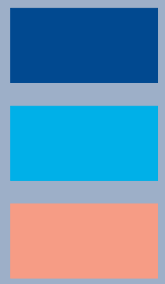
KAS-Schriftenreihe China
德国阿登纳基金会系列丛书



中德在世界政治中的角色
——相互挑战还是立场一致

China and Germany as Actors in World Politics - Mutual Challenges, Common Positions?

达斯汀·德黑兹
Dustin Dehéz

安杰·诺措尔德
Antje Nötzold

克里斯多夫·格雷梅斯
Christoph Grams

弗兰克·藻厄尔
Frank Sauer

斯托米–阿妮卡·米尔德
Stormy-Annika Mildner

Konrad Adenauer Stiftung
德国阿登纳基金会

No. 98 (ch/en)
Beijing 2010

Editor:
Project Office of the Konrad Adenauer Foundation in the PRC
Office C 813, Beijing Lufthansa Center
No. 50 Liangmaqiao Road, Chaoyang District, Beijing 100125

Tel: 0086-10 6462 2207 / 08
Fax: 0086-10 6462 2209
E-mail: beijing@kas.de
Webpage: www.kas.de www.kas.de/china

Responsible:
Wolfgang Meyer

发 行 : 德国阿登纳基金会中国项目执行人
地 址 : 北京市朝阳区亮马桥路50号燕莎中心写字楼C813室
邮 编 : 100125
电 话 : 0086-10 6462 2207 / 08
传 真 : 0086-10 6462 2209
E-mail: beijing@kas.de
主 页 : www.kas.de www.kas.de/china
主 编 : 梅砚

KAS-Schriftenreihe China
德国阿登纳基金会系列丛书

中德在世界政治中的角色
——相互挑战还是立场一致

China and Germany as Actors in World Politics - Mutual Challenges, Common Positions?

达斯汀·德黑兹
Dustin Dehéz

安杰·诺措尔德
Antje Nötzold

克里斯多夫·格雷梅斯
Christoph Grams

弗兰克·藻厄尔
Frank Sauer

斯托米–阿妮卡·米尔德
Stormy-Annika Mildner

No. 98 (ch/en)
Beijing 2010

目录

本书所收录的文章是在2009年7月22日由德国阿登纳基金会与中国国际战略学会共同于北京举行的题为“中德关系现状与前景”国际研讨会上的部分发言

Contents

The articles in this publication are based on speeches presented at the international Conference on "China and Germany as Actors in World Politics - Mutual Challenges, Common Positions?" held on July 22, 2009, in Beijing, organized by Konrad Adenauer Foundaiton together with China Institute for International Strategic Studies

Give Cyber-Peace a Chance! German and Chinese responses to a new security policy challenge*

Frank Sauer

Introduction

"Bytes, not bullets, are the new ammo!" the enthusiastic prophecies of think-tanks and defense ministries have read along these lines since the 1990s. And it is true - the technologies of the information age not only allow for the transformation of standard, routine elements of warfare; what to date had been nothing more than Science Fiction now appears to be within reach - a new theater of war is emerging: cyberspace.

In actual fact, "cyberspace" is a relatively recent phenomenon - but one that has already revolutionized our daily lives with the Internet. This article will critically evaluate the extent to which it is also relevant in terms of security policy. The key issue is whether the virtual world really poses a serious threat, or whether what we are dealing with here is instead "cyber hype", that is, the overestimation of cyberspace as the source of potential security risks.

Before we can illuminate this issue, the first step must be to reconstruct how cyber war, cyber terrorism and similar terms made it onto the security policy agenda. The second step will then be to investigate what precisely it is we are dealing with when talking about "cyber" phenomena. Lastly, several thought-provoking impulses and suggestions for German and Chinese foreign and security policy will be put forward. How could, or should China and Germany respond to the issue of cyberspace with respect to security policy in practice?

Cyber War and Cyber Terrorism

The concept of cyber war, which originated in the USA, has been the subject of debate in academic circles and among representatives of the military and security policy since the early 1990s. Now, however, cyberspace is attributed importance with respect to security policy not only in the USA, but also in China and Russia, as well as, to a slightly lesser degree, in Germany.

* This essay is based on a speech presented by the author on July 22, 2009 in Peking at a conference jointly staged by the China Institute for International Strategic Studies (CIISS) and the Konrad Adenauer Stiftung (KAS) called "China and Germany as Actors in World Politics: Mutual Challenges, Common Positions".

In 2001, the US government believed that 30 states have aggressive cyber war programs in place. George W. Bush's administration officially declared "cyber warfare" to be a growing threat for the USA, and even went as far as comparing "hack attacks" with the risk posed by Soviet nuclear weapons during the Cold War. President Barack Obama also considers American security in cyberspace to be under threat and has appointed a "cyber czar" in his administration to coordinate approaches regarding this issue. As far as cyber war is concerned, the American military forces take a proactive approach. For some time now, the US Air Force alone has deployed more than 40,000 soldiers in "cyber operations", to secure the supremacy of the American forces not only in the air and in space, but also in cyberspace. A dedicated Cyber Command has even been appointed. In the USA, China is seen as the greatest competition for supremacy in cyberspace. China has also expanded its forces with the necessary staff and a doctrine on cyber warfare. Russia even reserves the right - possibly due to the lack of any alternative - to use nuclear force to retaliate against a cyberspace attack. In Germany, the subject of cyber war is afforded slightly less attention in military discourse. However, the Federal Ministry of Defense, the secret service and even members of parliament have a steadily growing awareness of the subject, which is reflected, for instance, in inter-ministerial and inter-party task forces, simulations and a dedicated Computer Emergency Response Team for the German Federal Armed Forces. While the "White Paper 2006" only mentioned cyberspace in passing, the Federal Armed Forces have already set up an undercover cyber war unit under the command of the air force.

Cyber war garnered worldwide media interest among the general public for the first time in April 2007, when Estonia was facing a "Denial of Service attack" and newspapers reported the "first cyber war in history". This particularly intensively networked country faced an attack that varied in intensity on the websites of political parties, companies, banks, newspapers and the Estonian government that went on for several weeks. Estonian web servers were bombarded with excessive requests - such as requests to access a website - for such a prolonged period that, in view of the flood of data, they were forced also to refuse legitimate requests and to temporarily shut down their services (hence the term Denial of Service). The Estonian Hanseatic Bank, the largest national bank, calculated losses due to the suspension of online banking services at US$ 1 million.

Prior to the attack, the Estonian government had removed a Russian war memorial from the capital leading to diplomatic recriminations with Russia. As a result, Estonia was quick to accuse the Kremlin of waging "cyber warfare". But was this really a new form of inter-state warfare; a Russian attack against Estonia?

To this day it has not been conclusively ascertained whether the attack did in fact originate from the Russian government and military or whether it was carried out by private individuals. The consequences of the alleged cyber "war" on Estonia can by no means be compared with the effects of real war. While public life was made more difficult, no infrastructure was destroyed, nor were there any people hurt or killed. To put it bluntly: a couple of out of order ATMs do not a war make! There are also several

indications that this is just another - particularly serious - case of cyberspace activism or "hacktivism". Accordingly, it is unlikely that the attacks originated from the Kremlin and the Russian military; it is more likely that they were carried out by nationalistic Russians offended by the removal of the monument, who, spurred on by and coordinated through discussions in Internet forums, took it upon themselves to initiate the data flood against Estonia. Thus, the incident in Estonia was not the "first cyber war in history". Estonian Prime Minister Ansip compared the events on the Internet with an attempt in the real world to "block a port or an airport". This is a fitting comparison and without doubt this kind of blockade represents a serious situation for any nation; however it appears somewhat excessive to use the word "war" in this context.

What about the terrorist threat from cyberspace? For years now, many so-called "experts" have claimed that cyber terrorist attacks could easily be carried out by a large number of potential perpetrators, and with serious consequences. The issue here, then, is why, to date, there has not been a single terrorist cyber attack.

The first part of the answer to this question results from the fact that, thus far, terrorists have used the Internet not to carry out attacks, but rather for propaganda, PR or at most preparing attacks. The example of al-Qaeda and its many supporters around the world shows that on account of its wide audience and speed, the Internet plays a central role as an instrument for communication, but above all as a means of disseminating propaganda and recruiting new followers. The Internet allows text and audio messages, as well as expensive video recordings of attacks to be made easily available for kindred spirits across the globe. A drastic example of how terrorists use the Internet to wage psychological warfare is the videos depicting be-heading and similar atrocities. In addition, while they may not be entirely confidential, encrypted e-mails and Voice-over-IP calls can be used for talks and steganography can be used to secretly exchange sensitive information extremely quickly and directly. Together with mobile and satellite telephones, this facilitates the global coordination of activities in real time. Possible targets can even be researched from the comfort of home using Google Earth. Only as an aid for conventional attacks does cyberspace play an important role for terrorists today.

What about the fears of catastrophic, Internet-based attacks on "critical infrastructure"? Critical infrastructure includes, first and foremost, signals systems for road, rail and air traffic, control systems in gas, water and electricity supply as well as banking and telecommunications networks. Are these lifelines of modern industrialized societies actually under serious threat? Could terrorists use the Internet to cause black-outs, to flood dams or to detonate nuclear energy plants? Evaluating this question using a more differentiated approach, rather than merely joining the bandwagon of horror scenarios in circulation, is considerably more informative and provides the second part of the answer to the question of why there have not been any terrorist cyber attacks to date.

While it is correct on the one hand that certain critical computer networks are insular solutions,

distinct from other data networks, it is also true that this separation - as negative examples from the electricity supply network have recently illustrated - is not always observed strictly enough and that critical infrastructure that can be accessed from outside also has security deficits that could potentially be exploited. On the other hand, the operation and the targeted abuse of such specialized systems is not a trivial undertaking, but demands a certain minimum level of expert knowledge. Thus, despite the undeniable vulnerabilities of critical infrastructure in industrialized societies, it can by all means be assumed that, in fact, only a very small number of terrorists would be capable of carrying out a cyber attack on critical infrastructure that comes even close to "effective terrorism". Consequently, cyber terrorism is not a possibility "for a large number of potential perpetrators at any time, and with great ease". On the contrary: it can be assumed that only very few terrorists have the skills necessary to carry out such attacks. Attacks, incidentally, cannot be carried out easily but only with intensive preparation and with the corresponding financial and technical resources. What, then, of the "serious consequences"?

The Estonia example demonstrates that even a widespread cyber attack causes little "drama". Compared to attacks with explosives or even "dirty bombs", the effects of cyber attacks have, to date, been far less severe. To put it bluntly: while out of order ATMs are certainly an annoyance, no one feels terrorized through this inconvenience. Even more serious consequences, such as widespread power cuts, would have to last several days before these caused dramatic consequences. Thus, on closer examination, it is not surprising that there have not, to date, been any notable acts of cyber terrorism. From the point of view of the terrorists, there are other, far simpler methods of achieving serious consequences - the massacre in Bombay in 2008 demonstrated the degree of terror that ten determined attackers can spread using the comparably simple means of automatic rifles and hand grenades.

Cyber Hype?

Thus, although a critical evaluation of the threat posed by cyber war and cyber terrorism suggests that it is not a cause for serious alarm, cyberspace is nevertheless more present than ever in the headlines, as some examples from 2009 show. February: the Conficker worm in circulation since October 2008 infected hundreds of computers of the German Federal Armed Forces. March: Ghostnet, comprising more than one thousand computers worldwide containing very high value information is discovered - computers in foreign ministries, embassies and international organizations were specifically infected and spied on by means of Social Engineering. April: the Wall Street Journal reports that several terabytes of potentially security-relevant information about the Joint Strike Fighter, the US military's new fighter plane, were stolen. May: the Annual Report of the Office for the Protection of the Constitution 2008 states in regard to attacks on computer networks: "Broad-based attacks against authorities and business enterprises have also been registered in Germany since 2005. Spying activities are mainly ordered by the intelligence services of the People's Republic of China and of the Russian Federation."

There are two particularly striking things about all of these computer network attacks: first, the same or similar instruments are used in each case. Second, the instigators of computer network attacks are never identified. In fact, whether an effect can be attributed to a cause and the similarity of the means used are the main problems when analyzing attacks on computer networks. It is also striking that the attacks are obviously motivated by different goals: in some cases, specific information is accessed, while in others the target systems are scanned or shut down at random. So what exactly is it we dealing with here? Espionage? Economic crime? "Cyber vandalism"?

As a rule, both the media reports and the terms, concepts and opinions put forward in security policy literature vary hugely. Table 1, below, is intended as a guide to help navigate the jungle of terms used to describe players, motives and instruments involved and to facilitate a clearer assessment.

The table categorizes some of the most important "cyber phenomena" according to the crucial players, their scope, the instruments employed or their approach, as well as their objectives. This overview can be used to clearly distinguish between operations implemented by state military in the real world employing physical force ("Information Based Warfare:) and the cyber warfare referred to above, i.e. 'warfare' restricted exclusively to the virtual sphere by the state military. The objectives in both instances are the same; the means, however - physical weapons on the one hand, and virtual attacks on computer networks on the other - could not be more different.

In the next step it becomes immediately apparent that all players that operate in the virtual world - irrespective of whether these are state players or not - resort to more or less the same instruments and methods - summarized here under the term "computer network attacks". Equally it also quickly becomes apparent that the various players differ significantly in their objectives: while the goal of the state military when employing Information Based Warfare and cyber war is or should always to overcome enemy troops, the terrorists' goal is to instill fear and uncertainty among the civilian population. By analogy, espionage by state secret services primarily aims to obtain security-relevant information, while criminal non-state actors - primarily in economic espionage - hope mainly to make financial gains.

These distinctions - for instance between cyber war and cyber terrorism - are more than just an academic exercise; they are of paramount importance for security policy in practice. After all, let us be frank, defense following an attack should be targeted at the correct enemy. If, for instance, cyber attacks are indeed to be included in Article 5 of the NATO agreement in future, then surely it is not in anyone's interests for the military alliance to declare war on state A simply because a company or a private group of hackers in state A showed too great an interest in information on the armaments industry in NATO state B?

It can be seen that war, espionage and criminality do not all mean the same in cyberspace as they do in the real world. Often, however, attacks are countered as if this were the case, since the customary and accepted distinctions

Table 1: Comparison of information-based warfare and the main "Cyber Phenomena"

	Information Based War-fare	Cyber War	Cyber Terrorism	Cyber Espionage / Sabotage	Cyber Crime	Hacktivism
Agent	State (Military)		Non-State (Terrorists)	State (Military / Intelligence Services	Non-State (Criminals / Business Crime)	Non-State (Activists)
Space	Physical (Real) World	Virtual World				
Means	Physical Means of Violence (Weapons!)	Virtual Means of "Violence"(?) Computer Network Attacks ≈ "Virtual Weapons(?)"				
Mode	Disrupt / Destroy C^3Systems & Information Infrastructure	PsyOps and InfoOps as e.g. in: Distributed Denial-of-Service via Botnet Information Theft, Destruction or System Manipulation via Trojan or Rootkit				
Goals	Disrupt / Disinform / Deceive / Propagate			Extract Crucial / Security-Relevant / Valuable Information		Accentuate / Distort Information
	Gain Advantage Over Enemy Military Forces		Recruit/ Organize / Coordinate ⇨Terrorize Population	Gain Intelligence Advantage	Make Money Gain Business Advantage	Create Publicity

in the real world, such as state as opposed to non-state; attack as opposed to defense; military as opposed to civilian or even the criteria defining what constitutes a "weapon" are considerably more difficult in cyberspace. Next, the consequences and the suggested political response will be illuminated.

Conclusion

First, it cannot be denied that modern society's reliance on critical infrastructure brings with it a number of vulnerabilities. Electricity supply, traffic control systems and telecommunications networks are the lifelines of modern society. The mutual dependency of these critical infrastructures can furthermore mean that the failure of one of these systems can have a domino effect of more widespread consequence. Second, however, we aren't quite at that stage yet! This means that while cyber war and cyber terror are already relevant to security policy, at present they are more cyber hype than a concrete and immediate threat.

As far as terrorism is concerned, cyberspace will continue to act merely as an aid for terrorists planning and implementing conventional attacks. In addition, limited cyber attacks on critical infrastructure at most appear plausible, to intensify the effects of "conventional" attacks, for instance in that disruptions to communication networks hamper the work of emergency services. However, cyber terrorism does not pose a serious threat to the functioning or indeed the existence of even an industrialized nation that is particularly reliant on critical infrastructure. There is unlikely to be a "Cyber-9/11" in the foreseeable future. A worrying development in the area of terrorism is rather that cyber terrorism is already being misused today as a battle cry to restrict freedom of speech. Thus, state bodies censor content and prevent access to unpopular Internet activities under the guise of "tackling terrorism".

As regards cyber war, a war fought between states exclusively in cyberspace, with effects comparable to those of physical violence, this is liable to remain a military pipe dream for some time yet. The example of Estonia illustrates that, while the consequences of a data flood lasting a total of two weeks (with breaks) can be irritating and disruptive, the overall extent of the damage remains manageable.

Nevertheless, looking to the near future, we are beginning to see a worrying trend, which will now be examined in more detail. This is the risk of unregulated armament and "hostilities" in cyberspace.

What is striking in this context is that the ethical aspects of attacks on computer networks have not played a role in any key document, such as the American Joint Doctrine for Information Operations, nor in the literature on security policy. While categories of the laws on armed conflict are mentioned in official documents, it must be borne in mind that attacks on computer networks currently take place de facto in a lawless sphere, since it is considerably more difficult in cyberspace to distinguish between military and non-military targets or to attribute an effect to a cause, as the Estonia example clearly illustrates, than it is on the physical battleground.

When NATO brought Serbian substations to a standstill during the Kosovo conflict using graphite bombs, it was, justifiably, subject to a great deal of public criticism, since the results of these attacks affected primarily the civilian population. The anonymity of military cyber operations, which furthermore can be carried out without the risk of casualties to one's own side, means that states could in future be tempted to carry out such attacks. Furthermore, since in cyberspace there is no distinction between civilian and military infrastructure, there is always a particular risk in cyber war that civilian systems will also be affected or, in the future, very deliberately made the target of military maneuvers. But why should different rules apply in a virtual war than when real bombs are dropped?

From the military perspective, in cyberspace "anything goes" and current efforts are aimed at developing additional offensive capacity, since defense is considered a practical impossibility in cyberspace. In justification of these armament efforts, there is already talk of cyber "deterrence" - in blatant disregard of the fact that a deterrent threat (as in the field of nuclear weapons) can be effective only if it is aimed at the correct target. However, unequivocally determining identity in cyberspace is precisely the crucial problem, rendering the deterrent logic completely misplaced.

Instead of succumbing to a misguided logic of mutually assured destruction and forcing any kind of armaments movement in cyberspace, political efforts ought instead to concentrate on ensuring the peaceful use of cyberspace. After all, even on the "battlefield of cyberspace" the proportionality of the means and the identification of combatants and non-combatants should be observed. How should German and Chinese policies respond to this challenge?

As long as it is not too late and the negative results of the 'cyberspace arms race' can be checked, the foreign and security policy response to current developments in cyberspace must be: Give Cyber Peace a chance!

With regard to the security policy challenges posed by cyberspace, the international community is facing a unique situation, given that it has the opportunity to take action in terms of armament policy now and to find rules for peaceful cooperation before it is too late and the first "cyber war" in history does actually break out. Germany and China are likely to have a great interest in this process, since the German Annual Report of the Office for the Protection of the Constitution 2008 mentioned above is correct: many questionable activities in cyberspace do indeed originate from China. The allegations against China raised by the US company Google and by the US Foreign Secretary Hillary Clinton at the beginning of 2010, made it the focus of worldwide attention. However, since, according to the Chinese government, activities such as the creation of the aforementioned Ghostnet are erroneously attributed to China, there is likely to be even greater interest on the Chinese side in preventing such activities by means of concerted action and clarification of the situation. In turn, Germany's interests lie in protecting itself against attacks from cyberspace. In consultation with its European partners, Germany's foreign

and security policy could also promote policies aimed at tackling this issue by means of multilateral agreement and conflict resolution. As such, Germany and China could both take convincing leading roles in the field of cyber security.

Therefore, I would like to conclude by presenting three specific recommendations as to how Germany and China could join in dialogue with the international community and, through political action, together respond to the new challenges posed by cyberspace.

First: China and Germany should issue a clear foreign policy statement to the effect that neither will be first to use cyber war capacities in the event of a conflict. A self-denying ordinance of this kind, which can be implemented at short notice, or a no-first-use doctrine, could, as in the context of nuclear weapons, help to establish a culture of restraint and in the longer term stigmatize cyber attacks as taboo.

Second: in the medium-term, China and Germany should work towards the conclusion of an international agreement. Comparable with the "Treaty on the Peaceful Uses of Outer Space", a Cyberspace agreement, a "Treaty on the Peaceful Uses of Cyberspace" is conceivable, which would govern the peaceful use of cyberspace for the good of all mankind. In combination with a United Nations committee, this treaty could also provide a multilateral forum for international security debate with respect to cyberspace in the future.

Third: in order, lastly, to tackle in the long-term the problem posed by the confusion between the civilian and military spheres in cyberspace using a multilateral approach, German and Chinese foreign policy should push for the development of international humanitarian law so that stable definitions and agreements are reached, which will regulate the use of computer network attacks as weapons in inter-state conflicts. The insistence on the distinct identification of "civilian" and "military", or, as the case may be, the ability to trace acts of "violence" in cyberspace too should be the goal of this long-term process, which without doubt involves some extremely challenging technical and data protection law issues.

All projects linked with security policy in cyberspace bear an onerous responsibility. Regulative actions to protect public security may not at any time involve a disproportionate restriction of civil rights. The greatest blessings of the Internet Age - newly won freedoms created through the boundless openness of cyberspace - must continue to be protected, even in the face of new risks.

We will, however, have and will be able to live with the residual vulnerability that cannot be avoided in an open, democratic society even in the Cyber Age.