Federal Academy
for Security Policy

Security Policy Working Paper, No. 9/2017

More security in cyber space:
The case for arms control

by Paul-Jasper Dittrich and Björn Boening

It is a fact that arms control in the conventional sense is difficult to implement in cyber space at present. The reasons lie in the nature of the networks themselves on the one hand and in the lack of interest of some key players to change the status quo on the other. This does not mean, however, that cyber arms control is impossible. It will require an extended diplomatic process. In addition, will be decisive that the debate about security in cyber space does not only take place among IT experts but is made accessible for policymakers as well. International discussion platforms for cyber security should be strengthened with a view to also developing confidence-building measures for cyber space in the long term. The EU provides examples of what such measures could look like in practice.

In November 2016 the Federal Office for Information Security published its annual situation report on cyber security. It reveals that about 20 highly specialised attacks on the networks of the German government are carried out every day. Major German corporations such as Telekom, Volkswagen and ThyssenKrupp also experience multiple attacks every day. These findings lead to two key questions: Why is it so difficult for states to control cyber space and how can states work together internationally to counter internet-based threats?

When taking a look at the structure of cyber space and the players involved it becomes apparent that common accepted procedures and standards – a form of cyber arms control, as it were – would be necessary to achieve better security in this relatively unregulated environment. Frank-Walter Steinmeier, then German foreign minister, already called for a fresh start in conventional arms control last August. On the occasion he explicitly pointed to “offensive cyber capabilities” as a new technology that presented a considerable danger. Mr Steinmeier stated that international cooperation was required to counter this new threat. However, cyber space has a number of special technical characteristics that make international security cooperation difficult.

Cyber space is a difficult terrain

The difficulty of establishing control in cyber space begins with the architecture of the networks, and particularly its size and number of users. It was about 50 years ago that scientists in the United States and in Europe first connected two computers and thus built the first computer networks. The networks rapidly became larger and more stable, thereby making it possible for information of any kind to be exchanged at unprecedented speed and across almost all political borders. This resulted in a fundamental shift in the tasks computers were used for: away from mere computing and towards the exchange and management of information.

 | ISSN 2366-0805

Broadly speaking, one could say that there have not been many fundamental changes since then. Information can also be stored and shared via the internet today. The main difference between the early networks of the 1960s and today's network architecture is the continuously growing flow of information (data volume) and number of users and devices (nodes) in the network. In 2016 about 3.2 billion people around the globe, which is equal to nearly half of the world's population, were connected to the internet. But even without any involvement of human beings, an increasing number of devices are connecting themselves to the internet to share information amongst each other, for instance surveillance cameras, cars and household appliances. According to several studies, the number of devices connected to the internet reached approximately seven billion in 2016. The emerging "Internet of Things" could result in roughly 20 billion interconnected devices by 2020 according to some projections.

Complete governmental control is not possible

The larger and more difficult the terrain to be defended, the more difficult it becomes to protect against attacks. This principle also applies in digital space: the more information is stored in networks, the greater the incentive becomes to seek out sensitive information within them. Ever-growing and ever more complex networks often make it easier for attackers to find vulnerabilities. No state can effectively control cyber space in its entirety – neither technically nor politically. Besides the sheer size of cyber space, this has three main reasons. These reasons are the dynamic architecture of the networks, the composition of the participating players, and the impossibility of attributing attacks to specific players.

The dynamic architecture of the networks is based on a paradigm shift in telecommunications. In contrast to traditional telephony, today's networks are based on a method referred to as packet switching. An e-mail is not sent through the network as a whole, but disassembled into small data packets containing information about their sender and recipient. These packets are not reassembled before they reach their recipient. The individual packets may follow different routes to reach their recipient. This decentralised structure allows better flexibility and resilience. At the same time, monitoring the content and routes of these packets requires a considerable effort. Only very few companies and government agencies are able to do so.

The second problem is that the state is just one of many players in cyber space. Large parts of the internet's physical infrastructure consist of the telecommunications networks within individual states. The proliferation of telephone and, eventually, mobile telephone communications led to comprehensive infrastructures being built in many countries. These infrastructures are nowadays mostly used for data traffic by private-sector companies referred to as internet service providers. They manage the data streams within their own networks and pass on the packets to other networks (routing). The way in which two or more private networks are interconnected is intransparent and subject to freedom of contract. Any state can establish rules for the usage of networks on its own territory if so desired. However, the authority of the state is limited when data packets are passed on to a network outside its territory, which means that a connection with the global network is established.

Even if a state were able to monitor the dynamics of the huge data streams and control the access points to its "regional part" of the internet, for instance by nationalising the networks, there is currently still no way of effectively protecting all network participants against malicious software. The "Chinese part" of the internet is a case in point. It is assumed that Chinese authorities are able to monitor most of their regional infrastructure, for instance the points of entry and exit ("The Great Firewall"). At the same time, China is the country with the largest number of virus-infected computers in the world. Up to 70 percent of all systems in China are operated with pirated software that does not receive security updates and is therefore an easy target for any attacker.

There is a third characteristic of cyber space that makes it difficult for states to use their monopoly of power. In contrast to conventional weapons, the attribution of digital attacks to a specific party is quite difficult. Unlike in the physical world, there is no clear forensic evidence, such as a particular kind of ammunition or satellite imagery documenting a missile launch. It is therefore remarkably simple for an attacker to cover his tracks following an attack or to lay a false trail for the authorities regarding his identity (false flag).

The worldwide arms race is well under way

What, then, can a state do to assert control in cyber space and to effectively counter threats? To start with, it can take better precautions. It is important to differentiate between defensive and offensive cyber capabilities in this context. Achieving better security in the network infrastructure generally requires investments in defensive measures. It is known, however, that many states are also developing offensive capabilities (cyber weapons). Former US President Barack Obama already indicated the beginning of a digital arms race in 2009. During a White House press conference, he declared that the cyber threat is one of the most serious economic and national security challenges of the 21st century. Since then, the United States alone has invested approximately $60 billion in their defensive and offensive cyber capabilities.

Numerous governments have also adopted this stance and are themselves heavily investing in armaments projects for the cyber domain. Last year, for instance, the UK announced its intention to spend €2 billion on cyber security programmes; France, the United Arab Emirates and Australia are each planning to spend about one billion. The German government also announced the establishment of several new institutions last year. The plans include the creation of an armed services branch for cyberspace with roughly 13,500 personnel (of which only 300 will be newly recruited however). Civilian agencies, particularly within the remit of the Federal Ministry of the Interior, will also be equipped with numerous additional personnel and capabilities.

Many governments have stated they would only invest in defensive measures. However, it is safe to say that the 20 highly specialised daily attacks on German government networks mentioned earlier are not the work of private hackers operating alone. A specialised attack requires considerable resources and a team with extensive expertise. In its report, the Federal Office for Information Security therefore estimates that about five of the daily attacks are initiated by intelligence agencies operating on behalf of other states.

Cyber weapons are the new standard

The current frantic arms race in cyber space has repeatedly been compared to the situation at the beginning of the nuclear arms race. Michael Hayden, the former director of the CIA and the NSA, even compared the deployment of the Stuxnet computer virus with the dropping of the nuclear bomb on Hiroshima in August 1945. The CIA and the NSA had used the virus to cripple the Iranian nuclear programme. Mr Hayden said the following applied in both cases: “When the Americans use a new weapon, the rest of the world knows that this is the new standard. Others feel justified in developing and employing cyber weapons. There is a lack of any rules of engagement or international norms and standards.”

The international law of armed conflict was established at a time when weapons were only considered in terms of their potential for physical destruction. Cyber attacks, however, do not necessarily result in physical destruction. How far can we go before something is categorised as an attack? A former member of the US Cyber Command summarised the approach that currently prevails: “Right now, the norm in cyber space is, ‘Do whatever you can get away with.’” This problem is exemplified in the following incident. In 2007, several Estonian government websites could not be accessed for several days after an attack by Russian hacker groups. The Estonian government saw itself under attack and asked its NATO allies for assistance. Yet, the question whether this already constituted an attack in the traditional sense remains a contentious issue internationally.

Cyber arms control: a difficult start

Any arms race, and this also applies to cyber space, is a zero-sum game in the long run. Mutual trust should be promoted to avoid such developments. History has shown that, before any common rules, an agreement, or even an arms control treaty can be established, it is usually necessary to agree on fundamental definitions – for instance as to what constitutes an attack in cyber space. This process has proven to be particularly difficult at the political level, however, because different states have different threat perceptions. A range of different groups, for example within the United Nations and the OSCE, are currently working on definitions for the activities of government and non-government players in cyber space. If political consensus cannot be reached with respect to a definition, the IT experts could at least establish technical definitions and standards.

The problems of definition are apparent, for example, in the NATO document known as the Tallinn Manual, which was presented in 2013. It defines cyber attacks as "cyber activities that proximately result in death, injury, or significant destruction". However, various experts consider this definition to be too narrow because a number of key characteristics of cyber attacks are not sufficiently taken into account. These experts have also pointed out that many attacks are carried out with an intentional time delay or by manipulating subsystems, so that the attacker cannot be positively identified or located in most cases.

Even if a definition were agreed upon and the attacker could be identified, it would still remain unclear how the attacker should be dealt with. Is the attacker a combatant as specified in the international law of armed conflict, or a civilian who must be prosecuted under criminal law? It is assumed that government agencies in some cases try to appear as normal criminals so as to exploit this uncertain situation and to cover their tracks. These and many other open questions show that we are only at the very beginning of a long process with regard to establishing a cyber arms control regime. There are already a number of initial concrete solutions for intensified cooperation aimed at controlling the trade in cyber weapons. The Wassenaar Arrangement is one example: it was drawn up in 1995 to establish export controls for conventional arms and dual-use goods, and was expanded in 2013 to include software that can be used to penetrate IT systems (intrusion software). The key to making further negotiations possible, however, are internationally agreed definitions.

The EU as a role model and experimental laboratory

One thing should be clear: the objective is not to ensure that cyber weapons are never used again. Other arms control regimes have also faced repeated challenges; the recent missile tests in Iran and North Korea are evidence of this. The establishment of common rules or an international agreement to regulate cyber space, as well as any advanced cooperation to counter the proliferation of malicious software, will probably require a lengthy diplomatic, political and technical effort. There is no simple solution to the problem of implementing arms control in cyber space. In order to develop initial definitions and standards, the main goal currently is to develop processes and a framework for consultations that everyone can agree on. The following measures will be important in this context:

First, decision-makers must be made aware of the special technical aspects of cyber space outlined above. A basic understanding of these aspects is essential in order to define common security interests in cyber space and thus to make a first step towards arms control. Many governments, for instance, must first understand that they are vulnerable to cyber attacks due to the extensive interconnection that already exists, especially with respect to their critical infrastructures, and that they should therefore have a strong interest to cooperate at the international level. A closely related issue is the urgent need to spread the debate about cyber security beyond the IT community so as to also include the general public.

Second, due to the transnational nature of cyber space, a debate about cyber security and arms control can therefore only take place at the international level. These topics should be included on the agendas of as many international organisations as possible. Besides the OSCE and the United Nations, the G20 could also be a suitable setting for consultations. For instance, these organisations could also be used to define political interests in cyber space and to make a diplomatic effort so as to eventually develop a common understanding of threats in cyber space.

Third, regional groups of states could develop tangible definitions and protective mechanisms that could serve as an example for the rest of the world to follow. Germany and the European Union could play an important role in this respect. The EU sees itself as an exporter of norms and standards in many areas, including data protection. For example, the European Union hopes that its comprehensive approach to protecting personal data, which is enshrined in the General Data Protection Regulation, will also be adopted by other nations around the world. This strategy could also be successful in the area of security policy. The EU has already taken the initiative in the field of cyber security: the Directive on Security of Network and Information Systems (NIS Directive) adopted in 2016 established minimum standards for network security across Europe and a requirement to report hacker attacks. This mandatory reporting requirement applies to a wide range of different companies, including search engine providers. Furthermore, a strategic European cooperation group is being set up in order to exchange information between member states and provide mutual support for the establishment of national cyber security capabilities. The reporting requirement for cyber incidents, such as attacks against critical infrastructure or sensitive data, is seen as a particularly important first step towards better coordination and knowledge transfer among the member states and has received worldwide attention. In the long run, this cooperation within the EU could serve as a model and experimental laboratory for international cooperation and confidence-building measures aimed at achieving better security in cyber space.

Björn Boening is project director at the Stiftung Neue Verantwortung and focuses on digital infrastructure.
Paul-Jasper Dittrich is research fellow at the Jacques Delors Institut – Berlin in the research area "Digital Europe".