“Cyber Security as a Dimension of Security Policy”. Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London

18.05.2015 - Speech

Ladies and Gentlemen,

Germany is a strong advocate of a stable, secure, open and free Internet. It offers great opportunities: for economic growth and development, for good governance and democracy, as well as for the exchange of ideas between people around the world.

At the same time, the Internet presents us with new threats:

Numerous states are pursuing military cyber-capabilities.

Those programs are often of a defensive nature but may sometimes include offensive aspects. This is unsettling, especially, since cyber action is not limited to cyber space. It can cross domains and create real damage in the physical world: The attack on SONY Pictures caused millions or even billions of Dollars of damage.

One might also think of a virus disrupting critical assets and infrastructure in a given country.

Nevertheless, an all-out “cyber war” seems unlikely at present.

In fact, the term “cyber war” is inadequate and misleading.

It implies an extensive, existential threat to a state solely through targeted attacks by other states on computer systems and IT networks, or through other actions in cyberspace.

This seems unrealistic for the foreseeable future.

A more likely scenario is the limited use of cyber capabilities as part of a larger warfighting effort. Cyber-attacks in combination with conventional means of conflict can thus pose a substantial threat.

Making matters worse, cyber capabilities are not limited to great powers or even states – they transcend the established lines of state-centred warfare.

Private actors – be it legitimate business, criminals, or terrorists – can obtain or even design their own malware and conduct attacks on targets that were previously out of reach.

Groups like ISIS and Al Qaida have for a long time been skilfully using the internet as a propaganda and recruitment tool.

Recently, we witnessed a new development: The hacking attack on TV5 Monde in France this past April demonstrated that terrorists can use the internet as an attack tool.

Not just a television station or a movie production firm can be targeted. Critical assets, systems and infrastructure become vulnerable when they are connected to the internet.

Exactly this kind of connectivity is the working assumption of the “internet of things”. It opens new avenues of attack.

Attempts to access, manipulate or damage critical assets, systems and infrastructure are of particular concern. Such attacks can have severe consequences for governments, the private sector and society.

One might think of a virus disrupting a country’s power supply, which could have tremendous physical consequences in any advanced industrial society, both for the military and the society in general.

Every nation today uses information and telecommunication technology in its economic and social infrastructure. We therefore have to expect that cyber capabilities will play a role in future conflict situations.

Defence against these capabilities is difficult, especially since inordinate efforts may be required to attribute a cyber-incident to its originator.

Technology allows the originator to fake identities, reroute attacks, delay them, or even conceal the attack itself.

Therefore, at least for the foreseeable future, we will have to live with the fact that uncertainty is an inherent trait of incidents in the cyber sphere.

This is setting the cyber sphere apart from traditional military capabilities:

During the Cold War, the opposing parties built their defence on the idea that the best defence is to deter an enemy state from attacking. In the event of a failure of deterrence, an adversary should be denied the success of his or her action.

Deterrence and denial require that the consequences of any attack can be clearly and credibly communicated to any potential adversary.

This is next to impossible in cyber space:

Actors may not be known; they do not even have to be states.

If uncertainty about the origin of hostile cyber-action is a characteristic of cyber-incidents, it is impossible to threaten concrete, negative consequences of such action.

Under these circumstances, deterrence may not work.

All this can easily lead to an atmosphere of mutual distrust and conflict. Cyber capabilities therefore introduce an element of instability into the international security environment.

This instability is even greater given the potential of escalation of cyber incidents.

Picture the following scenario:

One state has a tense relationship to its neighbour – maybe because of a border dispute.

Suddenly a cyber-attack happens and all communications services are disrupted.

Telephones no longer work and nobody is able to access the internet.

The situation worsens; other sectors are affected, such as the power grid or the banking system. It might have been an individual who planted this virus, but suspicions run high that the less friendly neighbour perpetrated a cyber-attack.

How to respond? Is this a case where the attacked state may use its right to self-defence? The danger of escalation is evident.

To summarize so far:

Cyber capacities are available to a wide range of actors, ranging from states to malevolent individuals.

We need to expect the use of these capabilities both in the context of criminal and terrorist acts as well as in conjunction with “traditional”, inter-state conflicts.

Cyber capabilities make offense easy, while defence is difficult: The insecurity about the origin and purpose of a cyber-attack may provide an incentive to attack.

Ladies and Gentlemen!

The challenge is thus as follows: How can we achieve greater security in cyberspace?

To address this challenge, Germany is suggesting three areas of engagement:

First, working towards a common understanding of responsible state behaviour in cyber space.

Second, promoting confidence and trust.

And third, undertaking efforts to increase cyber-resilience.

In these three areas, we should engage internationally within existing fora, and we should also try to bring in civil society and business in the framework of a multistakeholder approach.

1.

The first task is to find a broad, international consensus on responsible state behaviour in cyber space.

Given the number of potent actors, rapid developments in the underlying technology and the need better to define how international law applies to state behaviour in cyberspace, the need for rules is in no area as apparent as in the internet.

Let me highlight a few pressing questions that need to be discussed:

Is a state authorized, under international law, to respond to hostile cyber action by the use of force?

Where is the threshold?

The United Nations Charter allows states the right to self-defence in the event of an armed attack. But is hostile cyber-action an armed attack?

In Germany's opinion, this depends on its scale and effects: If a state finds itself the target of a cyber-operation with effects comparable to an armed attack, it may exercise its right to self-defence. Factors to be taken into account include, inter alia, the seriousness of the attack, the immediacy of its effects, depth of penetration of the cyber infrastructure and its military character.
Even in cases where one cannot speak of a use of force, the use of cyber capabilities might constitute a violation of sovereignty, if the attack can be attributed to a state, which then in turn could lead to consequences within the confines of public international law.

Another question:

Is international humanitarian law applicable to the use of cyber capabilities?

We firmly believe so. It would be good for all states to share an understanding which cyber acts are permissible under international humanitarian law, without transgressing on the principles of humanity, distinction, necessity and proportionality.

Attacks on certain critical infrastructure, nuclear power plants or hospitals might well be inadmissible under the general rules of international law aimed at protecting civilians from the indiscriminate effects of weapons and combatants from unnecessary suffering.

But how would one assess, in the context of an international armed conflict, an attack on one side's power grid, crippling that country's war-fighting capabilities, but also provoking tremendous repercussions for the civilian population?

Discussing how international humanitarian law applies to cyberspace is highly controversial. Some argue that this encourages a militarization of this thus far civil resource; they refer to the threat of a new arms race.

However, we believe that it would not be expedient to ignore reality: Cyber space is already being used by the military.

More questions:

Analogous to the law of the sea: Is there a mutual assistance requirement in cyber emergencies?

That could be important when the critical infrastructure of a country is attacked, with considerable consequences for the civilian population.

Which obligations fall upon states regarding the safety of their critical IT infrastructure?

There is consensus that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of activities related to information and communication technology, and to their jurisdiction over the required infrastructure within their territory.

Such sovereign rights carry duties as well. We believe that States must provide an adequate level of protection for IT infrastructure on their territory, with a view of safeguarding the overall functionality and stability of the Internet.

A better shared understanding of the rules, norms and principles that apply to responsible state behaviour in cyberspace would enhance international transparency and predictability and thus contribute to peace and stability. To establish a universal understanding of such rules, norms and principles, we must turn to the United Nations.

Together with experts from around the world -- the UK among them --, Germany is actively participating in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, known as GGE.

The GGE's mandate is to study, with a view to promoting common understandings, existing and potential threats in the ICT sphere and possible cooperative measures to address them.

We are looking forward to the report by the GGE to the UN Secretary General next month.

From our point of view, the GE report is also the instrument of choice to take up initiatives and ideas brought forward by interested parties.

I am thinking here, in particular, of some of the elements in the draft Code of Conduct proposed by members of the Shanghai Cooperation Organisation. It seems preferable to reflect them in the GGE framework, rather than negotiating on parallel tracks.

Beyond this report, potential further steps are manifold. Some think we need a UN summit dedicated to cyber issues, flanked by establishing some sort of UN cyber agency.

Others prefer a step-by-step approach, continuing carefully with a series of select-member GGEs.

In all probability, agreement will fall somewhere between these extremes.

One interesting thought: Failing universal consensus, should a group of states develop a consensus among its members on rules for cyberspace? The experiences of the Proliferation Security Initiative (PSI) could be useful in this context.

2.

I mentioned three areas of engagement.

The second is to further confidence and trust among states in cyberspace.

Given the nature of cyber incidents and the ensuing dangers I described, mutual confidence and trust are paramount to increasing international stability.

This can be achieved through steps towards transparency and cooperation.

To this end, Germany strongly advocates transparency and confidence-building measures (CBMs).

Our work on developing CBMs takes place in various fora, in particular at the regional level.

Why do we focus on the regional level here?

Because regional organizations bring together those states that are most likely to have difficult relations. It is far more likely that two neighbours 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 neighbours to talk, and, ideally, to resolve their grievances. This is especially valuable regarding cyber-conflict.

As mentioned before: The perpetrators of hostile cyber action are difficult to identify. Consequently, a state that falls victim to such action often has to guess who is responsible. Chances are that suspicions will fall on a neighbour with whom relations are strained. This is similar to the scenario I described earlier.

If now, 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. An escalation of the conflict could be prevented.

This is why transparency and confidence-building measures will be most effective at the regional level.

In the Organization for Security and Cooperation in Europe (OSCE) Participating States agreed on a first set of such measures in 2013 – the first time ever such steps were taken. They are mostly aimed at increasing transparency. It is encouraging that the implementation of these measures has begun, in a serious and workmanlike fashion – regardless of the political turbulences that have been shaking Europe in the last year and a half.

But the implementation needs to be complemented by additional steps, aiming beyond transparency at cooperation and stability.

Since last year we have also been discussing a second set of CBMs, this one aiming at trust-building and cooperation. In the longer term, we hope to arrive at a third set that would be geared toward increasing risk-reduction and stabilization.

We want to take this issue further as part of Germany’s OSCE Chairmanship in 2016.

One thought is to explore if the “Vienna Document” pertaining to conventional armaments might be useful.

Similar work might be undertaken in other regional organizations as well as in bilateral formats. Germany entertains dialogues on cyber issues with a variety of partners, both formally and informally.

3.

Our third area of engagement is to undertake efforts to increase cyber-resilience.

On a national level, a key project of the Federal Ministry of the Interior is the proposed IT Security Act.

The draft of the Act defines minimum requirements for IT security of critical infrastructures. It establishes an obligation to report significant incidents with a view of improving the overall security of systems and public protection in general.

The Federal Government wants Germany’s IT systems and digital infrastructure to be the most secure in the world.

The IT Security Act is based on the notion that anyone who creates risks for others through the use of IT should also be responsible for protecting against these risks.

The more serious these risks are, the higher the standards for the necessary protection should be.

But we do not interpret this topic narrowly, focusing on our own, national IT-infrastructure.

Important work is being conducted in the EU:

The Network Information Security Directive aims at the creating high, harmonized standards of network security in all EU Member States. Critical infrastructure in particular will be protected through this measure.

The EU Cybersecurity Strategy recognises the need to adequately protect critical infrastructure.

In addition, Germany is helping third states improve their cyber capacities, for instance by assisting them in formulating their own Cyber Security Strategies.

We suggest that states form bilateral and multilateral cooperation initiatives, building on established partnership relations. These initiatives could foster mutual assistance between states in their response to cyber incidents.

The Global Forum on Cyber Expertise formed in April 2015 at the Hague Conference on Cyberspace is a step in this direction. In the future, it could be the United Nations who provide coordination and support for these initiatives.

Ladies and Gentleman,

There is one point I need to raise which is delicate. It has led to considerable discussion between us and some of our key allies:

The relationship between security and freedom in the digital age.

We all agree that international law applies in cyberspace, and that individuals enjoy the same rights online as they do off-line. This includes the right to information, the right to freedom of expression, the right of association and the right to privacy.

At the same time, these rights can be abused.

As I mentioned early on: Terrorists have been using the Internet as a recruitment and propaganda tool for a long time, and only last month, we witnessed an actual extremist attack using cyber capabilities. Individual freedom online finds its limits in the security concerns of others.

We need to balance freedom and security.

The balance needs to be well-defined, as a result of a thorough political discourse at the national and international levels.

It has to be reasonable and the gains of measures aiming at an appropriate level of security have to be proportional to the costs they impose on our freedom and privacy.

Germany and Brazil have taken the initiative in the United Nations for General Assembly resolutions on the right to privacy. We are glad that these found consensus, and that the Human Rights Council in Geneva recently passed a resolution – also unanimously – establishing a Special Rapporteur on the Right to Privacy.

Ladies and Gentlemen!

I hope to have given you some food-for-thought for these questions, and I look forward to discussing these issues with you.