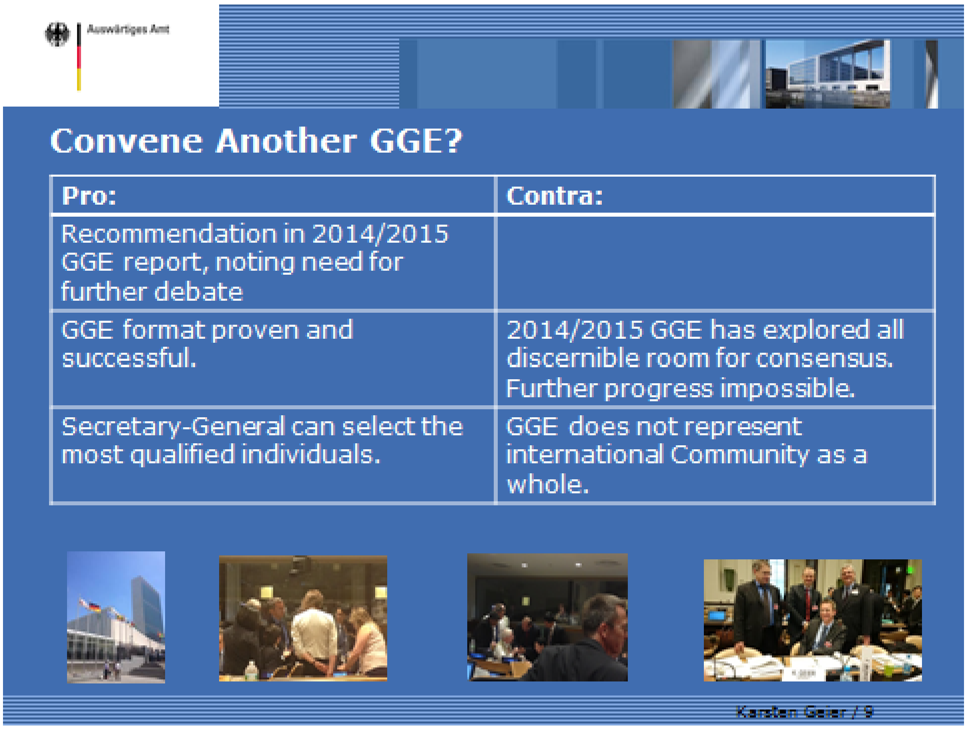
Proposals for taking this work forward:

- Convene another GGE;
- Establish an open-ended working group; or
- Take the matter into the Geneva Conference on Disarmament.

Karsten Geier / 8

The question now is how to take this work further. Various proposals have been brought forward, for example:

- Convene another GGE;
- Establish an open-ended working group; or
- Take the matter into the Geneva Conference on Disarmament.



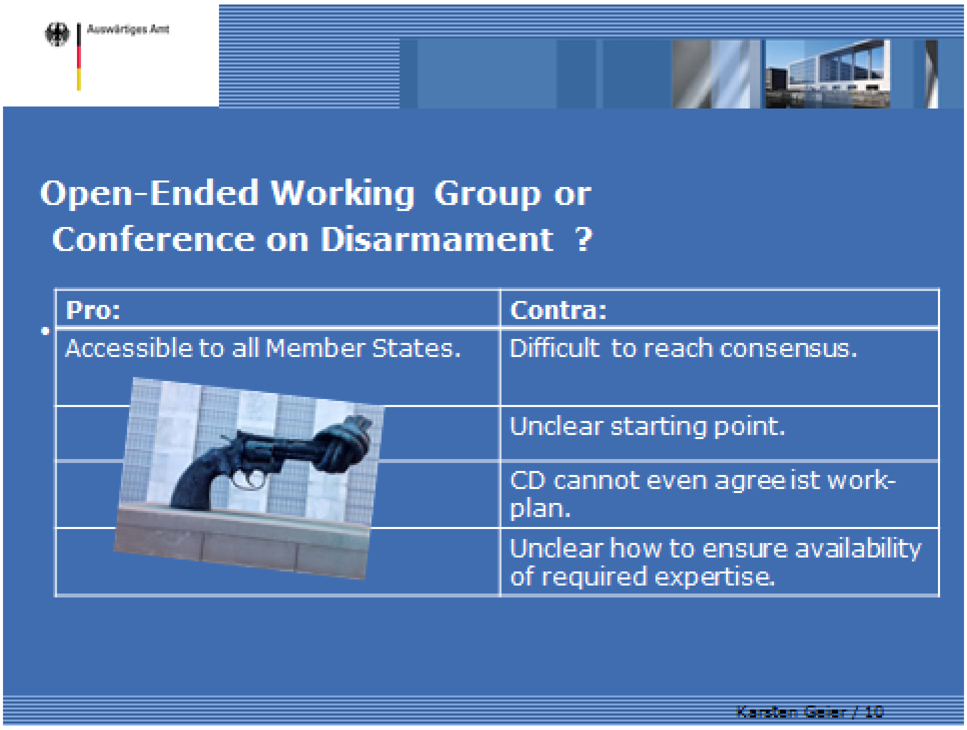
Auswärtiges Amt

Convene Another GGE?

Pro:	Contra:
Recommendation in 2014/2015 GGE report, noting need for further debate	
GGE format proven and successful.	2014/2015 GGE has explored all discernible room for consensus. Further progress impossible.
Secretary-General can select the most qualified individuals.	GGE does not represent international Community as a whole.

Karsten Geier / 9

The idea of convening another GGE has found its way into the recommendations of the 2014/2015 report, and a resolution to this end is being discussed in the UNGA’s First Committee as we speak. There are good reasons for following this recommendation: The 2014/2015 GGE felt a need to continue the discussion. The GGE format has proven successful. The Secretary-General can select the most qualified government experts, ensuring subject-matter expertise. However, important points can also be fielded against yet another GGE: The reports of the four cyber-GGEs since 2004 have become successively more complex and detailed; the process may have explored all possible room for consensus so that immediately convening another such group may not lead to progress. A problem is also that GGEs comprise a limited membership and therefore may not be perceived to be representative of the international community as a whole. At some point in the future, we can expect the GGE process to reach the end of its useful life. Until that time, Germany will do its level best to help support the work of the cyber GGEs!



Auswärtiges Amt

Open-Ended Working Group or Conference on Disarmament ?

Pro:	Contra:
Accessible to all Member States.	Difficult to reach consensus.
	Unclear starting point.
	CD cannot even agree ist work-plan.
	Unclear how to ensure availability of required expertise.

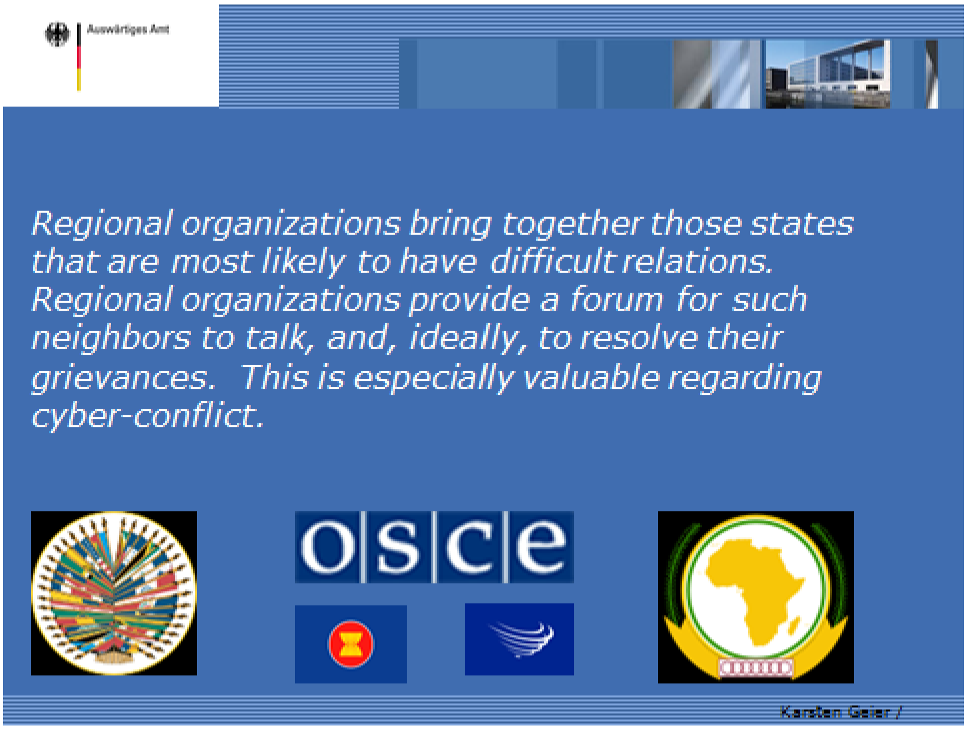
Karsten Geier / 10

What about the <u>proposal to establish an open-ended working group</u>? Such a body, which could be convened under the First Committee of the General assembly, could be made accessible to all Member States that wish to contribute. This would address the concerns about inclusiveness. On the other hand, the large membership and the open-ended nature of the mandate would mean that consensus would be very hard – nigh impossible – to achieve. And where would such a group start? Would it build on the reports of the GGEs? Or would it begin anew, undoing hard-won progress? Finally, there is a tension between demands for inclusiveness and the need for expert knowledge in a field as complex and technical as cyber security.

<u>A better case may be made for discussing cyber security in the context of the Conference on Disarmament</u>. The CD has a limited membership, made up of some of the most dedicated actors. At the same time, it has invited UN Member States that have expressed a desire to participate in the CD's substantive discussions, to take part in its work as observers. It is true that for the past 19 years, the Conference has been unable to

agree even on its work-plan. However, the CD and its predecessors have negotiated numerous major multilateral arms limitation and disarmament agreements, such as the Treaty on the Non-Proliferation of Nuclear Weapons, the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, and the Comprehensive Nuclear-Test-Ban Treaty. Once the GGE process will have run its course, it may be worth exploring whether the Conference's 65 member states, presented with international cyber security as a new issue, could break their current deadlock. This, however, would require very careful preparations, including a clear definition of the Conference's mandate. We are a long way from that point!

The second lesson learned from arms control for cyber security is to **enhance other actors' confidence that you will respect these rules.** This is best done through transparency and confidence-building measures.


Auswärtiges Amt
osce

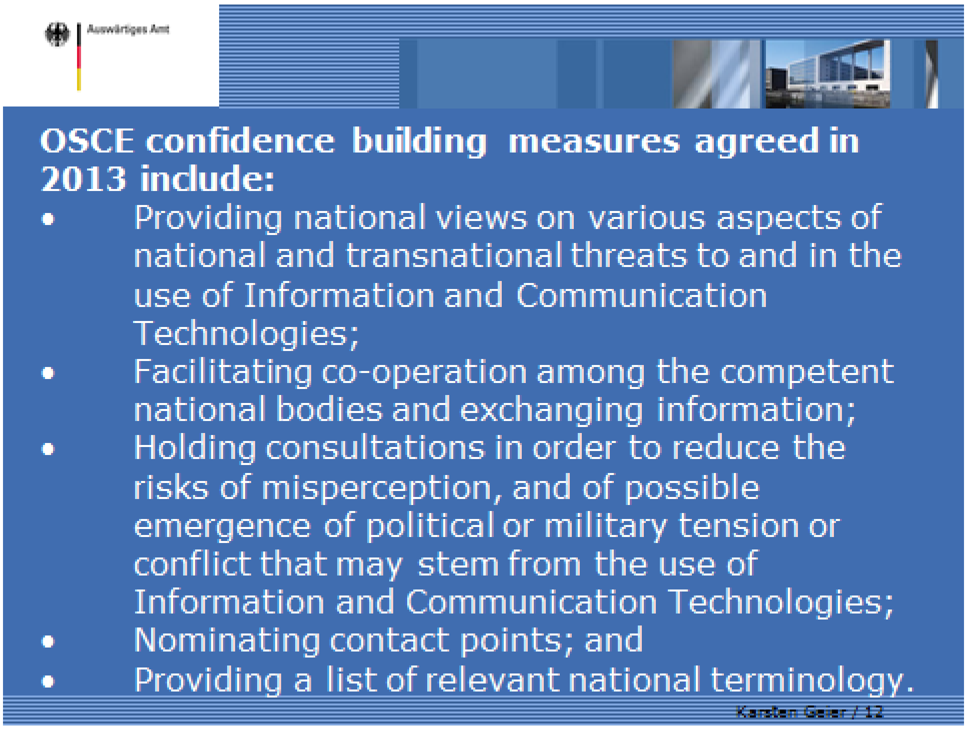
Regional organizations bring together those states that are most likely to have difficult relations. Regional organizations provide a forum for such neighbors to talk, and, ideally, to resolve their grievances. This is especially valuable regarding cyber-conflict.

Karsten Geier /

<u>Much of this work is usefully taken forward in regional organizations.</u> Regional organizations 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 <u>especially valuable regarding cyber incidents</u>. As mentioned before: The perpetrators of hostile cyber action are difficult to identify. Consequently, 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. If, on the other hand, relations are relaxed and mechanisms exist to resolve any incipient disputes, the danger of escalating international tensions over a hostile cyber act is much reduced.

In the field of cyber security, there are a number of concrete steps that can be agreed between members of a regional organization. The UN Cyber GGE has sketched out a number of them. 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.



Auswärtiges Amt

OSCE confidence building measures agreed in 2013 include:

- Providing national views on various aspects of national and transnational threats to and in the use of Information and Communication Technologies;
- Facilitating co-operation among the competent national bodies and exchanging information;
- Holding consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of Information and Communication Technologies;
- Nominating contact points; and
- Providing a list of relevant national terminology.

Karsten Geier / 12

The first agreement, endorsed by the OSCE Council of Ministers in December 2013, contained various voluntary steps, including:

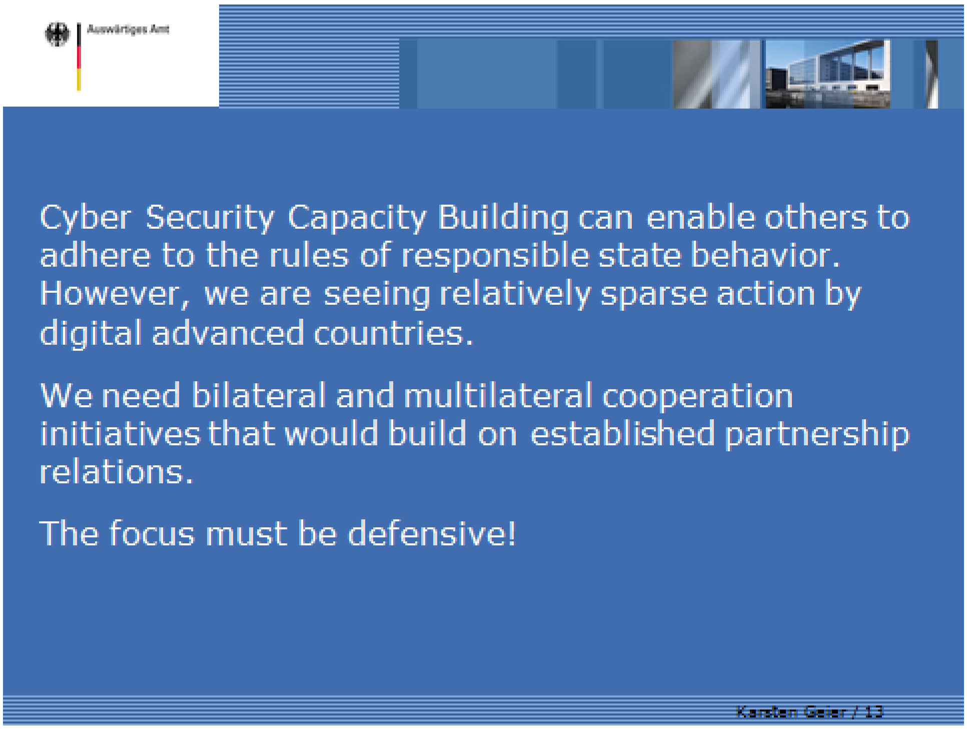
- Providing national views on various aspects of national and transnational threats to and in the use of Information and Communication Technologies;

- Facilitating co-operation among the competent national bodies and exchanging information;
- Holding consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of Information and Communication Technologies;
- Nominating contact points; and
- Providing a list of relevant national terminology.

It is encouraging that the implementation of these confidence-building measures has begun, in a serious and workmanlike fashion – irrespective of the political turbulences that have been shaking the OSCE area since late 2013.

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. We are looking forward to deepening and widening this engagement.

The third element we can take from arms control experience, is to **enable others to adhere to the rules of responsible state behavior**



Auswärtiges Amt

Cyber Security Capacity Building can enable others to adhere to the rules of responsible state behavior. However, we are seeing relatively sparse action by digital advanced countries.

We need bilateral and multilateral cooperation initiatives that would build on established partnership relations.

The focus must be defensive!

Karsten Geier / 13

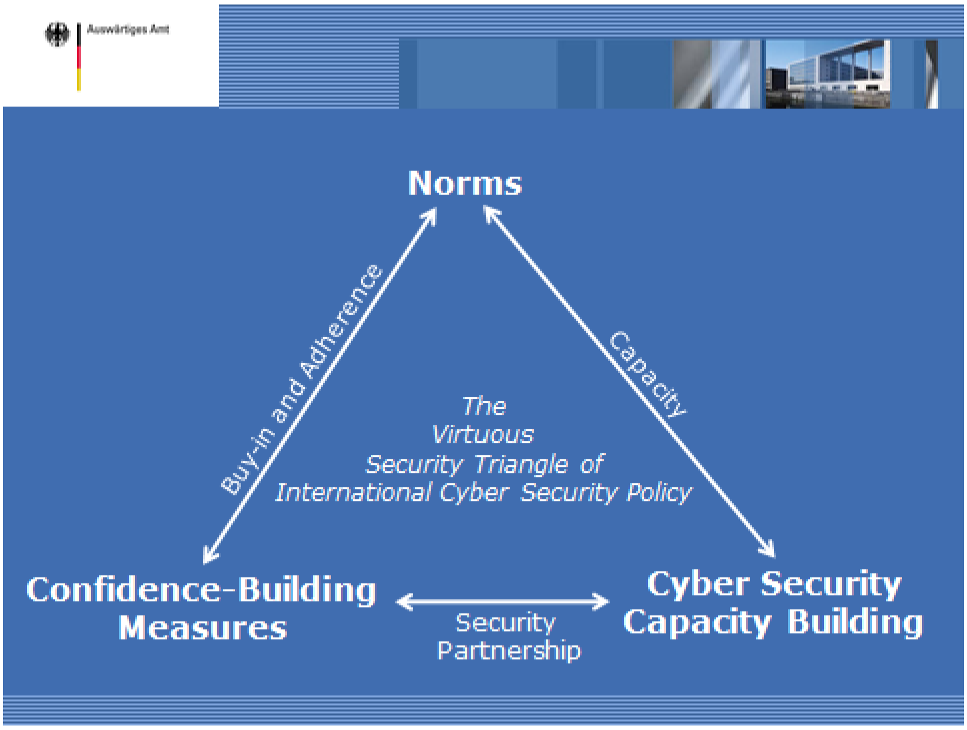
Cyber capacity building – including cyber security capacity building – is key to preserving and fully utilizing the Internet’s potential as a global, open, free, secure, stable and accessible instrument to safeguard and promote freedom and human rights online, to contribute to new forms of democratic participation and to foster economic and technical innovation. Cyber Capacity Building needs to be approached in a comprehensive manner. It entails bi-, multilateral and international support to develop, build and maintain secure information and communication technologies (ICTs) infrastructures as well as the capacities to use them securely. To this end, we need knowledge and capabilities, technical and administrative infrastructures, adequate legal frameworks, sustainable strategies and responsive policies. All of these elements must be reflected and developed in close stakeholder cooperation and consultation, and paying particular attention to local and regional contexts.

Cyber Security Capacity Building is an important variable in this approach. It 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. "Buy-in" to rules for state behavior is far from universal, with many states suspecting that these rules actually favor advanced industrialized countries at their expense. Looking at concerning transparency and confidence-building, we often find that states' readiness to engage is lowest where the need may be greatest.

Cyber security is an international concern of everybody, everywhere, and beyond any borders of ideology or politics. Every fisherman knows: A net will rip if it has a weak link. This is true for the Internet, a global web of webs, as well. The more international the problem the more international the answers have to be. It is no coincidence that the most recent GGE dedicated an entire chapter of its report to "International Cooperation and Assistance in ICT Security and Capacity-Building". This text provides a host of proposals for concrete measures that UN Member States could undertake. Previous such groups also recommended cyber capacity building measures. Cyber capacity building was also an important point of the discussions at the international Conference on Cyber Space, held in April of this year in The Hague. The outcome was an agreement to establish a Global Forum on Cyber Expertise: a pragmatic, action-oriented and flexible forum to strengthen cyber capacity and expertise and to make existing international cooperative efforts in this field more effective. The Forum's overarching and long term goal is to strengthen cyber capacity and expertise globally.

Much needs to be done. In an unequal world where political interests vary and countries differ in their stages of digital development, it is not easy to find and a consensus approach. While cyber capacity building has become a buzzword, we are seeing relatively sparse action by digital advanced countries. In our mind, we need bilateral and multilateral cooperation initiatives that would build on established partnership relations. Our armed forces are already working with select states on cyber defense. The Foreign Office supports the efforts by UNIDIR and NGOs such as ICT4Peace on trust and transparency building projects (e.g. digital database to track cyber defense measures). In order to streamline the already existing Cyber Capacity Building activities of different ministries and governmental agencies, the federal government is currently discussing to set up a common framework approach for Cyber Capacity Building. Let me be clear: When we engage in Cyber Security Capacity Building, the focus must be defensive! In this sense, one of the best measures states can take is to decentralize critical systems. An electricity grid, for instance, that is locally autonomous is far more resilient than one that is a central “cyber-attack node”. In a similar vein, e-government services, banking, health services etc. stand to gain in resilience from decentralized organization.

In conclusion: There are lessons for effective global cyber security that we can draw from decades of arms control experience. They pertain to the importance of rules for responsible state behavior, to confidence-building, and to cyber security capacity building.



Auswärtiges Amt

Norms

Buy-in and Adherence

Capacity

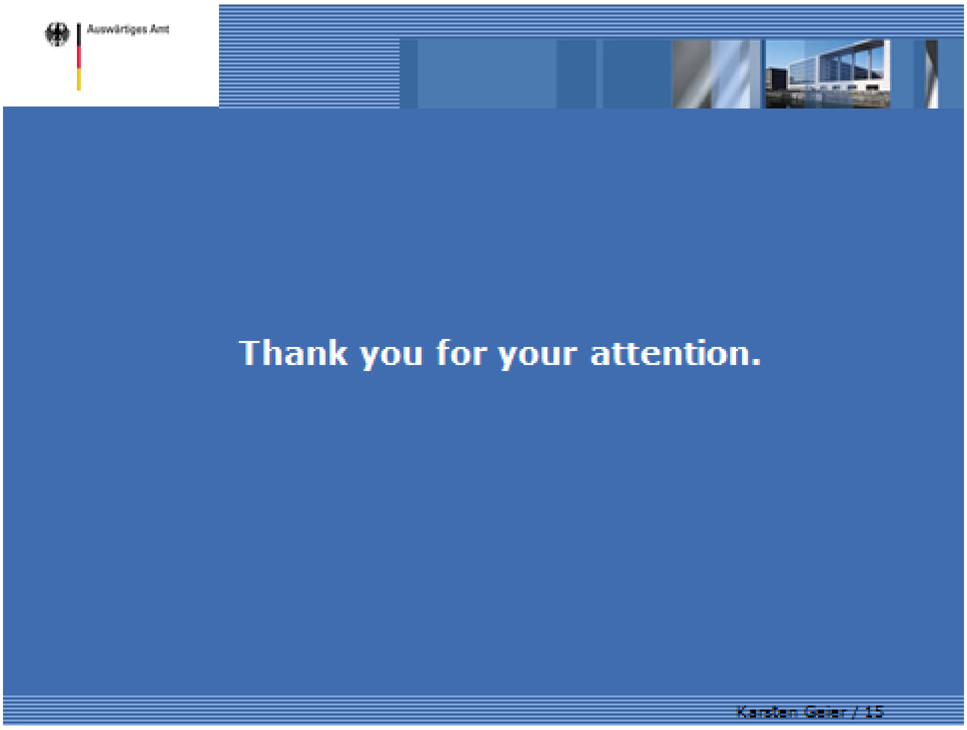
The Virtuous Security Triangle of International Cyber Security Policy

Confidence-Building Measures

Security Partnership

Cyber Security Capacity Building

Adherence to rules for responsible state behavior in cyberspace is related to inter-state transparency and confidence. We should recognize this link. 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. <u>There is a virtual triangle linking these three elements, and we need to work on them simultaneously.</u> That may be the most important lesson for us to learn.



Auswärtiges Amt

Thank you for your attention.

Karsten Geier / 15