Bericht des Bundesrats an die Bundesversammlung über die Sicherheitspolitik der Schweiz, 2015

Hearings

Transcription by: Dienst für das Amtliche Bulletin, Parlamentsdienste, 3003 Bern

Statement by Lars Nicander

Director of the Center for Asymmetric Threat Studies
at the Swedish National Defence College

"Cyber risks"

Bern, 28 August 2013

For his presentation we asked to address particularly the following questions:

1. ***How significant and imminent are cyber-risks or threats, and to what extent are they a (national) security problem? What could be the worst, and what the most likely scenario?***
2. ***Which objects or targets are most threatened by cyber-attacks? Is it more about disrupting infrastructure or about illegal access to information?***
3. ***What are in your view the measures that could enhance cyber-security most – should they be based primarily on technical or on political arrangements?***
4. ***What role could/should the state and its instruments play in preventing and combating cyber-risks and threats?***
5. ***What does that mean in particular for the armed forces; what kind of tasks should be assigned to them?***

I have been collaborating with Switzerland on defence issues such as information warfare since 1999. I was also invited as an external observer to an 'Armee XXI' exercise. As a result, I am not only familiar with Switzerland's problems and particularities but also very much aware of the similarities between the defence measures taken by Sweden and those taken by Switzerland.

As a political scientist, I have been working for the Swedish national security system for twenty-five years. Currently I am head of the independent Government think tank CATS that is being funded by the Swedish Cabinet Office, the Department of Defence and the Armed Forces. Until 9/11, CATS focused on state actors, for instance on cyber-threats in information operations. With 9/11, we had to widen our scope and to include non-state actors. To the information operations and cyber-security studies we traditionally had been focusing on, we added terrorist and intelligence studies. By now the pendulum is swinging back to state actors again.

There have been other paradigm shifts as well, namely the shift from the need to know to the need to share and the shift from the need to share information to the need to share analysts. The latter is a result of the huge amount of information analysts nowadays have to deal with.

Whereas in the Cold War era you were supposed not to talk to anyone, today you need to share both information and knowledge about counter terrorist missions.

1. How significant and imminent are cyber-risks or threats, and to what extent are they a (state) security problem?

Both Sweden and Switzerland have a 'total defence' heritage. This means that there are many redundancies in our power grid and telecommunication systems. These investments have made us less vulnerable in comparison to countries such as the US, who in the 1990ies suffered a shock as a result of their open lines. Having a 'total defence' system also meant horizontal cooperation between different branches of government. In this sense, 'total defence' is a good mind-set because it not only includes military issues, but advocates a whole-of-government approach.

In the late 1990ies, a Swedish Parliamentary Committee dealing with cyber-threats raised central questions such as what role does Government have in this and how do Government and private companies relate? It came to the conclusion that the role of Government was to make Sweden a secure market place for companies and to do so by assuring business that there are enough redundancies in the system so that there is no reason to worry all the time. The approach adapted by the Swedish Cabinet is imperative to promote business: not interfering with operational business decisions, but ensuring a solid infrastructure and fair playing rules.

In the aftermath of what happened in Estonia in 2007, another dimension of cyber-threats became visible and emphasized the need for an enhancement of the security policy toolbox. A state actor with big resources can act through cyber-attacks but conceal its involvement and remain anonymous – and what can you do against an adversary if you do not know what *he* is doing?

Cyber-attacks can be used in several ways: either as an add-on to economic sanctions or other non-military means of power projection, or as a force multiplier by taking out emergency systems after bomb attacks. In order to improve your preparedness you need real operational and technical experience, i.e. red team as opposed to just table top exercises. Such a penetration test takes some money and, above all, good and dedicated people, but it does get you further as it helps you to build competencies and to detect critical vulnerabilities in your governmental networks. Only when there is a red team attack will hardware people, software people and network people seriously – and jointly – discuss the consequences that changes brought about in one dimension will have on the other two. In Sweden, an interdependency and vulnerability analysis in the area of telecommunication brought astonishing results and showed that there were many real gaps. All findings were immediately declared top secret.

A keyword in this field is cooperation. You need cooperation not only between agencies and between the private and the public sector, but also on an international level. Of course it is helpful to have a situation awareness centre such as GovCERT, the Computer Emergency Response Team of the Swiss Government, but it has to work twenty-four hours a day and seven days a week. It is crucial to have a single centre; if there are, as a result of constitutional constraints, many independent agencies, as is the case in Sweden – a military agency, a

police agency, a Cabinet agency and a post and telecommunication services agency – then every decision has to be taken by the Cabinet as opposed to by one Minister. Consequently, the centrifugal power is overriding and no one manages to get the full picture. In this sense, we can all learn something from Estonia because in 2007 it managed to deal with a situation that was likely to put a government under severe stress. They chose an official within the Ministry of Communication who was very able, but three or four levels down in the hierarchy, and put him in charge of the whole thing. This courageous step worked out well.

In my estimation, there is no real risk of cyber-war. No civilized and no rationally acting state government would opt for uncontrolled cyber-war, and so far there have been no casualties as a result of IT intrusion. However, there still is a need for cyber-deterrence and for cyber-deterrence policy. Let me remind you of an example which shows that deterrence can work: in WWII, both Germany and the Allied Powers had biological weapons; although no treaty had been concluded, neither side used them.

Regarding cyber-intrusion, the highest level state actors might get involved at has been reached in dealing with the computer worm Stuxnet. While terrorists aim at creating chaos, states try to prevent collateral damage. In dealing with Stuxnet – one measure being upholding sanctions – that goal was achieved.

A potential victim of cyber-threats – and probably not so thought of in this context – is probably China. It could easily be attacked because defending Chinese systems would be very expensive. With the Communist party still in control, there is no governmental system as we know it and no chain of command either, so that in bilateral meetings you hardly know whom to talk to.0

You asked what I regard as the worst and what I regard as the most likely scenario. The worst scenario would be an information breakdown of critical infrastructure as a result of the interdependence between the power and the telecom sector. Although you might have a back-up system for the telecom net, such a system is not likely to last very long, and you hardly have redundancy with regard to the power grid. The most likely scenario is digital espionage – in spite of the fact that a lot of resources are needed to process the information gained by espionage.

2. Which objects or targets are most threatened by cyber-attacks? Is it more about disrupting infrastructure or about illegal access to information?

In the mid-nineties, the US invented the term Critical Infrastructure Protection (CIP). In the era after the Cold War, sixteen different sectors of government claimed to need extra money for protection. Later on, the term was diluted and every US state demanded money from Government. Even Mount Rushmore was considered by some to be critical infrastructure needing protection. As a result of this dilution, another, more precise term was coined: Critical Information Infrastructure Protection. CIIP is aimed at five prioritized key areas. The first key area is continuity of government, enabling the cabinet to work in spite of hazards, problems and attacks. This area includes redundancy of media communications, allowing government to send out messages to the public by radio and by TV. The second and third key areas are the inseparable power and telecom systems. The fourth area is the financial system;

although it is in private hands, government still has strong instruments such as oversight agencies that can set up rules regarding redundancy systems. The fifth key area is air-traffic control. This small part of the transportation sector was defined critical information infrastructure in a Swedish investigation in 2002, not because it is the most dangerous one, but because an attack on it might have immediate effects. If someone messes with the air-traffic control, you might see the disastrous results within milliseconds, whereas if an attacker puts biological agents in a water reservoir, it might take the agent days, if not weeks, to reach its target. The time factor being crucial, these examples show how important it is to set priorities when it comes to allocating money.

You asked whether it is more about disrupting infrastructure or about illegal access to information. For government actors, the latter is prevalent. Politically motivated attacks do not get much beyond the dimensions of say the attack against state-owned Saudi Arabian oil company Aramco by Iranian hackers. Al-Qaida and other groups do not have the systems and the skills needed for that kind of attack. Often cyber-attacks carried out by very skilled non-state actors are propelled by commercial interests; take the example of the Chechens who managed to take Russian money from a London bank.

3. What are in your view the measures that could enhance cyber-security most – should they be based primarily on technical or on political arrangements?

In a top-down perspective, the major domestic tasks in taking cyber-security measures are management issues such as how to create inter-agency cooperation, how to 'bend pipes'. The major international tasks consist of keeping up with the need for defence cooperation and getting international laws applied, so that hacking attacks can be traced back. However, to make this work, all actors need to have a common denominator. The overriding importance of such a common denominator may be illustrated by how in the 1970ies the problem of aircraft hijacking was tackled. At first no one knew what to do, but once the International Civil Aviation Organization (ICAO), an operational body under the UN, set up the necessary rules for all international airports, the hijacking problem was solved within eighteen months. If an airport did not comply with the set standards, simply no international carrier would land. Could something similar be done in cyber-space? There have been discussions with organizations such as the International Telecommunication Union (ITU), but the talks were somewhat pressurized by political interests. At any rate, the approach has to be universal; states have to understand that everyone gains if hacking opportunities are diminished.

Sweden also discussed whether the measures in question might be useful for offensive purposes under international law auspices for upholding sanctions. Parliament supported the idea and referred to the anti-Milosevic campaign in Kosovo in 1999, where according to international law it was considered okay to bomb a bridge and military trucks causing collateral damage, but where it was not considered okay to cut a telephone wire because the wire went to the paramilitary civilian troops in Serbia – who in fact committed most of the atrocities. These international laws have been imperative since the Napoleonic wars and have not been updated for the information age. There have also been discussions with regard to sanctions against Rhodesia in the 1960ies as to whether Article 41 of the UN Charter might have been

used to interrupt the post and telecommunication system, because by doing so the Rhodesian military might have been isolated and the sanctions turned into a more effective instrument. Balancing the pros and cons of such an adaptation of the law might turn out to be a mind-bending exercise.

4. What role could/should the state and its instruments play in preventing and combating cyber-risks and threats?

If a state wants to protect the private sector, how can it find a balance without intervening and using tax money to pay for the operational costs of companies? Let me give you an example from my country. During the Cold War, the Swedish Government approached the power producers, who had a business optimum for 95 per cent, and told them that from a national 'total defence' policy point of view Government needed 98 per cent and was willing to pay for that. Since both parties were to make a gain out of such a deal, they bargained till there was a win-win-situation. Could something similar be done with regard to cyber-space? Cyber-companies do not have access to the threat information gathered by the intelligence service. Even if they did, they might as well say: I cannot protect myself because it costs too much. They might even argue that protecting them is part of the governmental role as insurer of last resort.

Let me illustrate the problem with another example. Certain companies in the Silicon Valley at one point in time started to wonder whether they were actually insured against the loss of hundreds of millions of dollars a worst case scenario was threatening to bring about. At the same time, big insurance companies started to ask themselves whether their contracts actually excluded such risks. They set up sub-companies focusing entirely on IT insurances. These sub-companies were confronted with the question of how to measure risks without having an adequate amount of data. The reason for the lack of data simply was that the kind of incident in question happens so rarely. As a result of all these questions being raised, companies seeking an insurance contract in the end had to set up big information assurance manuals and imply the necessary measures. After six months, an independent consultant firm was to act as a red team and to test the companies. This procedure was to be repeated every six months or as often as the insurer wished to do so.

In the course of this process, information security turned from a Chief Information Officer issue into a Chief Executive Officer issue, because the entire costs involved were brought to the surface. The process also inspired hopes Government might pay for extra costs. However, with the financial crisis, everything went down the drain. In Europe, where the insurance industry is very conservative, the idea was supplanted by more old-fashioned ones; insurance contracts were to mirror again the very old British idea that once a contract is signed, nothing in it must be changed. In the US, companies were more flexible.

In Sweden, we think that information assurance in the day-to-day business should be in the responsibility of the company, although it may be regulated by governmental evaluation and certification bodies. The Department of Defence and its agencies should pay only for what is above the day-to-day business level, i.e. for expanded protection ('the collective good'). Of course, such measures only work if the insurance industry itself works; only then can you be

sure that the tax-payers' money is spent on infrastructure and not used to cover business losses.

Another step a government can take is to ensure that there are information sharing agreements such as InfoSurance, the agreement Switzerland made around the beginning of the last decade. As for Sweden, it set up a threat detection warning system that has been working for many years. It sniffs outside important networks, with information going to the intelligence and secret agencies. Unlike commercial systems, this system is able to detect threats long ahead. Moreover, it is sort of an impartial body a particular branch of the industry would not be able to set up.

In the US, the financial system works very well thanks to independent consultant firms. However, companies are very hesitant about communicating information to governmental bodies because these bodies themselves are very hesitant about sharing aggregated information with them, for instance when being told about potential attacks. The governmental bodies' hesitancy can be attributed to the laws that govern information gathering, as these laws have been laid out for courtrooms and for law enforcement bodies.

Another crucial issue is the link between law enforcement agencies and national security instruments. Law enforcement agencies must be told if it comes to an attack on your country, even if at the beginning you do not know whether the attacker is a state actor or a criminal hacker. As soon as you know that it is a state actor, you must open up the case and enable national security agencies to act. Often there is a gap between law enforcement agencies and national security instruments. To fill this gap is one of the major challenges. There may be, between these two kinds of bodies, non-disclosure agreements about the reporting of hacking attacks, but the question is whether national security bodies can give information to law enforcement bodies without hurting themselves and whether they can give information to computer hacking response teams without the information being spread out.

What is needed in the case of a severe IT problem within the government system is agility with regard to the reallocation of governmental funds. You should have an authority able to reallocate the funds necessary to fix the problem as quickly as possible so that you do not have to wait for years. In the world of information, a year is virtually an eternity. Since spotting the problem without having the resources to fix it does not help much, the missing link between those being aware of a problem and those having the capability to fix it, is something states should think through thoroughly.

Of course, not everything can be fixed by applying a top-down approach, so a bottom-up approach has to be considered as well. Here, one of the most important questions is how to raise the information assurance bar. One way to do it is to subsidize courses such as the chief information officer course our college has developed. It is aimed at one single person in a company focusing on information security and being responsible for the whole spectrum, from the setting of information assurance standards to their actual implementation. Such a person must have the opportunity to develop a holistic view, to give advice to senior leaders and to help the CEO or the Director General to have a full picture of what is being done. The US Congress was ready to pay extra money for courses which enable chief information officers to deal with government systems and with government agencies.

5. What does your answer to question 4 mean for the armed forces; what kind of tasks should be assigned to them?

The Swedish Cabinet assigned to our think tank the task of writing a report about Swedish cyber-defence policy, focusing among other things on the definition of widely discussed terms such as 'cyber-defence', 'cyber-security' and 'information assurance'. So far, the eight governmental agencies involved in such a policy all have had different views and different priorities because they belong to different Departments. Moreover, no single person is being in charge of it all. Initially, 'information assurance' was an American term; nowadays it is also used by international security experts and in Orange Books. Basically it means protecting hardware and software and shielding networks from interference. The keywords are rules, procedures, education and organization, the focus being 'vertical' dimension domestically and on cooperation between agencies.

The term 'cyber-security' has much been used in spite of lacking a definition. Being apllied more the 'horizontal' dimension, it mainly regards networks and focuses on the governmental level, which is due to international law aspects, to different Ministries being involved, for instance the Ministry of Foreign Affairs in cases of sanctions, and to discussions taking place between the EU and the US.

In the 1990ies, there were two schools of thought regarding cyber-defence policy. One school, including the British and the French, regarded cyber-defence as intelligence matter; they preferred not to talk about it at all. The other school, including Germany and the US, regarded it as a military matter to be treated as other operational military issues. Sweden joined the latter after deciding in 2002 that it should acquire knowledge about computer network operations in order to be able to defend such systems.

With regard to computer network operations, you have to distinguish between defending, exploiting and attacking networks. Exploiting networks is the most important role, the keyword in this area being signals intelligence. By ensuring seamlessness between the three activities or roles, you have to make sure that tax payers do not pay twice for one and the same thing. You also have to ask yourself whether the job should be done by the military, by civilians or by both. All three models have their adherents: the United Kingdom opted for civilians because in the UK signals intelligence is in the responsibility of the Ministry of Foreign Affairs; the Netherlands opted for the military because there the military and the Ministry of Defence work together when it comes to signals intelligence; the US opted for both military and civilians.

I would also like to say a few words about international cyber security developments. Stuxnet completely changed the US policy and had it switch from a 'criminal acts' to a 'no first use' approach. The new cyber-deterrence strategy was put forward by General Alexander and former national security planner David Elliot. Today, US politicians are still struggling over how the relation between the internal networks of the Department of Homeland Security and the military networks of the National Security Agency should look like. While Hillary Clinton pursued a top-down approach with cyber-norms, Cyber-Security Coordinator Howard Schmidt favoured a bottom-up approach. The latter was to comprise technical exercises, edu-

cation and bench-marking with the different hubs to make out the best practices with regard to raising the information assurance level.

There is also a dialogue between the US and the EU about cyber-issues, including the affair about Edward Snowden. The organizations involved carry out exercises such as Cyber Storm as well as multi-national experiments focusing very much on NATO. A few years ago, Secretary General Anders Fogh Rasmussen took a very defensive stand and announced that NATO was prepared to assume a big role in this. While NATO has the necessary structure, the EU has a mandate and has resources, so for a while NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn and the EU Agency for Network and Information Security ENISA competed over this. Since by now ENISA has adopted the NATO Centre's standards for protocols, it seems that the EU has given in, leaving the leading role to NATO and focusing its own activities more on cyber-crime. Sweden currently considers becoming a contributing partner. While at the beginning only Germany was part of it and even the US was just an observer, things have changed considerably, with the US, the UK and France being involved. By now it is much better to be inside than to be outside.

With regard to information assurance and other cyber-issues there are, in most countries and in the EU, split cabinet responsibilities – and thus split agendas. In the Ministries of Enterprise and the Ministries of Commerce e-government issues are being discussed; in the Ministries of Foreign Affairs and the Ministries of Commerce freedom of the internet is an issue; in the Ministries of Justice legal issues are on the fore such as how to take down websites fed with information by criminals or terrorists; in the Ministries of the Interior and the Ministries of Defence debates focus on information assurance and cyber-security; the Ministries of Foreign Affairs also discuss international law and cyber-security issues. These examples show that one of the tasks states have to address is thinking through properly who in government should be at the head of all these activities.

Statement by Julian Harston

Former Assistant Secretary-General, United Nations

"Peacekeeping and Peace Support

Where is multinational peacekeeping going and what will be the role of the military.
What are the threats and how best should member states react to them, together."

Bern, 28 August 2013

For his presentation we asked Julian Harston to address particularly the following questions:

1. ***Are military interventions in foreign countries basically an effective and legitimate instrument? What can realistically be achieved, and what not, under what conditions?***
2. ***What direction is military peace support – or, more generally, the idea of military engagement abroad – presumably to take (after the lessons from Afghanistan)?***
3. ***What is the role that European states in particular could and should play in this?***
4. ***What role will/should armed forces have in future peace support operations?***

Those of you who are aware of my background will understand that as a UN person I have a particular sensitivity towards the role that can be played by foreigners in matters of national security. For that reason I feel honoured to have been trusted by being offered a small opportunity to guide the Swiss ship of State.

I believe that all of us should have heroes. I have two. That they are both British may not surprise you. Their lives were separated by 200 years, but they both have something to offer in this debate.
Thomas Hobbes of Malmesbury was an English philosopher, best known today for his work on political philosophy. Hobbes conceived of the modern state in his *Leviathan*, published in 1651. He is known in these days, wrongly, as a gloomy philosopher because of his emphasis on anarchy. He was in fact a liberal optimist, who saw the state as a solution to anarchy, allowing people to procure possessions and build a community. Hobbes knew that the path toward a better world-order, let us call it peace, first has to be established. Only later can humankind set about making such order non-tyrannical.
Winston Churchill as a 23-year-old published his first book, '*The Story of the Malakand Field Force*'. In it, he gave advice on how an outside imperial power should deal with a country like Afghanistan. He was, of course, referring to how Britain should approach the population of the Pashtun frontier beyond the Indian subcontinent, but he might just as well have been referring to how the early 21st century United States should do so. For much as the

elites of the United States hate the expression, America remains in an imperial-like position in much of the world.
Churchill intimated three courses of action. The first course was to do nothing and leave. The second course was to initiate a large military operation until the people of the frontier are 'as safe and civilized as Hyde Park'.
Whereas the first course is irresponsible, the second is unfeasible, given the expenditure of resources required. Then there is the third course: to manage the situation by dealing with the tribes, subsidizing and encouraging the good ones, punishing the bad, and creating stability and 'good governance' (although this is not a phrase that Churchill would have understood). Churchill didn't think much of the third course but he saw no alternative for a great power, recognizing that any grand strategy must marry goals with available resources, and that in the end it is a sustainable peace that matters most.
What these two heroes of mine understood, and that was truly extraordinary in the 17th century, and only marginally less so in the 19th, was that a stable society and sustainable peace can only be built by creating enough security on the ground on which to build an inclusive political solution.

I worked with the United Kingdom Diplomatic Service for some 25 years before joining the United Nations as Head of the political department of the ill-fated UNPROFOR in 1995. My second career in the UN took me to Zagreb, to Belgrade (three times), to Sarajevo, to Haiti, to East Timor, to the Western Sahara and to New York. I was Head of the UN Missions in Haiti and Western Sahara, and I was Deputy in Sarajevo. In New York I was Director of Peacekeeping for Asia and the Middle East. I have worked in seven UN Peacekeeping Missions and directed the activities of five more. Above all I am a practitioner, not an academic. I have the added advantage of being retired. Thus the judgements I will offer you today are my own, not those of the UN or any of my previous masters.

The four questions I have been asked to address today involve among other things:
– the role of the armed forces in the support of Peace Operations, and their effectiveness;
– the future of peace support;
– what European states should be doing in this area in the future.

What do you think yourself about UN peacekeeping and its capabilities in dealing with issues of international peace and security through the mechanisms of peacekeeping and peace building? Perhaps not very much: too much politics and too little decisive action; waste of resources; bad command and control structures; poor security; difficult relations with regional organisations, e. g. with the African Union; soldiers who are only there for the money.
During my time in peacekeeping all these things have been true at one time or another, in greater or lesser measure. And yet, the UN can deliver large numbers of troops on the ground quickly, it has proven its ability to operate and sustain missions in some of the most hostile environments in the world. The UN has had some extraordinary successes and some very

bloody failures. UN peacekeeping is statistically more likely to succeed than any other variety, and it is cheaper.

Through the learning processes involved in our Missions in Cambodia, the Balkans, Haiti, Central America, Namibia and Mozambique the UN developed the concept that is now known as the 'comprehensive' or 'integrated approach':
an understanding that peace can neither be kept nor built on the basis of a military plan that is divorced from a political strategy.

Senator Rumsfeld's affirmation that the US Department of Defence's plan for post invasion Iraq was 'to have no plan' was the starting point of a steep learning curve in the US, NATO and the EU that has led us to where we are today.
The integrated approach is the coordination and synergy, at political and strategic levels, of all available instruments of power, in order to enable each of these instruments to accomplish, at theatre and tactical levels, actions leading to a change of initially unacceptable conditions into a set of acceptable ones; the comprehensive end-state, if you like.
I understand the instinctive professional military reaction to
peace building and the comprehensive approach. Life would be so much easier if we were all just allowed to do what we are good at. But life isn't simple. The most important lesson learned by the UN in the last twenty years of peacekeeping is that with the right resources, the right mandate and the right leadership the comprehensive, civilian led, approach works and must be the basis of the international community's efforts to deal with conflicts in the near future.
In the next few years you will hear more of Mali, the Central African Republic, the ungoverned spaces in North-West Africa, Yemen, Somalia and even perhaps a part of the Balkans as being real threats to us here in Europe which we need to deal with in a comprehensive way. What this kind of peacekeeping needs is professional military officers who understand that it is essentially a political process in which they are involved and professional civilians to manage the broader process. The more prepared the soldier, the easier it will be for the political side of the Mission to succeed to the point that it no longer needs the military and that they can move on with the job well done.

In January 2012 I was asked to undertake a Strategic Review of UNIFIL, the UN peacekeeping operation in Lebanon. I presented my report to the Security Council. UNIFIL was remodelled by the international community in the days which followed the war between Israel and Lebanon six or seven years ago. The new UNIFIL, with an authorized strength of 15,000 troops, together with a maritime component of six naval vessels, was operational within a few weeks. The Mission included significant contributions from NATO nations (France, Spain, Italy, Germany, Portugal) some wearing blue helmets for the first time since UNPROFOR in the late 1990s. The Mission has proven to be an outstanding military success. Southern Lebanon has had, until recently, the quietest five years in its history.

But Security Council Resolution 1701 which brought the new UNIFIL into being had a second and equally important objective. This was to bring about a permanent ceasefire between Israel and Lebanon. This has not happened. What my review says is that unless there is political progress all that has been gained by the military risks being lost. All my recommendations are designed to bring the political track up to speed. They are designed to encourage the two parties to invest enough in political stability and to persuade them that going back to war would be fundamentally against their national interests. There isn't a better example for the fact that peace support is about politics and that the process, if the politics are left behind, will fail.

This is perhaps a good moment to reflect on Afghanistan. Almost all the lessons I identify here have been ignored there. With the result that we are now limping towards a withdrawal and Afghanistan may well be seen in the future as a copy book example of how *not* to do these things.

Echoing Lord Ashdown I would like to say the following: We failed to concentrate first on the rule of law and now find ourselves burdened with a Government in Kabul so tainted by corruption that its power over the state declines by the day. Far too much of our military strategy was chasing the enemy, when we should have been protecting the people. We wasted lives, resources, money and opportunities on our own ambitions rather than delivering the simpler things with which Afghans would have been content. We are ignorant of local customs, traditions and language.

We failed to understand that in these wars it is politics, not weapons, that counts most. Even if you win on the battlefield (and there is absolutely no doubt that in the two wars they fought in Afghanistan the military have been incredibly successful), you lose if you lose politically.

Our greatest mistake of all is that when unity of command on the part of the interveners was crucial to success we have failed completely to achieve this. (Even today in Kabul there are no less than seven people of ambassador rank from the US.) A sustainable peace also requires that we do what we can to promote the constitutional structure that runs with the grain of Afghan tribal realities. It was arrogance compounded by ignorance that led us to press for a Western-style centralized constitution, complete with elections they can't afford without our money, in a country that has been decentralized and tribal for at least two thousand years.

And make no mistake, the blame for this cannot be simply attributed to NATO, to the coalition or even to the US, but must also be seen as a failure by those in the UN, who of all people should have known better.

You asked me in what direction the question of military support to peacekeeping and peace building is going. After a decade of considerable surge, it appeared until very recently that UN peacekeeping was headed toward a period of consolidation and perhaps even contraction. However, with the recent Missions in Syria, Libya, South Sudan and now Mali, this no longer seems to be the case.

The challenges peacekeepers are facing today remain daunting. UN peacekeeping operations are deployed to environments that are inhospitable, remote and dangerous, sometimes with-

out adequate logistical support and resources. The diversity of missions continues to grow, as are the expectations of what UN peacekeeping can deliver. Missions' mandates are increasingly complex and multidimensional. We still have traditional missions supporting a ceasefire agreement between two parties like the one I was in charge of in Western Sahara; at the other end of the spectrum we have missions which cover vast territories, such as the Democratic Republic of the Congo (DRC) and Sudan, and have complex mandates ranging from supporting elections and state capacity to disarmament and demobilisation, strengthening the rule of law, improving the management of the security sector and so on. Other missions provide security and protection in response to a conflict. Increasingly, UN peacekeepers are called upon to take a more *robust* approach to implement their complex mandates.

The UN Security Council on 29 March 2013 unanimously approved an 'offensive' peacekeeping brigade to fight rebels in the DRC, the first UN force of its kind: 2,500 troops authorized to 'neutralize and disarm' rebel groups. This further excursion into 'robust' peacekeeping is rather troubling me, not just because it brings further into question the status of the peacekeeping force and, more importantly perhaps, of the humanitarians operating alongside that force, but because I have not yet seen a convincing political strategy and end-state for the DRC. (I see from yesterday's press that the brigade is already getting into trouble. So we will see.)
The Security Council has got into the habit of giving the mandate to 'protect civilians'. Although this sounds simple, it carries significant policy and operational challenges, and I think that as a result of this there will be no more Chapter 6 Missions in the future.

Since the end of the Cold War, we have seen the emergence of a new type of operation which also seeks to address the underlying causes of conflict. What we have been trying to do – in East Timor for example within six to seven years – is to complete an evolutionary process that would normally take decades or even centuries. This is what we are all involved now in Afghanistan.

In the year 2000 the level of UN deployment was about 20,000. On 1 January 2013 some 100,000 military, police and civilian peacekeepers were deployed in 17 Missions, 1 AU operation and 10 Political Missions, budgeted at a total of $8 billion. The annual procurement bill for peacekeeping now approaches $3 billion. Each of these figures represents an all-time high.

Our discussions today are brought into sharper focus by recent events around the world, not least by what is going on or not going on in Syria.
The separation of military and civilian problem-solving no longer exists. There is no such thing anymore as dealing with the hart and soft issues separately. Conflict prevention, conflict resolution and post-conflict reconstruction are together the base upon which diplomacy in the area of peace and security is built. *But* – and this is the key to one of the themes of our discussion today – unless violence stops there is no basis upon which to build governance and stability. The mili-

tary must first build the platform on which all the other things that support activity over a period of some years have to rest.
The 'integrated approach' to stabilization is a reality. There is no magic in this. At its simplest it means before we intervene we must have a plan and that plan must include as many of the participants in the project as possible.
Without it, peacekeeping and peace building will not succeed.
In Afghanistan and elsewhere the message of the 'enemy' is a startlingly simple one: these foreigners will leave, we will stay. Stick with us, we are your future.
Our only response must be to give people a real choice by creating a secure and sustainable foundation upon which, with our continued help, they can build a better future and a real alternative.

The International Crisis Group says, the stakes of the game have risen dramatically as global implications of state fragility and failure have become more profound. Failure to consolidate peace in Afghanistan, Colombia, Somalia, Sudan, Yemen and beyond no longer just impacts on the people of those countries: it opens the door to training camps for global terrorists; it permits new routes for trafficking of persons, arms and illegal drugs; it disrupts international trade and investment; it facilitates even the incubation of pandemic disease; it brings piracy – just to name a few.

In studying more than two dozen successful and failed peacekeeping operations since World War II, Donald Steinberg, one of the leaders of the International Crisis Group, says he found six key challenges that must be addressed nearly simultaneously. These challenges are:
– to restore State and human security;
– to build a responsive political framework;
– to kick-start the economy;
– to balance national reconciliation and the need for accountability;
– to promote civil society;
– to address the regional context.

In 2011 a seminal World Development Report offers a much more 'rough and ready' approach to how development is done in post-conflict environments – stressing the need to prioritise given the short time horizons we often work within; to focus on 'inclusive-enough' political settlements and 'good enough' reforms. It isolates three essential areas in post-conflict settings: *security, justice and jobs.*
There is an explicit recognition that you have to get security and justice under control; otherwise you won't make any progress at all.

Peacekeeping operations can only succeed in the right political context, with a readiness for peace on the ground and a will to work for it in major capitals.

The question of whether UN peacekeeping can take on more must be seen in the light of the fact that there are so few global alternatives. Of all the world's organizations, the UN is least able to turn its back on those whose very lives hang in the balance. (I say that with some caution in a week where we are watching the world turn its back on Syria.)

As Lakhdar Brahimi, the wise man of the UN, said to the General Assembly not long ago, 'There will be plenty of surprises over the next decade. But I am fairly certain that one thing will remain constant, and that is that UN peacekeeping shall continue …'
So there will be more UN peacekeeping, and many of the operations that exist today will continue for some time to come. The comprehensive integrated approach is in my view the ideal. But as in Mali and Somalia and doubtless in Syria each operation will in fact be *sui generis*, and will be planned and executed within at least an accepted premise that the integrated approach is an appropriate aspiration and that the military have a vital role to play, but only within a plan based on political imperatives and designed to last much longer than the military engagement.

In Europe the OSCE and NATO are and will continue to be players on the international peacekeeping and peace support stage. I believe that the OSCE, as a responsible regional organization under Chapter 8 of the UN Charter, indicated at its meeting in Vilnius 18 months ago that it too is hoping to engage its member states in a much more comprehensive approach to early warning, conflict prevention, peacekeeping, and peace support. The resolution that came out of this meeting says: 'Acknowledging the need for timely and preventive responses to crises and conflicts, which requires, inter alia, a comprehensive early warning capacity across all three OSCE dimensions; timely, objective and verifiable information, also regarding the humanitarian and security conditions on the ground as well as the political will to take early and effective action; making full use of existing OSCE instruments, mechanisms and procedures …' And it goes on: 'Recognizing that a comprehensive, cross-dimensional response is required to address the … causes of crises and conflicts and that this also demands co-operation and co-ordination between the participating States …'

I sincerely hope that the OSCE, which by happy coincidence for me will in 2014 be co-chaired by Serbia and Switzerland, the two countries in which I spend most of my time, will be able to take a much more purposeful and better organized role in this, surely one of its most important tasks, than it has done in the past.

NATO of course remains a powerful alliance, but will be tempted to be far less ambitious in the near future. All but France and the United Kingdom have lost any appetite for expeditionary warfare.
It seems only yesterday that NATO was taking on the role of world policeman. 'Out-of-area' operations were all the rage in Brussels. Afghanistan, it was confidently predicted, would be only the first of many successes. Even the Germans turned a blind eye to their constitution and sent troops beyond Europe's shores.

That was then. A decade is several lifetimes in geopolitics. The appetite for intervention would now appear to have been sated – nowhere more so than in Washington. Barack Obama wants to be remembered as the
US President who brought troops home, despite the award of a Nobel Peace Prize when he was prosecuting two wars. After all, enemies can be dealt with at a distance, with drones and special forces. Syria can fight its own civil war – or, as we see today, maybe not.
As for Germany, it seems to be re-adopting its old attitudes. Not that long ago the Berlin Government found itself in political trouble for sending a handful of soldiers to oversee the evacuation of German nationals from Libya.
But while refusing to agree a definition of it, NATO has adopted the integrated approach, and now seems to understand the need for at least some interventions to be planned and executed within a plan which includes the civilian dimension and regards the military as just part of the solution.
I believe that we are most likely to see NATO involved in the medium term in operations, under a UN mandate, in support of the UN in surge operations or as short-term interventions, followed as quickly as possible by a handover to UN or regional forces, as the French in Chad and Congo or the British in Sierra Leone. France's intervention in Mali, where it was supported by considerable NATO resources, is an example of this.
In the short term then, there will be a continuing demand for UN and regional peacekeeping intervention, based on the integrated model. These operations will include, at least in their early stages, the deployment of military force.

I am asked: are military interventions in foreign countries an effective and legitimate instrument. If they are legitimised by a Security Council Resolution and only a part of a broader political construct, the answer is yes. What can be achieved is the preparation of a security platform upon which all the other parts of the international peace building effort can be continued after the departure of foreign forces.
What then is the role for Europe – one might say 'the North' – in all this. Above all, in my opinion, foreign and defence policy is about perceived national interest, tempered with domestic political expediency.
There is both a real security and political rationale for Europe to be involved in the military dimension of peacekeeping, and what might be described as a moral one, which, if ignored, takes on a significant political dimension.
You will doubtless be involved with other speakers in identifying the current security threats to Europe and the world, but I would suggest that you will conclude in the end, as did the UK Ministry of Defence, that the world is an increasingly dangerous place, and that 'the challenge has been to move from stability based on fear to stability based on the effective management of risks, seeking to prevent and contain conflicts rather than suppress them.'
'This requires', said the UK Defence Review, 'an integrated policy using all the instruments at our disposal, including diplomatic, developmental and military'.
I am reasonably sure that other speakers will identify the threats of interstate – and now more likely intrastate – warfare, transnational crime, dangerous regimes, Weapons of Mass destruc-

tion, international terrorism, radical Islam and cyber 'terrorism' as being those that should now be the centre of attention in security policy planning. And if they did, they would be right. For Switzerland one should add the threat to financial flows (there are, I am told, billions of dollars in Swiss banks from the Gulf alone) and to the flow of natural resources (Switzerland is unusual now in Europe in having a very dynamic production sector almost entirely reliant on the import of natural resources).

In the context of my presentation it is sufficient to say that UN peacekeeping is likely to take place in countries and locations – the vast empty spaces of northern Africa, Somalia, Syria and even a part of Europe, i.e. Macedonia – which will be easy for the North to identify as providing the breeding ground for many of the threats I have already identified and as being a direct or indirect threat to their security and well-being.

There are sound logical reasons for Europe and others in the North to take part in peacekeeping in the future. It will address real national political imperatives, including real economic and social threats.

I have mentioned also what I call the moral rationale.

In recent years there has been a growing pressure in the General Assembly, and in the Security Council, for the North, particularly the Permanent Members of the Council, to put their soldiers into harm's way. 'There is a huge mismatch between the mandates the Security Council gives to the peacekeeping missions and the resources they are willing to provide: rich countries are the worst offenders,' Anneke Van Woudenberg, the senior Congo researcher at Human Rights Watch, recently said. 'Where are the Europeans? Where is the United States? Where are the Canadians?'

The Council has been happy to vote for new Missions and allow willing troop contributors from the subcontinent and elsewhere to bear the military burden and risk, sheltering behind the argument that the North pays the bill.

India and others are now saying this has gone on long enough, and the UK, France and others are beginning to hear the message.

I believe that we will see British, French and other European troops taking an increasing part in UN peacekeeping operations in the next few years. Not, I think, as boots on the ground in large numbers for long periods, but in surge operations, in enabling units for short-term deployment and offering specialist skills and support in the increasingly complex peacekeeping environment. In the Congo the UN is now involved in the use of drones and, as I understand, in cyber-activity. The UK, France and others will find public support for peacekeeping despite the disenchantment for large-scale overseas military engagement which resulted, I think, from the losses and, dare I say, failure in Iraq and Afghanistan. Their military establishments will also see merit in opportunities to use their expeditionary warfare assets, on which large amounts of money is being spent. (The UK is in the throes of building the two largest ships in the history of the Royal Navy.) The military themselves will be happy to have a new focus, opportunities for 'active service' and the promotions that go with it.

I will finish by suggesting what I believe will best serve the Swiss national interest over the next few years in the area of peacekeeping and peace support. I have no doubt at all that it would be entirely legal and in your national interest to be involved in peacekeeping operations that have the sanction and legitimacy of a UN Security Council Resolution, whether with the UN, or the OSCE, or even, as is presently the case, with NATO. As I have said, Switzerland depends, perhaps more than most nations, on stability in world markets. Switzerland, too, is deeply concerned by the mass movement of peoples. Your country must be interested in preventing the conditions which encourage terrorist training facilities and the spread of Weapons of Mass destruction.

Switzerland shares the moral responsibility of the North to take a more active role. You are the 16th largest contributor to the overall UN budget, of which you cover 1.13%. In 2010, Swiss taxpayers paid roughly $120 million to the UN peacekeeping budget of around $7.7 billion. In the number of people deployed in uniform in peacekeeping the Confederation ranks 85th.

You are much admired for your humanitarian tradition, and it could be said that many people in the world continue to 'expect' neutral Switzerland to be present in the Conference Halls, at the negotiation table, both overt and covert, and on the battlefield to continue in its efforts to make the world a better place.

In its Security Policy Report of 2010, the Swiss Government advocated a qualitative increase in peacekeeping contributions, a greater focus on air transport, ground transport, logistics and high-quality niche capabilities. But an intermediate defence policy (the so-called 'Development Step 2008/11') identified the support to domestic civil authorities as the most likely deployment scenario for the Swiss Armed Forces.

I believe that there is not just a moral imperative for increased Swiss participation in making the world, not just Switzerland, a safer place, but a political imperative too. It is not in my view an exaggeration to say that the international community expects from a rich country that greatly takes advantage of the positive aspects of globalization to contribute significantly to solving some of the world's security problems. Contributing to peace operations is a very visible and cost-effective way of doing so.

As an amateur student of the tides of opinion in Swiss politics I do not believe that more than company-size contributions to military peacekeeping, beyond the current engagement in Kosovo, look likely. And in any event I would not ask for them. Stability in Kosovo was in Switzerland's interest not least because of its relative geographic proximity and a substantial influx of refugees from the region to Switzerland.

Switzerland is about quality, not quantity. I would rather support the provision of niche contributions in the form of high-value assets and experts, e.g. transport, security sector reform (SSR), disarmament, demobilization and reintegration (DDR), and I believe that these would be likely to attract wider support in Bern. In terms of international recognition, and the 'moral dimension' of course, expert contributions have much lower visibility than people in blue helmets, but politics is the art of the possible. My conviction is that with a well-targeted, high-value and well thought-out integrated increase in Switzerland's military and civilian

contribution, Switzerland would be seen to be taking on a clearer responsibility for international peace and security and that this would be the best ammunition against those who despite their admiration for the Swiss continue to believe that Switzerland is inclined to profit, whilst others take the strain.

I am encouraged by the exercise we are going through here and I hope at least that it leads to a clear strategy and a political commitment to implement that strategy. What is needed for such a progress are of course the financial and human resources, and, more importantly, that Government makes it clear that in future, peace operations will be one of the key roles of the Swiss Armed Forces. I cannot think of a serious military in Europe, including Sweden and Austria, which does not have specified as one of its main capabilities, indeed as one of its main raisons d'être, participation in international peace operations and which does not spend a great deal more than the one percent or so of the defence budget that Switzerland presently allocates to these endeavours.

The Swiss Armed Forces possess with SWISSINT a UN and NATO certified training centre, which offers domestic and international courses, especially for military observers. This training and expertise is complemented by the so-called Geneva centres: the Geneva Centre for the Democratic Control of Armed Forces (DCAF), the Geneva International Centre for Humanitarian Demining (GICHD) and the Geneva Centre for Security Policy (GCSP). The Swiss Armed Forces have limited but high-quality capabilities in logistics, engineering and transport. The professional civilian background of Swiss militia soldiers and officers is an asset in SSR, Rule of Law and many other specialist functions which benefit from civilian competencies and expertise. Switzerland could certainly provide more French-speaking soldiers and officers as Military Observers in an increasingly francophone peacekeeping environment. Indeed, the multi-ethnic Swiss militia can provide a better understanding and more expertise in a wide variety of international environments than most European militaries.

One area I believe demands attention is a feeling that I have identified in discussions with some of Switzerland's military leadership: that international service does not make better officers. It is thus undervalued. I would say what I used to say in Bosnia to visiting senior British police officers. 'We send you back much better police officers than you send us.' In the UN they tend to have had more responsibility than at home, they have worked in an international environment and have broadened their skills and experience. The same is true of the military. International military service is 'active service' and should, in my view, be one of the keys to promotion to the highest command positions.

When I asked the Department of Peacekeeping in New York what Switzerland could do, I found that their wish list was very close to my own: *Switzerland could contribute more United Nations Military Observers (UNMOs), French-speaking officers and well-trained females. Switzerland has in its army high-level technologies such as Unmanned Aerial Vehicles, radars, sensors etc. which our Missions could use. In general, we are looking for enablers, en-*

gineers, logistic and hospital assets etc. What is more, Switzerland could support developing countries in the areas of training and equipment.

In discussing with the UN Department of Peacekeeping, my experience has been that Switzerland has underplayed its hand in seeking both civilian and military command positions in the system. You need your charming diplomats to take a much more robust approach to the Secretariat. You have very widely recognized attributes which qualify you more than most to take a lead. My experience in New York was that those member states that are assertive succeed.

When I asked the OSCE what Switzerland could do, they were more modest: *Swiss parliamentarians should take note of the work which is currently being done to enhance the OSCE's role throughout the conflict cycle. Switzerland could make a valuable contribution to improving the OSCE's ability to address conflicts and respond to crises. The Swiss could for instance be encouraged to contribute with material to the virtual pool of equipment for use in early action.*
OSCE is thus recognizing that Switzerland could and should offer some of the world beating expertise that it has in order to help the OSCE and, consequently, to improve its own national security.

If I may sum up: yes, there will continue to be a worldwide demand for UN and other forms of multilateral peacekeeping in the next ten years. Yes, the military will continue to play a vital, effective and legitimate role, as part of an integrated plan. The European states (the North) will come under more pressure to take an active military role in peacekeeping, both for reasons of national security and as a result of moral pressure. Of course, each state will make its own decisions about participation.

Switzerland, too, is threatened in an increasingly unstable world. The threat is not now a localised existential one but a much more diverse one originating in the most part far from the borders of the Confederation. It is truly an international threat, and Switzerland should be seen to have an active part in the international response.
The Swiss should offer more to peace operations, not in terms of large numbers of boots on the ground, but in terms of the extraordinary abilities it has in both civilian and military areas, and above all in sharing its world class credibility and its humanitarian tradition in a more generous, well-planned way.

Statement by Dr. Emmanuel Kwesi Aning

Director Academic Affairs and Research Faculty, Kofi Annan International Peacekeeping Training Centre (KAIPTC)

"United Nations Peace Operations - West Africa's security challenges"

Bern, 28 August 2013

For his presentation we asked to address particularly the following questions:

1. ***What direction is military peace support presumably to take (after the lessons from Afghanistan)? How could modern peace support operations be characterized, and what will presumably be the central issues in the future?***
2. ***What role will the concept of 'protection of civilians' play with regard to future mandates and conducts of peace support operations?***
3. ***Where are the possibilities and limits with regard to peacekeeping in Africa?***
4. ***What kind of contributions could/should Western states make to support the management of regional security problems?***
5. ***What are the most urgent security problems in Western Africa, and to what extent do they affect Europe's security?***

In preparing my presentation, I have grouped your questions according to two main themes:
– What are the characteristics, possibilities and limits of United Nations Peace Operations?
– How might West Africa's security challenges affect Europe?

Multidimensional Peace Support Operations have become one of the primary mechanisms of conflict management used by the United Nations and by regional organizations. The nature of such operations has changed rather dramatically due to the complexity of contemporary conflicts and the changing international security situation. Unlike traditional peacekeeping operations, which were primarily limited to maintaining ceasefires, current missions encompass a broad range of varied tasks including humanitarian, human rights and development issues as well as socio-political functions and, of course, traditional peacekeeping. Basically, multidimensional peacekeeping is about rebuilding the state.

The lessons learned from NATO's International Security Assistance Force (ISAF) in Afghanistan demonstrate how peacekeeping processes have evolved. ISAF's mandate included military, police, government and economic reform and narcotics growth eradication. It signified a new direction towards more robust multidimensional peace support operations. The main issue that arises from robust missions such as the one in Mali – which will have to deal with

the same problems as ISAF and to which I am going to refer several times – is the fact that present conflict resolution strategies increasingly reveal political, socio-economic and militarized characteristics implying a dramatic shift from the traditional, strict principles of the non-use of force, consent and impartiality. Sometimes we cannot be impartial, sometimes we do not need the consent of the capitals; sometimes missions are even bound to use force.

Modern peace support operations are constantly evolving and adapting to the challenges of new peace and security environments. While traditional peacekeeping is far from being obsolete, the concept of peace support has undergone a substantial transformation due to the changes within the peace and security environment. Today's operations have become more diverse and complex, involving a range of actors including the UN itself, regional organizations (in the case of Mali the African Union and the Economic Community of West African States, ECOWAS), NGOs delivering humanitarian assistance, and, disturbingly but increasingly accepted, private security organizations. Such operations are undertaken in order to respond to humanitarian crises, often with complex mandates and ambiguous objectives. Furthermore, contemporary peacekeeping operations are carried out by a mix of peacekeepers drawn from different countries and different cultures and from a wide range of occupations: military, police, civilian and diplomatic. These four groups, although working for the same end result, have different backgrounds, different approaches and a different understanding of how the problems they encounter should be resolved. This leads to internal squabbles and to a bureaucratic display of power which in the long run does not help attain the missions' objectives. The four groups, therefore, have to learn to work together in order to be able to lay the foundation for sustainable peace.

In today’s missions, peacekeepers are often deployed to deal with internal conflicts in hostile environments where in fact there is no peace to keep. When, for example, people say that there is a new Malian precedent, that peace has come, they are deceiving themselves. What we are seeing is rather the beginning of a long, drawn-out period during which Mali and its leaders must justify the trust that the international community has put in them. The start, unfortunately, has been poor.

Sometimes – once more as in Mali – missions intervene where the conflict is still going on and where there is no legitimate government. All the same, peacekeepers are given a wide range of responsibilities including the protection of civilians, security sector reform, peace enforcement, disarmament, demobilization and reintegration of former combatants, reorganizing the military, police training, human rights monitoring, election monitoring and building sustainable institutions of governance. Modern peace operations can be described as being multinational, multidimensional, multilateral, multicultural, and, if I dare say so, multiproblematic because they are packed with such a wide array of requests and demands that it is almost impossible for them to succeed.

What will be the central critical issues in future peace operations?
Based on what I know after ten years of working in the area of peacekeeping training, I have made out the following nine critical issues:

1. Ensuring the legitimacy of missions. Even more important than legitimacy in the eyes of the conflicting parties and the contributing countries is acceptance from the local population. We cannot and must not intervene when the local population opposes intervention. If they have the perception that a mission is not doing what it is supposed to do, they immediately turn away.
That peacekeeping is always a common good is but a presumption. The rhetoric coming out of Northern Mali, 'If you send your people there, we will attack and kill them', makes that clear enough How to deal with this conundrum? How do we know what Northern Malians want?
Although legitimacy comes from the Security Council, it needs to be sustained on the ground through the mission's conduct and action, through firmness and fairness in exercising its mandate. Missions that are perceived to be legitimate will achieve their objectives, elicit the needed support of local populations and improve their intelligence gathering capabilities.

2. Application of peacekeeping norms. Given the complexity of the operational environments within which peacekeepers function today and given the ambitious and multidimensional character of mandates, we need to accept that is has become extremely difficult to uphold the traditional principles of peacekeeping – consent, impartiality and non-use of force – originally developed as a means of dealing with interstate conflict. Mali, where Tuareg wanting to buy weapons might well move down south, is a good example for the complexity of today's reality. The existing principles remain the core, but we must accept that between states, especially between those in the Global North and those in the Global South, there is increasingly a lack of consensus on the interpretation of these principles – the Global South being made up of developing countries and emerging powers like China, Brazil, India, Nigeria and South Africa. This lack of consensus has resulted in growing dissatisfaction with current peacekeeping approaches and with the key parameters for interventions in contemporary conflicts. Three cases in point are Libya, Côte d'Ivoire and Syria. Many in the Global South argue that what is called a responsibility to protect civilians is in fact a cover for a particular type of ad hoc intervention.

3. Ensuring an integrated or comprehensive approach. The challenges and complex nature of today's operations demand an integrated approach from a broad range of civil and military actors. A military intervention needs to be complemented by other efforts such as promoting good governance, justice, the rule of law, political inclusiveness, security sector governance and humanitarian assistance. To achieve such goals in the short term is extremely difficult in a weak country. Mali, for example, has gone through a successful election the world is full of praise about, but the situation in Northern Mali clearly cannot be dealt with only by a 'robust' military intervention. Mali's army, fractured as it is, is more respected than

the political elite, which is why there is a very delicate balance with regard to Captain – i. e. now, after his surprising promotion, General – Sanogo. In other words: if someone who has been disappointed attempts a coup d'état, tries to hang on to power, negotiates his way through and becomes, by doing so, a 'great statesman', then obviously something has gone wrong.

4. Matching mission objectives with required capacity. It seems to me that very often the UN does not ask the critical question whether the broad range of goals currently included into peacekeeping mandates have been matched with the necessary capacity regarding funding, human resources and logistics. Mandates also should be realistic with respect to the sustainability of resources. Deploying peacekeepers without adequate capabilities and resources weakens operational responses. It hinders an effective and efficient implementation of the mandate, signalling to the conflicting parties and to local populations a lack of political will.
MINUSMA for instance, the United Nations Multidimensional Integrated Stabilization Mission in Mali, is not sustainable. France is desperate to pull its troops out. When it does so, are those who remain capable of taking up the fight? My response is a resounding: no, they are not. Most of the forces sent to Northern Mali have never fought in the desert before and have no desert equipment either. As a result, the process of gaining the trust, confidence and respect of the local populations has already been seriously hindered. The fact that the support staff consisting of 129 persons Ghana sent to Mali was airlifted by the British Government is far from being the right message.

5. Ensuring the flexibility and coherence of mission mandates. These terms have been borrowed by the UN from the OECD. Mission mandates need to be clear, coherent, flexible and sensitive to the security situation at the theatres of conflicts. Peacekeepers need to understand the security environment in which they are going to operate, and they need to be aware of how the context affects and influences the nature and conduct of their operations.
The pre-deployment training I have been involved with for ten years now demonstrates that often peacekeepers are sent into theatres of conflicts because their governments have made political pledges but that the troops themselves are totally unaware of both those pledges and the operational challenges they are going to face. What police officers for Somalia, for instance, had been told about the Somali conflict before being sent to training at the KAIPTC did not correspond at all to the basic information they got from us within the first three days. As a result, their readiness to go to Somalia decreased dramatically. Nor were my beforementioned 129 countrymen well-informed about the MINUSMA mandate when being selected. In short: explaining the mandate to the troops before they are going into the area is a huge challenge for the contributing countries, particularly for those from the African continent.

6. Ensuring better entry, transition, and exit strategies. Knowing when, where and at what point peacekeepers should enter and leave the operational area is critical to the success of operations. A good entrance entails ensuring that a mission's mandate addresses the root

causes of conflicts; and the exit strategy must be thought through and incorporated from the very onset of a mission.

7. Increasing the deployment of female peacekeepers. Lessons learned from operations in Afghanistan, Darfur, Liberia, Côte d'Ivoire and Sierra Leone have shown that female peacekeepers not only enhance gender equality in peacekeeping missions but also improve local communities' acceptance of the mission. There is a whole number of security tasks female peacekeepers are better equipped to perform than their male counterparts. Among these tasks are sensitive body searches, screening female combatants and gathering information from local women, particularly in cases of sexual exploitation and abuse, as they are increasingly carried out by peacekeepers themselves. How to increase, improve and sustain female participation in peacekeeping operations will therefore be a central issue.

8. Designing peacekeeping partnerships between the UN and regional organizations. The complexity of modern peace operations means that no single organization can tackle the challenges on its own. The conflicts in Mali, Somalia, Darfur/Sudan and the Democratic Republic of the Congo (DRC) – think of the confrontations between M23 and government forces in recent weeks – are a testament to this fact. How the UN better collaborates with regional organizations to address peace and security challenges will become more and more important in future missions. I'll give you a blatant example for this: there is so much suspicion between New York and Addis Ababa that on the day the MINUSMA mandate was approved, the African Union issued a press statement criticizing the UN for non-consultation. I wonder how in such a case an international organization with 53 permanent representatives and two or three non-permanent members in the Security Council can claim not to have been consulted.
In 2007 I wrote a Security Council report for Ban Ki Moon precisely on this topic. In New York and Addis Ababa, Ambassadors asked me what the international community could do. When I retorted that they, too, were part of the international community, they did not appreciate that at all. For that reason, I am not surprised that today, six years after that report, we are still facing the same problems.
Better UN collaboration with regional organizations is imperative given the role of organizations such as the African Union, ECOWAS and the EU in peace operations. The comparative advantages of these organizations are also important because the resources of the UN are limited. The challenge will be how to make the existing ad hoc relationships between the UN and regional organizations more institutional, more predictable and more effective.

9. Protection of Civilians (POC) and future peacekeeping mandates. Due to the changing nature of contemporary intrastate conflicts, most future operations will not take place on a conventional battlefield but rather in civilian populated areas. Therefore, protecting civilians will be at the forefront of forthcoming peace operations. Due to the human cost of conflicts, POC mandates will become the yardstick by which peace operations, especially those in Africa, will be measured. However, there is always a lack of consensus among members of the Security Council as to how POC mandates should be implemented and how they will affect

timely intervention. Ensuring timely decisions at the strategic level and a co-ordinated response will be vital for the success of POC mandates.

What are the possibilities and limits of UN Missions in Africa?
Since different kinds of conflicts will continue to plague the African continent, UN missions will escalate in numbers and include a variety of mandates with different levels of robustness. Due to the changing nature of missions, cooperation between the UN and regional organizations is likely to continue. On the whole, the UN must be realistic about what a peace operation can achieve and where its limits are.

West Africa's security challenge is a topic about which, I truly hope, I will one day be able to speak with optimism. Today, however, I am afraid I have no message of hope.
In the course of the last years, *transnational organized crime* – human trafficking, drug trafficking and the fabrication of false drugs – has become the glue which binds many West African countries together. Narcotics have become so important in almost all countries of the region, that today it is impossible to disentangle legitimate and narcotics-related flows of money. To those who claim that only tiny amounts of drugs are seized I retort: it is not the quantity of drugs that counts, but what the money these drugs are turned into can do in a tiny economy as ours, e. g. the kind of influence it can buy. A sum that in a Western European country may amount to almost nothing may get you a far way in Western Africa. African kids today chose as role models those who managed to make swift money and show that they have done so by conspicuous consumption. In this way, narcotics are undermining societal ethics. They are creating a society in which a get-rich-quickly attitude prevails and no questions are being asked. That is how the challenge of narcotics should be understood.
In terms of profitability, the narcotics trade is now equalled by the piracy business that in the course of the last ten years has grown in West Africa to a considerable extent. The costs of piracy have been estimated at $2 billion a year, but this is a very conservative estimation as the sheer number of incidences and the kind or targets make clear. Two years ago, Lloyds Insurance and the Lloyd's Joint War Committee listed the West African region as 'a war risk zone for shipping'. This smart insurance move means that pirates are virtually invited to take hold of goods.

There are several reasons for the increasing success of piracy in West Africa. Firstly, there is no law governing this particular kind of crime; so, West African pirates do not care whether those they attack die. Secondly, there is an ever widening 'piracy stock-market' allowing interested parties to invest in future hijacks and the acquisition of items such as guns, boats, outboard motors and crew outfits. Even more disturbing is that pirates, in a mutually reenforcing development, are widening their areas of operations and are also attacking merchant vessels. They are trying to get access to sophisticated navigational instruments, to electronic chart systems, to authentication systems and to communication devices – tools that can be used as well as resold.

In 2010 the Security Council, through the United Nations Office on Drugs and Crime (UNODC), asked me to visit Senegal, Mauretania, Niger, Mali and Burkina Faso and to write a report on a possible connection between groups that are willing to use politically motivated violence and people who are in a position to supply them with narcotics. During a period of five months I collected primary data and forwarded it to the UNODC. The Report I wrote clearly demonstrated that in Mauretania, Niger and Mali there were close links between groups recognized by governments as terrorists and people dealing in drugs. Although in the final report all traces hinting at such a link were eliminated and although some people still pretend that such a link has been imagined by academics, I am telling you both as an academic and as a practitioner that it does exist and that it indeed needs to be examined further.

Governance and Development. While we can celebrate the last ten years of gains in democracy, there is no doubt that in this period almost all elections in West Africa have generated fierce debates and controversies, not least in Ghana, a country that is perceived as stable and functional and even as a beacon of democracy. Currently, the whole of Ghana is on tenterhooks, waiting for tomorrow's Supreme Court judgment as to who won the election. The real issue behind challenging the election results, however, was not the quality of the election process but – politics being the quickest way to making money in West Africa – the question as to who will get access to State resources, who will have the power and patronage that winning an election ensues.

These remarks explain why all the elections that took place in the course of the last three years in Côte d'Ivoire, Nigeria, Liberia, Togo and Senegal were met by violence. The problem lies in both the allure of ultimate power and in the possibility to misuse state resources with almost no check, once having won an election.

Therefore, in the future we will have to focus on the following issues: human security, transparency, accountability, adherence to the rule of law, electoral credibility, putting an end to endemic corruption and the economic mismanagement spanning all the way from Senegal to Nigeria. Due to this mismanagement, the optimism people had when their country gained independence is almost turned into a sham.

How do West Africa's security challenges affect Europe? The potential negative spill-over effects of West African security problems threaten Europe; given the geographical proximity, they should not be understated. Mali has demonstrated that even the Sahara, in spite of many people's vision of it as a bulwark, is no hindrance at all to movements. Europe's frontier is now clearly the Sahel.

These security threats pose immediate and long-term risks to Europe's internal security and its interests in the region. West Africa, especially the Sahel region, is an important haven of natural resources such as gold, bauxite, phosphates, iron and manganese as well as a haven of energy resources such as oil, gas and uranium, which propel a whole number of European economies. As the EU seeks to diversify its energy sources, one of its most vital interests is to secure key energy supplies and the trans-Saharan gas pipeline. The growing insecurity in

West Africa and the declining regional response capacity therefore put European strategic and commercial interests under threat.

One security threat is emanating from terrorist groups. The trans-Saharan gas pipeline is on the target-list of the five or six terrorist groups roaming in the Sahel. Accordingly, when the French boldly told us on TV they had driven the terrorists out, my immediate reaction was to ask: driven them *where*? France simply dispersed the terrorists. AQIM is focused on Western targets. This group has evolved from taking substantial ransoms – estimated at $60-80 million – from kidnapped foreign nationals, especially French, to taking the lives of victims or hostages. With its kidnappings, AQIM has become a financier of subsidiary groups. Belmokhtar, over the last couple of years, has become an expert in choosing victims and in negotiating ransoms according to their victims' nationality. Least threatened are those whose countries are known for not paying ransom money at all.

The threat of expansion and increased consolidation of AQIM and its affiliates in the region is turning the Sahel into a safe haven for terrorists and a springboard for terrorist activities further afield. Boko Haram has become considerably more effective in the last four or five months, running rings around the Nigerian Government. All this is not mere happenstance, but the result of well-trained, sophisticated and committed troops – not only Nigerians coming back from Mali.

A second source of threats is state fragility, in other words, state inability to respond to the humanitarian needs of their own citizens. The humanitarian consequences of such insecurity are uncontrolled migratory flows, of which in particular the Spanish enclaves in the region are beginning to suffer. Europe's mainland, too, has become one of the main destinations of such clandestine migration that poses health, economic and security threats to recipient states. A third source of threats is the by now established link between drug trafficking in West Africa and Western Europe, with Spain, Portugal, Italy, France, the UK and the Netherlands being aimed at in a first step.

The forth source relates to the Gulf of Guinea. The GoG is an important maritime route for commercial shipping from Europe and America. In 2011, the total oil supply from the region to the 28 EU countries was equivalent to 40%; Nigeria accounted for 47% of the region's total oil supply. This means that if in the Gulf of Guinea conditions are allowed to develop almost as in Somalia, Europe is likely to meet serious problems.

Managing West African security problems: what can European partners do?
In conclusion of my presentation, I would like to stress six points:

1. Taking up a dialogue being the first critical step, there is a need for a discussion between European partners and countries within the sub-region. These very innovative hearings are a good example for such a dialogue.

2. Improving access to quality education and to basic health care is key.

3. We have to strengthen governance institutions, for instance local institutions that are part of the justice and play a role in supervision. We have to strengthen them by improving their independence.

4. Regarding drug trafficking, governments of countries in the region have signed a great number of protocols and conventions. However, since national institutions are increasingly hollowed out, they are incapable of responding to the threats. As a result, strengthening national institutions and helping states to design legislation is of primary concern.

5. Issues of legislation regarding maritime piracy are a matter of prime importance. Since the phenomenon is a comparatively new one, the necessary laws have not yet been created and prosecutors have not yet been trained. Under such circumstances it is very difficult to bring pirates to book. It may be useful to engage ECOWAS and, hopefully, the African Union in this effort, in order to have a continental approach which will strengthen states in their response.

6. Finally, there is a need for stronger support of counterterrorism measures that focuses on strengthening cooperation amongst ECOWAS Member States and on training in areas such as intelligence, data-gathering ability and capacity-building in both the judicial and the security sector.

Statement by Prof François Heisbourg

Chairman of the Geneva Centre for Security Policy
and the London-based International Institute for Strategic Studies

"Les menaces, l'Union européenne, l'OTAN et la rationalisation de la défense européenne"

Bern, 28 August 2013

For his presentation we asked to address particularly the following questions:

1. ***What are in your view the (real) threats to Europe's security? And are there perhaps also threats that are somewhat over- or underemphasized in the current debate?***
2. ***How would you judge the current state and development of the European Union, and what does that particularly mean from a security perspective?***
3. ***What role is NATO presumably going to play in the future (after Afghanistan)? And what meaning will NATO have for Europe's security in general?***
4. ***Where are the opportunities and limits of cooperation in Europe with regard to security and defence issues? And to what extent is the idea of pooling and sharing military means and capabilities (or "smart defence") a realistic and reasonable option?***

Les questions qui m'ont été adressées peuvent être regroupées en quatre thèmes: les menaces, l'Union européenne, l'OTAN et la rationalisation de la défense européenne.

I. Les menaces

1. Nous vivons à l'ère de la mondialisation qui est aujourd'hui caractérisée par la révolution des technologies de l'information, de la communication et des transports. Les grands processus qui se déroulent aujourd'hui sont très largement partagés avec les autres peuples de la planète. Ils sont tous soumis au processus que l'on nomme "mondialisation" et ceci non seulement lorsqu'il s'agit de défis clairement planétaires. L'une des principales conséquences du processus de mondialisation dans le domaine de la sécurité est l'accroissement du risque de "ruptures stratégiques". Cette expression a été inventée lorsqu'on a fait le "Livre blanc sur la défense et la sécurité nationale en France" en 2008 et confirmé en 2013. Il s'agit d'un changement stratégique qui est le résultat d'événements qui peuvent être initialement lointains, qui a priori ne relèvent pas principalement de mesures de sécurité ou de défense. Ces événements se diffusent brutalement, ils changent de caractère au passage et ils deviennent des défis de sécurité et de défense. Je prends un exemple: en 2003, la pneumonie atypique (SRAS). Il

s'agissait au départ d'un petit problème de santé publique dans le sud-ouest de la Chine. A la fin, il s'agissait de la menace d'une pandémie mondiale avec, pour toute la région de l'Asie pacifique, la mise en place de mesures économiquement punitives. Dans ces divers pays, il avait fallu mettre en place des mesures à caractère militaire telles que des contrôles sanitaires à l'aéroport. A Singapour par exemple, les contrôles aéroportuaires sanitaires étaient faits par l'armée dans le cadre de réglementations relevant de la loi d'urgence. C'est un exemple de rupture stratégique. Les révolutions arabes et la prégnance de la dimension cybernétique dans le domaine de la sécurité en sont aussi des exemples. L'origine de ces différents phénomènes est totalement différente. C'est une autre façon de dire que dans l'organisation d'une politique de sécurité et de défense, il y aura une importance accrue de la connaissance et de l'anticipation, de ce qui permet de capter le plus tôt possible l'avènement d'une rupture stratégique, de pouvoir la caractériser et de tenter d'en prévenir les effets le cas échéant. C'est ce qui a été fait avec beaucoup de succès dans le cas du SARS, grâce notamment aux institutions genevoises. Dans le cas de la France, cela signifie plus de dépenses dans le domaine du renseignement, des conséquences sur l'organisation de l'action diplomatique, etc.

2. Les menaces existantes se situent dans le cadre créé par la mondialisation. Aujourd'hui, par différence avec le processus d'internationalisation du 19ème siècle, la mondialisation est caractérisée par la révolution des technologies de l'information, de la communication et des transports.

- *Terrorisme*

Au cours des douze dernières années, l'action antiterroriste a été assez efficace. Il n'y a pas eu de remake réussi du 11 septembre ni de terrorisme réussi de destruction de masse. Le réseau Al-Qaïda est largement débranché suite à la mort de Ben Laden. Par contre, indépendamment de l'activité courante de groupes terroristes divers, on constate un accroissement continu de la capacité de destruction par des individus ou des groupes non étatiques. Breivik a pu à lui tout seul conduire plusieurs attentats durant la même journée avec des modes opératoires très différents et en tuant plusieurs dizaines de personnes. Pour cela, il faut acquérir des connaissances, des savoir-faire qui sont beaucoup plus facilement accessibles que naguère. L'empowerment qu'autorise la révolution des technologies de l'information et des télécommunications vaut pour le terrorisme comme pour d'autres domaines moins néfastes. Autrement dit, la menace terroriste ne va pas se dissiper et elle ne va pas diminuer dans la durée. Elle devra donc demeurer une priorité constante, tout en sachant qu'une politique antiterroriste raisonnable peut fonctionner et produire des effets.

- *Les atteintes à la cybersphèr*e

Cette catégorie de menace est récente, on n'en parlait pas il y a 20 ans. La cybersphère est l'un des lieux de déploiement de la mondialisation. Elle fait partie intégrante d'à peu près toutes les activités sociales de l'espace humaine dorénavant et, par extension, des activités économiques, militaires, etc. La cybersphère n'est pas un domaine d'activité séparé, notamment dans le domaine militaire, ce qui a des conséquences en termes conceptuels, doctrinaux, or-

ganisationnels, humains et budgétaires. Les Américains en ont fait un domaine séparé et je ne suis pas sûr qu'ils aient raison. A l'inverse, ils ont raison de mettre la priorité sur le cyber et d'y accorder des moyens importants. J'accorde également une grande importance à ce domaine mais je ne suis pas sûr qu'il faille absolument faire comme si le cyber existait en soi en matière d'organisation. Le cyber existe partout, il imprègne tout mais je ne suis pas sûr qu'il existe en soi.

- *Moyen-Orient*

Cette région devient de plus en plus chaotique, dans un contexte où nous avons par ailleurs une Russie qui est redevenue plus forte et moins coopérative. Lorsque les révolutions arabes ont commencé en 2011, de nombreuses personnes se sont livrées au jeu des analogies et elles ont comparé ce phénomène à la Révolution française ou celle de 1989. L'analogie peut être faite avec le printemps des peuples de 1848. A part le cas particulier de la Suisse, les révolutions de 1848 ont été des échecs sur le moment. Elles ont échoué en Allemagne, dans l'empire d'Autriche, en France, etc. Mais les vingt années suivantes ont vu une transformation complète de la structure stratégique, politique, militaire et diplomatique de l'Europe. Ces révolutions ont débouché sur l'unité italienne et allemande et sur l'Ausgleich entre l'Autriche et la Hongrie. Mais ce processus a pris 25 ans et il a supposé des guerres. Cette analogie me permet d'attirer l'attention sur le fait que les révolutions arabes ne vont pas déboucher sur une nouvelle stabilité rapidement. Nous allons vivre longtemps dans l'instabilité et nous ne savons pas quel sera le nouvel état de stabilité. Je rappelle que la France a dû mener deux guerres au cours des trois dernières années et qu'elle va probablement devoir en conduire une troisième, ce qui n'est pas bénin. Par ailleurs, le problème de l'ensemble des Etats européens à l'exception de la Norvège est leur dépendance énergétique vis-à-vis du Moyen-Orient et de la Russie alors que les Etats-Unis cessent d'être dépendants. Ils deviendront même un exportateur d'énergie dans les deux à trois années à venir. Face à une différence d'intérêts et de situation stratégique aussi grande, les conséquences sont importantes.

La primauté doit être accordée à la connaissance et à l'anticipation afin de comprendre ce qui se passe dans cette longue révolution arabe. Nous avons connu entre 1990 et 2011 une embellie dans le fonctionnement du système international. Malgré la crise irakienne de 2003, le Conseil de sécurité a fonctionné dans l'ensemble. Il y a une dizaine d'années, il est même arrivé à se mettre d'accord sur l'extension de la sphère dans laquelle on pouvait recourir à la force avec l'établissement de la responsabilité de protéger (RtoP). On avait l'espoir - vérifié durant la guerre de Libye - qu'on allait pouvoir combiner la légitimité de l'emploi de la force à travers le système des Nations Unies et la capacité d'agir en temps utile pour empêcher les drames humanitaires. L'affaire syrienne est malheureusement la démonstration qu'il n'en est plus ainsi. Le RtoP n'arrive plus à se faire à travers le Conseil de sécurité et il risque de devoir se faire sans le Conseil de sécurité. Dans son discours d'hier, le président Hollande a prononcé une phrase très intéressante sur la responsabilité de protéger. Il n'est plus possible de compter sur des niveaux élevés de légitimité internationale du recours à la force lors de situation de crise humanitaire.

- *Dépendance de l'Europe par rapport à la situation de paix et à la stabilité en Asie Pacifique*
Seuls les Etats-Unis ont la capacité d'agir en la matière du côté occidental. Je ne sais pas s'ils agiront bien ou mal pour maintenir la stabilité et la prospérité en Asie Pacifique sans laquelle il n'y a ni prospérité ni stabilité en Europe. Mais les Américains attendent des Européens qu'ils ne leur mettent pas des bâtons dans les roues lorsqu'il s'agira de gérer les rapports entre les Etats-Unis et la Chine. En raison de son statut de neutralité, la Suisse est moins concernée. Cette dernière menace est sous-estimée. L'Europe n'a pas pris la mesure des conséquences du « pivot to Asia » non pas en tant que formule de la Maison Blanche pour caractériser l'action à l'américaine mais tout simplement d'un monde où dorénavant les intérêts primordiaux des Etats-Unis se situent par rapport à l'Asie orientale. A l'inverse, sur le cyber, on est parti parfois un peu trop vite dans des comparaisons qui me paraissent fausses en considérant par exemple le cyber comme la bombe atomique du XXIème siècle. Le cyber est le contraire: Quel que soit l'aspect de la question que vous regardez, vous constaterez qu'il y a une opposition polaire entre les manifestations du cyber et celles du nucléaire. Le cyber est extrêmement important mais il est également très important de bien réfléchir avant d'agir dans ce domaine.

II L'Union européenne
Les politiques de sauvetage de l'euro depuis 2010 ont eu et continueront d'avoir un double effet dans les années à venir qui a des conséquences dans le domaine de la sécurité:

- Effet récessif. Les politiques de réduction des déficits ont un impact négatif sur la croissance. La région du monde avec la croissance la plus faible aujourd'hui est la zone euro. On se félicite de la bonne santé de l'Allemagne mais le PIB allemand est supérieur de seulement 3 pour cent à celui de 2007. Pendant le même temps, le PIB de la Chine s'est accru de plus de 40 pour cent, celui de l'Inde de plus de 30 pour cent. En dehors de la zone euro, le PIB de la Pologne s'est accru de 20 pour cent. La zone euro et avec elle l'Union européenne dans son ensemble voit son déclin relatif et parfois absolu aggravé avec un effet en ricochet sur les budgets de la défense de la plupart des pays membres de l'Union européenne.

- Effet centrifuge. Le Royaume-Uni n'apprécie pas du tout la nature fédéralisante des mesures de sauvetage de l'euro et elle se détache progressivement de l'Union européenne. On assiste à une sorte de grand écart entre le bilatéral ad hoc dans le domaine de la sécurité et de la défense entre la France et le Royaume-Uni et une politique européenne de sécurité et de défense minimale qui est centrée autour du "moins-disant" allemand.
Ces observations ne tiennent pas compte d'éventuels scénarios de rupture. Elles sont le produit des politiques menées actuellement et qui ne vont pas changer fondamentalement au cours des années à venir. Pour un pays non-membre de l'Union européenne, le problème ne sera pas de se trouver face à une Union européenne politiquement et stratégiquement forte et cohérente, mais plutôt faible et incohérente. Par ailleurs l'élargissement de l'Union européenne continue, fût-ce à petite vitesse.

III L'OTAN

En raison des contraintes budgétaires et stratégiques, les Etats-Unis limitent leur présence permanente et leur implication militaire hors de la région Asie-Pacifique. La nouvelle donne énergétique aux Etats-Unis va jouer dans le même sens. Il n'y a pas de disconnect entre les évolutions budgétaires stratégiques et l'absence de dépendance énergétique. Toutes les forces jouent dans le même sens qui est celui d'une focalisation sur l'Asie-Pacifique et d'une réduction de l'engagement en dehors de cette région.

La relation avec les Etats-Unis au sens de l'OTAN deviendra plus instrumentale, passant d'une situation de rapports étroits durant la guerre froide à une sorte d'" amour vache". Les Américains attendent de la part de leurs partenaires de l'OTAN certaines actions en contrepartie du maintien de l'engagement américain en Europe, politiquement sur les questions de l'Asie-Pacifique, militairement au Moyen-Orient, économiquement en matière d'acquisitions d'armes au sein de l'OTAN en intégrant notre base industrielle et technologique de défense dans la chaine de valeur américaine. La relation devient moins confortable. L'OTAN demeurera le cadre principal car c'est le lieu où l'on produit l'interopérabilité qui constitue un bien public irremplaçable entre les pays membres de l'alliance. Ceci est renforcée par l'absence d'une politique européenne de sécurité et de défense tant soit peu sérieuse et cohérente.

IV Rationalisation

En théorie, l'Union européenne possède, avec le traité de Lisbonne, des outils substantiels pour développer une politique de sécurité et de défense à l'échelle de l'Union. Celle-ci ne se substituerait pas aux politiques nationales mais elle pourrait donner une certaine cohérence à l'ensemble des réponses en cas d'accord pour agir ensemble. Je rappelle la création du service d'action extérieure, le rapprochement des fonctions internationales du conseil et de la commission et la clause de solidarité. Le traité de Lisbonne aurait pu déboucher sur une relance de la politique européenne de sécurité et de défense mais cela ne s'est pas fait parce que les Etats nations ne l'ont pas voulu. Les instances de l'Union trouvent très difficile de travailler ensemble. Le rapprochement entre la commission et le conseil demeure largement fictif, parfois même conflictuel. On retrouve également la grande déconnection entre la non-hégémonie allemande et les pays extravertis que sont la France, le Royaume-Uni et quelques autres. Nous possédons les outils qui nous permettraient d'embrasser toutes les dimensions de la sécurité depuis la sécurité humaine jusqu'à la mise en oeuvre de la force militaire la plus brutale. Mais il n'y a pas ni volant ni instruments de bord ni carburateur. Compte tenu du fait que les chefs d'Etat et de gouvernement ont d'autres soucis en ce qui concerne les affaires européennes, la situation ne va pas s'améliorer rapidement, même avec le changement de commission l'année prochaine.

En ce qui concerne la rationalisation de la sécurité et de la défense en tant que telle, les termes du débat sont les mêmes depuis 60 ans. On parlait alors de la nécessité d'avoir une

division des tâches, de réduire le nombre de modèles de chars ou de bateaux, de rationaliser la base technologique et industrielle de défense. Les ministres en parlent encore plus aujourd'hui mais il ne se passe pas beaucoup plus de choses qu'il y a 20, 40 ou 60 ans.

La crise économique et budgétaire aggrave plutôt qu'elle n'atténue les réflexes de repli national. Je connais de nombreux responsables politiques qui parlent de "pooling and sharing". Mais je ne connais aucun responsable politique qui est prêt à confier au voisin le soin de produire tel armement si cela signifie la fermeture d'une usine dans son pays. Le "pooling and sharing" se heurte également aux différentes politiques de défense. On doit pouvoir compter sur la disponibilité des partenaires. Pendant l'affaire libyenne, on s'est aperçu que les AWACS de l'OTAN « appartenaient » à l'Allemagne. Ils sont basés en Allemagne et 40 pour cent des équipages sont allemands. Le gouvernement allemand a ensuite décidé que les équipages allemands ne pouvaient pas monter dans des AWACS qui devaient servir en Libye. Les Allemands ont été d'accord d'aller en Afghanistan, on a sorti les non-Allemands d'Afghanistan et on les a remplacés par les Allemands. Les non-Allemands ont été envoyés en Libye! Même pour des armements non létaux comme l' AWACS, le problème de la divergence des politiques se pose.

"Le pooling and sharing" est toutefois possible dans de nombreux domaines très lucratifs, en termes d'efficacité budgétaire comme le "European air transport command" basé à Eindhoven et qui regroupe les moyens de transport aériens européens de plusieurs pays d'Europe continentale dont la France et l'Allemagne. On peut étendre la rationalisation au niveau de l'entraînement et de la formation, des moyens d'essais et d'expérimentation. Le recensement des moyens d'essais et d'expérimentation hérités de l'époque de la guerre froide, voire de la Deuxième guerre mondiale, montrerait une surcapacité gigantesque qui représente des sommes considérables. Aucun audit n'a été fait jusqu'à jour afin de voir quels centres d'expérimentation pourraient être fermés ou regroupés. Dans un pays comme la France ou le Royaume-Uni, les moyens consacrés aux essais et expérimentation représentent plusieurs milliards d'euros par an. Il y a donc des gisements d’économie accessibles. Je suis fortement partisan du "pooling and sharing" mais cela ne permettra pas de régler l'ensemble des problèmes.

Statement by Sir David Omand

King's College, London

Main issues: Terrorism and conflict research

Bern, 4 September 2013

For his presentation we asked to address particularly the following questions:

1. ***How will conflicts in the 21st century generally look like? Under what conditions could they turn violent; and what are the aims, means and actors in such conflicts?***
2. ***What does national security mean in the 21st century?***
3. ***What does that mean for the future development and alignment of state security instruments? What could be a reasonable and effective division of labour/responsibilities in this respect; and which instruments are getting more important (and which less)?***
4. ***How could/should the right balance between state security and individual freedom be preserved in the current (cyber) era?***
5. ***What is the role that 'resilience' could/should play in national security? And what exactly should be 'resilient'?***

1. How will conflicts in the 21st century generally look like? Under what conditions could they turn violent; and what are the aims, means and actors in such conflicts?

Expect the causes of conflict in the 21st century to remain unchanged, since they are rooted in the human condition; the environment in which conflicts will take place, however, will be markedly different in some respects. That will affect the threshold for violence and the way in which conflicts are expressed.

Let me expand on that conclusion. In the coming decades we are going to see *multiple causes* of conflict. For the sake of simplification, I will categorise these causes into three types of motivation.

– The first global set of motivations concern *religion, culture and identity.*

There are many examples of historic struggles over religious identity and religious conviction that are likely to continue to feature in the 21st century: Sunni and Shia, Muslim and Hindu in India, Muslim and Copt in Egypt, Christian and Muslim in Northern Nigeria, Hutu and Tutsi in Rwanda. Of course, religion is also a social marker between communities that are in conflict for other reasons, as we know from Irish, African and Middle Eastern history. Syria is a current example. I would like to emphasise the impact of the extreme demonization of the

other in such conflicts. An example for that is the religious ideology that has driven Al Qaida and its associates.
There are also struggles over political ideology, although fewer, examples being the Naxalites in India and Nepal or the Shining Path in Peru. There may be other ideological causes that later in this century will drive global movements, for example to fight against capitalism and inequality, to protect the global environment, or even to oppose climate engineering, should that ever be seriously proposed.
Under the same heading I would put struggles over cultural identity and secession. There is a long list of areas with such struggles: Sri Lanka, much of the Mahgreb, Mali/Azawad, Tibet, the Punjab, the Basque Country, Catalonia, Corsica and Northern Ireland. Some of these conflicts will continue to lead to outbreaks of civil disorder and even terrorism.

– The second set of motivations concerns *State power, hegemony, control of resources and survival.*
The risk of conflict between emerging State powers cannot be ruled out, for example future naval confrontation between China and India in the Bay of Bengal, although I expect, and hope, traditional deterrence relationships to hold between the US and Russia, Russia and China, China and India, and India and Pakistan. Conflict through proxies must be expected below the threshold for all-out war, as we see today with Hezbollah. Longstanding *struggles over disputed territory* will continue, for example in Kashmir, Taiwan, the Sendoku islands, Kosovo, Palestine, Gibraltar, Ceuta and Melilla, and the Falkland Islands. Expectations of future sea-bed and mineral exploitation such as over the Spratly Islands, the East China Sea and the Eastern Aegean will accentuate some of those disputes; we will also see n*ew struggles over resources* in the Arctic and, possibly, the Antarctic. Struggles for regional hegemony will continue with Iran and the Gulf, the Middle East and on the Korean peninsula. In this category of motivations we might, more speculatively, add 21st century struggles for survival from climate change, such as drought and rising sea levels affecting major delta regions.

– A third category of less traditional motivations are *conflicts over criminal gains.*
There will be struggles over criminal gains by organised groups corrupting state authority. Examples for that can be found in Mexico, Jamaica, Colombia, Honduras, Somalia, Nigeria and Guinea Bissau. Piracy persists; we could even see the 21st century equivalent of the buccaneering Caribbean settlements of the 18th century, part pirate, part legitimate trader, part slaver, but with global communications and modern weaponry, hiding in the rapidly growing un-policed urban littorals of the developing world.
Most major conflict zones will be marked by having multiple overlapping causes, as is the case in the Middle East today. We should expect such multiple drivers of conflicts to be more prevalent in future.
Which of these 21st century struggles will break out into serious armed conflicts, open warfare, insurgency, terrorism or just armed gangsterism, is as hard to predict today as it was in the past. What may be more useful for future defence and security planning is to examine the influence of changes in the environments in which these conflicts will play out over the com-

ing years. To do that, we might look at three related themes: *the impact of global economic trends, the impact of technology and the impact of changing social attitudes.* I freely acknowledge that it is always easier to predict future risks than future opportunities. It is also easier, when looking back, to see the bad things than to see the good ones. My remarks, therefore, should not be read as inherently pessimistic.

– A first trend is *the global shift in economic power*, represented most notably in the emergence of new economic giants such as India, China and Brazil. Each of those is creating modern and capable armed forces, but I am more concerned over the indirect effect of the pressure on global resources and the scramble for access to them. A rising global middle class is aspiring to a Western level of lifestyle that would be impossibly resource intensive, with extensive pollution consequences. Pressure will be felt on arable farming and water as well as on energy and mineral use, including rare earth minerals for electronics.

World population growth itself will press on resources. We must expect greater variability in climate extremes leading to more drought, storm surges and large scale flooding. To give an example: Dhaka, the capital of Bangladesh, is already a mega-city of 15 million people, lying in the Ganges delta, only a couple of metres above sea level and still growing very rapidly. Another feature will be large-scale migration due to climate change, including migration across the Mediterranean into Europe, having an impact in particular on countries with domestic diaspora from the regions affected, and creating security issues for Europe.

Most of the additional global population growth, however, will end up in the overcrowded urban littoral of developing nations, in the vast slums of mega-cities. The capacity of these urban conurbations will be greatly exceeded in terms of security, governance and basic utilities such as water and sanitation. The implications for detecting and managing the outbreak of contagious and infective disease are likely to be significant. Inside the coastal urban sprawl will hide terrorists, religious fanatics, violent criminal and pirate gangs with international connections to the West.

Safeguarding Western interests and citizens, and, when necessary, organising rescue and evacuation is likely to be a preoccupation of military planners. What will be very different in the 21st century is that these hundreds of millions of poor people living on the margin will nevertheless be electronically connected to one another and to us by their mobile devices. As a result, they will be aware of global events as they happen. The implications of that will be profound and brings me to the second factor I have mentioned.

Technology is obviously going to shape the expression of conflict. Although it is very hard to predict when exactly such scientific advances are going to happen, we can assume that at some point in time there will be quantum computing, robotics, neural programming, man/machine interfaces, genetic engineering and molecular biology enabling animal and human pathogens to be more easily synthesised, and new mind enhancing drugs developed for criminal distribution.

Even the *banalisation* of existing technology will create dangers, for example with the development of drones linked to facial recognition systems, more sophisticated and more lethal

improvised explosive devices drawing on mobile phone and shaped charge technology, improvised communications networks and improvised weapons systems – where current conflicts already provide a reservoir, including surface-to-air missile systems. The protection of Western interests overseas, particularly in aviation, oil and extractive industries, is going to be more difficult, as was seen in the attack in 2013 by a 30 strong armed AQIM jihadist group on the In Amenas facility in Algeria run by Statoil and BP.

Existing proliferation concerns will continue, and obviously more nations could, if they wished, master the technologies required for nuclear devices and electro-magnetic pulse weapons. Key indicators here are whether the Non-Proliferation Treaty can be held together, whether what is going to happen in Iran can be negotiated, and whether Iran, even if it reaches a threshold status and was able to assemble nuclear devices, chooses not to do so, being held back by the Nuclear Planning Group framework. Of course, we would have similar concerns over the Chemical Warfare Convention given events in Syria.
In terms of delivering military effect, we have already seen the impact of surveillance and armed drones. I expect drones to become ubiquitous. Fully or partially autonomous drones and other weapons systems will be introduced and may be subject to some form of arms control, although their utility is likely to be lower in future urban conflicts than in the semi-desert conditions of countries like Iraq, Afghanistan and Yemen.

The biggest change in the conflict environment will, however, be in cyberspace given our increasing dependence on cyber systems and the connectivity provided by 8 billion mobile devices. This may accentuate the trend towards expressing violence from a safe distance, lowering the threshold of conflict.
We must expect military operations - land, sea, air and space - to have cyber-elements, ranging from suppressing enemy air defence systems to dislocating rear area communications. More significantly for everyday life, we will see crime, espionage, sabotage and subversion in the hands of criminal gangs, hacktivists, patriotic hackers and nation states. One consequence is that no longer can we expect the UN to impose sanctions on a country without that country fighting back using cyber-means, as we have seen with Iran. Another consequence is that commercial companies overseas will find themselves the subject of cyber-attack, for example if they are responsible for an environmental disaster or simply because they represent Western capitalism. On the upside, all advanced economies, including China, share an interest in securing the security of cyberspace. So, I am not entirely pessimistic about international understandings being reached in this area. The industry itself may come round to create an inner cyber-core where safe access to secure social media and business services can be organized depending on users giving up their anonymity and validating the identity of themselves and their machines to the system, giving a new twist to the current debate between security and privacy.

Social and political developments. My speculation is that these global economic and technological trends will intensify the tension between nations that unilaterally defend their inter-

ests with military means - including in cyberspace – and those who seek collective security. A current example is the use of international humanitarian law to justify drone attacks on those regarded by their past hostile actions as having forfeited their non-combatant status as civilians. Other nations will be seeking to defend themselves using the different constructions of international human rights law outside zones of conflict, authorising lethal force only when hostile intent is actually being shown. We will see more examples of overlapping different legal regimes being applied by different countries over the same geographical space as the latter try to protect their interests against terrorists and criminals in ungoverned spaces.

2. What does national security mean in the 21st century?

A number of European countries including France and the UK have recently addressed this question. Having been involved in the British case myself I would say that these countries have tried to redefine for modern circumstances the implicit contract between people and government under which in return for protection, the people empower government with coercive means, including armed forces, security and the power to tax in order to pay for them. Nations clearly still need protection from future threats of armed aggression and from subversive threats to democracy, the UK and France for example through membership of the North Atlantic Alliance and through collective solidarity in the European Union.

When in the past we talked about personal security, the security of the individual in their home or workplace or when travelling, has traditionally been seen as a matter for local police services. Over the last decade, however, it has become increasingly clear that important aspects of personal security are now national policy issues, because they have international roots in the activities of terrorists and criminal gangs trafficking in narcotics, in people, in pornography and in false identities. Internationally, internet and consumer fraud already occurs on a very large scale. The dangerous ideology of jihadist terrorism is here in Europe. We are now a widely travelled population in Europe, and travel, even vacation, brings risks. Latent dangers include the spread of bio-technology and of chemical, nuclear and cyber know-how falling into the wrong hands. There is the risk of insecurity in energy and raw material supplies. And, of course, there are rogue states.

If you apply the principle of subsidiarity, then security issues that can be handled locally should be so. There is no point in making the concept of national security broader than it needs to be. But my prediction is that in the 21st century it is the international dimension of our major security risks for people that drives the need for a redefinition of what national security actually means. We need only think of the increased vulnerability of cyber-networked societies, just-in-time logistics and product sourcing all around the world to realise that the boundary of everyday security is now global. Another part of that worth mentioning is international labour migration.

The starting point for a good analysis of security is with the citizen and the enterprise as consumers of security, not with the producers of security, traditionally the military, police and security authorities. Once you adopt that approach, it becomes natural to think about threats

and natural hazards in the same breath, because when the power supply fails, the citizen first wants to know how quickly it will be restored, and only secondly whether the cause was terrorism, an industrial accident or a natural disaster. If the supply keeps failing, then the question is how government could have allowed such lack of resilience in the system.

Concluding my answer to this second question, I define security as a state of confidence on the part of the public - and the international markets - that the major risks, whether from man-made threats or from natural hazards, are being satisfactorily managed 'so that people can go about their normal business freely and with confidence', to quote the aim of the current UK counter-terrorism strategy. We can see a nation enjoying national security when there is confidence in the ability of the authorities to enable normal life to continue freely, that is without people having to give up cherished freedoms and liberties, and with confidence, that is with markets stable, inward investment, overseas visitors arriving and international travel safeguarded.

3. What does that mean for the future development and alignment of the state security instruments? What could be a reasonable and effective division of labour/responsibilities in this respect; and which instruments are getting more important (and which less)?

Not everything needs to change. Since national structures and constitutions differ greatly, there are great risks in over-generalisation; but there are common characteristics all the same.
As a result of my analysis, I would expect to see a central national security authority to set strategies and priorities, supported by security staff, coordinating policy interests of defence, internal security, borders, immigration, environment, transport security and other relevant government functions including intelligence and of course cyber security, making sure they are given sufficiently high priority.

That structure has to span domestic as well as international dimensions. It also has to manage both malign threats and natural hazards, as far as they affect the security of the public. Government therefore has to have a good capacity for risk management, including crisis management, built around a national situation centre that is properly exercised.

Government information becomes more important to build public understanding and support. Sometimes it is objected that this type of analysis overstates the risk since the chances of any individual being affected by events such as a terrorist attack are very low, certainly in comparison with other everyday risks such as traffic accidents and illness. It is the national risk that has to be considered, however, given the impact of disruption on society and the potential loss of confidence in the ability of the authorities to manage the risk. That needs to be explained to the public.

Risk management implies that risks can be anticipated. So, horizon scanning and intelligence assessment are necessary. In my book 'Securing the State' I define the purpose of intelligence

as being to improve the quality of decision-making by reducing ignorance; secret intelligence simply does that in respect of information other people do not want us to have and we usually do not want them to know we have.

A 21st century intelligence capability designed to support what I just described will have to work very effectively and smoothly with law enforcement, span domestic and overseas dimensions, deal with open-source information and social media, and manage international liaisons. It is going to be a knowledge management organisation with flat hierarchies to encourage innovation and creativity, with the agility to adapt and put together teams, using talents from inside as well as from outside the organisation. In short, it will be the opposite of a late 20th century government department or commercial organisation. Much the same can be said for 21st century armed forces, where the emphasis will be on deployability and on the flexibility that enables forces to bring together the different capabilities involved.

4. How could/should the right balance between state security and individual freedom be preserved in the current (cyber) era?

It follows from my approach to national security that the balance to be sought is *not* one between State security and individual freedom. That is a misleading way to think about it. It is the balance *within* the basket of individual human rights we should seek. Our most fundamental human right is the right to security, the right to life - not to be blown up by a fanatical suicide bomber – and at times of threat that may mean some derogation from other rights such as the right to privacy. How the balance is struck will depend upon the level of dangers we face. In wartime, an existential threat may even justify suspension of some judicial rights, in order for example to allow the internment of enemy aliens. In peacetime, but faced with international terrorism, I have argued that above all else the rule of law should be safeguarded but that we should be prepared by law to concede a little bit of privacy to allow the intelligence to be gathered that protects our human right to security.

Achieving the right balance has been affected by the coincidence of two great shifts, the increased *demand* for intelligence on suspects after 9/11 coinciding with the ability of new cyber technology to *deliver* it. Modern national security as I describe it creates a huge *demand* for intelligence on individuals: terrorists, international criminals, proliferators and cyber hackers. On the technology side, rapid advances in electro-optics, cheap data storage, packet-switched networks, the internet and mobile devices make possible the *supply* of relevant information about the communications, location, movements, contacts, spending and beliefs of individuals of interest to the authorities.

The very existence of the technology in turn created new demands such as demand for data allowing the location of suspects to be determined from social media intelligence. Exactly the same thing has been going on in the private sector, as people have realised the commercial value of information about potential customers. So, the private sector has invested heavily in the technologies for commercial reasons, which in turn has generated the ability to gather

more intelligence of security value such as information from airline booking databases, financial payment systems and social media.

The public is, not unreasonably, beginning to ask whether too much privacy has been sacrificed in this market for information, and how we are to have confidence that the power it gives the State - and the market - over us is not being abused. The use of such information has got ahead of the public's awareness of what is possible.

So far, the debate has largely been uninformed, leaving the public in turn at the mercy of a combination of extreme individualists on the right and extreme libertarians on the left who warn of the so-called surveillance society. Governments, on the other hand, know that public security and future prosperity will depend on both the safe exploitation of these opportunities and the power of information.

If voting publics are going to support their governments in maintaining the right kind of balance, then more transparency about what is going on is essential to allow an informed debate about *what* is being done with our information, and *why* it is necessary and in the public interest. Reasonable people will accept that the internet cannot be allowed to be a safe space for criminals such as terrorists and child molesters to communicate without any fear of discovery. But we need to be assured that the major dangers we face justify the measures being taken and that we are being protected in ways that do not infringe beyond reasonable necessity our right to privacy for personal and family life or impose unconscionable moral hazard.
When it comes, however, to *how* exactly the authorities get hold of their intelligence and access the communications, I am afraid the public does not have a right to transparency. The 'sources and methods' of modern intelligence have to remain concealed or they essentially lose their value for security. If the 'how' is exposed, the criminals and terrorists will know exactly what they have to do to avoid detection, and public harm will result.

What goes on within that closed space has to be governed by open legislation in accordance with the democratic process. There needs to be assurance that the threat is as severe as the government maintains it is to justify what is being done. That oversight has to be by proxy; you cannot allow the public into this space, but you can allow judges and senior parliamentarians to oversee on our behalf what is going on. Trusted representatives of society who hold elected office should be allowed to examine not only the heads of the intelligence agencies and of police but also to see their top secret files, documents and intelligence raw material to satisfy themselves that all that is done is justified.

5. What is the role that 'resilience' could/should play in national security? And what exactly should be 'resilient'?

It is in the nature of many of the risks I have described that we cannot count on preventing them altogether. Trying to do that is likely to cause unwanted consequences even greater than the risks themselves. But given strategic warning of the possibility, we can prepare so as to

reduce our vulnerability and limit the initial impact and duration of disruption, should the risk crystallise. So, maintaining defence forces and emergency services that are adaptable and building national resilience have become central concepts in national security thinking in the UK.

First generation resilience thinking after 9/11 used the term in its engineering sense, as the ability of a material to withstand a blow and bounce back into shape. Obviously, the more energy has to be absorbed, the more internal damage to the structure the material is likely to suffer. That kind of thinking therefore focused on the engineering of infrastructures such as power grids, telecom networks and banking systems so that they could bounce back into operation quickly after a disruption by terrorists, by a cyber-attack or by a natural disaster. Since the advantage that greater redundancy of stand-by capacity, reserve equipment, better control systems and emergency response tends to be multi-purpose, you get value from this regardless of the cause of the disruption. A major test of this approach was the planning and execution of the 2012 Olympic Games in London, the largest security event in the UK since 1944. Of course, there is always more that needs to be done, especially in the cyber domain. Debates continue about who should fund the additional investments needed and about what is the role of the national, of European and of other international regulators that set a level playing field and insist that security as well as safety standards are met. If you do that, the commercial organisations that carry out the resilience investment can recoup the costs from consumers.

In the UK, a second generation of resilience thinking developed after 9/11, taking the concept down to the level of the community to improve local arrangements for mutual support through local government, local businesses and charitable organisations such as the Red Cross and the churches. Each local area in the UK – it is probably the same in Switzerland – has a resilience forum where local government works with business, charitable and community groups and military planners, all with an emphasis on the psychological dimension of resilience, the theme being how quickly can you get normal life back when it is disrupted. In the UK, so far this dimension of resilience has most often been tested by exceptional weather events rather than by terrorism.

We now see a third generation of resilience thinking; what some commentators have called ‘adaptive resilience’. If floods knock out an electricity station, the sensible thing to do would be not rebuild it in the same place but remove it to higher ground. Extending that thought and applying the learning means reinvesting over time. When investment decisions come to be made in the normal course of business life – most of the infrastructures being in the hand of commercial organisations, not in the hand of the State – new facilities should be built to improved new national standards of resilience and protective security, so that over a long period of time the fabric of society becomes stronger.

The resources available to do this being very limited, government has hard choices to make over the prevention of which risks it invests in. Certainly in the UK, governments have a preference for expenditure that is relevant to the widest range of risks. There will always be a few risks that dominate and where government adopts a 'mini-max' approach to *minimize the maximum* damage that a terrorist attack or a natural disaster can cause. Protecting nuclear power stations and having a resilient electricity distribution grid would be an example for the UK. But there are far too many low-probability, high-impact risks to be covered in that way; that simply would be too expensive. So we also need a concept of 'maxi-min' *to maximize the minimum level of assurance* you can give the general public, through general purpose security and resilience, when they are travelling or when they are in crowded spaces like sports stadia.

If we are, in such ways, to apply risk management as the guiding logic, then we need to improve the intelligence available to us on which to base our decisions. I would argue that it is possible for a wise government to anticipate surprise itself; to prepare, especially by building up national resilience, so as not to be so surprised by surprise.

Statement by **Alexander Golts**

Independent Military Analyst, deputy editor-in-chief of Russia's Yezhednevny Zhurnal

"Russian security and military policy"

Bern, 4 September 2013

For his presentation we asked to address particularly the following questions:

1. ***What direction will Russian security policy take in the next ten to twenty years? And what role will military means and capabilities play in this policy?***
2. ***Which factors are driving the Russian security policy and interests?***
3. ***In what direction will the Russian armed forces develop in the medium and long term?***
4. ***How is the situation and development in Western Europe – from a security policy point of view – perceived in the Russian Federation?***
5. ***Which ambitions is Russian politics pursuing vis-à-vis the 'West'?***
6. ***What intentions does the Russian Federation have with regard to cyber security?***

If an audience such as yours invites a journalist, they probably do so because they want him to make critical remarks and explicitly say things everybody knows to be true but no one takes the trouble to express.

I cannot foresee what Russian security and defence policy will look like in twenty years, since Mr Putin's regime might not last so long. The Russian elite is totally divided into several groups that have completely different and incompatible concepts of the future, of threat assessments and of Russian security. In my thinking, there are two possible developments. The first is that the regime will become more democratic and that Russia will cooperate with Western countries in trying to defend itself. This development is becoming increasingly unrealistic. The second possible development is that the regime will become more authoritarian, regard the West as an enemy and seek an alliance with China or other Eastern countries.

In today's presentation, I will try to analyse the basis of the current Russian security and defence policy and try to extrapolate it to the future. People often wonder why Russia, a big European country, is so concentrated on hard security. In fact, 80 or 90 per cent of Russian foreign policy consists of hard security such as missile defence and the balance of military forces in Europe. With regard to Central Asia and other issues, Russia uses only hard security instruments in order to reach its goals. By some people this is actually regarded as the beginning of another cold war. My understanding of it is rather different. In order to develop my own view, I would like to turn to Mr Putin's foreign policy which, in my assessment, is based

on Realpolitik – albeit not on a civilized, Henry-Kissinger-like, but on a wild, if not primitive, 19th century Realpolitik. It consists of alliances of states fighting one another severely, using every method to weaken 'partners', which amounts to an endless zero sum game. In this perspective, issues such as human and political rights or the freedom of the press are perceived in Moscow merely as instruments to weaken Russia.

The basic goal of Mr Putin's domestic and foreign policy is the prevention of another Colour revolution in Russia, as they happened in Ukraine, Georgia and in the countries affected by the Arab Spring. He is convinced that all such changes taking place in the world are the result of Western conspiracies initiated by the CIA, the State Department, MI6 and so forth. Mr Putin and those close to him are sure that all protests that took place in Russia last year were the result of that kind of conspiracy, although there is no reasonable argument for this view.. The problem is that this point of view is shared by a huge number of people and that no one tries to show to Mr Putin that this view has little to do with reality.

In analysing how this overriding goal of Russian domestic and foreign policy is achieved, I would like to turn to a famous speech given by Mr Putin in Munich in 2007. Many people considered that speech as a declaration of a new cold war. My own understanding of it is completely different. Mr Putin said that the period with the most stable relations between Moscow and the West were the 1980ies. At the time, I worked for Krasnaya Zvezda, the Soviet Military Daily. I would argue that Mr Putin's suggestion has nothing to do with reality. In that decade we were several times at the point of starting a big war. If Mr Putin nonetheless insists that the 1980ies offered a lot of stability, he does so because at the time everybody was concentrated on hard security. After 2007, the whole Russian international agenda was, in a totally artificial way, turned into an agenda of the 1980ies. By then, many people had forgotten that decade's particular strategic jargon with expressions such as delivery vehicles, Star Wars, Intermediate Range Nuclear Forces Treaty, Conventional Armed Forces in Europe Treaty and so forth. The Government is absolutely aware of how artificial this agenda is. The idea is to preoccupy Western countries with the old, yet beloved game of counting warheads and to have them reject the idea of bringing about some kind of Colour revolution.

I will give you two very clear examples showing that Mr Putin's and his subordinates' military rhetoric has nothing to do whatsoever with their real threat assessment. The first example is the following: with regard to missile defence they claim that the US is developing an opportunity to undermine the Russian nuclear arsenal, although only few people are brave enough to pronounce the whole chain of arguments. Imagine the US launching a huge first nuclear strike against Russia and wanting to intercept the missiles Russia might manage to launch as a response to the attack. An assessment of how realistic such a scenario is indicates how mad an American President would have to be to give such commands in order to check whether their missile defence works or not. Accordingly, Russian leaders themselves do not believe in that scenario.

In 2010 the Russian President signed the new Strategic Arms Reduction Treaty (START) in which Russia agreed to new rules for the estimation of delivery vehicles and warheads. This means that Russia accepts that the US have two times as many delivery vehicles as they have themselves. According to former Russian Defence Minister Anatoliy Serdyukov, Russia will reach the maximum number of delivery vehicles according to the new treaty only in 2028. If Russian leaders really believed that the Americans are considering an exchange of nuclear missiles, how could they permit the US to have twice as many delivery vehicles as Russia?
In the 1970ies oil prices were soaring and far higher than they are now. The Soviet people, however, had no chance to enjoy this boom because their leaders were convinced that they absolutely needed to reach nuclear parity with the US. At the end of that decade they thought they had done so. Current Russian leaders do not think in terms of nuclear parity. Russia currently has 1250 deployed warheads. That the US has twice as many delivery vehicles as Russia does not make anybody nervous, whereas the fact that the US, as a result of the new missile defence architecture, can intercept five to ten warheads – all expert estimations agree on these figures – is perceived as a great threat to Russian security.

The second example showing how little Russian military rhetoric has to do with a realistic threat assessment is the following: Russia is so preoccupied with the idea of military balance in Europe that as often as the topic is mentioned high-ranking Russian military officials start to talk about NATO superiority compared to Russian forces in terms of tanks, helicopters, jets and so forth. Ironically, nobody – with the exception of Georgia maybe – shares the Russian view that there is a military threat in Europe at all. However, if Russian officials compare NATO to Russia, they allow their country to play the role it played in the Warsaw Treaty. I say so because, after all, NATO consists of 28 countries. In my understanding, Russian preoccupation with military balance in Europe is not a real strategy, but a mere parody of Cold War thinking pursued in order to engage Western partners in the useless and endless game of armament counting.

With regard to Russian-American relations, Mr Putin was very successful in applying this strategy. Americans spent four years counting warheads and discussing what kind of missile defence architecture might be convenient for Russia, although in fact there is no such thing. Even pro-governmental experts in Moscow said that missile defence poses no real danger, while phase IV of the European defence system does; if the Americans were to reject phase IV, they said, all problems would be solved very quickly. However, two days after this statement, when the Americans in fact did reject phase IV, the same experts said that the American decision might be considered a step in the right direction but was far from being sufficient and from satisfying Russian interests. For these reasons I am convinced that every attempt to make plans convenient for Russia only provokes a new wave of Russian complaints. This pattern suggests that Russia has not been suffering any real military threat for twenty years or so.

Today, however, there is a rapidly rising threat. For Russia, the strategic situation with regard to Afghanistan is an awful one. There is no chance that limited American or coalition forces will manage to survive in Afghanistan much beyond 2014. The Taliban will take over power rather soon and radical Islam will spread rapidly. If Russia wants to complain about the US, then they should complain about the US leaving Afghanistan and leaving the whole mess to them.

What is more, there is a combination of weak authoritarian regimes and unbelievable poverty in Central Asia, so that the countries in this region will very soon become the arena of all kinds of public unrests and even of civil wars. The Russian-Kazakh border, which exists only on maps, is longer than the Russian-Chinese border. Through this fictitious border, Russia can be intruded very easily. A few years ago, Kazakhstan was supposed to be shielding Russia; by now, it is acknowledged that Kazakhstan is suffering from very serious domestic problems. President Nursultan Nazarbayev's regime is not as robust as it seemed a few years ago. The worst case scenario is that at one point in time tens if not hundreds of thousands of refugees will make it to the Orenburg or to the Kurgan region. They would consist a tremendous military threat to Russia because with such a huge number of refugees there will also be gangs of warlords and drug dealers.

In trying to confront this threat, Russia again focuses entirely on military measures. It is attempting to organize rapid deployment forces from Collective Security Treaty Organization Countries (CSTO) and to participate itself with sufficient armed forces, with a paratrooper division and a paratrooper brigade. Russia doesn't really need Kyrgyz companies or Kazakh battalions; the idea behind Russia's focus on CSTO forces is rather to gain the legitimacy that would be necessary to interfere in the early stage of a conflict. This is an understandable answer to a real threat, but at the same time Russia absolutely rejects all international cooperation in coping with this danger. One high-ranking Russian diplomat a year and a half ago went so far as to say: if American military presence is the price for security in Central Asia, then Russia is not ready to pay it. This shows that security in Central Asia is not a top priority for Russian leaders. Their top priority is to prevent what they think of as Colour revolutions. In other words: they do not want Americans spread their influence in Central Asia.

The most important case nowadays is Syria. There is no genuine strategic interest hidden behind Mr Putin's focus on Assad's defence; there is only a single Russian logistics base in Syria. The reason for the Russian focus is Mr Putin's conviction that his historical role is the prevention of Colour revolutions. He firmly believes that as the leader of his country he has the right to do everything he wants with his people without international interference. And he is ready to defend this principal.

Let us now turn to defence issues which up to recently were in total contrast to the militaristic rhetoric of Russian leaders. The military reform of former Defence Minister Anatoliy Serdyukov brought about a substantial change in the Russian armed forces. Let me illustrate this

by giving you a few numbers taken from official reports: the number of officers was cut from 355 000 to 220 000, the number of Praporshchik, the Soviet equivalent to non-commissioned officers, was cut by 100 000, the number of ground forces units reduced from 1129 to 180, the number of military academies from 46 to 10. There were also very severe reductions within the air force and the navy. Finally, the reform comprised great changes in command and control structures, replacing a division by a brigade organization. Six military districts were restructured in four united strategic commands. As a result, the reform also brought about enormous social changes in the army, and the wages of Russian officers and NCOs rose dramatically. Today, a Russian lieutenant receives 50 000 rouble, the equivalent of $1700, which seems to be rather sufficient. This rise in wages might turn the Russian officer corps into a part of the middle class.

The reformers themselves did not like to call these measures reforms. Rather they called it an attempt to deal with disproportions within the armed forces, with abnormalities and with remnants from Soviet military structures. In fact, when the reform began in 2008, the armed forces displayed no abnormalities and were structured in a very logical way, albeit in a way laid out for a very different kind of army, namely for an army of mass mobilization. The figure of 355 000 officers is only abnormal if there are a mere million troops on the ground, whereas an army with four to eight million reservists needs such a high number of lieutenants, majors and captains to ensure its command. The reformists claimed that of all units in the Russian armed forces 80 per cent were not battle ready, so they simply cut them by 80 per cent. In fact, in a mass mobilization army such a high percentage of not battle ready units is quite normal. These skeleton units have the full number of officers and comprise 500 privates in order to keep armament stock piles and to receive thousands of reservists in an emergency case. In brief, Serdyukov's reform rejected the traditional Russian concept of mass mobilization that had been relied upon for at least 150 years.

Although it seems that they have been rather successful in doing so, crucial elements of the reform came to a halt when it became clear that the reform was contradictory to certain basic principles of Mr Putin's regime. Accordingly, Serdyukov was removed from his post; the punishment inflicted on him has certainly nothing to do with the fight against corruption. In fact, implementing the reform was not an easy task at all because a huge number of people had to be fired, often with no social package being offered. It was something like a liberal reform implemented with Soviet methods. The reformers shied away from qualitative as opposed to quantitative measures, so that I am not sure whether they really understood contemporary threats. The quantitative measures also included conscription, in spite of the fact that the basic problem of Russian armed forces is manning, even more so as Russia's demographic development is coming to a halt: from 2013 to 2025, every year an estimated number of 600 000 young men will reach the age of eighteen. If Russia wanted a one million men armed force, it would need to draft 700 000 men each year, which of course is not possible.
Currently, conscription is losing its main meaning, i.e. the preparation of trained reserves. Under Anatoliy Serdyukov, Chief of General Staff Nikolai Makarov said that according to

their emergency planning the Russian army only needs 700 000 reservists even in the case of a war. My reading of that statement is that the army simply did not have enough military equipment for more than 700 000 reservists. If Makarov had been right, why should the army conscript 700 000 men each year? That would only be a waste of resources, money and time.
My reasoning has been countered with two main arguments. The military say that Mr Putin wants a one million armed force. However, no one has explained what such a number is needed for. According to official estimations, the Russian armed forces now comprise 800 000 troops. My own estimation is more conservative, i.e. between 700 000 and 750 000. In any case, there is no chance to reach the magic figure of one million if not by playing bureaucracy games aimed at creating exactly this illusion. With the number of conscripts changing each year, bureaucrats are able to manipulate the figures reported to the Commander-in-Chief.

The second argument brought forward by Mr Putin's ideologists is that the army is a great school of life. That holds true in the sense of the army offering a negative kind of socialization. Being in the army makes young people understand that they have to live according to a set of unwritten mafia-like laws saying that you are safe as long as you fulfil every order coming from your direct superior, without asking questions and regardless of whether they are compatible with your duties as a citizen and whether they involve criminal actions.
Another issue that has come to the fore with the reform is the officers corps. If the concept of multi-million armed forces is rejected, clearly another type of officer is needed, i.e. a type of self-confident officer ready to take decisions on his own. Accordingly, Serdyukov wanted to change officers' service and education radically and include even the studying of foreign languages, which would have amounted to a revolution in itself. However, by now all military academies are returning to a Soviet type of command and education. As a result, Russian officers are not what Huntington termed 'managers of violence' but rather what I would term 'handicraftsmen of violence'.
At least, all these contradictions help us in trying to foresee how the Russian armed forces will look like in 2020. The Russian defence will rely on the classical strategic nuclear triad of armed forces, but first of all on rockets. Huge amounts of money will be spent to this branch of the armed forces which will be aimed at any potential adversary. At the same time, the Russian armed forces will move very rapidly towards a complete professionalization of special elite troops. In fact, Russia plans to professionalize all fighting units of airborne troops, of the marine and of special forces brigades till 2016. This means that in the case of a local conflict, Russian leaders will be able to use between 50 000 and 60 000 ready troops. That is more than enough to deal with any local conflict. This raises the question what all the other armed forces are needed for. My answer is that the single function of such a huge military machine is to be an attribute of the imperial thinking.

Dr. Karl-Heinz Kamp
Director Research Division, Nato Defense College, Rome

"European security – armaments issues"

Bern, 4 September 2013

Für seine Präsentation baten wir um die Beantwortung folgender Fragen:

1. ***Welches sind die (realen) Bedrohungstrends, welches möglicherweise nur konjunkturelle oder aus politischen Gründen hochgespielte Modethemen (z.B. Cyber, Lenkwaffen mittlerer oder grosser Reichweite)?***
2. ***Wie ist die derzeitige Lage und Entwicklung der EU einzuschätzen, was bedeutet das aus sicherheitspolitischer Sicht?***
3. ***Wie wird sich die Nato (nach Afghanistan) positionieren, worin liegt künftig ihre Bedeutung für die Sicherheit Europas?***
4. ***Wo liegen die Möglichkeiten und Grenzen der sicherheitspolitischen Zusammenarbeit in Europa? Inwieweit ist die Idee der militärischen "Vergemeinschaftung" von Mitteln eine realistische Option (Stichwort: Pooling and Sharing, Smart Defence)?***

Ich freue mich sehr über die Möglichkeit, heute zu Ihnen sprechen zu können. Einleitend möchte ich festhalten, dass ich nicht die Meinung der Nato wiedergebe, sondern meine eigene.

Sie haben mir eine Reihe von Fragen zugeschickt, die Sie gerne diskutiert haben möchten: Hinter diesen Fragen steht die Frage, welche Rolle der militärischen Sicherheitspolitik nach dem Ende des Afghanistaneinsatzes 2014 zukommen wird. Diese Frage stellt sich nicht nur für die Nato. Der Afghanistaneinsatz war für eine Vielzahl von Staaten sehr wichtig, nicht zuletzt auch für die Schweiz. Viele fragen sich, ob man nun die Sicherheits- und Bündnispolitik dramatisch zurückfahren und sozusagen in einen Winterschlaf verfallen wird, bis uns die nächste Krise - wo auch immer sie sein wird - wieder zum Leben erweckt.

Ich möchte deshalb Ihre Fragen unter einen einzigen Titel stellen, der es mir erlaubt, die ganze Problematik in einem kohärenten Rahmen darzustellen:

Transatlantische Sicherheitspolitik nach Afghanistan – fällt die Nato in den Winterschlaf?

Diese Frage stellen wir uns in Brüssel. Wir führen demnächst einen Gipfel durch, bei dem sie zentral sein wird. Ich möchte mit Ihnen unter diesem Titel drei Fragen besprechen:

a. Warum und in welchem Masse ist das Ende des Kampfeinsatzes in Afghanistan ein Gezeitenwechsel für die Nato, die Europäer und die insgesamt fünfzig Staaten der ISAF (International Security Assistance Force) in der europäischen und transatlantischen Sicherheitspolitik, und was folgt daraus?
b. Was sind die künftigen Gefahren oder politischen Trends, die uns vor Probleme stellen?
c. Wie wird Sicherheitspolitik nach 2014 in der Nato und darüber hinaus aussehen, und warum glaube ich, dass die Nato nicht überwintern wird?

A) Die Konsequenzen von Afghanistan

Das Ende des Afghanistaneinsatzes wurde geradezu herbeigesehnt. Jetzt aber, wo es aktuell wird, sagen viele, dass es mit zahlreichen Problemen verbunden ist. Der Grund ist, dass Afghanistan das sicherheitspolitische Denken in den Nato-Staaten, den meisten europäischen und vielen nichteuropäischen Staaten seit weit mehr als einem Jahrzehnt dominiert hat. Streitkräfteplanungen und Beschaffungsentscheidungen, Sicherheitspolitik überhaupt wurden in der Öffentlichkeit sehr stark mit Afghanistan gerechtfertigt. Nicht wenige Verteidigungshaushalte wurden dadurch gerettet, dass man auf den GWOT (Global War on Terrorism) verwies. Militärische Praxis fand in Afghanistan statt, wo täglich 50 Staaten zusammen kooperierten. Nicht zuletzt führte Afghanistan in vielen europäischen Staaten - auch bei den zögerlichen - dazu, dass sich der sicherheitspolitische Horizont erweiterte. Es gibt zum Beispiel in Deutschland seit ein, zwei Jahren eine Tapferkeitsmedaille. Das wäre vor zehn Jahren noch undenkbar gewesen. Die Öffentlichkeit hat sich an die Realität von Krieg und auch an Opfer gewöhnt. Wenn gesagt wurde, dass wir in einer postmodernen Gesellschaft leben und keine Opfer mehr akzeptieren, stimmt das nicht. Alle Länder hatten Opfer, zum Teil sogar in grösserer Zahl, und das wurde akzeptiert. Nach dem Ende des Kampfeinsatzes am Hindukusch stellen sich deshalb mindestens sechs Fragen:

1. Kann ein politisch-militärisches Bündnis wie die Nato seine Existenz rechtfertigen, ohne einen laufenden Einsatz zu haben, der wichtig für die Sicherheit aller Mitglieder ist?
2. Können Verteidigungsausgaben begründet werden, ohne auf den Zusammenhang zu Al Kaida und Afghanistan verweisen zu können?
3. Bleibt Europa für die USA wichtig, wenn es keinen gemeinsamen militärischen Einsatz in der Grössenordnung Afghanistans mehr gibt?
4. Wie können die Nato-Staaten und ihre Partner die militärische Kooperationsfähigkeit “Interoperability“) erhalten ohne tagtägliche Praxis in Afghanistan?
5. Reicht es, wenn der Nato-Generalsekretär in einer Rede in München sagt, dass sich die Nato von der "deployed Nato“ zur "prepared Nato" entwickeln müsse – wenn nicht klar ist, für was sie denn "prepared“ sein soll?

6. Besteht die Gefahr, dass wir in eine ähnliche sicherheitspolitischen Identitätskrise rutschen wie 1990 nach dem Fall der Mauer, als der Nato scheinbar der Feind abhandengekommen war?

Bevor man in die Post-Afghanistan-Depression verfällt, möchte ich auf einige sicherheitspolitische Tatsachen hinweisen, die zeigen, dass wir - damit meine ich die Nato und ihre Partnerstaaten - in fünf Punkten deutlich besser dastehen als nach dem Fall der Mauer.

1. Die Nato und ihre Partnerstaaten haben in Afghanistan ihre militärische Leistungsfähigkeit bewiesen. Erstaunlicherweise ist das Aussenbild der Nato viel besser als ihr Innenbild. Von innen gesehen finden wir, es gebe keinen Konsens. Die Aussenwelt sieht aber kampferprobte Streitkräfte, die auch funktionieren. In Libyen hat die Nato gezeigt, dass sie rasch eingreifen kann, einen Einsatz aber ebenso rasch wieder zu beenden vermag. Man endet nicht immer notwendigerweise in einem Sumpf.
2. Die Nato und ihre Partnerstaaten haben einen politischen Zusammenhalt bewiesen, den ich mir so nicht vorstellen konnte. Wenn ich Ihnen vor 12 Jahren gesagt hätte. dass 28 Nato-Staaten und 22 Partnerstaaten zweimal länger in Afghanistan kämpfen werden, als der Zweite Weltkrieg gedauert hat, hätten Sie mir nicht geglaubt, und ich auch nicht. Die politische Kohäsion des Westens – nicht als geografische, sondern als politische Kategorie verstanden - war trotz Opfer und immenser Kosten erstaunlich.
3. Eine Allianz wie die Nato braucht zwar ein Rational, um ihre Existenz zu rechtfertigen, nicht aber notwendigerweise Grosseinsätze. Diese hatte sie auch in der Vergangenheit nicht. Es gab für sie ein Rational, so wie es ein Rational für eine Feuerversicherung gibt, auch wenn es lange nicht brennt. Angesichts weltweiter Risiken und Gefahren gibt es ein Rational für die Nato. Es macht Sinn, eine Allianz zu haben, weil man in einer Gruppe die Verteidigung besser organisieren kann als alleine. Niemand wird dieses Rational ernsthaft bestreiten wollen.
4. Der "transatlantic link“ der europäisch-amerikanischen Verbindung, die immer wieder totgesagt wird, ist viel stabiler, als man glaubt. Der Grund ist, dass diese Verbindung beiden Seiten nutzt. Trotz aller Diskussionen über mangelnde Lastenteilung und der Klagen der USA, dass die Europäer nicht genug bezahlten, und der Europäer, dass die USA alles ohne Konsultation alleine machten, sind zwei Dinge wichtig:
   Erstens sind die USA in Europa nicht aus Grossmut in Europa stationiert, sondern weil es ihren Interessen dient. Staaten sind keine Wohlfahrtsunternehmungen, und die USA würden das Geld für die Stationierung nicht ausgeben, wenn es sich nicht in Einfluss ummünzen würde. Die USA sind durch ihren Einfluss in Europa eine europäische Macht. Sie finden keinen anderen Kontinent, der gleichzeitig mehr oder weniger geeint und stabil, wohlhabend (immer noch) und aus US-Sicht "politically likeminded", d. h. zutiefst demokratisch ist. *Zweitens* profitiert Europa umgekehrt von amerikanischem Schutz. Für Deutschland und Portugal ist dieser nicht mehr so wichtig, für Polen und die baltischen Staaten aber sehr wohl. Zudem profitiert Europa von der Rolle der USA als globale Ordnungsmacht, und alle - auch die Schweiz - profitieren von den USA, weil sie die "global comments" sichern, d. h. "freedom of communication", Seewege, Satelliten, Weltraum

usw. Wenn es so ist, dass beide Seiten ihren Nutzen haben, bedeutet die transatlantische Beziehung keine Lastenteilung, sondern eine Nutzenteilung.

5. Die Nato wird nach 2014 ihren Betrieb nicht einstellen; sie hat eine Reihe von Aufgaben neben dem Afghanistaneinsatz. Sie bleibt weiter auf dem Balkan oder am Horn von Afrika engagiert, sie führt militärische Übungen durch, plant für Eventualitäten, entwickelt Standards für gemeinsames militärisches Handeln, pflegt Partnerschaften mit Ländern und Institutionen ausserhalb des Bündnisses und konsultiert die Mitgliedsländer im Falle aufziehender Sicherheitsgefährdungen – wenn auch meiner Meinung nach nicht genügend.

B) Gefahren und Trends

Auch wenn ich also der Meinung bin, dass wir aus den erwähnten Gründen besser dastehen als nach dem Fall der Mauer, heisst das nicht, dass es keine Probleme gibt. Es gibt nach wie vor "challenges", Risiken, Gefahren, oder welchen Begriff man auch wählen will. Ich möchte fünf Trends nennen, die nicht notwendigerweise eine Bedrohung sein müssen, aber zu einer werden können.

Trend 1: Die Finanzkrise

Soweit ich das als wirtschaftlicher Laie beurteilen kann, unterscheidet sich die Finanzkrise von früheren solchen Krisen dramatisch. Es ist nicht das erste Mal, dass Verteidigungshaushalte zu gering sind, und ich habe noch nie einen General sagen hören, dass er zu viel Geld habe. Diese Finanzkrise unterscheidet sich aber im Hinblick auf Sicherheitspolitik in drei Aspekten von den vorhergehenden:

1. Sie hat eine andere Dimension; sie ist grösser und intensiver.
2. Zum ersten Mal sind auch die "big spender“ - die USA, Frankreich, Grossbritannien - im militärischen Bereich betroffen. Die USA müssen zum ersten Mal kürzen, und es ist für sie eine völlig neue Erfahrung, dass man sicherheitspolitische Probleme nicht einfach mit mehr Geld lösen kann.
3. Sie dauert länger. Wir sprechen von Jahren, wenn nicht Jahrzehnten. Die griechische Handelskammer rechnet mit einer Dauer von 20 Jahren. Das ist wahrscheinlich noch sehr optimistisch. Es gibt schon Personen, die vom "finanziellen Dreissigjährigen Krieg" sprechen.

Die Folge dieser drei Aspekte ist *erstens*, dass es keine Chance für eine Erhöhung der Verteidigungsausgaben gibt, egal was sich die Politiker gegenseitig versprechen. Es gibt ganz wenige Ausnahmen, zum Beispiel Polen. Der Erhalt gewisser Levels ist schon ein Erfolg. Allgemein ist es so, dass das Militär in Zukunft mit dramatisch weniger Geld auskommen muss. Es gibt da auch keine Wundermittel wie Pooling and Sharing. Ein Generalsekretär sagte einmal, dass Pooling and Sharing bedeute, dass wir "more with less" machen. Das gibt es nicht. Es gibt nur "less with less“. Pooling and Sharing oder Smart Defence, d. h. eine militärische Kooperation und Rationalisierung, machen sehr viel Sinn, egal ob wir eine Finanzkrise haben

oder nicht. Aber man spart durch Kooperation nicht viel, und es ist eine Illusion, zu glauben, dass dadurch die Kürzungen kompensiert würden.
Zweitens birgt die Finanzkrise aufgrund ihrer Dauer eine Destabilisierungsgefahr für Südosteuropa. Es gibt Personen, die von einer Balkanisierung Südosteuropas sprechen. Was ist damit gemeint? Es ist anzunehmen, dass die Finanzkrise in Ländern wie Griechenland, aber auch Spanien und Italien zehn oder zwanzig Jahre dauert. In Italien zum Beispiel hat das Kürzen noch gar nicht angefangen. In Ländern wie der Schweiz, Deutschland, Polen usw. haben die Jugendlichen gute, faire Chancen, ihre Träume, zum Beispiel ein grosses Auto, viel Geld usw. zu erreichen. Ein griechischer Jugendlicher hat diese Chancen nicht, höchstens vielleicht wenn er sein Land verlässt. Wenn es um relativ kurze Zeiträume geht - drei, vier, fünf Jahre -, sind solche Situationen noch vertretbar. Ich weiss aber nicht, wie sich die innenpolitische Situation in Ländern wie Portugal oder Griechenland, wo wir schon jetzt Gewalt auf den Strassen sehen, nach zehn Jahren der Perspektivlosigkeit entwickeln wird. Rational müssten sich die Leute dort sagen, dass sie sich das eingebrockt haben, und nun schauen müssen, wie sie aus dieser Situation wieder herauskommen. Das wird aber nicht geschehen, sondern man wird die Vereinfacher, die Extremisten haben, die sagen, dass ein anderes Land schuld ist, zum Beispiel die Türkei oder Deutschland. Die Gefahr eines "spillover" besteht. Ich weiss nicht, was man in dieser Situation machen soll. Sie ist keine Aufgabe für die Nato; die Nato wird keine Anti-Riot-Teams dorthin schicken. Diese Situation betrifft uns aber alle, und sie gibt zu grosser Sorge Anlass.

Trend 2: Die Reorientierung der USA zur Asien/Pazifikregion
Dieser sogenannte pivot ist nicht so dramatisch, weil er nicht bedeutet, dass sich die USA von Europa abwenden. Sie machen das, was eine vernünftige Weltmacht tut: Sie geht dorthin, wo es "more unfinished business" gibt. Aus europäischer Sicht ist deshalb dieser "pivot" eigentlich eine positive Entwicklung, weil er zeigt, dass es in Europa weniger "unfinished business" gibt und dass die Problemzonen andernorts liegen. Allerdings stellt sich für Europa die Frage, was das für uns heisst. Müssen wir uns auch zu diesen Regionen hin orientieren, oder können wir uns nach wie vor auf Europa beschränken? Falls wir auch in irgendeiner Form im asiatisch/pazifischen Raum handlungsfähig sein wollen, stellt sich die Frage, wer dazu fähig ist und welche Beschaffungsmassnahmen ergriffen werden müssten. Für die Schweiz ist das nicht ganz so wichtig, aber Staaten, die eine Seestreitkraft haben, müssten sagen, dass sie das Maritime stärken müssten, wenn sie in diesem Raum agieren möchten. Die Europäer entscheiden nicht entsprechend, sondern gegenteilig. Die Frage ist, ob das zu einem Problem werden wird.

Trend 3: Die kontinuierliche Verschlechterung der Beziehungen zu Russland
Diese Verschlechterung liegt weder nur an den Russen noch nur an uns. Man lebt sozusagen auf unterschiedlichen Planeten. Putin ist kein lupenreiner Demokrat, auch wenn das ein deutscher Kanzler einmal gesagt hat. Der Ton aus Moskau ist sehr rau geworden. Man ist sich seiner eigenen vermeintlichen Stärke bewusst. Ich glaube aber nicht, dass diese Stärke da ist. Ich glaube, dass die Pfeiler, auf welchen die russische Rhetorik ruht, sehr hohl sind. Denn der

allgemeine internationale Einfluss Russlands ist dramatisch zurückgegangen. Man hat einfach kleine Triumphe wie jetzt in Syrien. Die Rolle Russlands ist aber auch primär deshalb schwächer geworden, weil Russland in den letzten zehn, fünfzehn Jahren jegliche Modernisierung versäumt hat, sowohl wirtschaftlich, politisch, gesellschaftlich als auch militärisch. Deshalb stellt Russland in dieser Form keine direkte Bedrohung dar. Aber es ist ein Problemfall, der grösser wird. Die Aussichten für Russland sehen aus russischer Sicht nicht gut aus. Wenn man die Entwicklung beim Schiefergas betrachtet, wird klar, dass die gegenwärtige Situation nur noch ein paar Jahre dauern wird, nämlich solange die Energieexporte den Haushalt noch decken. Danach ist die Party in Russland vorbei, und man hat keine Rücklagen gemacht, und überlegt, was man danach macht. In Russland ist der Phantomschmerz des untergegangenen Imperiums immer noch stark. Die Lücke, die sich zwischen Anspruch und Wirklichkeit russischen Grossmachtdenkens auftut, wird immer grösser oder mindestens bleiben. Wir werden immer mit einer aggressiven Rhetorik konfrontiert sein, die mit den Realitäten nicht sehr viel zu tun hat. Das bedeutet, dass das Verhältnis politisch konfrontativer werden wird, doch wird es nicht notwendigerweise zu einer militärische Konfrontation kommen. Das ist auch nicht das Bedrohungsszenario, das den baltischen Staaten Sorgen macht. Sie befürchten nicht einen Angriff, sondern eher ein Szenario wie in Georgien. Dabei würden gezielt die Minderheiten in den östlichen Regionen angestachelt. Wenn sie dann protestieren und man dagegen vorgeht, sagt Russland, dass es seine Minderheiten schützen müsse. So etwas kann Russland sehr wohl tun. Russlands Kraft ist also eher eine "nuisance-power“ als eine gestaltenden Kraft. Russland gestaltet nicht, es gestaltet auch im Nahen Osten nicht. Aber es ist ein Problem, das sich auftut.

Trend 4: Die Entwicklungen in der arabischen Welt

Der Begriff Arabischer Frühling ist nicht mehr angemessen, weil wir es eher mit einem islamischen Winter zu tun haben, der sehr lange dauern wird. Experten dieser Region sagen, dass im besten Fall jetzt das passiert, was in Europa vor 500 Jahren passiert ist, nämlich die Aufklärung. So etwas dauert lange, ist schmerzhaft, fordert Opfer, und niemand weiss, wohin die Reise geht. Das Problem, das sich uns dadurch stellt, sehen wir jetzt in Syrien. Ich persönlich bin nicht davon überzeugt, dass es die Aufgabe der Nato ist, sich in Bürgerkriegen im Nahen Osten zu engagieren. Ich war von der Libyenaktion nicht begeistert. Obschon sie militärisch ein Erfolg war, hat sie nicht viele Probleme gelöst. Das Problem ist, dass wir weitere Libyens oder Syriens haben werden. Man wird dann immer auch von den Bürgern hören, dass man etwas tun muss, dass man das nicht so hinnehmen kann. Die Frage ist dann wer "man" und was "etwas" ist. Wir werden deshalb immer - auch in der Nato und auch über die Nato hinaus - eine Streitfrage haben. Ein, zwei Staaten entscheiden sich, etwas zu tun, oder auch nicht - die USA sind sehr sprunghaft. Es geht dann darum, wer mitmacht und wer nicht, und es kommt zu Syrienszenarien, wo die einen der Bündnisflucht bezichtigt werden usw. Somit haben wir einen ständigen Spaltpilz in der Allianz und darüber hinaus.

Trend 5: Die Renaissance von Nuklearwaffen. Dieser Punkt mag aus schweizerischer Sicht etwas weiter weg liegen, er ist aber konkret. Der Traum von der nuklearwaffenfreien Welt (Obama Prag 2008) wird sich nicht realisieren lassen. Der Grund ist nicht nur, dass man die-

ses Ziel nicht erreichen kann, sondern - das haben die Befürworter dieser Idee nicht begriffen – weil eine Vielzahl von Staaten es nicht erreichen will. Israel, Frankreich, Indien, China, Russland wollen ihre Atomwaffen nicht aufgeben. Ob wir das verstehen, ist eine andere Frage. Aber die genannten Länder sehen das so. Wir stellen den gegenteiligen Trend fest, dass sich Länder wie Iran oder Nordkorea stärker an den Nuklearbereich annähern. Ich glaube, dass weitgehend Konsens besteht, dass Iran versucht, Nuklearwaffen zu bekommen. Die Frage ist, wann es soweit ist. Wenn Iran belegen wird, dass es dem nuklearen Klub beigetreten ist, stellen sich alle Fragen der Vergangenheit über Abschreckung, "commitments", Bündnisse völlig neu bzw. stellen sie sich von Neuem.

Diese fünf Trends sind meine grossen Sorgenkinder. Sie werden bei dieser Aufzählung wahrscheinlich einige Schlagworte vermisst haben, die man sonst immer hört, nämlich die sogenannten emerging challenges, d. h. Terrorismus, Cybersicherheit und Energiesicherheit. Diese Herausforderungen sind auch wichtig. Aber ich glaube nicht, dass sie für Militärbündnisse oder für den militärischen Aspekt so wichtig sind, wie es in den letzten Jahren schien. Auch Afghanistan hat dazu beigetragen, dass wir für diese Bereiche eine Redefinition vornehmen. Ich erläutere das für die genannten drei Schlagworte:
Terrorismus: Terrorismus war die allumfassende Gefahr; alles wurde nach dem 11. September 2001 mit Terrorismus gerechtfertigt. Zum Glück gab es keinen zweiten 11. September, obwohl wir alle damals dachten, dass es eigentlich einfach ist, ein Flugzeug irgendwo hin zu steuern und einen Anschlag zu verüben. Voraussetzung ist allerdings, dass man Leute hat, die bereit sind, zu sterben. Man kann sagen - da kann ich nur Einschätzungen wiedergeben - dass Al Kaida nicht mehr als strategischer Akteur existiert, der in der Lage ist, so etwas zu wiederholen. Al Kaida existiert nach wie vor - in einer vielleicht viel schwierigeren Form - als "franchising" in Jemen und anderswo. Wir haben aber eine andere Situation, und wir müssen Terrorismus redefinieren und unsere Bedrohungsvorstellungen ändern.
Cybersicherheit: Hier lässt sich Ähnliches sagen wie bei der Terrorismusgefahr. Datensicherheit ist ein dramatisches Problem, weil es all unsere Lebensbereiche betrifft. Es hat aber wenig mit dem Militärischen zu tun. Ich bin deshalb immer erstaunt, wenn man von "cyber war" spricht. Natürlich muss das Militär seine Netze schützen, und es gibt täglich Tausende von Angriffen in der Nato. Aber bei einem wahrscheinlichen Angriff auf die Flugsicherheit am Zürcher Flughafen oder auf das Bankensystem in der Schweiz oder auf die Stromverteilungsnetze in den USA holt man nicht das Militär. Man ruft auch nicht die Nato. Mit anderen Worten kann die Nato als Allianz, kann das Militär in solchen Fällen wahrscheinlich unterstützend tätig werden – ich wiederhole wahrscheinlich -, aber es ist kein Hauptakteur. Wir vermischen die Dinge, wenn wir dieses Thema in die Sicherheitspolitik hineinbringen.

Energiesicherheit: Hier gilt das Gleiche. Natürlich ist die Energieversorgung für viele Länder wichtig. Aber schickt man das Militär, wenn es zu einer Energiekrise zwischen der Ukraine und Russland kommt? Senator McCain sagte am einem Nato-Gipfel in Riga, dass die Nato einen "Energie Artikel 5" einführen müsse, um ihre Mitglieder zu schützen. Damals stand Polen in der Gefahr, das Energienetz abgestellt zu bekommen. Wir fragten uns dann, was ein

solcher Energie-Artikel bedeuten würde. Versorgen wir die Bedrohten mit Energie? Oder schicken wir die Armee nach Russland, um den Staat daran zu hindern, Energienetze abzuschalten? Das ist nicht klar. Da arbeiten wir mit falschen Begriffen.

C) Die Nato im Winterschlaf?

Was heisst nun das alles? Nach Afghanistan gibt es gewisse Probleme, aber die Nato und die Sicherheitspolitik stehen besser da. Trotzdem gibt es sicherheitspolitische Gefährdungen. Heisst das, dass die militärische Sicherheitspolitik sozusagen auf Standby geht, dass die Nato in den Winterschlaf fällt? Ich glaube es nicht, obwohl wir zwei Schwierigkeiten haben. Erstens haben wir weniger finanzielle Mittel, und zweitens wird Europa von den USA weniger beachtet. Die Nato hat deshalb weniger Relevanz. Trotzdem wird sie nicht auf Minimalbetrieb schalten. Sie wird erstens das tun, was ihre ureigene Aufgabe ist: Sie wird das Territorium, die Bürger und - das durfte man vor fünf Jahren noch nicht sagen - die vitalen Interessen ihrer Mitgliedstaaten schützen, wann und wo immer erforderlich, d. h. auch ausserhalb Europas. Es gibt immer noch Artikel-5-Szenarien. Ein Raketenangriff Nordkoreas auf Alaska würde Artikel 5 betreffen und den Nato-Bündnisfall auslösen. Ein Krieg zwischen Israel und Iran, in dessen Folge Iran die Strasse von Hormus sperren würde, betrifft Artikel 5 nicht. Aber die Nato würde in einem solchen Fall nicht tatenlos zusehen. Natürlich würden sich alle 28 Nato-Staaten daran beteiligen, und ich gehe davon aus, dass vorausschauende Militärs das auch planen, nicht als Nato, sondern als Staaten, um dann handeln zu können. Gleiches gälte für verheerende Cyber-Angriffe, wenn sie über das hinausgehen sollten, was man mit zivilen Mitteln bekämpfen kann.

Allerdings dürfte es in der Nato und in der militärischen Sicherheitspolitik mindestens drei grundsätzliche Veränderungen geben:

1. Bedeutung der Nato wird graduell abnehmen. Sie ist schon weniger wichtig geworden, als sie es vor zwanzig Jahren war, auch deshalb, weil die Streitkräfte in den meisten Mitgliedsländern schrumpfen werden. Sie wird auch deshalb an Relevanz verlieren, weil sie eine ihrer Kernaufgaben selber nicht wahrnehmen will. Was meine ich damit? Die Nato hat sich im strategischen Konzept drei Kernaufgaben gegeben: *erstens* Selbstverteidigung nach Artikel 5, *zweitens* Krisenmanagement ausserhalb des Bündnisgebietes und *drittens* Partnerschaften mit Nicht-Mitgliedern, und zwar hierarchisch in der genannten Reihenfolge. Die Nato hat aber immer weniger Appetit auf Krisenmanagement, auch weil man nach Afghanistan und Libyen gesehen hat, wie wenig man erreicht. In Syrien würde man sehen, wie wenig man erreichen würde, wenn man handelte. Man ist im Blick auf das, was man machen kann, sehr bescheiden geworden. Dazu kommt, dass auch die Bürger dieses Krisenmanagement nicht mehr wollen. Der schiere Hinweis auf humanitäre Katastrophen reicht nicht mehr aus, um Staaten zur Intervention zu bewegen. Es müssen vitale Interessen betroffen sein, wobei die Definition von "vitalen Interessen" sehr dehnbar ist. Ich glaube deshalb nicht, dass die Nato in Syrien handeln wird, und sie wird es wahrscheinlich auch bei allen künftigen Krisen nicht tun.

2. werden ein europäisches Führungsvakuum haben. Das gilt nicht nur für die Nato, sondern auch darüber hinaus. Es werden immer wieder zwei Dinge gesagt, die es aber beide nicht geben wird.
Erstens wird gesagt, dass die Europäer die Führung übernehmen müssen, dass die drei grossen europäischen Nato-Staaten Deutschland, Frankreich und Grossbritannien vorangehen und die USA ersetzen könnten.
Zweitens wird gesagt, dass die Europäer endlich mit der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) Ernst machen müssten.
Beides wird es auf absehbare Zeit nicht geben. Der Grund ist schlichtweg, dass wir in Europa selbst unter den grossen Staaten keine gemeinsamen Positionen und Prioritäten und nicht einmal eine gemeinsame strategische Kultur haben, um ein schwindendes amerikanisches Engagement ersetzen zu können. Deshalb wird die ESVP auf Jahre hinaus so bleiben wie sie ist. Als Ankündigung ist sie sicher eine gute Idee, aber es passiert damit nichts. Sicherheitspolitik passiert - wenn überhaupt - in der Nato. Man sieht das täglich, und wenn es eines letzten Beweises bedurft hätte, so wäre das Libyen gewesen. Wenn es eine Krise gab, für die die ESVP geschaffen wurde und für die "battle groups" geschaffen worden sind, so war das Libyen. Die USA wollten in der Nähe Europas nicht mitmachen, das Geschehen war aber für die europäischen Staaten von zentralem Interesse. Nachdem selbst da ein gemeinsames europäisches Handeln nicht möglich war, existiert die Sicherheits- und Verteidigungspolitik der EU nur auf dem Papier.

3. Nato wird ihre dritte Kernfunktion – die kooperative Sicherheit durch Partnerschaften - verstärken. Sie wird stärker mit internationalen Partnern, Nicht-Nato-Staaten zusammenarbeiten. Die Schweiz ist einer dieser Staaten. Das wird auf globaler Ebene geschehen. Der Grund ist, dass Partnerschaften für beiden Seiten von Vorteil sind. Für die Partner bietet eine Partnerschaft mit der Nato vor allem militärische Kooperation. Daran sind ganz viele Staaten äusserst interessiert, weil die Nato den Goldstandard für Interoperabilität setzt.
Die Nato ihrerseits bekommt durch Partnerschaften auch auf globaler Ebene - mit Australien, mit Staaten im Mittleren und im Nahen Osten - drei Dinge. Sie bekommt *erstens* (manchmal) Hilfe in ihren Operationen - siehe Afghanistan. Sie bekommt *zweitens* Einfluss in den Partnerregionen. Dieser ist zugegebenermassen nicht sehr gross, aber man wird wenigstens wahrgenommen. Es gibt Kontakte zwischen der Nato und der African Union oder der Arab League. Das ist bescheiden, aber ausbaufähig. *Drittens* bildet die Nato durch die Ausbildung von Partnernationen in Regionen wie Afrika oder dem Nahen Osten diese Staaten aus, damit sie ihre sicherheitspolitischen Krisen selber lösen können. Damit mindert die Nato den Druck, selbst intervenieren zu müssen. Bei der African Union sieht man erste Erfolge im Hinblick auf Somalia.

Das ist das Rational von Partnerschaften, und die Nato wird sie stärker aufbauen. Meine persönliche Meinung ist, dass die Nato eine stärkere und privilegierte Partnerschaft mit demokratischen Staaten wird aufbauen müssen, also mit Ländern wie Australien, Schweden, die

Schweiz oder Neuseeland. Denn ich glaube, dass Partnerschaften nicht hierarchiefrei sein können. Wenn sowohl die Schweiz als auch Weissrussland Mitglieder von "Partnership for Peace" sind, ist etwas falsch. Der Grad der Kooperation muss je nach Staat unterschiedlich sein. Das gleiche gilt für globale Partner wie Australien, Japan oder Südkorea. Diese sagen, dass sie von dem, was die Nato macht, unweigerlich betroffen werden. Sie fordern deshalb ein bisschen Mitsprache als Preis für ihre Unterstützung. Wenn diese Mitsprache schon nicht beim "decision making" - das ist den Mitgliedern vorbehalten – möglich ist, so möchten sie sie zumindest beim "decision shaping", d. h. bei der Konsultation erhalten. Ich glaube, dass die Nato langfristig für solche privilegierte Partner ein Gremium unterhalb der Mitgliedschaft schaffen wird, sozusagen eine "Red Carpet Lounge". Wir hatten dazu schon grosse Diskussionen in Brüssel. Ich finde, dass eine "Red Carpet Lounge" einen gewissen Sinn hat. Es wird die Frage zu lösen sein, wer die goldene Kundenkarte kriegt. Aber von der Logik her sehe ich keine Alternative zu einem solchen Modell.

Die Nato wird sich also nicht dem Winterschlaf hingeben können. Sie wird in einer Welt, in der wir nach wie vor Angriffe auf Datennetze, nukleare Gefahren und auch Terrorismus in anderer Form haben, mit ihren Aufgaben vollends ausgelastet sein.

Statement by Prof. Andreas Wenger

Leiter Center for Security Studies (CSS), ETH Zürich

"Schweizerische und europäische Sicherheit"

Bern, 4 September 2013

Für seine Präsentation baten wir um die Beantwortung folgender Fragen:

1. ***Welches sind die (realen) Bedrohungstrends, welches möglicherweise nur konjunkturelle oder aus politischen Gründen hochgespielte Modethemen (z.B. Cyber, Lenkwaffen mittlerer oder grosser Reichweite)?***
2. ***Welche Bedrohungen und Gefahren sollten für die Sicherheitspolitik der Schweiz in den nächsten 10-20 Jahren im Vordergrund stehen? Was ist neu, was nicht? Und welche Bedrohungen oder Gefahren werden weniger wichtig?***
3. ***Wie ist die derzeitige Lage und Entwicklung Europas einzuschätzen, was bedeutet das aus sicherheitspolitischer Sicht für die Schweiz?***
4. ***Wie sollte die Schweizer Armee aufgrund der Bedrohungslage und -entwicklung ausgerichtet werden, was sollten künftig ihre schwergewichtigen Aufgaben sein?***

Ich freue mich sehr, dass ich an diesem Hearing zum neuen Sicherheitspolitischen Bericht mitwirken darf. Wenn man sich mit einem Thema dauernd und sehr intensiv beschäftigt, fragt man sich immer, wie viel Neues man noch zu sagen hat. Ich hoffe aber, dass ich doch den einen oder anderen neuen Gedanken in die Diskussion einbringen kann. Die Hearings konzentrieren sich bewusst auf das Thema Bedrohungslage/Bedrohungsanalyse. Mir wurden dazu vier Fragenkomplexe zugestellt. Ich werde mich in meinen Ausführungen an diesen vier Fragen orientieren, mir aber auch erlauben, zu weiteren Punkten, die mir wichtig erscheinen, Stellung zu nehmen.

1. Frage: Welches sind die (realen) Bedrohungstrends, welches möglicherweise nur konjunkturelle oder aus politischen Gründen hochgespielte Modethemen (z.B. Cyber, Lenkwaffen mittlerer oder grosser Reichweite)

Diese erste Frage führt uns gleich zu einem Grunddilemma heutiger Sicherheitspolitik. Sie suggeriert, dass man klar zwischen realen Bedrohungen und hochgespielten Bedrohungen unterscheiden kann. So einfach ist dies nicht, insbesondere wenn wir einen Bedrohungshorizont von 10 bis 15 Jahren anschauen. Bedrohungen sind letztendlich immer auch eine Frage der Perzeption, und diese kann sich manchmal überraschend schnell wandeln. Je mehr Gefahren möglicherweise für die Sicherheit eines Landes relevant sind und je weniger gesichertes

Wissen wir dazu haben, desto schwieriger wird die politische Beurteilung der Bedrohungslage. Das ist das Dilemma der heutigen Sicherheitspolitik.

Das Hauptmerkmal der heutigen Bedrohungslage ist ihre begrenzte Berechenbarkeit. Das Bedrohungsspektrum wird durch Ungewissheit zu vielen Gefahrenherden charakterisiert: Welches sind die Akteure, von welchen geografischen Räumen gehen die Bedrohungen aus, welche Wirkungen und Kaskadeneffekte haben wir zu erwarten, wenn wir in Szenarien denken?
Wir haben es mit Bedrohungen von grosser Komplexität und mit teilweise weit entfernten geografischen Wurzeln zu tun. Das hat Rückwirkungen für die Bedrohungspolitik, also für den politischen Umgang mit dem Thema Bedrohungsanalyse. Aufgrund der Erfahrung der vergangenen Jahre können wir für die nächsten zehn Jahre davon ausgehen, dass die politische Beurteilung von sicherheitspolitischen Gefahren und Bedrohungen Schwankungen unterworfen sein wird. Wenn wir schauen, wie staatliche Akteure in ihren Papieren zur Bedrohungslage agiert haben, sehen wir zwei unterschiedliche Verhaltensweisen. Bei der einen Verhaltensweise haben wir Strategiepapiere mit langen abstrakten Gefahrenlisten, ohne dass von konkreten Akteuren und Interessenräumen gesprochen wird, und es wird auch keine eigentliche Gewichtung und Priorisierung der Gefahren vorgenommen. Bei der zweiten Verhaltensweise wird die politische Debatte von einzelnen Gefahrenkategorien dominiert, insbesondere nach Schlüsselereignissen. Das Thema Terrorismus erhielt nach den Ereignissen vom 11. September 2001 in den darauffolgenden fünf bis zehn Jahren grössere Aufmerksamkeit als in den zehn Jahren zuvor.
Schwankungen in der politischen Beurteilung der Bedrohungslage sind wie die begrenzte Berechenbarkeit eine Herausforderung für die Sicherheitspolitik, weil es schwer fällt, strategische Prioritäten zu setzen und dadurch auch eine nachhaltige Planung der sicherheitspolitischen Mittel schwierig ist. Cyberwaffen, Lenkwaffen und Terrorismus werden erst zu konkreten Bedrohungen, wenn wir sie zumindest implizit mit Akteuren, deren Möglichkeiten und Absichten, sowie mit geografischen Räumen verknüpfen, wenn wir sie also implizit in Szenarien einbetten. Ob wir das auch explizit machen, ist eine andere Frage. Aber eine Lenkwaffe ist nicht notwendigerweise eine Bedrohung. Es kommt darauf an, in welchen Händen sie sich befindet.
Ich möchte mich deshalb im Folgenden für die Beantwortung der zweiten Frage nicht auf einzelne Bedrohungskategorien konzentrieren und diese einzeln bewerten, sondern diese zu vier grösseren Bedrohungstrends bündeln.

2. Frage: Welche Bedrohungen und Gefahren sollten für die Sicherheitspolitik der Schweiz in den nächsten 10 bis 20 Jahren im Vordergrund stehen? Was ist neu, was nicht? Und welche Bedrohungen oder Gefahren werden weniger wichtig?
Die beiden ersten Bedrohungstrends können eher aus den Entwicklungen im globalen Umfeld der Schweiz abgeleitet werden, und die Trends 3 und 4 eher aus den Entwicklungen an der europäischen Peripherie.

Ich gehe zuerst auf das globale Umfeld ein. In den letzten drei bis fünf Jahren konnten wir unschwer zunehmende machtpolitische respektive geopolitische Rivalitäten zwischen den Grossmächten feststellen. Die letzten Jahre haben deutlich werden lassen, dass dem ordnungspolitischen Willen und den ordnungspolitischen Möglichkeiten des Westens - der USA und der Europäer - zunehmend Grenzen gesetzt sind. Wir erleben das gegenwärtig wieder in der Syrienfrage. Gleichzeitig sehen wir aber auch, dass die aufsteigenden asiatischen Mächte keine kohärente aussen- und sicherheitspolitische Agenda verfolgen, sondern primär auf ihre innere Konsolidierung ausgerichtet sind. Wir haben also globale Machtverschiebungen vom Westen in den Osten, sowohl im ökonomischen aber teilweise auch im militärischen Bereich. Die positive Einschätzung dieser globalen Machtverschiebungen besteht darin, dass direkte militärische Konflikte zwischen den Grossmächten unwahrscheinlich bleiben. Die negative Einschätzung besteht darin, dass ich nicht davon ausgehe, dass der Multilateralismus in den nächsten zehn Jahren besonders effizient und effektiv sein wird. Diese Entwicklungen bilden den Hintergrund für zwei Bedrohungstrends, die auch für die Schweiz Rückwirkungen haben können.

Trend 1: Politisierung der Global Commons. Es geht um See, Weltraum, Cyberraum. Diese Domänen sind bis anhin noch wenig reguliert, und wir sehen nun zunehmend politische Auseinandersetzungen um die Regulierung dieser Gebiete. Damit verknüpft können Unterbrüche in der Globalisierungsinfrastruktur entstehen. Stichworte sind Kommunikations-, Handels-, Energie- und Finanzmärkte und -netzwerke, die unterbrochen werden können. Das kann natürlich auch Rückwirkungen auf die Versorgungssicherheit und den wirtschaftlichen Wohlstand in der Schweiz haben.

Trend 2: Politisierung der Wirtschafts- und Finanzbeziehungen. Die liberale Wirtschaftsordnung wird nicht global unterstützt. Nicht nur in China, sondern teilweise auch in westlichen Staaten gibt es vermehrt staatliche Eingriffe in Märkte, und zum Teil sehen wir eine Integration von Handels- und Sicherheitspolitiken. Diese Entwicklung geht mit mehr politischen Druckversuchen an der Schnittstelle zwischen Wirtschaft und Sicherheit einher. Eines der Stichworte, das auch für die Schweiz relevant ist, ist die Wirtschaftsspionage. Die Schweiz hat als politisches Leichtgewicht, aber wirtschafts- und finanzpolitisches Mittelgewicht diese Druckversuche in den vergangenen fünf Jahren bereits in Bezug auf die Finanzplatzstrategie und das Bankgeheimnis zu spüren bekommen.

Die Bedrohungen, die von der europäischen Peripherie ausgehen, sind für mich noch relevanter für die Sicherheit der Schweiz als die Bedrohungen, die sich aus den globalen Entwicklungen ergeben, besonders auch mit Blick auf die nächsten zehn Jahre. Europa ist zunehmend von Zonen der Instabilität umgeben - Nordafrika, Afrika, Naher und Mittlerer Osten, Kaukasus, Südasien. Die Konzentration von politischen Gewaltkonflikten, die wir dort sehen, kann Rückwirkungen auf die Schweiz haben. Es gibt regionale Machtverschiebungen, zum Beispiel durch den Aufstieg der Türkei und den Rückzug der USA aus dem Nahen und Mittleren Osten, durch die Zusammenarbeit zwischen dem Iran und gewissen Gruppierungen in Syrien

sowie in Südasien im Dreieck zwischen China, Indien und Pakistan. Diese Machtverschiebungen im Staatensystem gehen mit einer Beschleunigung der Weiterverbreitung von Massenvernichtungsmitteln, -technologien und den dazugehörigen Trägersystemen einher. Ich knüpfe diese Entwicklung an die Machtverschiebungen im Staatensystem, weil mehrheitlich staatliche Akteure dahinter zu sehen sind. Diese Machtverschiebungen bilden den Hintergrund für zwei weitere zentrale Bedrohungstrends.

Trend 3: Wiederkehrende Bürgerkriege. Wir können davon ausgehen, dass sich auch in den kommenden zehn bis fünfzehn Jahren Bürgerkriege auf die skizzierten Zonen der Instabilität konzentrieren werden. Diese Bürgerkriege können indirekte, meist nichtmilitärische Rückwirkungen auf die Sicherheit der Schweiz haben. Beispiele sind Unterbrüche in den Versorgungssystemen, krisenbedingte Migrationsströme, Spannungen zwischen Minderheiten, die sich in der Schweiz widerspiegeln. Dieser Trend scheint mir sehr robust und zudem auch relevant für die Schweiz zu sein.

Trend 4: Überlagerung durch transnationale Gefahren. Überall, wo es Bürgerkriege gibt, gibt es auch rechtsfreie Räume. In diesen rechtsfreien Räumen können sich transnationale Gefahren einnisten, verknüpft mit Extremismus/Radikalisierungstendenzen, terroristischen Gruppierungen und organisierter Kriminalität. Das Gewaltpotenzial und die Gefahr nehmen tendenziell zu, dass nichtstaatliche Akteure Gewalt gegenüber Schweizer Bürgern und Bürgerinnen sowie Einrichtungen anwenden, und zwar sowohl im Inland als auch im Ausland. Das hat unter anderem auch damit zu tun, dass nichtstaatliche Akteure vermehrt Zugriff zu neuen Waffentechnologien haben. Ich würde in diesem Bereich auch ganz bewusst Cyberterrorismus und Cybercrime anführen.

Wo konzentrieren sich diese Gewaltkonflikte geografisch, und mit welchen Typen von Gewaltkonflikten haben wir es zu tun? Auf diese Fragen kann man mindestens generisch relativ robuste Antworten geben.
Geografisch konzentrieren sich die substaatlichen, also innerstaatlichen Konflikte auf Afrika, den Mittelmeerraum, den Nahen bis Mittleren Osten, den Kaukasus und Südwestasien. Es gibt genügend strukturelle Entwicklungen - wirtschaftliche Schwächen, politische Schwächen, Marginalisierung aufgrund der globalen Erwärmung, Wasserknappheit, dominante Abhängigkeit von Energieexporten usw. -, die darauf hinweisen, dass sich Bürgerkriege auch in den kommenden zehn Jahren auf diese Regionen konzentrieren dürften. Im Vergleich zur Situation anlässlich der letzten Hearings im Jahr 2009 hat der Destabilisierungstrend im Mittelmeerraum und im Nahen Osten zugenommen.
Bei der Typologie von Konflikten zeigt es sich, dass der klassischen Kriege zwischen Staaten sehr selten geworden ist und der Bürgerkrieg die dominante Konfliktform darstellt. Das ist nicht neu, aber man muss es sich wieder in Erinnerung rufen. Gerade in einer Region wie der arabischen Welt können sich Bürgerkriege zudem rasch internationalisieren.

3. Frage: Wie ist die derzeitige Lage und Entwicklung Europas einzuschätzen, was bedeutet das aus sicherheitspolitischer Sicht für die Schweiz?
Mit dieser Frage rücken wir in das unmittelbare Umfeld der Schweiz. In Bezug auf die Entwicklung Europas können wir erstens eine Schwächung der EU-Institutionen im Kontext der Eurokrise feststellen. Angesichts der Herausforderungen dieser Krise haben die supranationalen Mechanismen zumindest teilweise versagt haben. Die Staaten haben vermehrt zu Ad-hoc-Massnahmen auf der nationalen Ebene zurückgegriffen.

Das Resultat ist eine deutlicher zu Tage tretende politische Fragmentierung. Die Europäische Union war nie einheitlich, es gab die grossen drei Länder und die Kleinstaaten. Aber die politische Fragmentierung ist deutlicher sichtbar. Deutschland kommt klar die wirtschaftspolitische Führungsrolle zu. Aus sicherheitspolitischer Sicht ist auch die "Britische Frage" wichtig, die wieder zurück auf der Agenda ist. Die Frage ist, wie sich das britische Verhältnis zu den europäischen Institutionen entwickelt. Es scheint mir unbestritten, dass eine funktionsfähige Sicherheits- und Verteidigungspolitik im Rahmen der Europäischen Union ein Zusammengehen von Frankreich und Grossbritannien braucht. Wenn sich Grossbritannien abwenden würde, würde das auch die Sicherheitspolitik der Europäischen Union schwächen.

Zweitens halte ich aber einen Zusammenbruch der politischen Ordnungsstrukturen im europäischen Raum weiterhin für sehr unwahrscheinlich. Gründe dafür sind zum einen die Realität weitgehender Interdependenz zwischen diesen Staaten und zum andern die hohe Resilienz, die das europäische Einigungsprojekt bis jetzt gezeigt hat. Krisen führten eigentlich immer zu vermehrter Integration. Wichtig ist aus sicherheitspolitischer Sicht, dass die Mitglieder der Europäischen Union - mit wenigen Ausnahmen, die eher historischer Natur sind - ihre Nachbarn nicht als Bedrohung wahrnehmen.

Was heisst das mit Blick auf die europäische Sicherheitspolitik? Ich möchte die These wagen, dass im Krisenfall der Kooperationsdruck gerade wegen einer gewissen Schwächung der europäischen Sicherheitspolitik eher zunehmen als abnehmen dürfte, dass aber der Charakter der sicherheitspolitischen Kooperation eher zwischenstaatlich werden wird, d. h. eher ad hoc und weniger durch die Institutionen der Europäischen Union organisiert.

Die europäische Sicherheitspolitik ist durch weniger EU geprägt, und es gibt insbesondere unter den grossen Mitgliedstaaten eine Tendenz hin zu einer Renationalisierung. Dies wird am Bedeutungsverlust der Nachbarschaftspolitik und der Verlangsamung/Stagnierung des Erweiterungsprozesses sichtbar. Es ist ebenso unübersehbar, dass die gemeinsame Sicherheits- und Verteidigungspolitik eine Schwächung erlitten hat. Dies zeigt sich an einer Interventionsmüdigkeit, fehlendem strategischen Konsens in der Libyenfrage, der auch in der Syrienfrage fehlen dürfte. Dazu kommt, dass die Verteidigungsbudgets aufgrund der Finanzkrise schrumpfen, was natürlich auch Rückwirkungen auf die Gestaltungskraft der europäischen Sicherheits- und Verteidigungspolitik hat.

Ich möchte gleichzeitig aber auch in Erinnerung rufen, dass es auf diesem Kontinent weiterhin eine funktionierende Verteidigungsallianz gibt. Die kooperativen sicherheitspolitischen Strukturen sind dichter und robuster, als in jeder anderen Region dieser Welt. Zudem scheint die Nato die schwierigsten Jahre hinter sich zu haben, nämlich die grosse "Bush-Krise", als die USA die Nato zu einem globalen Bündnis der Demokratien umwandeln wollten, das ausserhalb eines Uno-Mandates handeln kann. Diese "Global-Nato" ist Geschichte und wird sich nicht umsetzen lassen.
Die Nato wird politisch gesehen wieder ein regionaleres Verteidigungsbündnis sein, das sich vermehrt auf Artikel V des Nordatlantikvertrages zurückbesinnt. Das hat auch etwas mit den Entwicklungen der Beziehungen zwischen Russland und den europäischen Staaten sowie dem Rückzug der Allianz aus Afghanistan zu tun und letztendlich auch mit dem deutlichen Nein Frankreichs und Deutschlands zu einer raschen Erweiterung um die kritischen Staaten Georgien und Ukraine. Hier haben die westeuropäischen Bündnismitglieder gegenüber der Administration Bush deutlich gemacht, dass sie einer solche Provokation Russlands, die während den ersten zehn Jahren nach dem kalten Krieg möglich gewesen wäre, nicht zustimmen.
Die Nato dürfte sich also wieder vermehrt auf Artikel V konzentrieren und in erster Linie ein regionales politisches Bündnis sein, das im militärischen Bereich etwas weniger ambitioniert ist und sich primär auf Krisenmanagement und Kriseninterventionen an der europäischen Peripherie konzentriert. Auch der amerikanische Druck, dass die Europäer gemäss dem Konzept "leading from behind" die Führung in Operationen an der europäischen Peripherie stärker übernehmen sollen, dürfte eher zunehmen. Dieser Druck ist eine Folge der sinkenden Verteidigungsbudgets und zum Teil auch der zunehmenden verteidigungspolitischen Ausrichtung der USA weg vom euro-atlantischen auf den pazifischen Raum.

Allgemein sehen wir in der Europäischen Union und auch in der Nato immer mehr pragmatische Verteidigungskooperationsformen. Die Stichworte sind hier Pooling and Sharing und Smart Defence. Teilweise findet das auch in subregionalen Foren statt. Diese Entwicklungen werden einerseits durch den Budgetdruck und andererseits durch die Technologieentwicklung vorangetrieben. Diese neuen ad-hoc-, intergouvernementalen, bottom-up getriebenen Kooperationsformen scheinen mir punktuell auch für die Schweizer Verteidigungspolitik relevant zu sein.

Ich komme zum zweiten Teil der 3. Frage: Was bedeutet die Einschätzung der Lage Europas aus sicherheitspolitischer Sicht für die Schweiz? Ich habe die Antwort in die folgenden drei Kernaussagen verdichtet.

1. Eine direkte militärische Bedrohung der Schweiz bleibt trotz volatiler politischer Lage in Europa für die nächsten 10 bis 15 Jahre sehr unwahrscheinlich. Auch für die Schweiz stellen die europäischen Nachbarn keine direkte sicherheitspolitische Bedrohung dar. Sie sind primär Kooperationspartner bei der Bewältigung von Gefahren, die von der europäischen Peripherie ausgehen.

2. Gleichzeitig muss man feststellen, dass die Schwächung der europäischen Institutionen zumindest teilweise einen Verlust der Resilienzpuffer gegenüber zunehmenden Destabilisierungstendenzen an der europäischen Peripherie nach sich gezogen hat. Damit verkleinert sich aber der Kooperationsdruck nicht - zumindest nicht im Krisenfall. Sondern es gilt:

3. Die Bedeutung der sicherheitspolitischen Kooperation bleibt essenziell, und zwar nicht nur im innerstaatlichen Rahmen (Sicherheitsverbund), sondern auch im europäischen Umfeld. Diese Kooperation kann bilateral sein. Zum Beispiel stellt sich die Frage, wie weit man das Abkommen mit Schweden zum Gripen im Rahmen einer Verteidigungskooperation im Ausbildungsbereich ausweiten kann. Die Kooperation betrifft zudem auch den multilateralen Bereich, nicht zuletzt weil die innere Sicherheit (Justiz und Polizei) weitgehend europäisiert ist. Schengen/Dublin bleibt für die innere Sicherheit der Schweiz relevant. Im Weiteren sehe ich in subregionalen Kooperationsformen ein gewisses Potenzial. Für die Schweiz ist es jedoch nicht einfach, sich in das verdichtende Geflecht subregionaler sicherheitspolitischer Kooperation einzuklinken. Das Land ist von drei grossen Staaten umgeben. Wenn die Schweiz eine subregionale Kooperation mit Deutschland und Österreich ("Dach") eingehen würde, stellte sich die Frage, wie man Frankreich und Italien einbinden kann. Trotz dieser Schwierigkeiten scheint mir ein solches Einklinken relevant. Die "Dach"-Kooperation nehme ich heute primär als technische Kooperation wahr. Ich könnte mir vorstellen, dass verstärkt die sicherheits- und militärpolitische Dimension hineingetragen würde. Beispielsweise könnte sich die Schweiz über eine "Dach"-Kooperation im Rahmen der "Special Operations Forces" an das deutsche Modell anschliessen.

4. Frage: Wie sollte die Schweizer Armee aufgrund der Bedrohungslage und -entwicklung ausgerichtet werden, was sollten künftig ihre schwergewichtigen Aufgaben sein?

Es ist mir klar, dass der Fokus dieser Hearings auf der Bedrohungsanalyse liegt und nicht auf der Frage, welche strategischen Prioritäten daraus für die Schweiz abgeleitet werden sollen. Im Sinne einer umfassenden Sicherheitspolitik möchte ich aber einleitend aufzeigen, dass die drei folgenden Bereiche aufgrund der skizzierten Bedrohungsanalyse generell an Bedeutung gewinnen:

1. Der Bereich strategische Führung. Im Sicherheitsverbund Schweiz stellen die Lageerkenntnis, Antizipation und Reaktionsfähigkeit angesichts einer von Unberechenbarkeit gekennzeichneten Bedrohungslage zentrale sicherheitspolitische Fähigkeiten dar. Das strategische Führungssystem sollte perfektioniert und ausgebaut werden.

2. Der Bereich Aussenpolitik. Der Beitrag der Aussenpolitik wird erstens wichtiger, weil die aussenpolitische Positionierung der Schweiz schwieriger geworden ist. Sie steht in einem Spannungsfeld, weil sie sowohl neutraler Kleinstaat als auch Teil Europas und ein globaler

Wirtschaftsakteur ist. Wenn eine der kritischen Bedrohungen Bürgerkriege an der europäischen Peripherie sind, ist zweitens der Bereich Mediation/zivile Friedensförderung bis hin zur Entwicklungszusammenarbeit sicherheitspolitisch relevant, mit Blick auf eine Eindämmung akuter Krisen oder Stabilisierung von schwachen Staaten. Wenn man zudem an die globalen Regulierungsfragen denkt - Cyberspace, Weltraum, Energie, Handel - kann drittens die Aussenpolitik auch einen Beitrag dazu leisten, dass wir globale Regulierungssysteme in einem liberalen Sinne haben, die den Interessen der Schweiz entsprechen.

3. Der Bereich innere Sicherheit. Wenn Sie mich fragen würden, ob es im Sicherheitsverbund Schweiz eine Lücke gibt, würde ich klar sagen, dass das am ehesten bei der Polizei der Fall ist. Das habe ich auch schon vor vier Jahren gesagt, doch orte ich dort nach wie vor gewisse Lücken.
Zudem gibt es ein gewisses Spannungsfeld zwischen den Kantonen mit der Polizei, die den Fokus vor allem auf die Alltagsgefahren richtet - den Gefahren mit hohen Häufigkeiten, aber relativ kleinen Auswirkungen, zum Beispiel Gewalt gegen Leib und Leben, Hooliganismus, Menschenhandel – und dem Bund, der vor allem auf mögliche Katastrophenszenarien fokussiert. Mit Blick auf die Bewältigung von Alltagsgefahren stellt der Föderalismus sicher eine Stärke des schweizerischen Sicherheitssystems dar. Mit Blick auf die Bewältigung von Katastrophen hingegen steigen die koordinativen Anforderungen an das Gesamtsystem jedoch deutlich. Wir sehen eine zunehmende regionale Ausweitung von Katastrophenpotenzialen, Krisenmöglichkeiten sowie eine zunehmende Verflechtung von immer mehr Akteuren.
Gerade die urbanen Sicherheitsdispositive im Katastrophenfall sind einem rasanten Wandel unterworfen. Wir haben dazu eine kleine Studie verfasst, die zeigt, dass wir neue private Sicherheitsakteure haben und dass sich die juristischen und baulichen Rahmenbedingungen sowie die Informationsbeschaffungsmittel in einem verstärkt urbanisierten Raum rasant verändern. Das ist ein globaler Trend, der aber für die Schweiz, die zumindest im Mittelland stark urbanisiert ist, eine wichtige Herausforderung darstellt. Damit wird die koordinative Rolle des Bundes wichtiger, nicht nur an den Schnittstellen zu den Kantonen, sondern auch an den Schnittstellen zu Privaten (beispielsweise den Betreibern von Infrastrukturen) oder auch an den Schnittstellen zu internationalen Akteuren. Dies gilt insbesondere für den Katastrophenfall, der ein überregionales oder sogar transnationales Ausmass haben könnte.

Wie soll nun die Armee angesichts der von mir skizzierten Bedrohungslage ausgerichtet werden? Bezüglich der Weiterentwicklung der Armee liegt der Fokus derzeit bei der Konsolidierung bis ins Jahr 2020. Die Debatte wird von drei Faktoren getrieben. Der erste ist der Finanzrahmen, bei dem wegen der Differenz zwischen dem Bundesrat und dem Parlament eine Unsicherheit über die Höhe der Mittel besteht. Der zweite Faktor ist der gesellschaftliche Rahmen. Hier geht es um die Frage, in wieweit das Ausbildungs- und Dienstleistungsmodell so flexibilisiert werden kann, dass es mit den Entwicklungen in der Gesellschaft und in der Wirtschaft in Übereinstimmung gebracht werden kann. Drittens gibt es den staatspolitischen Bereich mit dem anstehenden Referendum zur Wehrpflicht und dem Milizsystem.

Wenn wir den Blick auf die mittelfristige Weiterentwicklung über das Jahr 2020 hinaus richten, verorte ich zwei politische Blockaden, die vermehrt bearbeitet werden sollten. Der eine Punkt ist, dass in der Politik mit Blick auf die Priorisierung der Armeeaufträge Uneinigkeit herrscht. Stichworte sind die Aufträge Verteidigung, Unterstützung der zivilen Behörden und Friedensförderung. Diese Uneinigkeit ist störend. Der zweite Punkt besteht darin, dass man in der rüstungspolitischen Debatte immer noch rückwärtsschaut. Man spricht über die Redimensionierung der Infrastruktur, über den Abbau von schweren Systemen und über das Schliessen von Ausrüstungslücken für bestehende Verbände. Aber es geht noch nicht so sehr um die Frage, welche militärischen Fähigkeiten eine Armee 2020 und später braucht. Diese Fragen sollten vertieft diskutiert werden, weil sich die Aufgaben der Armee verändern.

Der zentrale Trend im Blick auf die Weiterentwicklung der Schweizer Armee ist eine zunehmende Verwischung der Schutz- und Kampfaufgaben. Der Grund dafür ist, dass sich das primäre Konfliktbild verändert hat. Im 20. Jahrhundert standen bewaffnete Konflikte zwischen symmetrischen Gegnern im Vordergrund. Das heisst nicht, dass es nicht auch Bürgerkriege gegeben hätte. Aber die Streitkräfteplanung war auf das Konfliktbild einer symmetrischen Auseinandersetzung zwischen militärischen Gegnern, natürlich an der Grenze zwischen Ost und West, ausgerichtet. Im 21. Jahrhundert verschiebt sich der Fokus gerade für Staaten wie die Schweiz eher auf bewaffnete Konflikte zwischen asymmetrischen Gegnern, also solchen Gegnern, die waffentechnisch, organisatorisch und in ihren strategischen Zielen sehr ungleiche Ziele verfolgen. Daher vermischen sich im militärischen Bereich zunehmend Schutz und Kampfaufgaben.
Im Kalten Krieg war es das Ziel, die Schutz- und Kampfaufgaben möglichst zu trennen. Im Neutralitätsschutz ging es um den Schutz der Grenzen aufgrund der dissuasiven Wirkung der Armee. Im Verteidigungsfall wäre es dann um die Kontrolle von operationellen Räumen gegangen. Im 21. Jahrhundert wird diese Trennung von Schutz- und Kampfaufgaben schwieriger. Das Primäre ist nicht mehr der Schutz der Landesgrenzen, sondern der Schutz von urbanen Räumen, von Schlüsselinfrastrukturen, von kritischen Verbindungslinien. In diesem Zusammenhang spricht man auch von einem Trend hin zu einer Konstabulisierung der Streitkräfte, sowohl im Kontext der inneren Sicherheit als auch im Kontext der militärischen Friedensförderung. Damit ist in der Regel gemeint, dass ein Teil der Armeeaufgaben Polizeicharakter annimmt. Es gibt auch andere Stimmen, die sagen, dass ein Teil der Polizeiaufgaben zunehmend militärischen Charakter annimmt. Sicher gibt es aber eine gewisse Überlappung. Dieser Trend zur Konstabulisierung der Streitkräfte scheint mir für die Schweizer Armee nicht zuletzt deshalb entscheidend zu sein, weil sich das Land nicht an den militärischen Interventionen im aussereuropäischen Bereich beteiligt, welche die grossen europäischen Staaten zusammen mit den USA im Bündnis- oder Koalitionsrahmen im Kontext einer sogenannten Vorneverteidigung durchführen. Das ist sowohl den Strategiepapieren der Nato als auch den Strategiepapieren der Europäischen Union so zu entnehmen.

Was heisst das nun in Hinblick auf die drei Aufgaben der Armee, also Verteidigung, subsidiäre Unterstützung und Friedensförderung? Man sollte sie nicht gegeneinander ausspielen,

sondern vermehrt integral betrachten. Die Schweiz braucht eine modular strukturierte und flexibel einsetzbare Armee. Die Armee ist und bleibt die zentrale strategische Reserve des Bundes, die die Souveränität und Abwehrbereitschaft der Schweiz in einem europäischen Rahmen stärkt. Gleichzeitig leistet die Armee mit ihren Schlüsselfähigkeiten tagtäglich Beiträge an die nationale und internationale Sicherheitsproduktion.

Wenn wir die drei Aufgaben der Armee betrachten, sieht man, dass sich das Konfliktbild über alle drei Aufträge anzugleichen beginnt. Überall haben wir es vermehrt mit asymmetrischen Gegnern zu tun. Die Armee stellt Schlüsselfähigkeiten zur Bewältigung solcher Krisenszenarien zur Verfügung. Sie tut das aber in der Regel zusammen mit zivilen Partnern und im Bereich Friedensförderung teilweise auch mit anderen militärischen Partnern. Ich gehe für Militäreinsätze in den nächsten zehn Jahren klar davon aus, dass sie zusammen mit zivilen Partnern oder allenfalls noch mit anderen militärischen Partnern durchgeführt werden.

Mit Blick auf die Erhaltung der Verteidigungskompetenz stellt sich zudem die Frage nach den mittelfristig relevanten militärischen Fähigkeiten. Die Frage ist, welche Waffen in Zukunft verbunden werden müssen und auf welcher Stufe das notwendig ist. Ist es die Brigadestufe, oder geht es bis zur Stufe Kompanie hinunter? Von der Antwort auf diese Fragen hängt es ab, in welchem Mass die Armee zur Kooperation mit zivilen Partnern bzw. mit anderen militärischen Partnern fähig ist.

Ich schliesse mit zwei Bemerkungen zur mittelfristigen Weiterentwicklung der Armee über das Jahr 2020 hinaus und unterscheide dabei die Ebene der Streitkräfteplanung und die politisch-strategische Ebene.

Im Hinblick auf die mittelfristige Streitkräfteplanung ist die zentrale Frage, welche Fähigkeiten diese Armee angesichts eines zunehmenden asymmetrischen Konfliktbildes, angesichts des skizzierten Bedrohungsspektrums braucht. Ich bin nicht Fähigkeitsspezialist, möchte aber hier doch ein paar Elemente erwähnen, die mir als Trends wichtig erscheinen: Aufklärung/Frühwarnung; geschützte Führung; geschützte Mobilität; leichtere, mobilere, präzisere Waffensysteme; Aufklärung und Schutz in der Luft; Spezialkräfte; Schutz und Rettung; Durchhaltefähigkeit. Natürlich sind die Entwicklungsmöglichkeiten in eine solche Richtung eingeschränkt, und zwar sowohl durch den Finanzrahmen, als auch durch den strukturellen Rahmen (Wehrpflichtmodell der Miliz) und auch den politischen Rahmen. Ein Treiber ist hingegen nicht zuletzt auch die Weiterentwicklung der Militärtechnologie.

Im Hinblick auf die politisch-strategische Ebene wird die zentrale Frage die bleiben, wann der Einsatz dieser Fähigkeiten im sicherheitspolitischen Interesse der Schweiz ist. Sie dürfte sich vor allem im Kontext der subsidiären Einsätze im Rahmen der inneren Sicherheit sowie im Kontext der militärischen Friedensförderungsbeiträge stellen.

Bezüglich der subsidiären Einsätze in Zusammenhang mit der inneren Sicherheit bleibt Diskussionsbedarf bestehen, insbesondere mit Blick auf die Aufgabenteilung zwischen Bund/Armee sowie Kantone/Polizei. Es geht erstens um planbare Spitzenleistungen, was Grossanlässe anbelangt, zum Beispiel das WEF oder andere Konferenzen oder auch Anlässe wie Europameisterschaften, wo zu klären ist, welche Unterstützungsleistungen die Armee den zivilen Partnern im Aufklärungs-, Führungs- und Logistikbereich liefern soll. Hier besteht auch ein gewisser rechtlicher Klärungsbedarf, zu verfassungsrechtlichen Fragen und auch auf der gesetzgeberischen Stufe. Das sind wichtige Fragestellungen, die bearbeitet werden sollten. Zweitens geht es um Grosskatastrophen und Gewaltphänomene unterhalb der Kriegsschwelle. Hier bleibt das Spannungsfeld zwischen der zivilen Einsatzverantwortung und der militärischen Führungsverantwortung bestehen. Dies ist vermutlich eine Frage, die erst im akuten Krisenfall einer Lösung zugeführt werden könnte.

Bei der Friedensförderung stellt sich die Frage, ob und wie weit der bereits seit zehn Jahren in Aussicht genommene Ausbau der militärischen Friedensförderungsbeiträge der Schweiz umgesetzt werden kann. Die Rahmenbedingungen werden nicht einfacher werden, weder innenpolitisch, noch was die internationale Politik anbelangt. Eine der Kernfragen ist, wo diese Einsätze stattfinden sollen. Wenn wir davon ausgehen, dass es nicht unwahrscheinlich ist, dass die Engagements in Bosnien und in Kosovo kleiner werden, und wir das Bedrohungsspektrum ansehen, wären Afrika und der Nahe Osten die logischen Räume und allenfalls noch der Kaukasus. Damit verbunden sind allerdings schwierige politische Fragen, da der geografische Horizont der schweizerischen Sicherheitsdebatte kaum nach Afrika und in den Nahen Osten hineinreicht. Mit der Frage nach dem *Wo* ist diejenige nach dem *Wie* verbunden. Die Spezialistenbeiträge sind unbestritten, zum Beispiel Militärbeobachter oder die Minenräumung. Da hat die Schweiz grosse, gute Kompetenz, die auch nachgefragt wird. Die zentralen Fragen sind, ob auch in Zukunft Kontingente in den Einsatz kommen sollen, und zwar vielleicht auch über den Balkan hinaus, oder welche hochwertigen Beiträge die Schweiz gegenüber der Uno oder internationalen Organisationen leisten kann. Ein Beispiel ist der Lufttransport, doch kann man den Logistikbereich auch etwas breiter denken.

Ich hoffe, Ihnen mit diesen Ausführungen den einen oder anderen Gedanken in Erinnerung gerufen zu haben. Im Rahmen der Vorbereitung habe ich auch meine Präsentation aus dem Jahr 2009 angeschaut. Was die Bedrohungsanalyse anbelangt, gibt es keine grossen Veränderungen in meiner Einschätzung. Abgesehen von einer gewissen Abnahme der Bedrohung durch den globalen Terrorismus und einer Zunahme der Destabilisierungstendenzen als Folge des Arabischen Frühlings im Mittelmeerraum, hat sich die Bedrohungslage in den vergangenen fünf Jahren nicht grundsätzlich verändert. Ich gehe davon aus, dass meine Schwerpunkte, zusammengefasst in Bedrohungstrends, nicht grundsätzlich anders ausfallen werden, wenn wir in fünf Jahren die nächsten Hearings durchführen.

Statement by Ambassador K. C. Singh

Distinguished Fellow at the Institute of Peace and Conflict Studies

Main issues: Terrorism, Islamic world"

Bern, 6 September 2013

For his presentation we asked to address particularly the following questions:

1. ***What are the most urgent threats to regional and global security from an Indian point of view?***
2. ***Which effect(s) will the retreat of the international troops from Afghanistan have (on the regional and international level)?***
3. ***Is it likely that we could face a scenario in which nuclear weapons get into the hands of terrorists (e.g. in the course of upheavals in Pakistan)? And what could/should be done to prevent such a scenario?***
4. ***How is the current situation and development in Europe (from a security perspective) perceived and judged in India?***

Introduction

For most people talking about militant or radicalised Islam, 9/11 is the starting point. In a historical perspective, 9/11 is rather what made the US realise that radicalised Islam existed – a phenomenon that in its modern form had been created by the US itself. Older forms, however, have existed for a long time, which is why I will outline the historical development of different forms of Islam before focusing on the recent past.

13th to 19th century

In its original form, Jihadism first surfaced in the 13th century after the Mongols had invaded Iran as well as Bagdad and Damascus and demolished the caliphate. In the course of this invasion, Muslims encountered, for the first time since Islam had been created, a force larger than they themselves, leaving them with a feeling of humiliation. As a result, in the 14th century militancy and a rigid, puritanical, pristine way of Islam emerged which stuck to a literal interpretation of the Koran. This kind of Islam re-emerged much later, in 18th-century Saudi Arabia, with the start of Wahhabism.

India at the beginning of the 18th century witnessed the decline of the Mogul empire and the rise of Western imperialism. The Ottoman Empire shrank, too, and the Persian Empire van-

ished altogether, both being replaced by surrogates of Western countries or becoming directly Western controlled, bringing Islam and Christianity into contact again. The encounter left Muslims with a feeling of losing control and being marginalized. As a result, a part of them resorted to a radical version of Islam that had never quite vanished in spite of not being the dominant version. Mainstream Islam resisted this radicalization until about 40 years ago.
From the 19th century onward, Ottoman and Iranian control of large parts of the Islamic world was one of several developments leading to a radicalisation of Islam. In the 1920ies and 1930ies, both Egypt and India were under control of the British who met resistance by militant Islam. The Egyptian Sayyid Qutb was exposed to Western culture when studying in America, and revolted by it. Back in Egypt, he developed a puritanical interpretation of Islam, sowing thereby the seeds of Iquan, i.e. the Muslim Brotherhood. Although Nasser had him arrested and put to prison for ten years, he resisted all attempts to have him recant his convictions and re-join mainstream Islam. Sayyid Qutb's strand of Islam went on in Egypt after his death in 1966 and resurfaced in different forms once Mubarak was gone. What is now happening in Egypt with Mursi and his followers started in the 1930ies. The real beginning of Iquan, however, is to be found in Saudi Arabia where two desert tribes made a pact with the ruling family.

At the same time as in Egypt, the Muslim Brotherhood resurfaced in India, i.e. in the post-Taliban, pre-9/11 era. Its roots, though, go back to the Mogul empire, which at the time controlled what is now Pakistan. Its Northern parts were ruled by a Sikh empire developing an assimilative and inclusive way of ruling, counting many Muslim and Hindu generals. There was also a version of radical Islam with both Pashtun and Wahhabi qualities. Pashtuns living in arid mountains and Wahhabi tribes living in the Saudi Arabian desert shared similar conditions supplying them with only a minimum of resources. When that kind of tribe accepted Islam, it did so with total submission and a severe code of conduct. This combination of Islam and Pashtun tribal values turned out to be deadly, as we are witnessing now.

The problem, however, had already started in the Sikh empire, when around 1800 people from the North-Eastern region travelled to Medina, where Wahhabism had seen a revival. They brought it to their region, spreading it all over and triggering a desire to get the Mogul empire back, i.e. the rule of a small Muslim minority. Mogul ruler Akbar once had started a new brand of Islam, Din-i-Ilahi, which was neither Shia nor Sunni. He did so for geopolitical reasons: had he declared himself a Sunni, he would have had to bow to the Ottomans, who had the caliphate and were controlling Mecca and Medina; had he declared himself a Shia, he would have had to bow to the Safavids, who were ruling over Iran. So he started a new version. There remained Shia and Sunni strands in his empire, but people rising to high positions at the court did not openly profess their adherence to those strands.

The dividing line in India started with the sons of Akbar's grandson Shah Jahan. The first son was a Sufi, the second son, Aurangzeb, might be compared to a Taliban. He revolted against his father and killed his brother. Aurangzeb exhausted himself trying to conquer the rest of

India and to forcibly convert people. As a result, the Mogul empire collapsed, the vacuum being filled by the British. Aurangzeb's stream of intolerant Wahhabi Islam is exactly what the US is fighting today. When President Obama visited the Mausoleum where Aurangzeb's elder brother's beheaded body is buried, he clearly showed that he understood the historical and political significance of this battle in mid-17th century India between two competing streams of Islam, one being assimilative, the other being an intolerant, puritanical stream defying Christians, considering Hindi as idolaters and even Shiites as enemies.

When the British took over control in India, the hurt in the Islamic mind continued to simmer and led to the rebellion of 1857 joined by the Hindi. After the failed upsurge, many rebels went into today's Pashtun Af-Pak area, taking shelter in the mountains and continuing from there their terrorism by kidnapping people.

This summing-up of historical developments shows that in India, Saudi Arabia and Egypt this kind of battle started very early on. It recurs when Muslims are isolated, when they encounter a foreign power making them feel helpless, or when they are facing modernity and unable to adjust to it. Under such conditions it recurs in the form of an extremely puritanical and rejectionist Wahhabism, an inward-looking version of Islam taken back to desert values, a version that clearly distinguishes itself from the global stream of Islam, which, in large parts of its history, was much more tolerant.

1970 to 2010

What we are witnessing now is the result of several things happening in the 1970ies. In 1977 Pakistani Premier Bhutto, wrongly considering General Sia a devout and tolerant man, superseded three Generals and made Sia chief of army staff. Sia, however, took over power, had Bhutto arrested and ultimately hanged. Soon, Pakistan and its army were completely isolated. Sia brought about a convergence between the right wing and one of the three schools of thought started in the 19th century, the Deobandis, which turned out to be a depository of intolerant Wahhabi philosophy. The Wahhabi did not espouse terrorism, but they trained hundreds of thousands of people who then moved on to Pakistan. In 1972, there were around a thousand Madrasas, i.e. Islamic schools, out of which 40 per cent were Deobandis and al-Hadith. At the end of 1980, already 65 per cent of Madrasas were Deobandis. Up to 2002, when the first census in Pakistan was carried out, their number had risen to ten thousand. By then, the Pakistani education system had collapsed. The expanding poor population went to these Madrasas and were taught a literal Wahhabi interpretation of Islam. In 2002, out of 1.7 million Madrasas students 1.25 million were Deobandis and al-Hadith. So, almost 80 per cent of these students were imbibing that kind of indoctrination.

1979 was a crucial year. Ayatollah Khomeini was determined to export the Iranian Shia revolution. The Sunni world was completely startled. In November 1979 militant Muslims, followers of the Mahdi emerging from the desert, took the grand mosque at Mecca; the Saudis

had to call in French Special Forces to get rid of them. Only three weeks later, Soviet troops marched into Kabul. These events made the Saudis very nervous. After killing the followers of the Mahdi, they had become great supporters of the Wahhabi cause. The big export of Wahhabi propaganda started.

Pakistan witnessed the influence of three forces: US cold-war politics, CIA assistance and arms, Saudi-Arabian money. The money and the training camps were used both to train militants fighting the Soviet Union in Afghanistan and to train militants from Punjab. Money and arms were always given to Pakistanis, but they could steer it into whatever other cause they wanted. America was successful in its desire to make the Soviets stumble into their 'Vietnam': the Soviets exhausted themselves and the USSR collapsed within two years of the withdrawal from Afghanistan. As a result of the alliance between Taliban, al-Qaida and salient groups there, Al-Qaida got a foothold between 1989 and the rise of the Taliban in 1994/95. It was only in 1998, when al-Qaida attacked US embassies in East Africa, that the US realized they were having a serious problem; in fact, that should have been clear by 1980. After the attack on US embassies, President Clinton ordered the firing of missiles onto suspected al-Qaida camps in Afghanistan, but by that time the camps had been vacated. The complicity between Taliban and Pakistani was perceptible when an Indian plane was hijacked and taken to Kandahar. However, no one was ready to act against the plane and to seriously offend the Taliban who had been recognized by Saudi Arabia, the United Arab Emirates and Pakistan. At the time, the US thought that al-Qaida was devoted to a selected militancy; they did not understand that al-Qaida had a global vision that was ultimately leading to global Jihad. With 9/11, al-Qaida's attack on the core of the US, the Pentagon and the financial capital, it became obvious that a new phase had begun.

Although Pakistan and Saudi Arabia offered mediation, they would not let go of al-Qaida and Osama bin Laden. The Pashtun code of honour, demanding to respect guests, combined with Pakistani sympathy for Taliban philosophy and al-Qaida's world view. The flight of al-Qaida members was seen as a Taliban defeat, but al-Qaida leaders shifted to Pakistan and found, together with militant Pakistani groups, the protection of the Pakistani Inter-Services Intelligence (ISI) and enjoyed inside support. Pakistan of course denied sheltering these people; it was clear that, if Taliban enjoyed inside support in overrunning air-bases, soon questions would arise as to whether they would also get access to nuclear assets. It is true that these assets recently have been spread around in order to avoid attacks, but by spreading them, the Pakistani also multiplied potential targets. Pakistan claims that they keep fuses and warheads separated, so that weapons cannot just be picked up and fired; but even if militants only got hold of plutonium or enriched uranium, they would be able to build a dirty bomb and – Taliban and al-Qaida being experts with regard to explosive devices – to create contamination and panic in a city.

When the US went into Afghanistan, they soon thought they had won, not realizing that Taliban youngsters had just gone back to their villages and merged into the population and that

the leadership was under protection in Pakistan. While the Taliban waited, the US got stuck in Iraq, wrongly accusing Saddam Hussein of possessing chemical weapons – which is why they are now having difficulties in convincing the world of Syria possessing such weapons. Saddam did not admit having no weapons of mass destruction because doing so would have made him more vulnerable. In the meantime, the US got trapped by the Iranians and their surrogates, Muqtada al-Sadr and the Mahdi army. Iraq became a battlefield in the way Syria is now, with al-Qaida being sucked in, with US troops, Shia militia and al-Qaida fighting ferociously. One explanation for that is that militants are always in need of active confrontation with a great power in order to distinguish themselves, rise in ranks, attract and inspire adherents, promise success or martyrdom.

Another decisive year was 2005. US troops being neck-deep in trouble in Iraq, several capitals in the region concluded the US had no capability to attack them and was going to leave soon. So, newly-elected Iranian President Achmadinechad broke the IAEA seals and started processing uranium again. In the same year, the Taliban re-emerged in Afghanistan, first in small, then in large groups. In the meantime, with General Petraeus in Iraq, the US rewrote the book on how to deal with counterinsurgency, realizing that they had been fighting it all wrong. Had President Bush not backed the Generals, things would probably be even worse today. The new strategy included small foot patrols, reconquering areas slowly, holding it, connecting with the people, protecting them and trying to seek their co-operation instead of going for ever fugitive militants. After three difficult months in 2007, Sunni tribes finally started to co-operate, Mahdi was chased out of Iraq and the US were able to stabilize the situation.

By that time, of course, there were serious troubles in Afghanistan, so that the US had to relocate their resources. However, the strategy they had applied in Iraq did not work in Afghanistan. Moreover, when President Obama came in, it took him a year to start the search for al-Qaida leaders, not committing as many soldiers as the army wanted. The US, nonetheless, was able to stabilize the situation, but for domestic reasons President Obama had to fix a deadline. With a deadline you cannot fight insurgents, who have no deadline at all. The Taliban hissed their flags again, achieving moral successes and claiming to soon re-establish pre-2001 conditions. Although the US had a response to that, the Taliban until today show no real will for co-operation.

2010 to 2013

In the course of the last three years, there have been three developments complicating things further.

The first such development could be summed up as ‘the Internet’. While the US managed to target al-Qaida's top leadership by means of drone attacks, al-Qaida evolved into a more loosely-connected, decentralized network which no longer needs to move resources, trainers

and motivators around. Nowadays, these things are done by means of electronic communication. Even Twitter helps the militants by directing people from one propaganda website to another, so that militants can easily shop and share ideas. This is also relevant to Switzerland because today's cyber-world has made communication seamless and borderless, with no islands being left. The virus of militancy therefore has become global and has to be fought in different ways: by deterring or detecting people and by engaging in winning hearts and minds.

The second development complicating things is the Arab spring. What originally started in Tunisia, very rapidly spread to Egypt and Libya and is now being contested in Bahrain and Syria. In the beginning, the Arab spring confused al-Qaida; apart from a tape that was never even put on the net, there was no reaction, neither from Osama bin Laden, then still alive, nor from Shihri. The reason for al-Qaida's confusion was a simple one: if non-violent methods of protest such as street demonstrations lead to regime change, they undercut the al-Qaida view that rulers in the Arab world whom they reject are serving the US agenda and will not leave till they are forcibly driven out through an armed rebellion. At that stage, by the way, President Obama played his cards very well by exerting pressure from behind the scene to make sure that the Egyptian army allowed a transfer of power. Today, with a counterrevolution taking place and the army hitting back, it is difficult to say how things are going to turn out in Egypt; it is unclear whether the revolutionaries will be able to purge the movement of radical elements and take the development back to democracy. At any rate, what will happen there is very important because Egypt, with a third of the Arab population, is the heart of the Arab world. It has always been a leader in terms of ideas and of media. If things are going the wrong way in Egypt, then Egypt is feeding al-Qaida propaganda which demands a radical approach.

At least, there is currently a positive development in Tunisia, where after the stalemate even the right-wing forces conceded that they were not to bring the Sharia into the constitution. Therefore there is hope that Tunisia may adjust its transition from totalitarian control to democracy, with different elements having a voice and democratic forces not being used as a means of changing the country into a Sharia-compliant Islamic state.
The third development complicating things is the rivalry between Shia and Sunni. By going into Afghanistan and Iraq, the US in a sense knocked out the two great enemies of the Iranians, i.e. the Taliban and Saddam Hussein. With Saddam gone, a Shia majority in Iraq, a Shia minority government in Syria, and Hezbollah in Lebanon, the sphere of Iranian influence today runs from India's borders all the way to the Mediterranean and the Aegean See. As Putin recently put it, the real question with regard to Syria is why the US is not conceding that, in the form of al-Nusra, al-Qaida is entrenched there. The focus should not be on Assad alone, because if Assad were taken out, al-Qaida would be built up. At any rate, there won't be a neat solution. After what Western powers experienced in Afghanistan and Iraq, they realized that in societies with a complex suppression of inner feelings over decades as a result of totalitarian control, values cannot just be supplanted. In those countries, civilian opposition

had been knocked out by the rulers, the only opposition left being the one in the mosque, the only organized opposition therefore being right-wing. Under such circumstances there cannot be an easy transition to democracy.

For these three reasons, things are much more complicated today than they were in 2001. If the West had stayed in Afghanistan, spent more money and paid more attention to developments there, things might have turned out in a different way. If, in other words, some kind of good governance had filtered down to the people, winning their minds and hearts, maybe the Taliban would not have been able to come back and find support in the villages.

Conclusion

In what way are these developments relevant to a country such as Switzerland? The discussion about which side in Syria used chemical weapons shows that weapons of mass destruction today are more widely available. What might be the consequences of chemical weapons being in the hand of militants? Where were they to blow such weapons? Even Switzerland is not immune to militant attacks – firstly because people disliked by militant groups are staying here, secondly because money from dictators or totalitarian regimes has flown to your country, thirdly because attacking a banking centre might be a means to create confusion in the capitalist world.

Switzerland may be able to control migration; unlike many other European countries, it does not have a large Islamic population. Immigrants from Pakistan tend to go to the UK, immigrants from North Africa to France, immigrants from the Anatolian region to Germany. Those host countries, therefore, are worried about these regions. There may be different entry points in different countries, but ultimately there is a convergence because migration of people and migration of information is a global phenomenon. Although the information necessary to build a bomb may be found in the Internet, people express their anger locally. The question therefore is what steps Switzerland needs to take to contain such people's anger. To be prepared you have to remain alert, but in order not to create more militants by doing so, you have to avoid strong-arm tactics and use subtle means instead.

Statement by Mohammad-Mahmoud Ould Mohamedou

Visiting Professor at the Graduate Institute of International and Development Studies,
Head of Regional Development Programme at the Geneva Centre for Security Policy (GCSP)

"Transnational terrorism and developments in the Middle East and North Africa"

Bern, 6 September 2013

For his presentation we asked to address particularly the following questions:

1. ***Which consequences has the Arab Spring had on the security situation and development in the region? Will the net effect in your view be presumably positive or negative?***
2. ***What are the most urgent security problems in North Africa and to what extent is Europe's security affected by them?***
3. ***How would you judge the threat potential and development of Islamist terrorism in North Africa, and what could/should an effective counter-strategy look like?***
4. ***What kind of contributions could/should Western states make to the resolution of regional security problems (in North Africa or the Middle East)?***

In answering your questions, I will address the themes of transnational terrorism and of developments in the Middle East and North Africa, dividing my remarks in four sections.

1. A changed international security context

The issue of transnational terrorism and security developments in the Middle East and North Africa cannot be understood in isolation from the global security context which has steadily emerged over the past few years. If, at times, the desire to see the novelty of some of these changes to be recognised and dealt with has arguably led some to be hasty in their conclusions, equally, the reluctance to acknowledge the passing of some structures has confined others into a problematically static perception of what in fact is fast evolving.

In earlier writings and building on the work of others, notably on that of the German political scientist Herfried Münkler and the Israeli military historian Martin van Creveld, I have attempted to identify the characteristics of this transformed conflict scene. The seven elements relevant to our discussion are the following:

1. Privatisation, that is the use of force away from the states by armed and non-armed groups such as private military contractors and private corporations who today have much political purchase.
2. The civilianisation of conflicts, that is the increasing involvement of civilians into conflicts as actors and as victims, although the development of international humanitarian law over the past century and a half could have let us to believe that civilians were at bay from conflicts even though the conditions on the ground were never perfect.
3. The widening and virtuality of the spatial dimension of these engagements.
4. The geographical indeterminacy of conflicts, the battle*space* replacing the battle*field*.
5. The dilution of the temporal element, raising the question of how, in policy, to handle the acceleration and deceleration and how to deal with elusive actors.
6. The expansion of the nature of targets to religious buildings such as mosques, churches and temples.
7. The systematisation of asymmetrical conflict.

The fifth and the seventh element are probably the most important ones in this new grammar, because the might of the state has become paralysed and because the agility of the new groups enables them to be present and to project their force in a transnational manner.

As we enter the second decade of the twenty-first century, twelve years after the era-defining events of 9/11 and close to a quarter of a century after the fall of the Berlin Wall, the transformation of the contemporary security scene has arguably reached a plateau. It has done so within an extended three-part transition — post-Cold War, post-9/11 and post-Arab Spring. In a transition process that is today primarily taking place as a result of both the Arab Spring and the nature of the different elements of that new grammar, the sum total of these momentous changes has more or less coalesced into a mutated type of armed conflict, which for the time being we can take stock of — with all its complexities and confused and confusing characteristics — and use that assessment, however imperfect, to try to devise, revise and reaffirm our international responses to transnational terrorism.

In terms of dynamics, the security implications concern primarily three dimensions. Firstly, *the very notion of victory and defeat* has been altered. Power is no longer just might. What matters today if it comes to reaching success is the ability to identify a goal, give oneself means to achieve it, reach it and manage to stay ahead of the opponent's game.

Secondly, the implications concern *the pull effect that the weaker side* in the asymmetrical martial equation is having on the stronger party, and which shows that the components of might have changed. These elements appeared early on with the United States 2001 military campaign in Afghanistan. Mimicking in many ways Al Qaida, the irregular enemy it was fighting, the US army relied — effectively at that, compared to what they achieved in Iraq — on very light forces, operating in a penetrating mode, at times even on horseback or on foot,

to disrupt and confuse the other side. It has continued to do so in recent years, with militaries seeking to emulate transnational armed groups' control of cyberspace and aiming at disrupting cyber-operations.

Thirdly, the implications concern the *evolution of the forms of and resort to violence*, the ways in which violence is now being used by such groups, at a strategic level, both within and without societies. The use of violence has become endemic, widespread and pervasive and has acquired familiarity. With no obvious targets to choose from amongst the armed groups, states are now forced to track groups and follow them on a terrain, which they do not control and in fact never will be able to control. A good example of this is what the French are experiencing in Mali. Although there is a success narrative, not much has been settled in the field. The groups seem to have migrated up north, some to Libya and to Niger. This shows that states are no longer dealing with a settled situation, but with constantly morphing and mutating groups. Being confronted with fast-changing armed groups calls for a different mindset.

As compared to the role of non-state actors in previous decades — during which the armed groups were essentially using military force in a rather predictable, classical way as an alternative means to achieve political goals — most contemporary non-state actors are no longer modelled on political resistance movements whose *modus operandi* was primarily domestic, hence the contiguity to territory, and aimed at national liberation, i.e., an identifiable, recognisable and even negotiable goal. These things are gone; meetings such as the ones between the French and the FLN in Evian are in effect things of the past. The new groups at times have an ability to deploy state-like military infrastructure, for instance in Syria, or state-like infrastructure in terms of public services (in health, education, law and order, and so forth) as in the case of Hezbollah, generating some sort of 'legitimacy' and challenging directly the relevance of the state concerned as the quasi-exclusive legitimate actor. Therein lies a new type of challenge for the fragile state, particularly in the case of a state being in transition.

Furthermore, the interactions — peaceful or not — between international actors and non-state actors exemplify, and in cases amplify, the *de jure* disconnection between the international status of the formal state — in terms of monopoly of force — and the non-state actors.

2. The security consequences of the Arab Spring

The new grammar and the situation in the Middle East are interlinked and interlocked, so much so that the former is not only reflected by the latter but in fact *furthered* by it. The activities of the groups — and of the states, for that matter — in the Middle East and in North Africa are an illustration of the new grammar, but are also taking us into new territory.

Just as there is no grasping the nature of the current changes in the Middle East and in North Africa without setting them against the backdrop of the above-discussed global transfor-

mations, there is no overstating the historical importance of the events that took place in the Arab world in 2011 and that continue to play out since. Hence, I would like to take a step back from the media narrative of the Arab Spring with its excessive optimism and the narrative of the Islamists' winter with its excessive pessimism. By doing so, I would like to emphasize two crucial elements.

Firstly, the Arab Spring *itself* is a security implication. The uprisings were the culmination of systemic dystrophies which had social origins such as dispossession, humiliation and repression as well as political origins: a lack of accountability, the authoritarian systemic dead-end, police and intelligence, i.e., *mukhabarat* and *istikhbarat* state culture — which was increasingly institutionalised as a set of repression mechanisms — and failed state-building since at least the 1920s in the context of the Sykes-Picot Agreement.

Secondly, the Arab Spring is *not a regional event.* It would therefore be a mistake to look at its security consequences under a 'Middle East and North Africa area studies' perspective. With such an approach we would indulge in the very same Orientalist mind-set that made us, in terms of security, miss out on the uprisings in the first place. We, rather, have to look at it as a global event. The region should be regarded as today's security centrepiece of the world, as Europe was in the middle of the 20th century, as Cambodia and Vietnam were in the 1970s and as the Balkans were in the early 1990s. Looking at the Arab Spring as something that has to be dealt with internally does not do. In the course of the last two years, we repeatedly witnessed a transnational beaming back from these events to the world, having implications onto France, Spain, Greece, the UK, Russia, Canada and the US, with uprisings taking place for cultural or economic reasons or as a result of student riots. In brief, any policy addressing the issues in the region affected by the Arab Spring has to be multisectorial, taking thereby into account all elements of this complex global event.

Let me, on this basis, try to identify some consequences of the Arab Spring in the phase immediately after the events.

The first and most important one is *the weakening of the state in the region.* States have been weakened to an extent which makes clear that the events constitute a rupture from the earlier, fallen system and the inception of a transition. By virtue of being the object of reform and reconstruction, they are inevitably going through a period of transformation and need to be rebuilt.

Transitions are by nature the scene of volatility and disruption. Such instability does not have to translate into conflict, but in this case it has. The conundrum is that the very thing that is in need of reform, that is the state as a whole, firstly, is physically uncertain with Ministries coming under attack by militias or by people besieging them for months; secondly sees its authority and legitimacy systematically questioned; thirdly is looked upon suspiciously by the silent majority of the population, which sees in it either the old regime in the remaking or the

Islamists lurking; and, fourthly, represents the seat of intense struggles. This weakens the state's ability to provide security and triggers vigilantism, as was seen from the very first days in Tunisia after the fall of Ben Ali. It also leads to a weakened response to serious incidents; remember the September 2012 attacks on the US consulate in Benghazi and the embassy in Tunis. Accordingly, any higher level security issue can trigger diplomatic evacuation, as was shown in the region-wide US travel alert warning in August 2013.

De-statisation therefore plays from day one of the Arab Spring. It partakes of a larger process of a weakening of the state that began in the 1990s and is playing out beyond the area, notably in the Sahel and in Central Africa. This dimension of a weak state in many ways holds the key to what type of new authorities will emerge in the region as security partners.

The second consequence of the Arab Spring is *the strengthening of non-state actors*. With the weakening of states, transnational armed groups almost inevitably become stronger. It flows from de-statisation which benefits all those that are not the state, for instance civil society and peace-oriented actors, but in particular armed groups: from the *thowar* (revolutionaries) in Libya, to tribesmen in Yemen, not to forget previously organised insurgencies in Iraq or Yemen.

This crucial dimension also benefited Al Qaida. The initially widely-circulated argument that the Arab Spring spelled the defeat of Al Qaida was misplaced. For one thing, the defeat of regimes which Al Qaida had fought could hardly play out as a defeat to them. Al Qaida, by the way, was never interested in democratising the region; it had a much more radical agenda. In fact, Al Qaida has been able to use the fluidity of the new and changing Middle Eastern and North African context to engineer an attempt at rebirth through a franchise. This important development still in the making specifically concerns Al Qaida in Iraq. On 9 April 2013, Al Qaida in Iraq's leader, Abu Bakr al Baghdadi, announced that his organisation, Al Qaida fi Bilad al Rafidayn, was merging with Jabhat al Nusra in Syria — the front that was created in the fight against Bashar al-Assad — to create a new entity called Al Qaida fi Bilad al Rafidayn wal Shaam, meaning 'Levant' in Arabic, that is led by one Mohamed al Joulani. Since Joulani is from the Golan, this also implies a threat to Israel. Al Qaida is therefore *in mutation* rather than being defeated. The transition landscape from Tunisia to Iraq by way of Sahel, Libya, Egypt, the Sinai, Yemen, Lebanon, Levant, and, most importantly, Syria, on which Al Qaida is increasingly focused, is providing it with opportunities to re-emerge as a new type of organisation, differing clearly from the classical, hierarchical, Bin-Laden-led type.

The third security consequence in the phase immediately after the Arab Spring is *the ongoing remapping of the region*. This is not so much important in and of itself — there has been much academic debate about whether the so-called Sykes-Picot architecture is now obsolete — but rather regarding the reconfiguration of a major sector of global security politics. In addition to the dangerously weakened state apparatuses and the further empowered non-state actors, the Arab Spring opened the Arab state system, something that had not happened

since the so-called Arab 'Cold War' of the 1960s. Some characteristics of this opening are: firstly *fluidity* within the set of interrelationships amongst Arab actors, an important characteristic for policy making; secondly *uncertainty* as to which particular configuration will emerge as dominant (a year and a half ago one could have argued that Egypt, Saudi Arabia or Qatar would be the dominant factor, but things keep changing); thirdly an *open-endedness* to these dynamics. As it is, any small development in the region, whether a bombing in Libya or a coup in Egypt, can have, regardless of its nature, a wide impact. This generates difficulties in planning and in the readability of an event: how not to make too much of it, how not to underestimate it? This is all the more difficult in relation to a maximised contest wherein all actors feel empowered, be it Al Qaida, Qatar's diplomacy, Saudi Arabia's regime seeking to survive the Spring, the militias in Libya or Bashar al Assad.

3. Emerging security trends in the region

In the past two and a half years, we had to learn to live with two phenomena. One is the guessing game regarding the next development. In 2011 the question was: which regime will be next to fall? In 2012, the question was: how will the dust settle? In 2013, the guessing was about Syria not ending. The other phenomenon is the longer-term, rear-view and forward-looking deciphering of the region's reconfiguration. From the 'unexpectedness of the revolutions' to the 'unpredictability of the transitions', we are still very much in the midst of an evolving context. There is no escaping from the five month/five year horizon scanning. What does such instability reveal?

This landscape has at least five cementing patterns. The first of these patterns refers to planning and reading. *There is no separating the 'Middle East' (the 'Near East' or the 'Proche-Orient') from 'North Africa'*. For all the atomization and all the different narratives — the Tunisian story for instance is completely different from the Syrian one — Mashreq and Maghreb, for the time being, are very much one; not in terms of history, of course, but in terms of influence, of people listening to one another and watching each other on Al Jazeera. This plays out beyond the traditional Arab culture dimension and the narrative of Arabhood and unity. We see that from the staccato events in 2011, from Tunisia to Syria by way of Egypt, Libya and Yemen, to the inception of transitions that influence one another, with sub-regional idiosyncrasies having been de-emphasised.

The second cementing pattern is the following: Whereas the revolution moment was about the shortcomings of authoritarianism, unpacked domestically, *the post-revolution phase is playing out fully under the theme of transnational dynamics*. Transnationalism is inundating these developments in every single aspect, it increasingly reveals itself to be problematic, whether as it relates to conflicts or to political processes. How, for instance, do you define a political way out of Syria if there are so many actors being present? This release brings as much opportunities for constructive support by external actors as it holds the key to potential undue influence — think for example of global Jihadists going to Syria. It is like magma that

is at once overflowing countries and engulfing actors from outside: Libya onto the Sahel, the Sahel onto Tunisia, Iraq and global Jihadists onto Syria, Syria onto Lebanon. Seldom in the history of the region has there been such fluidity.

As regards armed groups, this plays out in two ways: firstly in the rise of mid-level managers such as Abou Iyad, who has become a powerhouse in Tunisia, Abdelmalek Droukdel, the leader of AQIM in Algeria, or Mokhtar Belmokhtar in Mali; secondly in the proliferation of new groups such as Ansar Al Sharia in 2011, MUJAO in 2012 and Jabhat al Nusra in 2013.

The third cementing pattern is *the persisting and spreading weakening of central authorities*. There is rivalry for authority and a plethora of competing streams. In the whole region, the state has neither exemplarity nor pull, nor is it generating fear. An example for this is the fact that the 1 April 2012 deadline set by the Libyan General National Congress for the militias to lay down their weapons was deliberately and fully ignored by the groups. In terms of legitimacy, such systematic defiance towards authority means that there is still no new narrative, while the previous one remains unresolved. This raises the question of functioning authority precisely at a time where the countries are in need of a new stewardship to lead these processes. Instead, we witness the setting up of parallel control rooms and the carving out of sectors of power. It is needless to say that this undermines institutionalisation attempts.

The fourth cementing pattern is that, out of this restiveness, volatility and reconfiguration, will emerge in the medium term *security deterioration with two key centres: Libya and Syria*. The Libyan security vortex began with the intervention and the founding violence in and around the Libyan revolution — from the killing of Major General Abdelfattah Younes, the first military leader of the uprising who had defected from the regime, to the lynching of Mouammar Kaddafi himself. It has subsequently overflown into Mali, furthering the security deterioration there. The aftermath of Operation Serval is still playing out problematically, with security fluidity persisting. In the Sahel, the groups, in particular AQIM, have demonstrated tactical opportunism, operational ambiguity and lethality, but they have never enjoyed an enabling environment. In Timbuktu and in many other places, the people were happy to see the groups depart. On the whole, we will have a short-term lethality combined with a long-term diffuse security scene in which these groups can reposition themselves in and around the region, in Southern Algeria, Southern Libya and Niger. In effect, the Afghanisation of Mali, thought to be a self-fulfilling prophecy, is already taking place. MINUSMA is now arriving with a very long list of different elements in its mandate, comprising stabilisation, the rule of law, democratisation and human rights.

Related to this is the fact that there is less cohesion than ever in North Africa: tensions between Algeria and Morocco persist, Morocco is transitioning through reform, Algeria is in a high-stakes waiting game with an unfinished story from the 1990s and an indeterminate nature of power associated with the President's disease, Tunisia is too small to lead although it was the first to mark a rupture. Most importantly, Tunisia is faced with the nascent front of a

new organization, somehow linked to AQIM, in the area of Tabarka and Gadames. The Tunisians just set in place buffer zones in its borders with Algeria and Libya.

It is very important to keep an eye on the groups in Tunisia because they can project very easily on to the Mediterranean and to Europe. That is precisely what AQIM was trying to do. They are explicitly attempting to reshape themselves on the model of the training camps of the late 1980s and early 1990s in Afghanistan; they have sent fighters to previously improbable destinations such as Syria and Mali. These groups will be able to spread out further in Sinai, should the situation in Tunisia deteriorate.

4. The role of Western countries

How can external actors engage with this series of complex and challenging developments in the Middle East and North Africa? The turmoil of 2011 has invited three main dynamics: perplexity at the one extreme, *intervention* at the other, and *repositioning* in the middle. There clearly is a repositioning of every actor in the area, from the UN to the single countries; in the next phase, the area will still be facing that phenomenon in one form or another.

The dominant element in this new equation is the materialisation of a democratisation process. We should not indulge into excessive pessimism; after all, the region is opening, there is more democracy, elections have taken place. However, the difficult process goes on in the context of unresolved power competition, in the realm of concentric security circles of armed conflict, active separatism, transnational terrorism and regional geopolitical competition. Hence, any external partner seeking to engage should factor the interconnectedness of political crises and security crises, interlocked in unpredictable ways.

All of this highlights the need for stabilisation and for institution rebuilding. Contribution to the pursuit of these two goals will be difficult for three reasons. First of all, the enterprise is cast under a sense of urgency. Anyone travelling the region will have only a very limited attention span from any partner. The strategic positions are in bargain, everyone is seeking to maximize, generating thereby unrealistic short-term performance expectations. Secondly, the United States stance in the region is weaker than ever. The US has long been the dominant factor and the major power in the region, having been present militarily for twenty-five years. The weakening of its stance reveals a foreign policy leadership vacuum, but opens opportunities for many other actors. Thirdly, the interim governmental authorities still lack acceptance, which of course raises the question of how to engage and who to partner with.
Above and beyond these dimensions, Western actors — whether state or non-state — should take to heart two key dimensions of the Middle Eastern and North African scene after the Arab Spring. The first key dimension is that *the original uprisings were not about the West,* or indeed about the region's historical relationship with the presence of the West. Europe and the United States are merely actors — albeit powerful ones — among a wider cast, which includes China, Russia, Brazil and India as well as regional actors such as Qatar, Turkey and

Iran. The West has influence but no control; it provides support, but with limited purchase on the situation. The second key dimension to keep in mind is that *there is no short term fixing* to the problems; hence the need to develop a careful and prudent long-term strategy. Stabilisation, demobilisation, institutionalisation and transitioning are multifaceted tasks which cannot be micromanaged and which are calling first and foremost for local patience and leadership.

That being as it may, Western countries can help. Lack of European attention and support would be neither wise nor constructive, and indeed would be ultimately lamented by the local actors. The imperative, however, is on the manner in which such an engagement can be pursued. Constructive international influence can be harnessed in a cohesive message through coherence in the international community, decisiveness in engagement and focus on supporting the capacity in local actors when handling stabilisation, demobilisation and institutionalisation. Helping to connect the capacity levers of government to address the challenges can gradually spell a more secure environment for both the countries of the region and their external partners.

Statement by Mu Changlin

Senior Research Fellow, China Institute for International Strategic Studies, Beijing

"China's Security Challenges and National Defence Policy"

Bern, 6 September 2013

For his presentation we asked to address particularly the following questions:

1. **What are the most urgent security problems from a Chinese perspective (at the regional and global level)?**
2. **What direction is the Chinese security and defence policy presumably to take in the next ten to twenty years? And what role will military means and capabilities play in this policy?**
3. **What intentions and ambitions is China pursuing in the cyberspace? What role is cyberspace playing in Chinese security considerations and security policy?**
4. **How is the current situation and development in Europe (from a security perspective) perceived in China?**

I. China's security challenges and national defence policy

With the process of globalization, the situation of China and the world is undergoing rapid changes. Many uncertain and destabilizing factors pose challenges to China's security, but peace and development is still the common aspiration of Asia-Pacific countries. Dramatic changes in the security situation in the Asia-Pacific region will not fundamentally reverse the momentum of the relatively stable development we have witnessed over the past ten or twenty years. So what are the most urgent security challenges China is facing? Let me focus on five security issues.

1. The Taiwan issue. This issue affects one of China's core interests. The fact that the Taiwan issue has not been resolved for over sixty years is mainly due to the intervention of foreign forces and to obstruction from separatist forces in Taiwan. In 1979, when China and the United States of America decided to establish diplomatic relations, the United States agreed to cut off its diplomatic relationship with Taiwan, abolish the US-Taiwan Defence Treaty and recognize the Government of the People's Republic of China as the sole legitimate government. But only three months after establishing diplomatic relations with China, the US Congress passed the Taiwan Relations Act, asking the US government to provide Taiwan with arms of a defensive character, which was an act of interference in China's internal affairs. In

1995, seventeen years later, the US lifted the ban prohibiting Taiwan's top leaders visiting the United States, which resulted in the Taiwan Strait Missile Crisis in 1996. In 2000, after taking power in Taiwan, the Taiwan Democratic Progressive Party engaged in secessionist activities, increasing tensions in Cross-Straits relations to a high level.

Since 2008, the year in which the Kuomintang took power in Taiwan, Cross-Straits relations have improved greatly. However, the danger of 'Taiwan independence' has not been eliminated; 'Taiwan independence' still has a certain ground there and the Taiwan issue is still the most sensitive issue in Sino-US relations.

China is the only country among the Five Permanent Members of the UN Security Council who has not yet achieved national unification. The basic policy of Chinese Government to resolve the Taiwan issue is 'peaceful reunification – one country, two systems'. China does not undertake to renounce the use of force – targeting not at the people, but at the separatist forces in Taiwan and at foreign intervention and intrusion.

2. The East China Sea issue. The dispute between China and Japan over the Diaoyu Islands greatly damaged the bilateral relations of the two countries and caused concern in the international community. First some important historical facts need to be mentioned. The Diaoyu Islands were first discovered, named and explored by China. China was the first country in history exercising jurisdiction and sovereignty over the Islands. The records of the Diaoyu Islands can be found in a Chinese book published in 1403; they are therefore over 400 years older than relevant records in Japanese historical documents. Taking advantage of the Qing dynasty's defeat in the first Sino-Japanese war in 1895, Japan illegally seized the Diaoyu Islands and renamed them 'Senkaku Islands'.

During and after WWII, the Cairo Declaration and the Potsdam Proclamation stated in explicit terms that 'all the territories Japan has stolen from the Chinese, such as Manchuria, Formosa (Taiwan) and the Pescadores, should be restored to the Republic of China', and 'Japanese sovereignty shall be limited to the Islands of Honshu, Hokkaido, Kyushu, Shikoku and such minor islands as we determined'. On September 2, 1945, the Japanese government accepted the Potsdam Proclamation with the Japanese Instrument of Surrender and pledged to fulfil the obligations enshrined in the provisions of the Potsdam Proclamation. After its defeat in WWII, Japan returned Taiwan to China, but on September 8, 1951, it signed the one-sided Treaty of San Francisco with the United States which privately placed the Diaoyu Islands, Taiwan's affiliated islands, under the United States' trusteeship. On September 18, 1951, the Chinese Government issued a statement stressing that the Treaty of San Francisco is illegal and invalid and can under no circumstances be recognized. In 1971, the United States and Japan signed the Okinawa Reversion Agreement that privately transferred the administrative rights over the Diaoyu Islands as well as over the Okinawa Islands to Japan. In 1972, during the rapprochement talks, the Chinese and the Japanese Prime Minister reached a consensus on leaving the issue to be resolved at a later time.

Right now, the differences between China and Japan over the Diaoyu Islands issue are the following: China claims that Diaoyu Dao and its affiliated islands have been an inherent part of China's territory and that China has indisputable historical and legal evidence in this re-

gard; Japan claims that 'Senkaku Islands' are Japanese territory. According to China it is an objective fact that there is a dispute between China and Japan over the Diaoyu Islands, whereas Japan claims that there is no sovereignty dispute, thereby not recognizing the understanding and consensus reached by the two Prime Ministers with regard to sovereignty over the Diaoyu Islands.

In September 2012, Japanese Government took provocative action by purchasing the Diaoyu Islands. This 'nationalization' stirred up a strong response from the Chinese Government and people. Sino-Japanese relations are facing serious difficulties as a result of the Diaoyu Islands dispute. China is not responsible for that; China is always willing to talk and stands for managing and settling the dispute through dialogue, while Japan has always been unwilling to engage in substantial dialogue aimed at resolving the issue. China and Japan, the second and third largest economies in the world, are neighbouring countries; the dispute over the Diaoyu Islands not only damaged their bilateral relations but also had a serious negative impact on peace and stability in the East Asian region. Since both China and Japan are taking strong positions over the issue with no sign of compromise, the dispute cannot be solved easily. The Japanese Government's attitude towards World War II history and its attempt to revise the pacifist constitution make the China-Japan relationship more complicated. At present, both Chinese and Japanese Coast Guards vessels are patrolling the waters off the Diaoyu Islands; the real danger is that any incident may lead to military clashes.

3. The South China Sea issue. This issue concerns islands in the South China Sea which have been part of China's territory from ancient times, when China acquired sovereignty over the islands and their adjacent waters. Records show that they have been marked on the territorial map of China as early as in the Tang Dynasty, which lasted from 618 to 907. , Up to the 1990s, no country ever challenged China's sovereignty and governance in this area.

The situation in the South China Sea basically remained calm until a UN resource agency released a report in 1968, revealing that the South China Sea is rich in oil and natural gas. After the release of the report, the countries neighbouring the South China Sea raised sovereignty claims to the islands and took actions to occupy them, ending up with the so-called disputes with China. According to the UN Convention on the Law of the Sea, ratified in 1982, the 200 nautical mile exclusive economic zone (EEZ) and continental shelf requirements overlap, which added to the complexity of the dispute. Some countries' unilateral claims on 200 nautical miles of EEZ or continental shelves have overlapped with China's traditional maritime territory to different degrees.

Currently, 44 of the 53 islands and reefs in the South China Sea are occupied by Vietnam, the Philippines and other countries. China's position is to respect historical facts and international law and resolve the disputes through negotiations. This means: firstly, finding a solution through peaceful negotiations by the parties directly involved in the dispute; secondly, continuing to implement the Declaration on the Conduct of Parties in the South China Sea (DOC) and thereby gradually advancing towards the consultation on the Code of Conduct in the South China Sea (COC); thirdly, actively exploring ways of joint development before the final settlement.

China and ASEAN have begun the consultation on the COC in September 2013. China has always taken a positive and open attitude to the formulation of the COC. China believes that since the COC involves various interests, its formulation needs a detailed, complex and coordinated process. All parties concerned should have rational expectations regarding the COC, seek the broadest consensus, remove outside interference and make progress step by step.

4. The North Korea nuclear issue. North Korea insisted on conducting nuclear tests and a missile launch, disregarding the international community's strong opposition. The United States, South Korea and Japan made strong responses to North Korea, which led to tensions on the Korean Peninsula in early 2013. Maintaining peace and stability on the Korean Peninsula serves China's interests. As a signatory to the Non-Proliferation Treaty, China opposes North Korea's nuclear tests and missile launch. China voted in favour of the UN Security Council's relevant resolutions imposing sanctions against North Korea. Over the years, China has made positive efforts to maintain peace and stability on the Korean Peninsula. China insists on the denuclearization of the Korean Peninsula, on maintaining peace and stability on the Korean Peninsula and on pursuing a peaceful resolution of the issue through negotiations and dialogues.

5. The terrorist issue. The terrorist threat has become a problem that no country in the world can avoid. China, too, is faced with terrorist threats. One of the most threatening terrorist organizations in China is the East Turkistan Islamic Movement (ETIM) in the Xinjiang Autonomous Region. After its re-establishment outside China in 1997, ETIM was designated as a terrorist organization by the United Nations in 2002. ETIM has close ties with al-Qaida; many of its members went abroad for training and were then sent back to China, to the Middle East and to South and Central Asia to conduct terrorist activities. From 1990 to 2001, ETIM conducted more than 200 terrorist attacks in China, killing 62 people and injuring more than 440. In April 2013 the terrorists killed 15 people in an attack in the Xinjiang Autonomous Region, which seriously endangered the security and the normal life of the people in this region.

China believes that terrorism, being an international problem, should be addressed through strengthening international cooperation. For this reason, every year China conducts anti-terrorist exercises with Member States of the Shanghai Cooperation Organization. China believes that the terrorist problem cannot be resolved by force alone; there should be greater efforts to accelerate economic development, narrow the gap between the rich and the poor, ease ethnic and social contradictions and make sure there is no soil to breed terrorism on.

II. China's national defence policy – a policy defensive in nature

Although facing the above-mentioned challenges, China is pursuing, and will continue to pursue, a national defence policy that is defensive in nature. This is an inevitable choice, due to China's historical and cultural tradition, to China's military practice in the past sixty years

and to China's strategic decision to take the road of peaceful development. The main contents of China's national defence policy include the following aims:

1. To defend China's sovereignty, security, territorial integrity and peaceful development, ensuring that China's territory, territorial waters and airspace are not encroached, as well as preventing and combating all forms of terrorism, separatism and extremism. China will unswervingly follow the road of peaceful development and make efforts to resolve international disputes and problems left over by history through peaceful means. But under the current international situation, China must maintain the capability to defend state sovereignty, security and territorial integrity, the capability to cope with crises, preserve peace, constrain conflict and win the war in various complex situations.

2. To build up a strong national defence and armed forces which match China's international status and accommodate the needs of China's national security and development interests. The international and China's peripheral security situation has undergone profound changes and are continuing to change. China is facing various security challenges, with traditional and non-traditional security threats being intertwined. As China's international status has increased considerably and as China is enjoying fast economic development, its interests are also expanded. At present, China is implementing a three-step development strategy of national defence and military modernization: the first step has been to lay a firm foundation for the modernization strategy until 2010, a step that has already been taken; the second step is to realize military mechanization and make important progress in informatization till 2020, a step China is now taking; the third step is to achieve the goal of national defence and military modernization by the mid-21st century.

3. To implement the military strategy of active defence. China's active defence strategy is a concrete embodiment of its national defence policy that is defensive in nature. The policy emphasizes strategic defence and self-defence and insists on striking only after having been struck. This kind of defence is not passive defence; China may also launch offensive attacks operationally and tactically. This means that China will not attack unless it is attacked; if China is attacked, it will certainly counter-attack.

4. To insist on self-defence and defensive nuclear strategy. The fundamental goal of China's nuclear strategy is to deter other countries from using or threatening to use nuclear weapons against China. China is the only nuclear country that adheres to the policy of no-first-use of nuclear weapons at any time and in any circumstances, committing itself unconditionally not to use or threaten to use nuclear weapons against non-nuclear weapon states or nuclear weapon-free zones. China advocates the complete prohibition and thorough destruction of nuclear weapons, pursues the principle of counter-attack in self-defence and establishing a nuclear force which is small in number but highly effective and could meet its security requirements. China has always exercised utmost restraint in the development of nuclear weapons. It has

never engaged, and will never do so in the future, in any nuclear arms race with any other country.

5. To pursue an independent national defence policy. This goal is a result of China's independent foreign policy. Accordingly, China will not forge a military alliance with any other country or any group of countries, not seek foreign expansion and not establish military bases outside China. China will protect its security interests by its own strength, make its decisions and strategies according to its own judgment and national conditions and build up a defence industry, defence science and a technology system relying on itself.

III. China's goal and purpose in cyberspace

China has the largest population of Internet users in the world today. By the middle of 2013, its number has reached 591 million. The development of Internet in China has boosted the advancement of social civilization and changed people's life. However, China is also one of the victims suffering the worst cyber-attacks in the world. As the data collected by China's National Computer Emergency Response Team shows, from 1 January to 28 February 2013, no less than 6747 overseas 'Trojan' or 'Zombie' virus control servers controlled well over 1.9 million mainframes within China. 2194 of these control servers are based in the US, controlling about 1.287 million mainframes in China. Although it is fair to say that China has greatly benefited from the development of networks, it also must be admitted that China has suffered considerably from cyber-attacks. China will pursue the following goals in cyberspace:

Firstly: to respect states' sovereign rights and to continue and develop thereby the international legal principle of respecting state sovereignty in cyberspace. Doing so is the fundamental requirement for safeguarding cyberspace order and promoting cyberspace security. It is not advisable to use the network as a tool for violating the sovereign rights of other countries or for whipping up disputes and unrests.

Secondly: to use cyberspace only for peaceful purposes. As the result of the development of modern information technology, the network must be turned into a novel platform for promoting people-to-people communication and a bridge for enhancing cooperation between states. The cyberspace should be used for peaceful purposes. China opposes cyber warfare and cyber contest, opposes using cyberspace to interfere with other countries' internal affairs.

Thirdly: to maintain the cyberspace order according to international law. The sound governance of cyberspace could benefit the entire globe. Now, many countries are engaged in network legislation, improving network management and addressing issues that popped up as a result of the fast development of the network. Network legislations and law enforcement should be set up in order to define normative rights and obligations for the subjects of cyberspace and to punish various types of cyber-crimes according to law. For this purpose, China and some other countries in 2011 submitted a draft entitled 'Code of Conduct on Information

Security' to the UN. They did so in order to push forward the establishment of an international code of conduct in cyberspace.

Fourthly: to promote international exchanges and cooperation in cyberspace. With the openness and transnational features of the network, cyber security is bound to be a global challenge that defies a single country's capability to deal with it effectively. Although the concern over cyber security varies from country to country, international cooperation should not be prevented from promoting cyber security. In addressing the issue of cyber security, we should shape up a fair, reasonable and friendly environment for the development of cyberspace through international cooperation.

With the extensive use of cyberspace in China's economic and social life, cyberspace will play an increasingly important role in China's security considerations and policy-making. In the future, China may take the following into consideration when defining its security policy:

1. China should formulate and issue a national strategy on cyberspace and information security. So far, there are about forty states in the world which have issued a national strategy on cyberspace security. With the largest number of Internet users in the world, China should formulate its own strategy and relevant policies on cyberspace in the future.

2. China should establish an independent and reliable cyberspace protection system. Although China has the largest number of Internet users in the world, 70 per cent of its information equipment in important national economic sectors comes from aboard; especially the core technology and core equipment heavily rely on foreign manufactures. China's network is vulnerable to outside attacks. So China should make preparations for future cyber-threats and achieve breakthroughs in critical technology and important means of protection.

3. China should establish a crisis management mechanism in cyberspace. According to reports, 46 states have established cyber-warfare units and more than 100 states are developing cyber-warfare equipment. The United States, the UK, Japan and Israel have openly declared that they will develop cyber offensive capabilities. Russia recently stated that it would establish a cyberspace unit by the end of 2013. China should establish crises management mechanisms in cyberspace in order to be able to predict any possible incident, to make plans to avoid misjudgements and to prevent incidents from escalating into conflict.

IV. China's view on the current situation in Europe and its development

Since the outbreak of the European debt crisis in 2009, Europe has witnessed political, economic and diplomatic difficulties. On the political level, in several countries the ruling parties lost general elections and had to step down. Economically, some Southern European countries have run into a deep recession for several years. The unemployment rate in the Eurozone has been hovering about 10 per cent; in some Southern European countries it is even above 25 per cent. With regard to diplomacy, Europe's influence and actual ability in major interna-

tional affairs were weakened to a certain degree. The European debt crisis also led to major changes in the internal setup of the EU, with Germany again becoming the strongest and most influential EU-country and with the gravity centre of the EU shifting to Northern European countries, while Southern European countries' influence was greatly reduced. In the security and geopolitical area, the European debt crisis made many EU Member States face serious economic problems. They had to cut their defence budgets, making the construction of the EU Common Security and Defence Policy more difficult. According to statistics, from 2008 to 2010 overall EU defence spending fell about 4 per cent. The cuts also affected the implementation of the EU Common Security and Defence Policy. The European countries took serious measures in order to deal with the debt problem, such as signing the Fiscal Compact and officially launching European stability mechanisms. These measures have achieved obvious effects in stabilising markets and in boosting confidence, but there is still a long way to go before the European debt problem is completely resolved. Therefore, it may beset European political, economic and social development for some time.

In the next few years, as the US is implementing its strategy with regard to the Asia-Pacific, Europe may pay more attention to the Asia-Pacific security area. As an ally of the US, Europe supports the idea of the US being increasingly involved in Asia-Pacific affairs and supports the US Asia-Pacific rebalancing strategy. On the other hand, Europe is concerned that by rebalancing the Asia-Pacific, the US might alienate Europe, damage Europe's own interests and have Europe take more responsibilities.

China is the EU's second largest trading partner and the main dialogue partner in dealing with the European debt crisis. I believe that Europe will pay more attention to the development of economic relations with Asian countries than to the rebalancing strategy. Europe may also take more responsibilities in the Middle East and in Africa and play a greater role in resolving the Iran nuclear issue and the current crises in Egypt and Syria.

Europe is the most concentrated region of developed countries as well as an important and unique force in today's world. Although facing difficulties, Europe is still the largest economy and the largest single market in the world. Europe has a strong economic base, comprehensive institutions and mechanisms, a recovering economy and the ability to be highly innovative. If it can get out of the current difficulties and continue to promote integration, Europe's strength could be restored. Europe will remain to be one of the great powers in the world.

Statement by Catherine Kelleher

Senior Fellow, Watson Institute for International Studies, Brown University
College Park professor, University of Maryland, College Park

"Arms Control - European Security"

Bern, 9 September 2013

For her presentation we asked to address particularly the following questions:

1. ***What are in your view the most imminent threats to security? Are there perhaps also threats that are somewhat over- or underemphasized in the current debate?***
2. ***What is your view on ballistic missile defence? How important do you consider this issue, and what direction will the discussion and development most likely take?***
3. ***What role is NATO presumably going to play in the future (after Afghanistan)? And what meaning will NATO have for the US in particular?***
4. ***How would you assess the current state and development of Europe's security (policy)? What could/should be done to ensure and foster security in Europe?***

As an Associate and Visiting Fellow of the Geneva Centre for Security Policy I have had the opportunity to discuss the topics of these hearings for a number of years. Right now we are at an important point in time at which we need to look very critically at our own assumptions about this current period, i.e. the Post-Cold War Era.

The short answer to the question you put to me is that we are running out of time using the old ideas and the old methods that worked quite successfully in the last decades of the Cold War and that allowed, without much direct violence, the remarkable transition from the Cold War stalemate to a system of security focusing primarily on stability and on moderated and mediated change. We are running out of time because in today's very different environment new ideas and new instruments are needed.

From a Cold War perspective, there are very few threats with regard to *Europe.* Since the fall of the wall we have essentially pursued the idea that Europe is a stable zone of peace and that this peace has been secured by the instruments that were created in the 1970s and 1980s at both the governmental and the intergovernmental level. Defence budgets and defence capabilities are not only falling all around Switzerland but will also fall in the US, even more significantly than has been the case so far. One could argue that we are following a tradition that was established in the 1920s when, after WWI, the British Government made it a matter of Cabinet policy that there would be no war for the next ten years. To act as if this assumption

were true was convenient, politically satisfying and economically desirable. Today, most of the political instances in Europe and in the US have similar intentions.

I would therefore like to reflect a bit more deeply about recent developments, particularly about the failure in terms of a forward motion of the European idea in the financial crisis and, before that, in the crisis of terrorism beginning with 9/11 and continuing through various instances in Europe. These crises have left Europe asking not just the usual questions – What is Europe? Who belongs to it? Who is outside? – but also questions such as: How much power, how much authority and how much legitimacy can Europe claim? The violence against the Greek Government and the violence that threatens some of the other European countries suggest that much of the rhetoric and the philosophy behind the European idea is now, if not outdated, at least questionable. To be honest, I was shocked at how unprepared civil order forces in Greece and, to a lesser extent, in Spain were to deal with the kind of civic violence that took place, although I am by no means suggesting that we are at the verge of a civil war. The European idea was that prosperity would be the rising tide lifting all boats: small and big, capable and less capable, old and new ones. However, with economic prosperity unequally distributed within the EU, the question is how to insure that the actors stick to the bargains that have been made in the 1950ies and the 1960ies. From German actions during the crisis it has become clear that Germany's role as the paymaster of Europe has come to an end. However, this intention is not matched by political developments that allow the burden to be eased at the regional and the state level, which is why I would like you to think of a scenario in which economic prosperity remains unevenly distributed and in which the demands of austerity and of sacrifice are put on the poor rather than on the rich.

The promise the EU long made to countries outside as an allure for other countries – if you behave yourself, you will be allowed access to the EU – has lost much of its attraction. So has the extra cash that used to be so useful in trying to make sure that the behaviour of outside countries was beneficial to the EU. Under these circumstances it has become more difficult to imagine a continuation of the complacency about Europe's role in the world. Everything indicates a loss in status, in economic capability and in the ability to set the terms of international trade. Unless Europe enters a new and more binding relationship with the US, this adds another dimension forcing us to look at the economic roots of the security we have enjoyed.
There is no doubt that Chinese growth rates will slow; so will the amazing growth rates of some of the BRIC states. Keeping the level of economic stability we have had so far will require an enormous effort. Europe might face a decreasing share of prosperity being gained without much effort. All of this suggests a need to rethink what the economic basis of security is. So far, we have focused on stability: no change in borders, relatively transparent and open notifications of changes in capabilities, undying pronouncements of non-aggressive intent. However, over the last five or six years a *new set of threats* to security has emerged, some of them, such as cyber activities, based on technology. Providing adequate defence of critical infrastructure against such attacks will be enormously difficult and equally expensive. There have been many examples showing the vulnerability of critical systems to hacking at-

tacks from state-sponsored or non-governmental actors. Riga's entire electricity, telephone, banking and transport system was shut down for three days by a hacking group. Needless to emphasize how much we depend on these systems to regulate our lives and how many people would be required to carry out those functions that these systems normally perform.

Since we are not talking about a war in the traditional sense but rather about that kind of threat, governmental thinking will have to change in a number of ways. The US Government is currently up to its ears in trouble because it took the easy way: watch everything and everybody, no one will know; keep the data in a large vault; if we need something, we can just reach in and find it. Well, recent developments have made clear that constant monitoring and the unsupervised searching of personnel and public files does not work, neither in technological nor in democratic terms.

What else can we do? Keeping in mind that there is a continuing threat of terrorism and civil unrest, a threat that all major industrialized states have experienced over the last twenty years, it seems to me that at the moment we have no answer to this question. We are not in a position to estimate what a response to these threats is going to cost and what we have to give up if it costs too much. It will not be an easy task to train four or five year old children in password security and in the use of cell phones. Neither will it be an easy task to make sure that everybody in the security system is aware of the need for caution at every point where it interacts with broader information systems.

It may therefore be helpful to look more closely at the assumptions we have made as to how threats arise. Most of you have probably watched with alarm certain tendencies towards repression of civil rights in Eastern Europe and certain leaders' discovery of how easy it is not to have to deal with an opposition at all. We seem to have assumed that prosperity would at least bring about a tendency to democratization. However, it can also bring about nationalism and complex identity politics and a preference for the rich and the powerful as opposed to those in need. Such developments can lead to civil unrest. Unfortunately, we seem to lack much of the institutional structure on a living basis that would allow us to deal with these problems.

The biggest change, however, is perhaps that both the US and Russia are having great difficulties rediscovering the *domestic basis* of their foreign policies. In the eyes of Mr. Putin, his opposition thrives when he does not succeed or when he does not sufficiently live up to his tough guy image. For the first time now he has to be careful whatever the level of bombast in public. I wonder whether he can do much in foreign policy except what he has done so far, if he intends to keep his base mobilised and behind him, given that the very foundation of his popularity, that is economic prosperity, is under considerable threat. Mr. Putin needs the price of $129 per barrel of oil to sustain the Russian Government at an economic, stable level– and we have been, and still are, ways away from that. In spite of all projections of the availability of energy through fracking and other alternative sources, there is no doubt that the natural

resources on which Russia has depended are insufficient to keep increases in economic prosperity and widespread economic satisfaction on the level that has been a keystone of Mr. Putin's reign. It is true that he has no serious politically-organized opposition, but the opposition he does have paradoxically represents the very people who benefitted most from the economic transition. He initiated in his first terms. The reason for that is that the middle class does not like to be repressed the way the old classes were. If Mr. Putin were to falter or to demand greater economic sacrifices at home, he would face real difficulties. This means that domestic politics becomes far more of a priority than it has been, and far more of a constraint on what Russia is willing to take on. Syria can be framed as a world achievement; things closer too home that involve buying favor or giving "loans" may be harder to sell to those who see them in terms of their own economic satisfaction level.

Unfortunately, the same holds true for the *United States*. Firstly, there is a stalemate between the various branches of government. There is no basis for agreement. Secondly, the fact that in the last session the House of Representatives passed exactly 47 pieces of legislation may tell you how bad things are. Thirdly, the Republican party is going to splinter into various factions, not only operationally, as it is now, but also officially. Fourth, in the course of Obama's second term it has become more evident that he is virtually hated by a significant portion of the population; estimations about the size of this portion range from 15 to 25 percent. They will simply not vote for something he is for. It is probably a good thing that there is no official report on the number of assassination efforts, threats or attempts made each week. The President faces the problem of constructing a workable majority that allows him to take tough decisions. Finding such a majority is not easy with a splintered Republican Party and given the fact that a portion of the Democratic Party does not care for the President much either.

Last but not least we have to keep in mind the question where *China* fits in all of this. Although the Chinese pledge eternal devotion to peace and non-violence, they are spending quite a lot of money on military equipment and making a great political effort to restore their claims to sovereign space and to a zone of economic and political manoeuvre in Asia. The US in January 2012 very deliberately announced its tilt to pursue a stabilizing policy almost everywhere but in Asia and in the Middle East. There is a lowered footprint, as we call it, a substitution of missile defence, a number of passive measures and a limitation of the more active overseas presence we have pursued for almost six decades. The essential question is to what degree the engagement with China and the great economic debt to China will lead to a different outcome than the traditional one of great power competition in the Pacific.

In any case are we dealing with three major actors either not willing or not being in a position to take the same kind of role in interventionist international control they have exercised in the late 1980s and in the 1990s. Middle powers, too, have given up much of their capability on the ground. Had the conflict in Libya happened only one month later, the British would not have had two thirds of the capability they used there. France is heading in the same direction,

although for economic as opposed to political reasons; France will not be able to do many more operations as the one in Mali. The German capability is liable to shrink, too. We are therefore faced with the inability of major powers to intervene or to use the military instruments on which they have relied in the past, be it for deterrence or for defence purposes. The ability to act quickly is now restricted to the US, to France and – if it is a good day and the wind is right – to Russia. Given the pace at which things are currently evolving in different places, this restriction is not such a good thing. Who pays later for the ability to constrain or to dampen a conflict pays more.

The institutions we have relied on are similarly less robust, in part because we have taken them for granted. The pan-European institutions such as the OSCE and the Council of Europe were very important, particularly for their new members, in guiding the transition, but they have been a victim of their own success. They no longer provide a framework for the political and economic bouncing and are therefore largely not being used. The functions they perform beyond the minimum – i.e. the monitoring of elections, good behaviour and, at least at the rhetorical level, the protection of civil and human rights – are not sufficient to generate political allegiance and to dampen the political conflicts that already exist within them.

NATO has been more successful, if only because it has managed to reinvent itself at least two or three times since the beginning of the 1980s, moving from an operational defensive alliance largely based on a nuclear tripwire for US reaction to an alliance much more capable of containment on the ground and later on to an institution that allowed for a transition to a different kind of security structure in Eastern and Central Europe, creating a base that could be extended to states of interest outside NATO. Evolving institutionally, NATO in some ways has gone beyond the Partnership for Peace concept, although it has not yet found a new concept that works in the same way. There was a flirtation with NATO as a kind of buckle of the global belt of democracies, but this idea fell by the wayside for lack of enthusiasm.

The new question for NATO will be to what degree the politics of the coalition of the willing, which have satisfied NATO for the last two or three years, will continue to work so well. The Libya exercise may perhaps be the last one, because it will be difficult to extend the strategy of allowing some states to act collectively, if not with the blessing, at least with the general agreement of the organization. Another open question is what role Germany is going to play. Germany still is reluctant to take on the economic and military role many would like it to play. Your neighbour is convinced that the anti-German sentiment throughout Europe makes it impossible for them to take on a military leadership, although the present Government might well continue the remarkable change in German deployment patterns that has taken place since the first medical personnel was sent to Somalia almost two decades ago. However, there will be no effort to step forward and become the linchpin – a step that would be required if anything serious were to develop in terms of a response capability within Europe.
As for *Russia,* it is too big to fit in Europe and too big to be ignored in Europe. Eastern and Central European countries still depend on Russian energy, even if the terms of energy sup-

ply have somewhat softened. Their market structure is still very much oriented towards the East. Russia has not hesitated to apply the kinds of pressure that are made possible by these countries' dependency on Russian energy resources, neither has it hesitated to threaten, at times quite vividly, with what might happen if things do not go as Russia would like them to go. This is typical centre-periphery politics well known in history, but we are not yet at a point where the Eastern and Central European states feel that they are sufficiently backed by their NATO partners to take it with aplomb. In 2007, when asked about the conditions for a missile defence assignment in his country, Polish Prime Minister Donald Tusk famously said: Let's have a direct American guarantee, let's have an American force here; NATO is too slow, their guarantee isn't worth very much, whereas an American guarantee is something we can rely on. I am not sure whether today this sentiment would be echoed with that degree of certainty, but at the time an almost 19th century-style guarantee given by a protector was seen as the best Poland could do with regard to its relationship with Russia.

The *missile defence case,* particularly the decisions taken vis-à-vis Europe, illustrate the very general miasma of threats and the assumption that with regard to institutions and instruments everything was fine. The four-stage-programme put forward by Obama was reduced to a three-stage-programme in which a sea-based capability served as a deterrent and as a limited defence against a limited attack coming from the East, purportedly from Iran, as Iran's missile capability grew. In the first two stages the programme comprised Aegis-based missiles, backed-up by radars situated in Turkey, triangulated with similar radars in Israel and other secondary radars – available through the early warning system of the US – and with radars that had been put in place during the Presidency of George Bush senior to support a national missile defence system and that were renewed under George Bush junior.

The allies hoped that the Obama plan was to be conditional on their agreement. Most of them were happy to be consulted on this topic and agreed to the deployment. The promise was made that national systems would be integrated in a combined response system. Britain and France have developed systems, the Netherlands, Spain and Italy have certain systems, too, and Turkey and Poland at least would like to have a system. The links with the early warning system of the US for the queuing of missile defence would be a new step in this kind of co-operation. The expectation was that attacks would be limited, that they would consist either of one or of two shots and that there would be a chance between 70 and 80 per cent of intercepting such shots so that countries or groups of countries with limited inventory and limited capabilities might decide not launch missile attacks at all.

The US promised they would continue to spend $9 billion a year on research and development in missile defence, as they have done for almost thirty years. The US also promised to coordinate this with a threat assessment dealing not only with possible locations for launches but also with the technological development elsewhere. According to the Western logic and to arguments made in Washington, this was in no case intended against any established nuclear power. Leaving the rhetoric and some of the Putin campaign literature aside, even Rus-

sian analysts said that this might actually be true. Given the progressive improvement in US capabilities, Russian objections were primarily that planned deployments could well be the basis on which to develop a capability limiting the effectiveness of offensive forces launched from Russian territory. Of course, US Presidents have been known to change their minds about past promises, so in 2020 or 2024 a new President might well say "let's develop such a capability," which would constitute a new threat. Obviously, this is not what you are hearing, but at the many bilateral meetings,this was the kind of argumentation brought forward by the Russian side. Russia put forward the political demand that they should have a direct cooperative role, that there should be joint decision-making and sharing of intelligence, and that dealing with objects travelling over Russian/Soviet air space should perhaps be a Russian responsibility while dealing with objects travelling over canonical NATO air space should be a NATO responsibility. This of course was met with complete consternation by the Baltic states that were to be included in the Russian space, not to mention Poland. It was altogether badly handled, certainly under Bush 43, and seemingly continued to be badly handled, certainly in terms of the level of agreement, even on the technical side, that has been reached in the negotiations between the US and Russia on the many meetings.

The major question is whether the missile defence technology is good enough. Even if you are confident that you can get 80 per cent you have to ask whether you can get 80 per cent all of the time. This question has provoked a lot of discussions among experts. As in previous times there is an enormous amount of disagreement in the technical community as to whether the goal of getting 80 per cent all of the time is achievable or not. To get beyond 80 per cent is a very hard task; there is nothing in the offing to suggest that this problem will be solved soon. The seaborne idea has turned out to be a very good one as far as the problem of negotiating access is concerned, but it does force some limitation, particularly on radars. This difficulty has to be overcome. $9 billion a year can buy you a lot of research time but will not necessarily buy you more success. The situation therefore is still evolving. One reason for the fourth phase being cancelled was the admission at least in the U.S. government that the technical problems were not yet solved, particularly not those regarding the effort to move the Aegis system, although well-proven and well-tested, to the so-called Aegis Ashore deployments that were going to take place in Eastern Europe and elsewhere, This technical test had not yet been passed. No one knew when it was going to do so, it was only clear that it was going to cost more and more as time went by.

Today there is a fourth wave of enthusiasm in the US for the concept of missile defence: it sounds nice, it sells well politically, it has a lot of domestic support because it suggests that, particularly if projected on to a nuclear conflict, there is an answer and a way of defence. It takes away the feeling of being a target and inevitable victims. The concept of missile defence has been sold in this way since Ronald Reagan came up with the idea of SDI. In the US many people actually still believe that there is a sort of glass dome, i.e. a system protecting them from incoming missiles. While the missile defence programme will not quite absorb the entire US defence budget, it will devour more and more of it as a result of assisted integra-

tion, progressive updating and improvement of signal intelligence. It has been assigned to the Navy which above all else wishes to retain all twelve aircraft carriers rather than just eight as those in favour of budget cuts suggest from time to time. Since it has not reached the level of a national system being supported broadly by the defence budget, there is a very large Navy interest in making sure that it does not consume the service's entire budget. That is a powerful argument in the debate that counts: Washington'sbudgetary politics.

Let me now come back to the topic of *institutionalization* and ask how this fits into NATO. At the moment, this question is not difficult to answer, but it could be so in the future. We are talking about decisions that have to be made within minutes, i.e. much more quickly than with previous systems. So far, NATO has managed to maintain the fiction that the system is just updated air defence; it is not by accident that Headquarters have been located at Ramstein. So, the relevant question – How does one give the alliance as a whole a role in decision-making? – has not yet been thought through. This question is particularly important for those states that have no stakes in the deployment of the system. Currently, the decision-making is most likely shared by those states that will participate or have deployments on their soil or in their waters.

Another question that has yet to be asked is how associated systems of non-member states are to be integrated. While at the moment there is a US-Israeli agreement, the one that is being proposed for the Middle East at least involves Qatar and perhaps other Gulf states, which raises the question of the link to radar information fed in at critical points in the tracking and identification system. Moreover, the European Phased Adaptive Approach template is being suggested as a first step towards a kind of global tying together with the Japanese-American agreement on top of other very different systems currently being discussed with South Korea, Australia and a number of states in the Middle East that are concerned about their future.
So, all in all we are left with many *unresolved issues.* What are the threats? What is the organizational response? What instruments that fit both within a domestic and an international context can be relied on? At the moment, no one seems to be anxious to have an argument about missile defence, we all are content playing the game we have played for almost ten years now. The US pushes ahead with a particular conception which may change in the future, their allies confirm that they see advantages but are anxious to be told when there is a change of mind, which may never happen. Those outside feel what the system might become as opposed to what it is, and worry about the future.

Postponing this debate and seeing it simply as another aspect is 'wasting a good crises', as we are now used to saying. Having this debate would be an opportunity to change the way in which we do things and an opportunity to use some of the new technological instruments we have to foster more stability and more cooperation – even with states that are, if not hostile, at least not friendly. Five years from now we will look at a wasted opportunity and realise that by then the costs are higher and perhaps less bearable than they would have been now.

Statement by Alexander Klimburg

Alexander Klimburg is a Fellow at the Austrian Institute for International Affairs

"Cyber Power and Cyber Defense"

Bern, 9 September 2013

Für seine Präsentation baten wir um die Beantwortung folgender Fragen:

1. ***Wie gross und real ist die Cyber-Bedrohung? Was könnte im schlimmsten oder im wahrscheinlichsten Fall geschehen?***
2. ***Welche Objekte sind am meisten gefährdet? Geht es primär um die Lahmlegung von Infrastrukturen oder um den illegalen Zugang zu Informationen?***
3. ***Woher ist der wichtigste Beitrag zu mehr Cyber-Sicherheit zu erwarten, von technischen Vorkehrungen oder von politischen Vereinbarungen?***
4. ***Welche Rolle soll und kann der Staat bei Cyber Defence spielen?***
5. ***Was bedeutet das für Streitkräfte, welche Art von Aufgaben sollten sie übernehmen?***

Ich bedanke mich, dass ich heute zu Ihnen zum Thema *Cyber Power and Cyber Defense* sprechen kann und möchte gleich mit einer Entschuldigung beginnen. Ich halte meinen Vortrag grundsätzlich auf Deutsch, doch werde ich immer wieder auch englische Begriffe brauchen. Das hat nicht nur damit zu tun, dass der Vortrag auf Englisch geschrieben wurde, sondern auch damit, dass gewisse Fachbegriffe nicht wirklich übersetzbar sind.
Einleitend ein paar Bemerkungen zu meiner Biografie: Ich trage sozusagen drei Hüte. Erstens bin ich Fellow am Österreichischen Institut für internationale Politik, also unabhängiger Forscher und Mitglied der Zivilgesellschaft. Zweitens unterstütze ich als ein Senior Advisor die österreichische Bundesverwaltung und erstelle unter anderem für das Bundeskanzleramt und Verbindungspersonen des nationalen Sicherheitsrates seit etwa sieben Jahren Studien, vor allem im Bereich Cybersicherheit. Drittens bin ich als Privatberater tätig. In dieser Eigenschaft bin ich zum Beispiel Herausgeber des im Jahr 2012 erschienenen *National Cyber Security Framework Manual*, bei dem unter anderen Melissa Hathaway, die ehemalige Direktorin für Cybersecurity im Weissen Haus, Jason Healey, Director of the Cyber Statecraft Initiative at the Atlantic Council, und Gustav Lindstrom, Head of the Emerging Security Challenges Programme at the Geneva Centre for Security Policy, mitgewirkt haben. Ein Jahr zuvor habe ich im Auftrag des europäischen Parlamentes die Studie *Cyberpower and Cybersecurity* herausgegeben, die auch als eines der Basisdokumente für die europäische Cybersicherheitsstrategie gedient hat. Ich bin auch Mitglied verschiedener Arbeitsgruppen auf EU-

Ebene und manchmal für Österreich in einer Arbeitsgruppe der OSZE (IWG 1039 – Vertrauensbildende Massnahmen) tätig.
Heute bin ich in rein persönlichem Kontext hier, und alles, was ich sage, ist meine Meinung und nicht die Meinung der österreichischen Regierung oder ihrer Stellen.

Ambiguität des Cyberraums

Wer sich mit dem Cyberraum befasst, wird schnell merken, dass hier alles zweideutig ist. Das beginnt schon damit, dass nicht klar ist, wie wir das Wort Cybersicherheit schreiben. Man findet die Versionen *Cybersecurity, Cyber Security* oder *Cyber-Security*. Es ist deshalb nicht erstaunlich, dass wir nicht genau wissen, was dieses Wort bedeutet. Es ist aber nicht unwichtig, wie man es schreibt. Die Nato zum Beispiel schreibt *Cyber Security*, um zu verdeutlichen, dass *Cyber Security* lediglich eine Art von *Security* ist und dass die Nato auch für diese Art von *Security* zuständig ist.

Es gibt aber im Cyberraum nicht nur verschiedene Schreibweisen, sondern auch verschiedene Akteure, und es besteht auch keine einheitliche Meinung darüber, wer diese Akteure sind. Es gibt staatliche Akteure, nichtstaatliche Akteure, Terroristen, Kriminelle, Cyberkrieger und manchmal vereinigt eine Person gleichzeitig diese verschiedenen Akteure in sich. Ein Cyberkrimineller kann zum Beispiel im Auftrag eines Staates agieren, oder ein staatlicher Akteur kann in eigener Regie kriminell handeln. Es gibt keinen einzigen Begriff von Cybersicherheit, es gibt auch keinen einheitlichen Auftrag, sondern es gibt erstens eine militärische Interpretation *(MilCyber)*, zweitens eine polizeiliche Interpretation *(law enforcement LE oder counter-cyber crime)*, drittens eine nachrichtendienstliche Interpretation *(intelligence community IC)*, viertens *internet governance* und *cyber diplomacy* sowie fünftens den Schutz kritischer Infrastruktur *(critical infrastructure protection CIP)*. Alle fünf Aufträge oder Mandate haben ihre eigenen Begriffe, und weil die gemeinsame Sprache fehlt, können sich die Personen, die in diesen Bereichen tätig sind, manchmal untereinander nicht verständlich machen. Ich gebe ein paar Beispiele von Begriffen:

- LOAC: *Law of Armed Conflict* (Kriegsvölkerrecht);
- LI: *Legal Intercept;*
- RT/RG: *Real Time Regional Gateway*, ein Programm der NSA;
- CoE: *Council of Europe's Convention on Cyber crime;*
- ISO27000: Eine Risikomanagementpraxis.

Ich kann mir gut vorstellen, dass es unter den hier Anwesenden keine Person gibt, die alle diese fünf Abkürzungen kennt, da es unwahrscheinlich ist, dass jemand schon mit allen fünf Begriffen gearbeitet hat. Das zeigt, wie vielfältig dieser Cyberraum ist und wie schwer es ist, sich mit allen Aspekten nationaler Cybersicherheit auseinanderzusetzen.

Es gibt auch keine physischen Gesetze im Cyberraum. Man kann zum Beispiel nicht sagen, dass *attribution* ein unlösbares Problem ist (d. h, dass es unmöglich ist, die Akteure hinter einem Cyberangriff genau auszumachen). Manchmal ist es ein Problem, doch wenn man ge-

wisse nachrichtendienstliche Mittel hat, ist es vielleicht weniger gravierend. Es gibt als keine klaren Aussagen zum Cyberraum.

Was ist Cyber?

Wenn wir über den Cyberraum sprechen, geht es um mehr als nur Internet. Alle Netzwerke, die mit Internettechnologie arbeiten können, gehören zum Cyberraum. Darüber hinaus umfasst der Cyberraum auch die zugrundeliegenden sozialen Netzwerke. Cyberraum wird oft als Pyramide mit vier Stufen dargestellt:

- Die unterste Stufe ist die physische Stufe. Das sind zum Beispiel Kabel, Router, d. h. die Hardware.
- Die zweite Stufe ist die logische Stufe, eine Programmierstufe mit den Codes, Protokollen, d. h. die HTML, DNS, BGP. usw..
- Die dritte Stufe ist die Content-Stufe. Hier greift der Datenschutz - bzw. greift er vielleicht nicht.
- Die vierte Stufe, die Spitze der Pyramide, wird von der Sozialebene gebildet. Sie umfasst die gesamten sozialen Kontakte, die durch den Cyberraum ermöglicht werden.

Alle Angriffe, die im Cyberraum erfolgen, zielen grundsätzlich auf die soziale Ebene. Der einfachste Cyberangriff, den es gibt, ist, wenn ich jemanden anrufe und sage: "Geben Sie mir Ihre Daten" und er mir seine Daten gibt. Alle anderen Vorgänge sind sozusagen ein Umweg zu diesem Ziel. Sei es ein Hack über die logische Stufe oder das Anzapfen eines Kabels auf der physischen Stufe: Es geht immer darum, eine Wirkung auf der sozialen Stufe zu erzeugen. Ein Modell der US-Airforce stellt das anhand eines *target decision cycle* mit drei Dimensionen dar: Zuunterst steht die physische Dimension. Auf der zweiten Ebene folgt die Informationsdimension, und zuoberst haben wir die kognitive Dimension. D. h., dass man immer versucht, eine Entscheidung zu beeinflussen oder herbeizuführen. Genau da fehlt aber immer der Schwerpunkt.

Cyber operations sind information operations

Wenn wir über *cyber operations* sprechen, sprechen wir eigentlich über *information operations*. Im Wesentlichen ist dabei nur etwas relevant, nämlich *computer network operations*. Im amerikanischen Sprachgebrauch wird dafür eine dreifache Unterteilung benutzt, die für uns Wissenschaftler sehr problematisch ist: *computer network exploitation*, c*omputer network attack* und c*omputer network defense* (Quelle: JP 3-13 2006). Es wird also unterschieden zwischen grob gesagt Cyberspionage (*computer network exploitation*) und Cyberangriff (c*omputer network attack*). Diese Unterscheidung ist in Europa nicht üblich. Denn wenn man einen Cyberangriff ausführen möchte, muss man fast immer vorher Cyberspionage betreiben. Die Amerikaner bestehen aber vor allem aus rechtlichen Gründen auf dieser Unterscheidung.
Wir können verschiedene Modelle der *information operations* unterscheiden:

- *Information warfare*. Dieses Modell wird vor allem in China und Russland verwendet. Es gibt dort ganz klar ausgearbeitete Strategien, was Informationskriegsführung eigentlich bedeutet, die sowohl auf die strategische als auch auf die operative Ebene greifen.

- *Cyber warfare.* Zu diesem Begriff gibt es keine offizielle Begriffsdeutung, und er kommt auch in offiziellen Dokumenten eigentlich nie vor. In den letzten zwei, drei Jahren haben sich zwei andere Paradigmen herauskristallisiert:
- *National cybersecurity*. Dahinter steht eine eher defensive Sicht. Der Cyberraum wird als etwas Gefährliches verstanden, und man versucht, sich defensiv zu schützen.
- *Cyber power*. Dieser Ansatz ist viel offensiver. Er geht davon aus, dass man die Schwächen des Cyberraumes ausnützen kann, um die nationalen Interessen zu vertreten.

In Europa ist eher das Modell der *national cybersecurity* gängig. C*yber power* können nur ein paar Staaten ausführen. Eigentlich hängt es vom Ambitionsniveau ab, welchem Modell man folgen möchte. Ich unterscheide drei verschiedene Ambitionsniveaus:

1. *Protect own network*: Man schützt sich selbst.
2. *National cyber security*: Das umfasst zum Beispiel den Schutz kritischer Infrastruktur.
3. *Project cyber power.*

Ich möchte dazu zwei Definitionen vorstellen, eine für *cyber power* und eine für *national cyber security:*

"Cyberpower is the ability to use cyberspace to create advantages and influence events in all the operatonal environments and across the instruments of power." (Aus: Krammer/Starr et al. "Cyberpower and National Security", National Defense University 2011).

"A nations's national cyber security is the focused application of specific government levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security." (Aus: Klimburg (ed.) "National Cyber Security Framework Manual", NATO CCDCOE 2012.).

Cyber defense gibt es als solches offiziell nicht. *Cyber defense* wird sehr oft als Unterkategorie der nationalen Cybersicherheit bezeichnet, und es gibt Tätigkeiten, die mit c*yber defense* in Verbindung gebracht werden können. In erster Linie sind das die sogenannten *military cyber operations* und ein bisschen weniger die sogenannten *strategic cyber operations*. Noch weniger gehört *cyber espionage* dazu, und ganz wenig das *nationale Krisenmanagement*. Ich gehe im Folgenden auf diese verschiedenen Tätigkeiten näher ein.

• *Military cyber***:** Das erste Ziel von *military cyber* ist *protection of your own ICT systems*. Das ist sehr umfangreich und bedeutet nicht nur *computer network defense*, sondern auch *information assurance, ID management, business continuity management/disaster recovery*, und viele andere damit verbundene Tätigkeiten. Es bedeutet aber zum Beispiel auch die Möglichkeit, dass man seine eigenen Systeme testet, indem man einen Pentest durchführt, ein *red team* aufstellt, um sich selbst anzugreifen und zu testen, wie anfällig man ist.

Im Weiteren gibt es das sogenannte *battlefield cyber*, das nur auf dem Schlachtfeld eingesetzt wird. Es handelt sich um Tools, die verwendet werden, um konventionelle militärische Angriffe zu unterstützen. Ein berühmtes Beispiel ist das *Senior Suter tool*, das von British Aerospace entwickelt wurde. Man kann mit diesem Tool beispielsweise eine Radaranlage lahmlegen. Eine Version davon wurde wahrscheinlich im Jahr 2007 in der *Operation Orchard* verwendet, um das syrische Luftabwehrsystem lahmzulegen, um einen israelischen Luftangriff auf ein Kernkraftwerk zu ermöglichen.

• *Strategic strike:* Der sogenannte *strategic strike* ist nicht unbedingt Sache des Militärs. In den meisten Staaten sind mindestens zur Hälfte die Nachrichtendienste sehr stark eingebunden. *Strategic strike* hat nichts auf dem Schlachtfeld zu suchen, sondern zielt auf die Infrastrukturen oder die Finanzsysteme oder dergleichen ab. Er bedarf des *pre-deployment*, d. h. dass man, bevor man ihn ausführt, schon ziemlich lange im System gewesen sein und es ausgekundschaftet haben muss. Wenn man den *strategic strike* wirklich beherrscht, gibt es auch die Möglichkeit, *multidimensional campaigns* zu starten, d. h. drei, vier, fünf verschiedene Cyberangriffe gleichzeitig, die auf verschiedene Teile des Systems abzielen, die verschiedener Fähigkeiten bedürfen und sehr schwer abzuwickeln sind.

• *Cyber espionage / counter espionage:* Dazu gehören gemäss meiner persönlichen Definition drei Elemente: Als Erstes braucht es *access*. Das ist zum Beispiel Zugang zu strukturierten Datenbanken. Das kann die eigene Datenbank sein, aber auch diejenige eines Freundes, einer Privatfirma wie Facebook oder Google, einer Partnerorganisation oder einer Datenbank, die man gehackt hat. Das zweite Element ist *intercept*. Das ist das, was traditionell unter s*ignals intelligence (SIGINT)* zu verstehen ist. Es schliesst *deep packet inspection (DPI)* ein, aber auch Möglichkeiten wie *full packet capture* direkt auf Kabel oder Satellitenverbindungen oder dergleichen durchzuführen und die Daten zu kopieren. Das dritte Element ist *presence*. Man ist auf einem System selbst vorhanden, sitzt zum Beispiel durch einen Trojaner auf dem Laptop. Somit kann man nicht nur die Daten lesen, sondern kontrolliert den Laptop und kann Daten auch modifizieren oder sogar zerstören. Diese dritte Form von Spionage ist sehr gefährlich, weil sie auch sehr zweideutig ist. Wenn jemand schon im System sitzt, weiss man nicht, ob er einen Cyberangriff ausführt oder "nur" spioniert.

• *National crisis management:* Für *cyber defense* ist vor allem *crisis assistance* relevant. Das kann für das Militär alles Mögliche bedeuten, zum Beispiel dass man alternative Funkverbindungen aufstellt oder Mannstärke zur Verfügung hat. Wenn man zum Beispiel Tausende von Rechnern neu auflegen muss, braucht es dazu viele Personen; oder man muss zum Beispiel Generatoren für die Stromerzeugung zur Verfügung stellen. Zudem gibt es auch unterstützende Funktionen für nachrichtendienstliche Aktivitäten.

Steigende Komplexität

Im Jahr 1990 hatte eine Sicherheitssoftware im Schnitt 2000 Codezeilen. Im Jahr 2000 waren es schon 2 000 000. Heute stehen wir bei 10 000 000 Codezeilen. Die Angriffe sind aber im-

mer gleich geblieben, sie haben im Schnitt 125 Codezeilen. Es ist also fast achttausendmal leichter, anzugreifen, als zu verteidigen. Zudem ist zu berücksichtigen, dass es im Schnitt alle 15 000 bis 25 000 Codezeilen einen Fehler gibt. D. h., dass es in der Sicherheitssoftware selber ziemlich Fehler, sprich mögliche Angriffsvektoren haben wird. Auch bezüglich der Malware hat die Komplexität stark zugenommen. Ende des Jahre 2012 waren 127 000 verschiedene Malware-Variationen im Umlauf. Heute stehen wir bei ungefähr 140 000. Die Entwicklung neuer Malware geht sehr schnell vor sich, und es ist sehr schwierig, sich davor zu schützen.

Auch Staaten benutzen Cyber crime

Malware kommt fast ausschliesslich aus dem nichtstaatlichen Bereich. Sogar die NSA hat sich nachweislich sehr stark auf nichtstaatliche Akteure gestützt. Das bedeutet im Wesentlichen, dass die nichtstaatlichen Akteure teilweise auch für den Cyber-Defense-Fall die wichtigsten Akteure sind.

Ein Beispiel ist ein APT-Angriff (*advanced persistent threat).* APT-Angriffe gehören zu den gefährlichsten Angriffen in der Cyberspionage. Es handelt sich um einen Trojaner, den man zum Beispiel durch ein PDF Dokument ans Ziel bringt. Vor ein paar Jahren wurde das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) auf diese Weise angegriffen. Ein APT kann monatelang in der Vorbereitung sein und jahrelang im System liegen. Ein APT-Angriff läuft in verschiedenen Phasen ab, mit folgender Ressourcenaufteilung: Am Anfang steht *intelligence logistics* (Aufklärungsphase) mit 40 Prozent der Ressourcen. Es folgen die Phasen *live/system discovery* (5 Prozent), *detailed preparations* (30 Prozent) und *testing und practice* (20 Prozent). Am Schluss steht die Phase der *attack execution*, die Ausführung des Angriffes, die nur 5 Prozent der Ressourcen beansprucht. Ein solcher Angriff ist extrem kompliziert und konnte lange nur durch Staaten ausgeführt werden. Jetzt können ihn auch Cyber-Crime-Gruppierungen ausführen, und Staaten ziehen zum Teil *cyber crime* für ATP-Angriffe bei.
Ein weiteres Beispiel für Cyberangriffe, bei welchen Staaten *cyber crime* beiziehen, sind die sogenannten Spear-Phishing-Angriffe. Sie sind zu unterscheiden von Phishing-Angriffen, wo man zum Beispiel von einem nigerianischen Prinzen eine E-Mail bekommt, die Geld verspricht. *Spear phishing* ist detaillierter. Man schickt ganz gezielt eine E-Mail an eine Person, weil diese Person interessant ist. Diese Person bekommt dann die E-Mail zum Beispiel von einem Freund. Staaten greifen zum Teil auf *cyber crime* zurück, wenn es darum geht, auszuforschen, welche Personen für Angriffe via *spear phishing* anfällig sind.

Unterschiedliche Akteure – unterschiedliche Fähigkeiten

Eine Zusammenstellung aus dem Jahr 2006 listet die verschiedenen Akteure, deren Motivation, Fähigkeiten und Ressourcen auf (Cilluffo, Frank J.; Nicholas, Paul J. (2006): Cyberstrategy 2.0). Sie hat im Wesentlichen auch heute noch Gültigkeit.

Die Deltas in den Unterschieden bei den Fähigkeiten der verschiedenen Akteure sind eigentlich logarithmisch. Nehmen wir ein *script kiddy*. Das ist jemand, der gewisse Softwarepakete benützen kann, aber keine Ahnung davon hat, wie man sie programmiert. Seine Ressourcen sind minimal. Wenn man diese Fähigkeiten mit den Fähigkeiten zum Beispiel eines *foreign intelligence services* vergleicht, haben wir nicht eine zwei- oder dreifache Steigerung, sondern eine vielleicht zehntausendfache Steigerung. Es gibt also sehr grosse Unterschiede zwischen dem, was ein *script kiddy* kann, und dem, was ein Staat kann. Das bedeutet auch, dass Cyberangriffe auf unterer Ebene sehr einfach zu machen sind. Jeder kann sich dafür irgendein *script kiddy* holen. Wenn man aber einen richtig guten Angriff machen will, wird das sehr schnell sehr teuer. Ein Grund ist, dass man viele Cyberwaffen bauen muss, um einen Cyberangriff ausführen zu können. Bei konventionellen Waffen ist es so, dass ihr Wert über Jahre bestehen bleibt. Wenn man zum Beispiel 10 lasergesteuerte Bomben hat, wird man ein Jahr später immer noch 10 lasergesteuerte Bomben haben. Wenn man aber zum Beispiel 10 Cyberwaffen hat, hat man ein Jahr später nur noch drei, weil sie obsolet werden, und zwar sehr schnell. Man muss also immer wieder neue Cyberwaffen bauen, und das kostet sehr viel Geld. Das bedeutet, dass Einzelakteure sehr wohl schwerwiegende Angriffe ausführen können, aber wahrscheinlich keine katastrophalen Angriffe - das können nur grössere Gruppen von Experten.

Nichtstaatliche Akteure auf der Ebene krimineller Organisationen können aber fast oder genauso fähig sein, wie ein kleiner oder mittelgrosser Staat. Das absolut Fähigste, was man sich vorstellen kann, das ich *whole of nation cyberpower* nennen würde, ist das Zusammengehen des Staates mit den beiden anderen mächtigen Akteuren, nämlich den kriminellen sowie den grossen nichtstaatlichen Akteuren, wie zum Beispiel Konzernen, die im Verteidigungsbereich tätig sind

Zusammenarbeit mit nichtstaatlichen Akteuren

Wie sieht es konkret aus, wenn ein Staat *cyber power* offensiv mit nichtstaatlichen Akteuren zusammen ausleben möchte? Ich gebe dazu ein paar Beispiele.

Cyber Attacker Taxonomy

Ein sehr interessanter Bericht des *US-Defense Science Board (DSB)* von 2012 unterscheidet sechs verschiedene Stufen von Cyberakteuren. Auf der Stufe 1 stehen die *script kiddies*, die ich schon erwähnt habe. Die Personen in Stufe 2 kennen sich schon etwas besser aus; das kann durchaus im Cyber-Crime-Bereich angesiedelt sein. Die Unterscheidung geht dann bis zu Stufe 5. Dieser Stufe werden zum Beispiel Personen zugeordnet, die die *supply chain* beeinflussen können. D. h., dass sie einen Halbleiter so bearbeiten können, dass er auch zu einer Waffe wird. Eine Waffe ist im Übrigen nicht nur ein USB-Stick, es kann auch eine Maus sein. Die *supply chain* kann auch beeinflusst werden, indem man Standards beeinflusst. Vor ein paar Tagen wurde zum Beispiel bekannt, dass die NSA absichtlich eine ISO-Organisa-

tion, also eine Normorganisation, beeinflusst hat, eine gewisse *encryption* zu akzeptieren, die eigentlich unsicher war. Die NSA forcierte das, weil es ihr erlaubte, überall hineinzukommen. *Supply chain management*, d. h. wie man ein System gegen solche Angriffe absichert, ist sehr schwierig und auch auf europäischer Ebene ein grosses Thema.
Ich habe selber eine ähnliche Kategorisierung gemacht, die vier Stufen unterscheidet:
Stufe 1 sind die Staaten mit *hyper cyber power*, zu denen ich die USA, Russland und China zähle. Man könnte aber auch sagen, dass nur die USA die Fähigkeiten haben, extrem komplexe Angriffe auszuführen. Interessanterweise sind diese Staaten bei der Verteidigung immer mittelschlecht. Ein Grund ist, dass sie sehr gross sind und deswegen auch der Schutz und die Verteidigung ihrer Systeme sehr schwierig sind. Ein Grund ist aber auch, dass sich diese Staaten hauptsächlich mit Abschreckung auseinandersetzen. Zu Abschreckung gehört eine gute Angriffsmöglichkeit. Sehr vieles, das man im Cyberraum wahrnimmt, sind Versuche, diese Abschreckungsstrategie klar auszubilden.
Stufe 2 sind die Staaten mit *cyber power*. Dazu gehören Grossbritannien, Frankreich und Israel, vielleicht auch Estland. Sie haben einen guten Cyberschutz und auch die Möglichkeit, Cyberangriffe auszuführen. Sie sind aber vor allem auf Spionage ausgerichtet.
Stufe 3 sind die Staaten mit *national cyber security*. Darunter sind die meisten europäischen Staaten, vielleicht auch die Schweiz, zu fassen. Die Cyberangriffe sind für sie relativ unwichtig, die Priorität liegt bei den Cyberschutzfunktionen. Die Aktivitäten werden praktisch nur zum eigenen Schutz hochgefahren. Bei den Systemen gibt es aber teilweise sehr grosse Unterschiede.
Stufe 4 sind die Staaten, die man als *cyber aspirant* bezeichnen kann. Beispiele dafür sind Indien, Pakistan, Brasilien, Indonesien. Diese Staaten möchten eigentlich gerne zur Stufe 2 gehören, also eine *cyber power* sein. Sie haben aber nicht die Möglichkeit, sich am extrem teuren Cyberangriffswaffen-Markt zu beteiligen, sondern benutzen hauptsächlich *cyber crime*. Indien zum Beispiel hat einen sehr grossen Cyber-crime-Markt, und es ist anzunehmen, dass sich der Staat irgendeinmal mit diesen Akteuren auseinandersetzen wird.

Was bedeutet Cyber-Krieg?
Das *Air Force Scientific Advisory Board (AF-SAB)* hat 2007 den Bericht "Levels of Cyber War" verfasst. Er ist leider geheim, doch wurde ein Auszug veröffentlicht, der die Definition der Stufen von *cyber warfare* beinhaltet.

Die erste Stufe ist *network wars* oder *system adminstrator versus system administrator* oder auch einfach *business as usual*. Sie umfasst ganz normal das, was dauernd vorkommt, zum Beispiel Spionage. Das gilt nicht als Kriegsfall und oft nicht einmal als richtiges Verbrechen. Gegen solche Sachen muss man sich schützen können, und wenn man es nicht kann, ist man selber schuld.

Die zweite Stufe umfasst *cyber adjunct to kinetic combat*. Das bedeutet, dass man einen solchen Angriff gleich wie einen militärischen Angriff bewerten könnte bzw. handelt es sich

rechtlich um eine Gewaltanwendung *(use of Force*) Ein Beispiel ist der vermutlichen israelische Cyberangriff auf die syrische Radareinrichtung im Jahr 2007.

Die dritte Stufe ist die *malicious manipulation of information*. Das ist das Gefährlichste, was es gibt. Beispielsweise werden die Kontrollsysteme eines Reaktors so beeinflusst, dass man es nicht merkt, womit ein bleibender Schaden angerichtet wird. Das sind die Angriffe, vor welchen man sich am meisten schützen muss. Sie gelten als *armed attack*, d. h. im Extremfall auch de facto als Kriegsfall.

Es gibt eine Cyberrisiko Matrix, die vom österreichischen Innenministerium bestellt wurde.
Ich habe im Jahr 2013 eine eigene Version erstellt, die davon ein wenig abweicht. Meines Erachtens stellen die folgenden Kategorien die gefährlichsten Angriffe dar:

- *Manipulation of unsecure hardware*
- *"Collateral" cyber war damage*. Damit ist der Fall gemeint, dass man zufällig in die Schlusslinie gerät. Ein bestimmter Staat verfolgt zum Beispiel seit zwei Jahren eine sogenannte *active defense*-Strategie. D. h., dass er bei einem Angriff unter Umständen auch via einen neutralen Staat hindurch reagiert, falls dieser nicht schnell genug ist, um diese Angriffe zu unterbinden. Ein Beispiel wäre, dass in der Schweiz ein Computer steht, der Cyberangriffe auf diesen Staat lenkt. Wenn die Schweiz nicht schnell genug reagiert, greift dieser Staat direkt ein und jagt den betreffenden Server weg, hoffentlich nicht mit kinetischen Mitteln, sondern mit einem Cyberangriff. Die Schweiz wäre in diesem Fall rein zufällig zwischen die Fronten geraten.
- *Extremely Large Denial of service attacks*. DDoS-Angriffe hat man zum Beispiel 2007 in Estland gesehen. Solche Angriffe zielen darauf ab, ein System dermassen zu überfordern, dass es seine Funktion nicht mehr erfüllen kann. Solche Angriffe sind in den letzten Jahren viel grösser und mächtiger geworden und können das Internet als solches auch betreffen.
- *Severe Attack on DNS/BGP*
- *"Accidental Release" of cyberweapons*

Was *cyber war* ist, bleibt aber eine Auffassungssache. Die westliche Definition und die „östliche“ Definition unterscheiden sich. Die Sicht des Westens entspricht dem, was im "Tallinn Manual“ wiedergegeben ist – und dieses wiederum gibt wieder, was seit Jahren auf der Ebene der Uno besprochen wird. Im "Tallinn Manual“ heisst es zum *cyber war*:
„an equivalent to an armed attack, with significant casualties and/or economic loss, or weakening of national security" …"Non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks."
Unter *cyber war* fällt aber auch ein *single-act of sabotage with "catastrophic damage"*. In diesem Zusammenhang könnte man fast – aber nicht ganz - auf das Beispiel Stuxnet verweisen, die Beeinflussung von Urananreicherungsanlagen im Iran. Dabei handelte es sich zwar tatsächlich um einen Cyberangriff. Die Anreicherungsanlage wurde hochgefahren und zerstört, aber nicht katastrophal zerstört. Katastrophal zerstört hätte bedeutet, dass die Zentrifugen in die Luft gejagt worden wären. Damit wäre alles kontaminiert gewesen, und es wären

auch mehrere Leute gestorben. Die Angreifer sind nicht so weit gegangen, da das tatsächlich ein Kriegsfall gewesen wäre. Sie blieben deshalb eine Stufe unter einem *catastrophic damage*.
Im Weiteren gibt es auch noch die Möglichkeit, *multistage cyber campaigns* zu fahren. Das sind sehr komplexe Cyberangriffe, die auf verschiedenen Ebenen gleichzeitig stattfinden.
Die russische und chinesische Definition von *cyber war* ist ganz anders. Für Russland fällt auch ein psychologischer Angriff darunter, und für China auch ein Medienangriff. Beides gilt im Westen nicht als Cyberangriff.
Die Frage ist, was man überhaupt unter Kriegsführung versteht. Für Clausewitz ist *warfare an extension of politics.* Lenin sagt hingegen, *politics is merely an extension of warfare.* Diese zweite Sicht ist durchaus präsent, und gewisse Staaten richten sich danach aus.

Wie plant man eine Cyber-Defense-Organisation?
Ich kann in diesem Rahmen diese Frage nur ganz kurz anreissen. Wenn ein Land eine solche Organisation aufbauen will, muss man natürlich zuerst überlegen, welche Ambitionsstufe man anstrebt. Für die Schweiz müssen das Personen machen, die sich besser mit den schweizerischen Gegebenheiten auskennen, als ich. Ich kann dazu einfach auf ein paar Punkte hinweisen, die allgemein als wichtig erachtet werden.

- Das Militär muss für den zivilen Katastrophenfall genügend Fähigkeiten für den Assistenzeinsatz zur Verfügung stellen können. Das bedeutet alles Mögliche, da ein Cyber-Katastrophenfall sehr umfassend und sehr bedrohlich sein kann. Wenn zum Beispiel Stromnetzwerke breit angegriffen werden, fallen sie nicht nur für ein paar Tage aus, sondern können nicht mehr angeschaltet werden.
- Das Militär muss auch für den „normalen" Krisenfall – und das kann durchaus zum Beispiel alle paar Jahre eintreten - Personal zur Verfügung stellen können. Dies betrifft vor allem den nachrichtendienstlichen Bereich, aber auch allgemein Personen, die unterstützende Aufgaben – zum Beispiel Forensik oder Malware-Analyse – wahrnehmen können.
- Das Militär muss vor allem auch seine eigenen Systeme schützen. Das bedeutet, dass das *computer emergency response team (CERT)* eine Funktionalität hat, die sich über das ganze System erstreckt. Das ist nicht immer gegeben. Sehr oft haben die Militärs fünf oder sechs verschiedene CERT. Ich rate dringend, das nicht zu machen.
- Man muss die Möglichkeit haben, sich gegen Hardware-Angriffe und ähnliche nachrichtendienstliche Angriffe zu wehren. Ein Stichwort ist hier TEMPEST proof, eine Sicherheitskategorie, die es ermöglicht, abschirmarme Bedingungen herzustellen. Sonst ist es zum Beispiel extrem einfach, von einem ungesicherten Rechner / Computer sehr viele Information zu bekommen. Dies ist aber im Vergleich zum Schutz gegen Hardware Angriffe noch einfach – diese Aufgabe gilt als eine der schwierigsten (teuersten) Tätigkeiten überhaupt.
- Die Streitkräfte müssen die Möglichkeit haben, unter den Bedingungen eines *sustained cyber conflict* zu operieren, d. h. wenn zum Beispiel die IKT-Elektronik grossflächig während Wochen nicht zur Verfügung steht.

• Man muss *battlefield support* leisten können. Dabei ist zum Beispiel an Angriffe auf Radaranlagen zu denken, aber auch an die Möglichkeit, selber die Kommunikationsmöglichkeiten des Feindes auszuschalten
• Es ist auch zu überlegen, ob man einen *strategic strike* als Möglichkeit mitberücksichtigen möchte. Man kann aber Abschreckung natürlich auch mit anderen als militärischen Mitteln betreiben, zum Beispiel mit aussenpolitischen, diplomatischen Mitteln.
• Die *Informationssicherheit* muss grundsätzlich auf allen Stufen als Kultur verankert sein.
• Es ist wichtig, *Resilienz* zu machen, aber man sollte sich dabei nicht auf die Ausrede stützen, Resilienz sei gegeben, wenn man verschiedene Systeme aufrechterhalte. Es stimmt sicher, dass man einen gewissen Schutz hat, wenn man die Systeme nicht vereinheitlicht. Man muss aber auch bedenken, dass das mit wahnsinnig hohen Kosten verbunden ist.

Das Wichtigste ist aber Zusammenarbeit. Sie ist enorm wichtig, und zwar auf drei Ebenen:

Whole of government: Wenn man sich auf der staatlichen Ebene mit der Arbeit in abgeschlossenen Sektoren zufriedengibt und nicht zusammenarbeitet, hat man keine Cybersicherheit, sondern Cyberunsicherheit.

Whole of nation: Das bedeutet nicht nur die Zusammenarbeit innerhalb des Milizsystems. Dieses ist natürlich sehr wichtig, doch müssen nach Möglichkeit auch Personen einbezogen werden, die nicht zum Militär gehören. Zum Beispiel kann man eine Kooperation mit Firmen aufbauen, die im Verteidigungsbereich oder im Infrastrukturbereich tätig sind, aber eben nur in einem der beiden Bereiche. Aber auch die Wissenschaft oder Einzelpersonen, die nicht so einfach zu kategorisieren sind, aber oft etwas beizutragen haben, können einbezogen werden.

Whole of (international) system: Man muss auch international ein vertrauenswürdiger Partner sein, und zwar auf jeder Ebene, d. h. sowohl auf der operativen als auch auf der strategischen und der politischen Ebene.

Ohne Vertrauen funktioniert das alles nicht und nützen auch die Cyber Defense-Einrichtungen wenig.